Date de dépôt : 31 juillet 2020

Rapport

de la commission législative chargée d'étudier le projet de loi de M^mes^ et MM. Jean-Michel Bugnion, Boris Calame, Sophie Forster Carbonnier, Sarah Klopmann, Yves de Matteis, François Lefort, Salika Wenger, Frédérique Perler, Bernhard Riedweg, Delphine Klopfenstein Broggini, Mathias Buschbeck, Marie-Thérèse Engelberts, Olivier Baud modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)

Rapport de majorité de M. Edouard Cuendet (page 1)
Rapport de minorité de M. Jean Rossiaud (page 215)

RAPPORT DE LA MAJORITÉ

Rapport de M. Edouard Cuendet

Mesdames et
Messieurs les députés,

La commission législative a étudié ce projet de loi durant 15 séances. Elle s'est réunie pour traiter cet objet aux dates suivantes : 30 juin 2017, 1er septembre 2017, 20 octobre 2017, 10 et 17 novembre 2017, 8 décembre 2017, 12 et 19 janvier 2018, 2 février 2018, 15 juin 2018, 28 septembre 2018, 16 novembre 2018, 7 décembre 2018, 21 juin 2019 et 27 septembre 2019. La commission a travaillé sous les présidences successives de MM. Mathias Buschbeck, Edouard Cuendet et Cyril Mizrahi.

M. Fabien Mangilli, directeur des affaires juridiques de la Chancellerie d'Etat (DAJ – PRE), Mme Lucile Stahl Monnier, directrice adjointe (DAJ – PRE), Me Massimo Scuderi, avocat-stagiaire à la direction des affaires

ATAR ROTO PRESSE – 100 ex. – 08.20

juridiques (DAJ – PRE), Mme Tina Rodriguez, secrétaire scientifique du secrétariat du Grand Conseil (SGGC) ainsi que Mme Giselle Toledo Vera, juriste à la direction des affaires juridiques du DIP et M. Manuel Grandjean, directeur du service écoles-médias (SEM – DIP), ont assisté la commission dans ses travaux. Le rapporteur de majorité saisit cette occasion pour adresser ses plus vifs remerciements à Mme Tina Rodriguez, secrétaire scientifique, qui a su guider la commission avec compétence dans les méandres de ce dossier aussi technique que tentaculaire.

Les procès-verbaux ont été rédigés par M. Sylvain Maechler, Mme Noémie Pauli, M. Sacha Gonczy, Mme Virginie Moro, Mme Giulia Piermartiri, M. Aurélien Krause et Mme Anja Hajdukovic. Le rapporteur de majorité tient à les remercier vivement de leur remarquable travail, sur un sujet souvent complexe.

Organisation des travaux

Les travaux se sont déroulés de la manière suivante :

- 30 juin 2017 : Présentation du PL 12103 par M. Jean-Michel Bugnion, auteur.
- 1er septembre 2017 : Audition de M. Manuel Grandjean, directeur du service écoles-médias (SEM – DIP) et de M. Eric Favre, directeur de l'office cantonal des systèmes d'information et du numérique (OCSIN – DI, anciennement la DGSI).
- 20 octobre 2017 : Organisation de la suite des travaux.
- 10 novembre 2017 : Audition de Mme Marie-Claude Sawerschel, secrétaire générale (DIP), Mme Giselle Toledo Vera, juriste à la direction des affaires juridiques (DIP) et M. Manuel Grandjean, directeur du service écoles-médias (SEM – DIP).
- 17 novembre 2017 : Audition du vice-recteur de l'Université de Genève, M. Denis Hochstrasser, de M. Jean-François Rossignol, directeur adjoint des systèmes d'information en charge de « Infrastructure SI et Exploitation » et de M. Pierre-Yves Burgi, directeur adjoint des systèmes d'information en charge de « SI-Enseignement et Apprentissage, Recherche, Collaboration » (UNIGE).
- Audition du préposé à la protection des données et à la transparence, M. Stéphane Werly (PPDT).
- 8 décembre 2017 : Audition de M. Antoine Geissbuhler, professeur et médecin chef de service aux HUG.

- Audition de M. François Abbé-Decarroux, directeur général et de M. Cyril Epiney, responsable des systèmes d'information (HES-SO Genève).
- 12 janvier 2018 : Audition de M. Jean-Daniel Zeller, président de la commission consultative en matière de protection des données, de transparence et d'archives publiques (CCPDTA).
- Audition de M. Karl Wimmer, directeur suppléant du centre suisse des technologies de l'information dans l'éducation (CTIE – educa.ch) et responsable du projet FIDES (Fédération des services d'identités numériques pour l'espace suisse de la formation).
- 19 janvier 2018 : Audition de M. Pascal Verniory, expert-juriste de l'OCSIN (DI).
- 2 février 2018 : Discussion et vote d'entrée en matière.
- 15 juin 2018 : Discussion sur la suite des travaux.
- 28 septembre 2018 : Audition de Mme Giselle Toledo Vera, juriste à la direction des affaires juridiques (DIP) et M. Manuel Grandjean, directeur du service écoles-médias (SEM – DIP).
- 16 novembre 2018 : Audition de M. Stéphane Koch, spécialiste médias et réseaux sociaux.
- 7 décembre 2018 : Audition de M. Manuel Grandjean, directeur du service Ecoles-Médias (DIP).
- 21 juin 2019 : Discussion en présence de M. Manuel Grandjean, directeur du service Ecoles-Médias (DIP).
- 27 septembre 2019 : 2e et 3e débat en présence de Mme Giselle Toledo Vera, juriste à la direction des affaires juridiques (DIP), de Mme Noémi Paparou et de M. Jean-Luc Corsini du service écoles-médias (SEM – DIP).

Contenu du PL 12103

En substance, le PL 12103 prévoit trois mesures :

- Les systèmes de messagerie, ainsi que les espaces numériques de dépôt et de partage de données mis à disposition des élèves, des étudiants et d'autres personnes en formation, ainsi que des collaborateurs du DIP du canton de Genève doivent être fournis par les services informatiques de l'Etat.
- En cas de nécessité, ils peuvent être fournis par des entreprises suisses et domiciliées en Suisse.

– L'Etat garantit que les données échangées ou déposées dans l'espace numérique mis à disposition par les personnes mentionnées à l'alinéa 1 sont stockées dans un data center en Suisse et sont uniquement soumises à la loi suisse en matière de protection des données.

Audition de M. Jean-Michel Bugnion, premier signataire

M. Bugnion expose que le PL 12103 vise à rapatrier en Suisse le stockage des données personnelles des élèves majeurs et mineurs qui fréquentent les filières du DIP et à soumettre ces données exclusivement au droit suisse.

Il expose qu'à l'heure actuelle, Google stocke les données dans le Cloud, soumis au droit américain. Or, les entreprises américaines ayant leur siège aux Etats-Unis sont soumises au Data Privacy Act qui les oblige à fournir les données aux autorités américaines, sur demande de ces dernières.

Les mesures prises par Google pour l'anonymisation de l'identité des élèves ne fournissent pas de garanties suffisantes et l'on peut les contourner en procédant à des recoupements ou en analysant le contenu des messages.

Il relève que les élèves n'ont pas toujours conscience de communiquer des données sensibles. Les mesures de prévention ne garantissent pas une protection suffisante.

Il ajoute que les auteurs du PL ont sollicité une offre de la société VTX pour assurer la même capacité de messagerie que celle du DIP. Cela reviendrait à un montant mensuel de 10 500 francs, soit 126 000 francs par an.

L'enjeu de ce PL est par ailleurs clairement politique. Il faut se demander s'il est opportun de rester dépendant de l'économie et du droit américains ou s'il ne faut pas plutôt privilégier une solution localisée sur le territoire suisse et soumise à la juridiction helvétique, tout en encourageant l'économie du pays. Il ajoute que le coût ne devrait pas être exorbitant.

Pour répondre à un commissaire UDC, M. Bugnion indique qu'il ne s'agit pas d'obliger les enfants à utiliser chez eux une autre messagerie que Google. Il s'agit de faire en sorte qu'à l'école, les données ne soient pas stockées sur sol américain. A son avis, l'Etat a une part de responsabilité lorsque ces données ont été collectées dans le cadre scolaire.

Un commissaire EAG souligne que l'on ne parle pas seulement du coût d'une messagerie. Le sujet est plus large. Il relève également le caractère flou du libellé de l'art. 37 A, al. 2 du projet qui inclut la formulation « en cas de nécessité ».

M. Bugnion répond que le flou évoqué a été voulu par les auteurs du PL, dont le but est de signaler un problème à l'Etat, sans être en position de dire ce qu'il faut faire. Il évoque diverses pistes pour résoudre ce problème.

Un commissaire PLR estime que la rédaction du PL est peu aboutie, notamment dans ces aspects financiers. Il prévoit en outre une forme de garantie de l'Etat qui constitue un risque considérable. Il estime qu'une motion aurait été préférable.

M. Bugnion est d'avis qu'il appartient aux services de l'Etat de procéder à une estimation des coûts.

Suite à l'intervention d'un commissaire socialiste, M. Bugnion précise qu'il faudrait restreindre la définition des personnes en formation. La question de la prise en compte de l'Université se pose.

Pour répondre au même commissaire socialiste, M. Bugnion précise qu'une entreprise suisse est une entreprise dont la majorité du capital appartient à un Suisse.

Pour répondre à l'intervention d'un commissaire PLR, M. Bugnion indique que les HES n'appartiennent pas au DIP.

Le même commissaire PLR se demande comment seront gérés les cas des apprentis en formation duale. Les entreprises formatrices souhaiteront avoir un retour du DIP sur les rapports d'évaluation, par exemple.

Pour M. Bugnion, les entreprises continueront à fonctionner comme elles le souhaitent, mais le stockage des rapports d'évaluation au DIP se fera différemment.

Audition de M. Manuel Grandjean, Directeur du service écoles-médias

M. Grandjean expose que l'une des raisons qui a fait que le DIP s'est intéressé à Google Apps est la qualité de cette plateforme. Par ailleurs, il est intéressant d'utiliser à l'école des outils également en vigueur dans le monde civil et professionnel. L'utilisation de cette plateforme se fait avec un accompagnement particulier, dont un discours de prévention.

Il ajoute que Google Apps ne peut pas être utilisé à des fins privées ou à des fins administratives. Aucune donnée personnelle ne doit figurer sur cette plateforme.

Il s'agit d'un environnement clos dont le DIP possède le droit d'administration. Il est impossible pour un élève de stocker un fichier et de le partager avec quelqu'un qui ne relève pas du DIP.

Le cadre juridique fixé contractuellement exclut toute utilisation des données par Google. Par ailleurs, les données supprimées de la plateforme sont définitivement effacées 6 mois après leur suppression. Par ailleurs, le contrat conclu avec Google n'est soumis ni au droit, ni au for aux Etats-Unis.

M. Grandjean insiste sur le fait que les outils en question ne sont pas simplement une messagerie ou un poste de stockage, mais constitue un ensemble d'outils intégrés (traitement de texte, tableur, classroom, etc.). Il s'agit d'un écosystème cohérent et efficace.

M. Grandjean relève que le PL suscite des inquiétudes à l'Université et dans les Hautes Ecoles. En effet, si toute personne en formation doit stocker les données en Suisse, cela met en péril des collaborations en matière de recherche.

Il rappelle que le cadre prévu actuellement par la loi est le suivant : il est possible d'héberger des données à l'étranger si la garantie offerte est identique à celle que l'on a en Suisse. A ce jour, les Etats-Unis figurent toujours sur la liste tenue par le préposé fédéral à la protection des données comme pays sûr du point de vue de l'hébergement des données.

Pour répondre aux préoccupations exprimées dans le PL, M. Grandjean indique que l'une des pistes pourrait être le renforcement de l'anonymisation des noms.

Pour répondre à une question d'un commissaire PDC, M. Grandjean explique que la maintenance technique de la plateforme est assurée par Google. Le DIP ne se charge que de l'administration. Le coût est ainsi nul pour la mise à disposition de la plateforme. Ce qui coûte est le contrôle de l'utilisation du support, mais pas son exploitation technique.

Le président (Ve) demande si les manquements constatés dans l'utilisation de la plateforme sont plutôt le fait des élèves ou celui du corps enseignant.

M. Grandjean précise que ces manquements sont peu nombreux. Ils peuvent venir des élèves ou du corps enseignant. Le service écoles-médias intervient en cas de problème. Cette intervention a aussi une portée éducative.

Un commissaire socialiste s'intéresse à l'utilisation possible de la solution ownCloud.

M. Grandjean indique que ownCloud est une solution actuellement exploitée par la DGSI et, partiellement, par l'administration. Le problème est que ownCloud est simplement une interface ou un moyen d'accéder aux données. Or, le principal problème réside dans la capacité de stockage des

données en question. OwnCloud pourrait être utilisé dans une optique de complémentarité et non pas de substitution.

Pour M. Grandjean, demander à l'Etat de Genève de remplacer fonctionnellement Google dans tous ses aspects, y compris en ce qui concerne la capacité de stockage, serait disproportionné en termes d'efforts et impossible en termes de coûts.

Audition de M. Eric Favre, Directeur de la DGSI

M. Favre comprend qu'il est entendu sur la faisabilité technique et les coûts induits par le PL 12103. Concernant la faisabilité technique, il est parti de quelques hypothèses :

– la brique de base : un annuaire pour les élèves et les enseignants
– une messagerie pour les élèves (les enseignants du DIP en disposent déjà)
– un espace de dépôt et de partage des données
– 45 000 élèves (par conséquent, l'Université, les HES, etc. sont hors du périmètre de l'estimation).

Dans ce cadre, la loi est faisable techniquement. Néanmoins, il est très difficile de rivaliser avec Google. Le service fourni par Google est intégré et comprend d'autres fonctions que la messagerie et le partage de données (visés dans le PL). Si l'on supprime Google, il faudrait recréer ces autres fonctions dans d'autres environnements. La DGSI n'aura pas les moyens de fournir un service avec la même « expérience utilisateur » que ce que Google ou Microsoft offrent dans le Cloud.

M. Favre précise que la proposition est limitée à ce qui est décrit dans le PL, mais pourrait être d'une autre envergure s'il fallait vraiment englober tous les services fournis par Google. Les services fournis par la DGSI s'appuient notamment sur des logiciels achetés chez des éditeurs tels que Microsoft. Mais les données sont hébergées sur les serveurs de la DGSI, sans connexion avec le Cloud.

S'agissant de l'estimation des coûts, M. Favre explique que la fourniture du service conforme au PL coûte 2.60 francs par étudiant et par mois. Ce projet coûterait donc 7 millions de francs sur 5 ans. La part d'investissement serait d'un peu moins de 1,8 million de francs. On doit aussi prévoir des charges de fonctionnement annuelles (maintenance, support et exploitation par la DGSI) pour environ 900 000 francs par an. La présentation de la DGSI est jointe au présent rapport.

Suite à une question du président (Ve), M. Favre confirme que la DGSI n'héberge aucune donnée dans le Cloud. Le DIP est le seul département qui

agit de la sorte. Les SIG ont conclu un contrat avec Microsoft pour avoir leur bureautique sur le Cloud de cette société. D'un point de vue technique, l'avantage pour l'utilisateur est énorme. Sous l'angle de la protection des données, il laisse les députés en juger.

Pour répondre à un commissaire MCG, M. Favre ajoute que le DIP s'est lancé dans le Cloud pour son coût et sa qualité de service. Le Département a pris des précautions en édictant des directives d'utilisation. S'il avait été consulté par le DIP à l'époque, il n'aurait pas forcément cautionné cette démarche.

Suite à une intervention du président, M. Favre indique que les données de la DGSI sont stockées principalement dans deux centres de calcul sur le territoire genevois. En matière de sécurité, il serait toutefois préférable d'éloigner ces deux lieux.

Toujours pour répondre au président, M. Favre insiste sur le fait que s'il fallait reconstruire l'ensemble du périmètre Google, l'Etat serait capable de faire quelque chose, qui ressemblerait à un patchwork. Il ne serait pas possible de faire quelque chose d'aussi fluide que chez Google. Il ne sait pas si c'est l'expérience utilisateur ou bien la protection des données qui est le plus important aux yeux du Grand Conseil.

Pour répondre à une question d'un commissaire socialiste, M. Favre indique que ownCloud est une solution en logiciel libre qui permet de faire de la synchronisation de fichier, comme on le fait sur Dropbox, mais qui permet aussi le partage de fichiers ou l'accès à des fichiers à distance. Ce système est déjà utilisé à l'Etat, mais à une toute petite échelle. L'estimation financière qu'il a fournie permet la généralisation d'un ownCloud.

Pour conclure, M. Favre indique que l'on se trouve face à deux choix bien distincts. L'un est celui d'être particulièrement attentif à la protection des données. L'autre choix est de se dire que Google Apps est un magnifique outil, qui présente de nombreux avantages, aussi en termes de déploiement car tout est disponible en ligne. La pesée d'intérêt revient au politique.

Première discussion en commission

Ces différentes auditions donnent lieu à une première discussion en commission.

Un commissaire PLR relève qu'il existe un conflit interne à l'administration, dans la mesure où le DIP ne semble pas être du même avis que la DGSI. Il relève que le coût du projet a été estimé à près de 7 millions de francs par la DGSI, mais que l'histoire a démontré que les projets

informatiques de l'Etat ont souvent coûté beaucoup plus cher que prévu. On est donc loin des 126 000 francs articulés par M. Bugnion, auteur du PL. Il relève également que ce projet est impraticable en lien avec l'Université, les HES, les entreprises qui forment des apprentis et les écoles professionnelles.

Le président (Ve) remarque que grâce à la nouvelle équipe de la DGSI, il n'y a plus eu de dépassement de crédits. Il relève aussi que le DIP s'est tourné vers Google car le service proposé par cette société était gratuit. Or, il lui paraît évident que le but est d'offrir la gratuité du service contre l'obtention des données des personnes concernées. Il n'a toutefois pas d'amendement à proposer en l'état.

Un commissaire socialiste est d'avis qu'il conviendrait d'étudier le contrat signé avec Google. Il ajoute que le PL ne prévoit pas que tout doit être internalisé au niveau de l'Etat. Si le contrat est clair et garantit le stockage des données en Suisse ainsi que la confidentialité des données, cela serait acceptable. Il veut par ailleurs connaître la contrepartie pour l'accès gratuit aux services de Google.

La commission fixe la suite des auditions et sollicite la remise des contrats conclus avec Google.

Audition de M^me^ Marie-Claude Sawerschel, Secrétaire générale du DIP, de M^me^ Giselle Toledo Vera, Juriste à la direction des affaires juridiques et de M. Manuel Grandjean, Directeur du service école-médias

Les documents contractuels avec Google sont joints au présent rapport.

M^me^ Sawerschel expose que la question est de savoir comment utiliser les outils informatiques comme matériel d'apprentissage. Il s'agit également de connaître l'outil informatique, ses usages et ses risques. Cette dimension doit aussi être enseignée. Il ne doit pas y avoir d'utilisation administrative de cet outil.

Elle relève par ailleurs que plus un outil est utilisé plus cet outil s'améliore. On parle d'un « effet réseau ». Genève ne peut pas créer un tel outil actuellement, alors que Google a développé le sien pendant des années avec une réserve de millions d'utilisateurs.

Il est important de sécuriser l'utilisation de cette suite et de tirer vers la Suisse des garanties contractuelles pour conserver notre indépendance. Avec le nouveau contrat, la loi américaine ne pourra pas s'appliquer à l'école suisse. Ainsi, pour éviter que cette loi américaine ne s'applique, le DIP va signer le contrat avec Google Irlande. Les données seront stockées dans cet Etat.

Pour répondre à la question d'un commissaire PLR, M^me^ Toledo Vera expose que le changement de partenaire contractuel en faveur de Google Irlande est intervenu en été 2017. Google doit en effet s'aligner sur le nouveau règlement européen (le RGPD) qui entrera en vigueur en mai 2018. Ce texte de l'UE offre parfois des garanties plus élevées que le cadre légal suisse.

M^me^ Toledo Vera fait également référence à l'art. 107 al. 3 LIP qui dispose que le Département « met en place des outils pour favoriser l'utilisation pédagogique des médias, images et technologies de l'information et de la communication ». « Google for education » n'est certes pas la seule offre, mais elle constitue la plateforme la plus « user friendly ».

M^me^ Toledo Vera cite aussi le nouvel amendement à l'art. 7 du contrat avec Google qui répond aux préoccupations européennes et suisses. Google a ainsi pris l'engagement de détruire les données au plus tard dans les 180 jours. A partir du moment où l'utilisateur décide qu'une donnée ne doit plus être sur la plateforme, elle sera détruite. Enfin, il a été décidé d'empêcher une élection de for en faveur du droit américain.

M^me^ Toledo Vera précise encore qu'il ne faut effectivement pas être naïf. Si Google offre la gratuité, c'est pour créer des habitudes chez les consommateurs. Une fois que l'on est habitué à un format d'applications, on a davantage tendance à se diriger vers des plateformes qui présentent un tel format. Mais elle précise qu'il n'y a en l'occurrence pas d'utilisation commerciale possible des données concernées.

Pour répondre à une question du président, M^me^ Toledo Vera relève que l'avertissement sur l'interface était présent depuis plusieurs mois mais qu'il a été rendu plus visible.

Un commissaire PLR relève que l'art. 37 al. 1 du PL 12103 impliquerait la résiliation de tous les contrats conclus avec des tiers, pas seulement avec Google.

M. Grandjean confirme ce point. Cela conduirait notamment à la résiliation du projet Voltaire. Ce dernier est constitué d'une plateforme d'apprentissage de la langue française en ligne. Il en irait de même de la plateforme utilisée par de nombreuses écoles en Suisse pour détecter le plagiat dans les travaux de maturité. Dans les deux cas, les données se trouvent en France.

Audition de M. Denis Hochstrasser, Vice-recteur de l'Université, de M. Jean-François Rossignol, Directeur SI adjoint en charge de « Insfrastructures SI et Exploitation » et de M. Yves Burgi, Directeur SI adjoint en charge de « SI-Enseignement et Apprentissage, Recherche, Collaboration »

M. Hochstrasser expose que la protection des données préoccupe l'UNIGE, que ce soient les données administratives des étudiants, des patients ou des données de recherche. On constate une ambivalence. D'un côté, la protection des données est capitale. De l'autre, l'Université est obligée de partager les données, sinon la Suisse sera exclue du monde. A titre d'exemple, on peut citer le financement européen de la recherche, qui a décidé d'octroyer un financement à la Suisse pour autant que les données soient ouvertes et partagées.

M. Hochstrasser ajoute que pour les données de la recherche, l'Université a décidé d'avoir une personne chargée de surveiller la protection des données. Certains éléments sont sur le Cloud et d'autres uniquement en interne, sur un système de stockage des données. L'Université recommande l'utilisation de SWITCH et non pas de Dropbox, qui a été piraté.

Il indique que l'UNIGE étudie les systèmes d'information pour la gestion des étudiants, qui sont actuellement obsolescents. Les premiers travaux montrent qu'il serait déraisonnable que l'Université développe elle-même un nouveau logiciel dont le coût serait d'environ 23 millions de francs, contre 3 ou 4 millions pour l'achat d'un logiciel.

Suite à une intervention du président (Ve), M. Rossignol expose qu'il est certain que Google ne peut pas fournir le même niveau de garantie de sécurité que le système d'UNIGE. Il ne connaît pas le système de l'Etat, mais il relève qu'il est possible de faire du chiffrement de données, même si le système lui-même n'est pas protégé. Il ajoute que l'EPFL utilise Google pour ses collaborateurs et étudiants. Mais Google s'est engagée à ne pas utiliser ni divulguer les données. D'autre part, Microsoft offre à tous les élèves et étudiants une solution dans le Cloud nommée « Office 365 » qui a été approuvée par la Commission fédérale « Privatim ». Cette dernière a donné son aval après avoir négocié avec Microsoft pour que les données soient hébergées en Europe et que le for juridique soit en Suisse.

Pour répondre à une question du président, M. Rossignol indique que seules les données de recherche sont hébergées sur le Cloud.

Suite à une intervention du président, M. Hochstrasser expose qu'il faut prendre en compte l'aspect du coût évolutif et celui de l'indépendance. Une solution Google ne coûte peut-être rien maintenant, mais l'on est prisonnier.

Par ailleurs, le fait de déposer des résultats de recherche sur Google crée un risque considérable pour la propriété intellectuelle.

Au sujet du PL 12103, M. Burgi relève que le périmètre d'application n'est pas clair. On ne sait pas s'il englobe les chercheurs et les enseignants. Mettre dans le même panier les élèves du primaire, du secondaire et de l'Université va trop loin, car ils n'ont pas les mêmes besoins. Ce PL n'aiderait en rien l'UNIGE en matière de protections des données, car cette institution dispose déjà d'une solution qui fonctionne.

Audition de M. Stéphane Werly, Préposé cantonal à la protection des données et à la transparence

A propos du 1er alinéa de l'art. 37A du PL, M. Werly relève que l'idée est de limiter la protection aux étudiants en formation. Il se demande s'il ne faudrait pas étendre la protection à tous les mineurs. En effet, plus on est jeune, plus les risques sont importants. Le terme « en formation » devrait être défini dans l'exposé des motifs.

En lien avec la question de la sous-traitance évoquée aux alinéas 2 et 3 du PL 12103, M. Werly fait référence aux art. 13 et 13A du RIPAD qui sont entrés en vigueur le 15 février 2017. L'art. 13A prévoit que « s'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat ».

M. Werly précise que la LIPAD elle-même ne parle pas de la sous-traitance. Toutefois, la pratique a démontré que beaucoup d'institutions utilisaient le Cloud, alors que la loi genevoise ne le permettait pas, contrairement au droit fédéral. Il a donc fallu inclure dans le RIPAD une disposition pour permettre la sous-traitance. Concernant le PL 12103, il se demande s'il ne serait pas préférable de reprendre l'art. 13A RIPAD et de l'adapter.

M. Werly relève à ce propos que l'art. 37A al. 2 du PL impose des entreprises suisses domiciliées en Suisse. La sous-traitance en Suisse est certes préférable, mais elle coûte très cher. Il se demande s'il ne serait pas préférable de prévoir que la sous-traitance peut être fournie par des entreprises soumises à un droit qui assure un niveau de protection adéquat. Il ajoute que beaucoup d'institutions publiques se tournent vers l'Allemagne qui a des mesures de protection similaires à la Suisse.

Pour répondre à un commissaire PLR, M. Werly indique que tous les Etats membres de l'UE offrent des garanties suffisantes. Le Préposé fédéral à la protection des données établit la liste de référence. M. Werly précise qu'il est tenu par la liste établie par le Préposé fédéral.

M. Werly relève que les Etats-Unis font d'ailleurs partie de cette liste. Mais pour les USA, cela dépend des entreprises concernées. Elles doivent avoir signé le « Privacy Shield ». A titre personnel, il déconseille le choix des Etats-Unis car les règles du « Privacy Shield » peuvent être contournées par le « Patriot Act ».

Suite à une intervention du président, M. Werly expose qu'il a été approché par des institutions publiques qui pratiquaient beaucoup le Cloud et qui lui ont demandé de les aider à rédiger les contrats de sous-traitance des données. Il évoque notamment les SIG, les HUG et les TPG.

Pour conclure, M. Werly indique que le canton de Genève a la loi la plus contraignante en matière de protection des données en Suisse. Les garanties vont plus loin que le droit fédéral.

Audition de M. Antoine Geissbuhler, professeur et médecin chef de service aux HUG

Le Prof. Geissbuhler expose que la norme actuellement en vigueur est que toutes les données concernant les patients sont physiquement dans les locaux des HUG. Ce principe s'applique également dans le système de cyber-santé « mon dossier médical » qui met en réseau les données du patient. La situation devient plus compliquée car un certain nombre de solutions logicielles qui intéressent les HUG sont basées sur le Cloud ou sur des logiciels hébergés par des serveurs dont les HUG ne sont pas propriétaires. Pour l'instant, les HUG ne sont pas entrés en matière pour ce type de logiciels en ce qui concerne les données des patients. Il est toutefois clair qu'un certains nombres de solutions modernes n'existent plus que sous ces formes. La question de leur utilisation va donc se poser. La loi permet d'ailleurs actuellement d'utiliser des services qui sont hébergés non seulement en Suisse, mais aussi dans les pays qui répondent au même niveau de fiabilité. Il s'agit avant tout des Etats membres de l'UE.

M. Geissbuhler ajoute que Dropbox n'est pas accessible sur le réseau des HUG, car ces données sont stockées aux Etats-Unis, qui ne répondent pas aux exigences en termes de fiabilité et de protection de la sphère privée. Les HUG disposent d'un outil SWITCHdrive qui est le réseau informatique académique, dont les données sont hébergées en Suisse. Ce système est géré par une association d'organisations universitaires suisses, dont font partie toutes les universités. SWITCHdrive permet de partager des données en Suisse, mais donne aussi l'accès à une personne à l'étranger à ces données en Suisse.

En réponse à une question d'un commissaire PLR, le Prof. Geissbuhler expose qu'il faut pouvoir travailler en réseau dans le domaine de la santé et de la recherche.

Suite à une intervention du président, M. Geissbuhler indique que le PL 12103 pourrait poser problème en ce qui concerne des logiciels de gestion de processus qui ne manipulent pas forcément de données très sensibles. Il peut aussi s'agir de logiciels traitant de données RH de collaborateurs des HUG. Un projet en cours prévoit que ces données soient hébergées aux Pays-Bas, qui font partie de la liste autorisée par le préposé à la protection des données. Savoir si ces données sont hébergées en Suisse ou aux Pays-Bas n'est pas un enjeu majeur pour les HUG car un certain nombre de précautions sont prises.

M. Geissbuhler précise encore que les HUG ont décidé d'investir dans le développement de leur système « cœur de métier ». Pour ce qui ne relève pas de ce « cœur de métier », mais de la gestion de l'entreprise en général, il faut prendre la meilleure solution possible sur le marché, qui n'est pas forcément développée et exploitée en Suisse.

Suite à une intervention du président (Ve), le Prof. Geissbuhler ajoute que l'art. 37A al. 2 poserait problème car il dispose que « en cas de nécessité, ils peuvent être fournis par des entreprises suisses domiciliées en Suisse ». Or, un certain nombre de solutions importantes pour le fonctionnement de l'hôpital ne seront probablement pas produites par des fournisseurs suisses. Dans le domaine de la santé, la Suisse ne procure quasiment pas de solutions universitaires avec des systèmes d'information achetés en Suisse. Dans tous les autres hôpitaux, les solutions sont étrangères (par exemple, le CHUV utilise une solution des Etats-Unis). A son avis, les dispositions concernant les pays qui répondent au même degré de fiabilité et de protection des données paraissent acceptables et suffisantes comme garde-fou.

Audition de M. François Abbé-Decarroux, Directeur général de la HES-SO Genève, et de M. Cyril Epiney, responsable des systèmes d'information

M. Abbé-Decarroux expose que toutes les bases de données de la HES-SO Genève sont aujourd'hui stockées sur le territoire suisse. Des données sur les étudiants sont stockées à Fribourg, car il existe des applications communes entre les différents sites.

M. Epiney ajoute que jusqu'à l'été 2017, la messagerie était hébergée à la DGSI. Un transfert a été effectué sur leurs serveurs internes dans les locaux

de la HES-SO à Genève. Il précise qu'une partie des données financières se trouvent sur le Cloud de l'entreprise Oracle.

Concernant la recherche, M. Abbé-Decarroux indique que la HES-SO échange énormément d'informations avec leurs pairs dans les universités et les institutions spécialisées situées à l'étranger. Il n'est pas possible de limiter ces contacts.

Pour répondre à un commissaire PLR, M. Epiney indique que, parfois, le contact peut se faire par simple échange d'e-mails. D'autres fois, les institutions étrangères mettent à disposition des espaces où les externes peuvent se connecter. La HES-SO utilise aussi la plateforme SWITCHdrive avec des accès sécurisés pour des échanges de données. La HES-SO n'est pas forcément l'initiatrice de tous les projets et les données peuvent être hébergées dans l'université partenaire où la recherche est faite.

Suite à l'intervention d'un commissaire PLR, M. Abbé-Decarroux expose avoir mal compris le PL 12103. En lisant l'exposé des motifs, il était persuadé qu'il concernait uniquement les données personnelles.

Le même commissaire PLR explique que l'exposé des motifs a été mal rédigé. Le texte de la loi est beaucoup plus restrictif que l'exposé des motifs.

Le président indique qu'il faudrait peut-être modifier le PL pour les 10% des données qui sont liées à la gestion d'entreprise et qui sont stockées à l'étranger. La volonté du législateur est que les données sensibles soient stockées en Suisse, ce que la HES-SO fait déjà sur SWITCHdrive. Il faudrait modifier légèrement le PL pour la question du stockage des données non-sensibles.

Audition de M. Jean-Daniel Zeller, président de la commission consultative en matière de protection des données, de transparence et d'archives publiques (CCPDTA)

M. Zeller rappelle que la CCPDTA est formée de délégués élus par le parlement et d'une série d'experts nommés par le Conseil d'Etat. Il expose que le projet Ecole en ligne (EEL) avait fait l'objet d'un examen par les bureaux des préposés à la protection des données. Les préposés de l'époque n'avaient pas trouvé que le système proposé était suffisamment protecteur en termes d'anonymisation des adresses e-mails des élèves et de sécurité par rapport aux services de Google. La décision avait été prise sur la base de l'accord Safe Harbor, qui était une évaluation par la Suisse et des pays européens portant sur le caractère équivalent ou non des législations relatives à la protection des données. A l'époque, le Safe Harbour permettait de

conclure que tel était le cas concernant les Etats-Unis, mais c'était avant l'affaire Snowden.

Pour M. Zeller, l'obstacle d'une gestion à l'interne de la messagerie et des dossiers partagés est a priori parfaitement gérable. Plusieurs institutions gèrent des messageries à l'interne de manière pertinente. Il ne voit pas pourquoi le DIP ne pourrait pas le faire. A son avis, on peut se passer de Google.

Pour répondre à une question du président (Ve), M. Zeller estime que le périmètre d'application du PL est adéquat, dans la mesure où il inclut également les enseignants et les étudiants adultes. Il est judicieux de ne pas faire de discrimination en fonction de l'âge. C'est donc le statut d'élève qui est pertinent. Le personnel enseignant mérite aussi une protection.

Suite à une intervention du président, M. Zeller répond que si le PL impacte l'Université, celle-ci devra préciser ses bonnes pratiques. Il existe des règles formelles précises pour les publications, donc ce n'est pas un problème. Un amendement relatif aux bonnes pratiques devrait suffire.

M[me] Toledo Vera, juriste au DIP, fait référence à la situation des doctorants qui ont un statut d'étudiant. Lorsqu'ils participent à des recherches en lien avec les Etats-Unis, ils doivent pouvoir transférer des données. Si toute la communication des doctorants doit être hébergée en Suisse, elle demande comment ils pourraient mener à bien leurs recherches.

M. Zeller répond qu'il n'a pas songé à cette problématique. Il serait judicieux d'ajouter un article dans la loi pour les exclure du champ d'application. En intégrant un article « exceptions », cela permettrait de réviser la loi dès que l'on s'apercevrait qu'un autre groupe de population souffrirait aussi de cette protection.

M[me] Toledo Vera précise que le Safe Harbor évoqué par M. Zeller en lien avec les Etats-Unis a été révisé par les autorités fédérales. Il est devenu le « Swiss-US Pravicy Shield » qui est entré en vigueur le 1[er] janvier 2017. Elle souligne surtout que le champ d'application du PL 12103 ne se limite pas à la problématique des Etats-Unis. Tous les accords existants, notamment avec les autorités françaises, seraient touchés. Elle indique que le nouveau Règlement européen pour la protection des données (RGPD) entrera en vigueur en 2018. Il sera très restrictif.

M[me] Toledo Vera relève que le PL 12103 pose deux problèmes. Le premier concerne le champ d'application personnel en lien avec les personnes majeures. Le second réside dans le fait que le PL ne fait pas la différence par rapport aux prestataires de services situés dans l'UE.

M. Zeller répond que l'art. 13A RIPAD devra être adapté en lien avec le Règlement européen.

Audition de M. Karl Wimmer, directeur suppléant du Centre suisse des technologies de l'information dans l'éducation (CTIE- educa.ch) et responsable du projet FIDES (Fédération des services d'identités numériques pour l'espace suisse de la formation)

M. Wimmer expose qu'educa.ch est l'agent spécialisé de la Confédération et des cantons pour toutes les questions concernant la problématique de l'éthique dans la formation. Le CTIE essaye de coordonner l'action des cantons. La marge de manœuvre est toutefois étroite. Un contrat de prestation a été conclu pour la période 2017-2020 au sujet des défis liés à la transformation numérique du système éducatif des écoles.

Pour lui, l'école doit travailler avec les services en ligne qui viennent du Cloud. L'utilisation de ces services génère nécessairement des données qui sont produites volontairement par l'utilisateur. Il faut protéger ces données.

M. Wimmer soulève quelques questions en lien avec le PL 12103, en lien avec les différents alinéas :

- Alinéa 1
    - Le DIP devrait-il vraiment développer des services en ligne comme Google ? La concurrence avec les grandes entreprises est une tâche difficile.
    - Education aux médias ? Il est important de travailler dans l'environnement habituel connu en dehors de l'école. L'école ne doit pas se renfermer sur elle-même.
    - Conséquences financières ? Le monde de l'informatique coûte cher. On risque de payer beaucoup pour exploiter un système, mais aussi pour pouvoir en sortir. Il faut établir une stratégie sur l'utilisation et l'implémentation de ces systèmes dans l'école.
- Alinéa 2
    - Contrats avec des fournisseurs de services ? Une entreprise comme Samsung a un siège en Suisse. Il se demande si elle n'est alors pas considérée comme étant une entreprise suisse. Ils disposent également d'un contrat-cadre avec Microsoft qui est conforme aux lois suisses. Les écoles peuvent acheter des licences pour ces produits. Le for juridique est à Berne et la loi suisse s'applique.

- Alinéa 3

  - Lois suisses (et genevoises) en matière de protection des données en vigueur ? Ces lois sont déjà en vigueur. Le préposé à la protection des données joue un rôle central. Privatim est la conférence des préposés suisses à la protection des données. Privatim a élaboré des recommandations pour le traitement et la gestion des données dans les écoles. Ils distinguent les données personnelles, qui peuvent être stockées dans l'espace européen, et les données sensibles, qui doivent être cryptées. Les serveurs ne doivent pas forcément être en Suisse selon Privatim.

M. Wimmer présente ensuite le projet FIDES (Fédération des services d'identités numériques pour l'espace suisse de formation). Il s'agit de créer un service permettant de se connecter en ligne avec une identité sûre (la personne n'est plus anonyme, mais identifiable). Ce système protège l'utilisateur des données, mais aussi le fournisseur de services, car il sait qui utilise ses différents services. Il protège également l'Etat, qui est responsable vis-à-vis des écoles.

Audition de M. Pascal Verniory, expert-juriste de l'OCSIN (anciennement la DGSI)

M. Verniory indique que le fait que des données des élèves et des autres personnes en formation soient stockées dans un data center en Suisse et qu'elles soient soumises uniquement à la loi suisse semble possible par rapport au droit existant, le reste relevant d'une volonté politique. Il observe qu'il est possible d'envisager une sous-traitance qui soit limitée à des sociétés domiciliées en Suisse, qui acceptent des audits sur leurs sites et soient exclusivement soumises à des lois d'un pays offrant des garanties suffisantes.

Il souligne que le terme « uniquement » de l'alinéa 3 exclurait par définition toute maison mère ou entreprise ayant son siège aux Etats-Unis.

Suite à une intervention du président, M. Verniory indique que l'on se trouve face à une option : soit l'on accepte d'utiliser des logiciels gérés par des tiers et l'on accepte donc de perdre en sécurité, soit l'on mise sur une option interne.

Concernant les Etats-Unis, M. Verniory mentionne un arrêt de la CEDH, qui a relevé 3 points dans le droit américain qui violaient très clairement selon la Cour le noyau des droits fondamentaux des citoyens européens.

Pour répondre à une commissaire MCG, il indique que le premier point soulevé par la CEDH est l'accès à un juge, le second concerne la protection de la sphère privée. En revanche, il ne se rappelle pas du troisième.

Pour répondre à un commissaire PLR, M. Verniory indique ne pas être certain que, dans ce domaine, le droit fédéral soit le droit supérieur puisqu'il s'agit de droits parallèles. Il souligne que la LIPAD n'entend légiférer que sur l'administration cantonale genevoise et les administrés genevois, ce qui implique qu'il n'y a en quelque sorte pas de droit supérieur. Il observe que cela n'est pas contraire au droit fédéral si cela peut être justifié. Il ajoute qu'il n'est pas contre Privatim mais relève que les recommandations de cette entité ne sont pas contraignantes.

Un commissaire PLR attire l'attention de M. Verniory sur le fait que le DIP avait mentionné des contacts en France et en Allemagne pour des programmes d'apprentissage, étant précisé que des données sont stockées dans ces pays. Or, l'adoption du PL 12103 impliquerait automatiquement la fin de ces programmes.

M. Verniory reconnaît que l'on peut admettre que des données soient traitées dans des pays offrant des garanties suffisantes, ce qui est un choix politique.

Le même commissaire PLR relève que l'opinion de l'auditionné apparaît comme plus ouverte qu'au début du débat. Il ajoute que l'Université est très préoccupée par ce PL.

M. Verniory observe qu'il est difficile d'avoir une solution optimale pour tous.

Un commissaire MCG demande s'il ne serait pas préférable d'apprendre aux gens à mieux utiliser les messageries, notamment par le biais du cryptage. Il pense que ce genre de loi n'a pas de sens si l'on n'indique pas aux gens un comportement à adopter.

M. Verniory répond qu'en effet, les gens peuvent être éduqués, que la loi peut inciter aujourd'hui au cryptage et que l'Etat peut mettre en place des solutions de cryptage.

M^me^ Toledo Vera, juriste au DIP, relève qu'à l'heure actuelle, pour le DIP, il n'existe aucun lien ou contrat faisant application du droit américain. Dans les contrats en vigueur, l'application du droit suisse est prévue. Elle ajoute que le nouveau Règlement européen (RGPD) est beaucoup plus strict que le droit suisse, notamment à l'égard des mineurs.

M. Verniory conclut en reconnaissant qu'il ne peut que se satisfaire de ces éléments. Il indique avoir axé son intervention sur le droit américain car il

semblerait que certaines clauses n'empêchent pas de l'appliquer. Il remarque que, lorsqu'il est question de pays offrant une protection adéquate, il faut penser aux pays européens, mais également aux USA. Il souligne que les pays européens ont effectivement pris une direction extrêmement protectrice.

Deuxième discussion en commission et vote d'entrée en matière

Un commissaire PLR rappelle que sa première impression sur le PL 12103 était qu'il avait été rédigé sur un coin de table sans beaucoup de réflexions. Cette caricature a été largement confirmée par les auditions. La commission a auditionné le premier signataire. Ce dernier a fait un procès d'intention au DIP en affirmant qu'il y avait des négligences dans le traitement des données des élèves du secondaire. Le premier signataire a affirmé que la solution consistait en un logiciel libre coûtant 126 000 francs. La commission a ensuite auditionné la DGSI. A cette occasion, M. Favre a indiqué qu'il réussirait à sortir une solution pour la somme de 7 millions de francs. Ce dernier a exprimé des doutes sur la bonne foi du DIP, qui avait eu le mauvais goût de ne pas consulter la DGSI dans le cadre de son projet. La commission a également entendu M. Pascal Verniory, expert-juriste de la DGSI, qui a grosso modo affirmé qu'il fallait développer une solution maison, et tant pis s'il fallait arrêter la recherche internationale et les projets linguistiques avec la France et l'Allemagne.

Parmi les auditions plus intéressantes et pertinentes, la commission a entendu l'Université, laquelle a expliqué l'importance cruciale de ces échanges internationaux qui peuvent se faire dans des conditions de sécurité acceptables. A défaut, Genève se trouverait complètement isolée au niveau des étudiants, des doctorants et de la recherche. La commission a aussi entendu M. Karl Wimmer d'Educa.ch (CTIE) qui a expliqué que des mesures pouvaient être prises en termes de for juridique et de droit applicable. Il a rappelé que la Confédération a considéré comme équivalentes les juridictions des pays européens. Pourquoi Genève devrait agir différemment de tout le monde en se privant de ces contacts vitaux pour notre système d'éducation ?

La commission a également auditionné les HES qui avaient la même préoccupation que l'UNIGE.

Le même commissaire PLR ajoute que, dès le départ, ce PL fait un procès d'intention contre le DIP. Or, M^me^ Toledo Vera, juriste au DIP, a expliqué à plusieurs reprises les démarches contractuelles prises, les garanties, etc. L'encadrement, tant scolaire que juridique, est une préoccupation abordée et réglée de manière raisonnable afin de ne pas prétériter la qualité de

l'enseignement à Genève. Le PLR ne rentrera pas en matière sur ce PL, qui est mal construit et fait un procès d'intention à l'égard du DIP.

Le président (Ve) fait une lecture totalement opposée des auditions. Quelques soient les conclusions sur ce PL, les travaux n'auront pas été inutiles car ils ont permis de mettre le doigt sur les défis qu'auront les administrations à l'avenir concernant la sécurité de leurs données et leurs liens avec le Big data. Les auditions l'ont plutôt aidé à voir ce qu'il faut changer dans ce PL pour ne pas poser de problèmes à l'Université et aux HES, ainsi qu'au sein du DIP. Il rappelle que l'objectif premier de ce PL est de protéger les élèves, surtout les mineurs, contre la commercialisation de leurs données dans le big data, comme tel est le cas aujourd'hui.

Pour le président, dans l'ensemble de l'Etat, la pratique est relativement prudente et saine. L'ensemble des e-mails des collaborateurs de l'Etat sont stockés sur des serveurs de l'Etat et physiquement dans le canton de Genève. Tous les collaborateurs ont droit à la sécurité et les élèves mineurs dont on a la responsabilité ont actuellement une adresse chez Google. Toutes les auditions auxquelles la commission a procédé ne l'ont de loin pas convaincu que la situation était satisfaisante de ce point de vue-là. Ce n'est pas tant sur la sécurité des données elles-mêmes, car des dispositions ont été prises par le DIP pour assurer la sécurité et la confidentialité des données. D'autres mesures seront prises car le DIP a bien entendu que l'anonymisation actuelle n'était pas satisfaisante. La problématique, qui est pour le président encore centrale, est que Google est en possession des données et les utilise pour créer des algorithmes. Le fait que ce soit gratuit est uniquement dû au fait que nous leur offrons un produit qui est les données, mêmes rendues anonymes.

Pour le président, il ne faut pas mettre les HES-SO et l'Université dans le périmètre de ce PL. La raison est que, lors des auditions, ces deux institutions étaient complètement conscientes des problèmes posés par la protection des données et la confidentialité de celles-ci, ainsi que de leur utilisation. Elles ont décidé d'avoir des systèmes hermétiques et ont totalement intégré cette problématique en prenant les mesures nécessaires. Le périmètre de ce PL ne changerait pas beaucoup concernant le problème du stockage des données des adresses e-mails. Concernant l'aspect soulevé par l'al. 3, auquel le DIP a rendu la commission attentive par rapport à l'utilisation d'autres types de logiciels, il s'agirait de la disposition la plus compliquée. Le plus simple serait de le supprimer car ce n'est pas le cœur de ce PL, qui est que les élèves bénéficient du même degré de sécurité qu'un employé de l'Etat concernant son e-mail. Si l'entrée en matière sur ce PL est acceptée, le président demandera la suppression des al. 2 et 3. Réduire à ce point-là le champ des possibilités d'ouvrir le marché uniquement à des entreprises suisses ayant

leur siège en Suisse poserait problème. L'al. 2 devient inutile car il était introduit par la présence de l'Université et des HES-SO, dont les données pouvaient difficilement être stockées sur les serveurs de l'Etat. Le cœur du PL est l'al. 1, qu'il faudrait justement amender en ajoutant « à l'exception de l'Université et de la HES-SO ».

Une commissaire MCG indique que son groupe considère que les auditions étaient intéressantes. Son groupe entera en matière sur ce PL.

Une commissaire EAG indique que son groupe était intéressé par la problématique de ce PL. Il y a lieu de se préoccuper de ce genre de questions et de ne pas simplement donner un outil aux étudiants, collégiens et élèves du C.O. EAG entrera en matière sur ce PL. Son groupe est intéressé par les propositions d'amendements présentées car les auditions l'ont alertée sur un certain nombre d'éléments dont il conviendrait de tenir compte.

Un commissaire socialiste indique que son groupe acceptera également d'entrer en matière sur ce PL. Il est favorable à la proposition d'amendement de l'al. 1.

Un commissaire PDC relève que tout au long des auditions, il a constaté une bagarre entre le DIP et la DGSI, ce qui ne donne pas une très bonne image du fonctionnement de l'Etat. Pour avoir travaillé avec la DGSI, il constate que tout projet émanant de ce service coûte quatre à cinq fois plus cher que ce qu'il serait possible d'avoir ailleurs. A Genève, on veut faire mieux que les autres et cela ne fonctionne manifestement pas beaucoup mieux. La DGSI est très susceptible et n'admet pas du tout que d'autres moyens puissent être utilisés. Elle veut garder un contrôle total. Il comprend la proposition d'amendement visant à enlever l'Université et les HES car elle correspond aux conclusions des personnes auditionnées. Il pourrait entrer en matière sur ce PL, mais il a de la peine avec le fait que le président dise dans son amendement qu'il appartiendrait à la DGSI de fournir cette prestation, car il sait que cela coûtera cher. Concernant le fond du PL, il est clair que les adresses, même cryptées, peuvent être utilisées d'une façon ou d'une autre. L'autre problème est le contenu de ces données : ce sont des travaux des élèves, des exercices de mathématiques, de français, etc. Ce ne sont pas vraiment des données sensibles, sous réserve du fait qu'il y a les coordonnées des élèves. Il a beaucoup de peine à prendre une décision en la matière. Autant il trouve que cela vaudrait la peine de faire quelque chose, mais il refuse de commander une usine à gaz. Si la DGSI pilote ce projet, il mettra 5 ans à être mis en place et coûtera au minimum 6 à 7 millions de francs.

Le président répond que les pratiques de la DGSI ont changé avec la nouvelle direction. Il est vrai qu'il y a eu de gros problèmes à une époque,

mais il a l'impression que la situation est meilleure qu'avant. Il comprend les doutes du commissaire PDC et les partage dans le sens où il aurait bien voulu défier la DGSI en faisant un appel d'offres. Le débat pourra effectivement avoir lieu dans le PL sur le maintien ou non de l'al. 2.

Le même commissaire PDC demande s'il ne serait pas simplement possible de prévoir que l'hébergement physique se trouve en Suisse ou dans un Etat reconnu plutôt qu'aux Etats-Unis.

Le président répond que non car cela autoriserait à utiliser Google suisse, ce qu'il veut éviter.

Vote en 1er débat

Le président met aux voix l'entrée en matière sur le PL 12103 :

Pour : 5 (1 Ve, 1 EAG, 1 S, 2 MCG)

Contre : 4 (2 PLR, 1 PDC, 1 UDC)

Abstention : -

L'entrée en matière sur le PL 12103 est acceptée.

Deuxième audition de Mme Giselle Toledo Vera, juriste à la direction des affaires juridiques du DIP

Mme Toledo Vera rappelle que ce projet a été considéré avec beaucoup de sérieux par le département car il pose une problématique importante, à savoir celle de la protection des données personnelles. Par rapport à cette problématique, il y a d'autres impératifs, ceux de la recherche, des possibilités de collaboration internationale ainsi que de l'accès à des outils informatiques qui peuvent aider aux apprentissages. Le département est arrivé à la conclusion que le projet de loi tel que libellé posait trop de restrictions et allait poser trop de problèmes notamment sur l'accès à des outils pédagogiques comme par exemple le projet Voltaire qui aide à l'apprentissage de l'orthographe française. Cette plateforme est mise à disposition par une petite entreprise en France. Avec ce projet de loi tel que libellé, l'accès à ces ressources serait compromis. C'est la raison pour laquelle le Conseil d'Etat et le DIP ont proposé un projet amendé pour tenir compte des préoccupations. D'après ce qui avait été compris, la grande problématique était la messagerie, soit l'échange de courriels entre les élèves, par rapport aux données des élèves. Une des solutions serait que les messageries et annuaires d'élèves soient fournis par l'Etat. Mais le bémol est que cette nouvelle prestation aurait un coût.

Le projet d'amendement du Conseil d'Etat est joint au présent rapport.

Afin de répondre à plusieurs questions d'un commissaire socialiste, Mme Toledo Vera expose ce qui suit :

Elle indique tout d'abord que l'on se trouvait confronté à une question concernant l'outil pédagogique certes fourni par Google, mais avec un contrôle très accru de la part du Département et du SEM. Il existe un contrat qui régit l'utilisation de cette plateforme pédagogique. Les enseignants peuvent l'utiliser (ce n'est pas une obligation), pour animer leurs cours. La problématique était venue du fait que, ce qui gênait certains députés, était que le partenaire contractuel soit Google.

Concernant plus spécifiquement la protection des données, Mme Toledo Vera ajoute que le 25 mai 2018 est entré en vigueur le Règlement européen sur la protection des données (RGPD). Elle rappelle qu'il y a plusieurs serveurs Google dans le monde. Effectivement, il y en aux USA mais aussi en Europe. Le contrat en question implique Google Irlande et il est explicité que ce sont les normes européennes sur la protection des données qui s'appliquent. Cela touche tous les contrats Google avec l'Union européenne. Cette réglementation a un niveau de protection qui est équivalent voire supérieur sur certains points par rapport à la réglementation au niveau genevois et suisse. De ce point de vue-là, le Département a considéré qu'il n'y avait pas de violation de la loi sur la protection des données.

Mme Toledo Vera précise qu'avant l'entrée en vigueur du RGPD précité, il y avait de toute manière le bouclier de protection suisse (Swiss-US Privacy Shield) qui garantissait un niveau de protection élevé et le contrat avec Google Irlande garantissait que la protection des données devait être équivalente à celle en Suisse. Aujourd'hui, l'Union européenne a renforcé sa protection avec ce RGPD.

Mme Toledo Vera répond également que ce qui figure dans le contrat avec Google est un renvoi à la loi fédérale sur la protection des données. La loi fédérale est équivalente en termes de protection de l'individu à la loi genevoise. Google s'était engagé à respecter ces normes de protection. Cela a été remplacé par le RGDP pour toute l'Union européenne. Pour la Suisse, c'est la loi fédérale sur la protection des données qui s'applique (LPD). Elle affirme qu'il est possible de faire parvenir à nouveau le contrat qui avait été analysé lors de sa première audition.

Mme Toledo Vera insiste sur le fait que la loi telle que libellée est trop limitative car cela reviendrait à interdire les espaces numériques de dépôt actuels. La problématique est qu'il n'est pas possible d'avoir un espace

numérique de dépôt qui est limité à la Suisse car cela veut dire qu'il n'est plus possible de travailler avec d'autres plateformes. Cela est trop restrictif.

Mme Toledo Vera explique que la proposition d'amendement du DIP porte sur la messagerie. En revanche, rien n'a été proposé pour l'espace numérique de dépôt. En réalité, rien n'a été proposé car limiter à la Suisse uniquement est trop restrictif et coupe toutes possibilités d'avoir des espaces partagés avec l'Union européenne.

Mme Toledo Vera complète sa réponse en indiquant que si la commission souhaite que le DIP propose une solution à la problématique du stockage, à savoir la définition des espaces numériques de dépôt et la manière de garantir que les données ne soient pas communiquées aux USA, alors, on se trouve confronté au problème que les USA figurent dans la liste des pays qui offrent le niveau de protection adéquat.

Un commissaire vert est d'avis que ce qui lui apparaît compliqué dans la réponse de Mme Toledo Vera est de croire que les données transmises à Google ne sont pas utilisées à des fins commerciales.

Mme Toledo Vera précise qu'il n'est pas possible d'interdire à Google de faire des algorithmes et des calculs. A l'heure actuelle, avec le cadre légal en vigueur et la définition des données personnelles, il n'est pas possible d'empêcher Google de traiter des données qui ne sont pas des données personnelles. Pour illustrer son propos, elle ajoute que ce sont des données au sens large, pas forcément les données personnelles. Quand Google comptabilise sur un site combien de personnes ont cliqué, il n'y a pas de noms qui apparaissent. Ils savent simplement qu'il y a eu X clics et qu'il y a une offre poussée à ce moment-là. Or, la loi sur la protection des données protège l'identification des personnes.

Suite à une autre intervention du même commissaire vert, Mme Toledo Vera explique que ce n'est pas parce qu'un logiciel a une part libre que cela garantit forcément une non utilisation à des fins commerciales. Elle prend l'exemple du système d'Androïd qui a une partie libre mais cela n'empêche pas l'utilisation à des fins commerciales. Le logiciel libre est aussi récupéré par les GAFA. Il faut une réflexion de fond sur toutes ces problématiques, y compris pour ces régimes mixtes, c'est-à-dire qu'une partie est libre et l'autre est utilisée à des fins commerciales. Cela se développe de plus en plus et beaucoup de personnes sont empruntées face à ce type de pratiques. La réflexion à avoir va au-delà de ce projet de loi.

Une commissaire PLR se réfère à la réponse du Conseil d'Etat comportant la proposition d'amendements. Elle souhaite comprendre si le Conseil d'Etat, en résumé, dit que si une loi doit être adoptée, alors il préfère

cette version-là ou alors, s'il partage cette problématique. Elle se demande si cette problématique vaut l'investissement financier. Elle souhaite savoir, également du point de vue juridique, si la situation actuelle a des lacunes.

Mme Toledo Vera répond que les acteurs de terrain ont été consultés, c'est-à-dire les directeurs d'établissements, les enseignants mais aussi les élèves. Il ressort de ces consultations qu'il y a un besoin véridique d'une messagerie pour les élèves. En effet, à l'heure actuelle, la communication entre la direction d'établissement et les élèves se fait par voie d'affichage, par téléphone ou par écrit. Mais de plus en plus, les personnes soulèvent la possibilité d'avoir recours à une messagerie. Cela rentre dans les mœurs des gens.

Mme Toledo Vera ajoute qu'actuellement, il n'y a pas de messagerie officielle pour les élèves. Les enseignants ont des adresses avec « @etat.ge.ch » mais pas les élèves.

La même commissaire PLR déclare qu'il ne s'agit pas d'une problématique de protection des données mais plutôt d'une question d'amélioration du service en assurant la protection des données. En résumé, cela concerne l'élargissement de l'offre.

Mme Toledo Vera ajoute que cela n'empêche pas les parents ou les élèves de communiquer avec les enseignants via leur boîte de messagerie privée. Ces messageries privées des parents d'élèves ou des élèves eux-mêmes sont souvent chez les grands fournisseurs qui les fournissent gratuitement. Elle ajoute que les plus petits des élèves n'ont pas ce besoin.

En guise de complément, Mme Toledo Vera indique que tout fonctionnaire a une boîte électronique qui est mise à disposition par l'Etat, avec toutes les garanties. C'est l'adresse avec « @etat.ge.ch ». Néanmoins, le reste de la population, y compris les parents d'élèves et les élèves, n'ont pas ce service de l'Etat et utilisent des boîtes électroniques choisies par leurs soins. Par conséquent, quand ils transmettent des données à l'enseignant, ils transfèrent avec la boîte choisie. La plupart du temps, les contrats liés à l'utilisation de ces messageries sont des contrats génériques avec des fors aux USA.

Un commissaire socialiste déclare que finalement, l'amendement du DIP concernerait une autre prestation. Puis, il indique que selon sa compréhension, il y a deux aspects dans ce projet de loi. Il y a la question de l'espace numérique de stockage et la messagerie. Sur l'espace numérique, il se demande si le DIP pourrait proposer un amendement qui fixerait un lieu pour l'espace numérique de stockage et qui indiquerait une juridiction semblable aux standards suisses.

Mme Toledo Vera répond que c'est la voie choisie aussi au niveau fédéral. Pour déterminer la liste des pays qui ont une protection de données adéquate, ils se réfèrent à la liste établie par le proposé fédéral à la protection des données et à la transparence. Les USA figurent dans cette liste. A cet égard, elle se réfère aux déclarations du préposé fédéral : « les organismes qui adhèrent au Privacy Shield pour les données provenant de Suisse et qui figurent sur la liste des départements américains du commerce garantissent un niveau de protection adéquat au sens de l'article 6 al. 1 LPD ».

Audition de M. Stéphane Koch, spécialiste médias et médias sociaux

M. Koch indique que l'utilisation d'applications développées par Google ainsi que l'éventuel transfert des données vers les Etats-Unis, soulève de nombreuses questions. En effet, la législation américaine au travers notamment du *Patriot Act* et de la loi *FISA*, permet aux agences de surveillance d'accéder aux bases de données des grandes entreprises d'internet. Toutefois, il est nécessaire de savoir si les données qui concernent ce projet de loi sont liées à ces contrôles. M. Koch explique qu'il existe des centres d'hébergement en Europe. Les pays membres de l'Union européenne sont soumis au *Règlement général sur la protection des données* (RGPD) dans lequel la protection des données est plus importante qu'en Suisse. Il souligne à cet égard que la protection des données risque d'être plus faible si elles sont hébergées en Suisse.

M. Koch ajoute qu'une part de la discussion sur le choix de l'hébergeur dépend des coûts d'une telle procédure. En effet, il est nécessaire de comparer les coûts proposés par Google et ceux d'autres hébergeurs. Il note cependant que les coûts d'un hébergement en Suisse risquent d'être plus élevés que ceux des services de Google. Il souligne également l'importance d'inscrire le système informatique dans une vision à long terme en évitant de changer d'opérateur d'année en année, car les utilisateurs s'y habituent. Enfin, M. Koch soulève la question de la confidentialité et du caractère privé des e-mails. Il indique que l'e-mail est par principe peu sécurisé. Toutefois, la manière dont les e-mails sont transportés par Google permet de s'assurer d'un certain niveau de sécurité. Il pose la question de savoir si ce niveau de sécurité peut être garanti par d'autres services.

Le président (PLR) évoque un projet de l'Etat de Genève qui vise à financer, pour un montant de plus de 10 millions de francs, un système interne de haute sécurité permettant le stockage de données. Il note en outre que la Confédération a émis des doutes sur les garanties de sécurité du système d'e-voting genevois. Il se demande si une solution locale, avec le

développement d'un espace de stockage genevois, permettrait véritablement une meilleure sécurité.

M. Koch ne nie pas que l'Etat est capable d'offrir un système local et sécurisé. Il explique toutefois que le système actuel d'e-voting, censé être très sécurisé, possède des failles. Ce système a été repris en main dans une volonté de travailler sur ces failles, ce qui est positif. L'argument de la protection des données doit être considéré à la lumière des menaces qui pèsent sur ces données : l'utilisateur doit savoir contre qui il doit se protéger. D'une manière réaliste, le risque zéro n'existe pas, toutefois, il est nécessaire de faire le tri entre les informations qui nécessitent une protection vis-à-vis de la NSA, ou celles qui nécessitent un niveau de protection moindre. Dans le contexte technologique actuel, le fait de vouloir créer une infrastructure propre à l'Etat de Genève semble difficile à réaliser, au vu de l'évolution constante dans le domaine. Il souligne qu'un tel projet nécessite un temps de réflexion approfondi notamment en mettant en perspective les besoins de l'institution, le coût, la durée, la maintenance et le personnel nécessaire. Google offre pour le moment, sans pour autant être infaillible, un système de haute sécurité. Les enjeux pour l'Etat sont actuellement d'encadrer l'arrivée de nouvelles technologies, comme la signature électronique.

Suite à l'intervention d'une commissaire PLR, M. Koch explique que les questions de technologies doivent être abordées en fonction de deux facteurs : la technique et l'humain. L'utilisation de la technologie est intimement liée à l'éducation. En effet, il est important que les élèves connaissent les enjeux de sécurité liés à l'utilisation des plateformes internet. Il note que le fait que les données demeurent en Irlande, pays soumis au RGPD, est une bonne garantie. Toutefois, s'il est possible de s'assurer que ces données ne seront jamais transférées ailleurs, cela offrirait une protection supplémentaire. Enfin, il explique que ce cadre est cohérent, s'il est lié à une prévention sur les types de fichiers à stocker, ou non, sur ces plateformes. Il confirme que la création d'une messagerie est un projet différent.

M. Koch indique qu'à l'heure actuelle, chacun se construit une identité numérique. La sécurité de cette identité doit être garantie et maintenue de manière confidentielle. Il cite l'exemple d'un étudiant de l'Université de Lausanne qui avait pu, à l'aide d'un logiciel, aspirer les informations de 2 300 comptes d'étudiants. Les personnes piratées n'étaient pas au courant de l'existence des possibilités supplémentaires de sécuriser l'accès à leur compte. Une meilleure connaissance aurait permis d'éviter un accès si facile à des données personnelles. Il note que dans de nombreux cas, les utilisateurs ne mettent pas à profit toutes les protections offertes par un système. Il rappelle à cet égard l'importance de l'éducation dans ce domaine, notamment

au travers de la « littératie numérique » qui décrit l'ensemble des connaissances qu'un utilisateur devrait posséder dans le domaine du numérique pour en comprendre les enjeux et pouvoir se prémunir contre d'éventuels abus.

La même commissaire PLR rappelle qu'un des projets vise à fournir une messagerie sécurisée pour tous les élèves. Elle demande si cette mesure est véritablement utile ou s'il serait plus pertinent de se concentrer sur la prévention et la sensibilisation dans le domaine des technologies.

M. Koch répond que cette question dépend du contexte. En effet, il est utile de savoir si les utilisateurs sont suffisamment disciplinés pour utiliser l'adresse e-mail de manière à minimiser les risques. Le fait d'avoir une messagerie sécurisée n'empêche pas les élèves d'utiliser une autre messagerie à côté, en négligeant les aspects liés à la sécurité. Il indique qu'il est important de fournir aux élèves une connaissance approfondie du système, pour garantir un maximum de sécurité. Il note à cet égard que certaines professions ont accès à une sécurité plus grande que d'autres. En effet, les données des psychologues sont mieux protégées que les données des enseignants.

Un député vert indique qu'il existe un intérêt pour l'Etat de protéger l'identité numérique de ses citoyens. Il note qu'actuellement les discussions s'articulent autour de micro-espaces d'actions telles que l'éducation, la profession et l'espace familial, sans pour autant encadrer la problématique de manière globale. Il souligne que le projet de loi met en exergue une vaste problématique de la protection des citoyens.

M. Koch confirme que l'identité numérique est fondamentale et qu'elle devrait être gérée par l'Etat, à l'instar de l'identité passeport. Un des objectifs liés à la protection des données vise à proposer une loi qui puisse protéger les utilisateurs tout en leurs garantissant une certaine marge de manœuvre. A cet égard, il est possible de considérer les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), soit comme un ennemi de cette sécurité soit comme un partenaire qui possède des aspects positifs et négatifs. En effet, leur service permet d'offrir à la population certains avantages, notamment dans le domaine de l'éducation. L'enjeu principal pour les citoyens est d'avoir suffisamment de connaissances sur le sujet afin de faire des choix conscients sur les technologies qui les entourent. Il note que ce projet de loi ne vise pas à empêcher Google de fournir une plateforme, mais à s'assurer que l'utilisation de celle-ci permet une bonne protection des données.

Le même député vert indique qu'il est nécessaire de distinguer les données sensibles des données utilisées à des fins commerciales. Il estime

que l'Etat devrait également réglementer l'acquisition d'informations de type commercial de la part de ces entreprises.

M. Koch souligne que l'acquisition de données par les entreprises fait office de paiement de la part des utilisateurs pour un service considéré comme gratuit. Il rappelle que le chiffre d'affaires de Google s'élève à 40 milliards de francs, dont 20 milliards constituent le bénéfice. Cela signifie que les données des utilisateurs valent 20 milliards de francs, ce qui semble abusif. Toutefois, il note que les 20 autres milliards sont investis dans l'économie réelle. Il ne s'agit pas de fustiger l'entreprise, mais de permettre aux utilisateurs de choisir si leurs données peuvent être vendues et par qui elles peuvent l'être. Il note que dans le domaine des technologies, il existe des projets novateurs, et d'autres qui représentent un potentiel danger.

Le même commissaire vert constate qu'une adresse Google est nécessaire pour accéder aux programmes éducatifs. Il demande pourquoi un tel programme n'est pas possible sans l'utilisation d'un service de Google.

M. Koch répond que pour le moment, un tel niveau de service n'existe pas dans des entreprises européennes.

Le même commissaire vert demande s'il est possible de masquer l'identité des utilisateurs par un pseudonyme.

M. Koch indique qu'une telle possibilité est envisageable. Toutefois, certaines données peuvent être recoupées et reliées aux profils des personnes. Un système informatique éducatif permet dans certains cas d'offrir une valeur ajoutée à l'enseignement. Il permet également de sensibiliser aux plateformes auxquelles les élèves seront confrontés dans le marché de l'emploi.

Le même député vert note qu'un recoupement d'informations est possible dès lors qu'il existe une base de données qui permet de faire le rapprochement entre les pseudonymes et les profils réels. Il demande s'il est possible de séparer ses données afin qu'elles ne soient pas recoupées.

M. Koch note qu'il s'agit d'une pseudo-anonymisation ou d'une carte d'identité virtuelle. Il s'agit de trouver un équilibre entre l'anonymat et la divulgation de l'identité. En effet, il est possible de mettre en place un système qui permet d'identifier le compte d'une personne au sein de l'établissement, mais pas par Google. Il rappelle que l'anonymat peut également donner lieu à des abus. Il souligne que la question de l'e-voting a donné lieu à un débat sur la gestion des risques, car le risque zéro n'existe pas. Il rappelle que la législation européenne dans le domaine est plus complète que la législation suisse.

Le président précise que l'accès à la plateforme en ligne qui est mentionnée dans le projet de loi a pour but de perfectionner l'apprentissage des langues. Il s'agit de produits étrangers qui ne seraient plus compatibles en cas d'existence d'un système sécurisé fermé. Il note que cette précision ne concerne pas la question des e-mails.

M. Koch ajoute que lors de l'utilisation d'un traducteur en ligne, l'aspect éducatif concerne à la fois le logiciel en lui-même qui permet un apprentissage de la langue et à la fois une sensibilisation sur les mécanismes qui sous-tendent l'application. En effet, il est important d'expliquer que lors d'une traduction, le texte est traduit par des serveurs qui se trouvent probablement à l'étranger et que lors de ce transfert de données, un certain nombre d'informations peut être prélevé.

Un commissaire socialiste comprend la dimension éducative que peut offrir un accès aux technologies. Il note toutefois la nécessité d'informer les élèves sur les éventuelles alternatives qui existent. En effet, une fois que les problématiques de sécurité ont été soulevées, il est important que les élèves puissent se tourner vers des plateformes plus adaptées ou plus respectueuses de leurs droits. Cela permettrait qu'ils ne demeurent pas prisonniers des outils qui leur sont présentés, sans pouvoir se tourner vers d'autres outils.

M. Koch souligne que des systèmes alternatifs plus respectueux des données existent. Il rappelle que le logiciel *Siri* enregistre l'empreinte vocale ainsi que la géolocalisation de l'utilisateur. Une connaissance approfondie des outils permet de comprendre l'engagement de l'utilisateur en termes de données, de responsabilité et de cadre légal. Il s'accorde avec l'idée que ce travail d'éducation doit être effectué en parallèle avec la présentation d'alternatives possibles. Il rappelle que des alternatives existent.

Le même commissaire socialiste demande pourquoi l'Etat, et particulièrement le DIP, n'utilise pas ces alternatives.

M. Koch indique que le rôle de l'Etat est d'offrir une connaissance approfondie qui permet de garantir la capacité d'un choix éclairé. Il s'agit d'une utilisation responsable des technologies. Il s'accorde avec l'idée qu'une des missions de l'école est de présenter les alternatives possibles. Il rappelle à cet égard qu'avant que l'application *WhatsApp* soit interdite dans les écoles, il avait proposé aux enseignants de faire signer aux élèves une charte d'utilisation détaillée, comprenant les risques et la sécurité liés aux données.

Le même commissaire socialiste constate que ce projet de loi découle du besoin des écoles d'avoir accès à des outils mutualisés. Il note que le DIP ne propose qu'un seul outil possible. Il estime que le DIP doit, soit proposer

plusieurs outils, soit proposer un outil qui répond à des exigences accrues en termes de protection des données. Il souligne que la question du choix doit être en lien avec l'âge des élèves. De plus, il constate que le RGPD contient des standards plus élevés que la réglementation suisse. Il demande dans quelle mesure il est possible de demander aux entreprises sous-traitantes de respecter le RGPD.

M. Koch indique que les GAFAM appliquent le RGPD en Europe. Il rappelle qu'actuellement il est nécessaire de mettre l'accent sur la littératie numérique et le choix à faire à l'intérieur d'un programme donné, tout en présentant des alternatives possibles. Il note qu'il existe un problème dû au fait que les personnes pensent utiliser un service gratuit alors qu'ils payent avec leurs données. Il note qu'une des missions de l'éducation est de montrer différents modèles d'entreprises qui existent. A cet égard le modèle Wikipédia, également gratuit, ne fonctionne pas sur les données, mais sur une collaboration des utilisateurs et sur des dons. Il s'agit de montrer que des systèmes payants peuvent être plus profitables que des systèmes gratuits en termes de protection des données.

Le même commissaire socialiste souligne que l'e-voting a également été victime de fishing. Il constate que personne n'est à l'abri d'un tel risque.

M. Koch explique que l'éducation dans ce domaine est importante et permet de détecter les indices d'une éventuelle fraude. Il souligne que le domaine des technologies, à l'instar de tous les domaines, n'est pas prémuni à 100% contre le risque. Dans le cas du e-voting, il est nécessaire de réévaluer, lors de chaque vote, la possibilité de fraude. Il s'agit d'une remise en cause perpétuelle du système, qui permet d'offrir des améliorations satisfaisantes. Il note qu'un domaine aussi évolutif que la technologie ne peut pas être géré uniquement par l'Etat. Il rappelle que même les GAFAM demandent à des utilisateurs externes de tester leur sécurité, notamment en faisant appel à des hackers qui ont pour mission de briser leur sécurité pour en détecter les failles. Cette pratique sera appliquée pour l'e-voting.

Un commissaire PDC demande de quelle manière il est possible de hiérarchiser les risques. Il note que les risques existants peuvent être notamment liés au lieu d'hébergement des données, au manque de concurrence entre les grandes entreprises (GAFAM) ou au manque de littératie numérique de la part des utilisateurs.

M. Koch indique qu'il s'agit d'un mélange de tous les domaines évoqués par le commissaire PDC. Il souligne que la littératie numérique est un volet important de la prévention. Le fait d'entreposer des données à l'étranger dépend du lieu. Une donnée présente dans l'Union européenne engage la

responsabilité des hébergeurs de manière plus importante que dans d'autres pays. D'autres risques sont à évaluer comme les coupures de courant, les faillites d'entreprises ou leur rachat éventuel. Il est nécessaire pour un utilisateur de connaître la relation juridique qu'il entretient avec ses données entreposées à l'étranger. De plus, M. Koch note qu'une entreprise de 20 personnes basée en Suisse risque d'offrir une protection plus faible qu'une entreprise de 200 personnes.

Il s'accorde avec le constat du commissaire PDC sur le caractère évolutif des menaces. A cet égard, il indique qu'une personne travaillant dans le domaine de la sécurité informatique devrait consacrer 50% de son temps à se former sur les nouvelles menaces. Toutefois, cette règle est rarement respectée. De plus, il souligne que des menaces peuvent être présentes au sein même des entreprises, dans lesquelles le personnel peut abuser de certaines données. Enfin, les gouvernements peuvent exercer des pressions sur les entreprises de données afin d'obtenir des informations. L'évaluation en besoin de sécurité requiert de définir des priorités. Il estime qu'en l'état actuel des choses, les priorités concernant les données sont respectées. Toutefois, il est possible que le cadre évolue et fasse appel à une modification des priorités.

Le même commissaire PDC demande s'il est possible d'identifier des menaces propres aux écoles.

M. Koch répond que le risque dépend du type d'école. En effet, les risques liés à l'école primaire ne sont pas les mêmes que ceux de l'EPFL. En effet, les écoles actives dans la recherche de pointe risquent davantage d'être sujettes à des vols de données. Il est donc nécessaire de déterminer le risque en fonction du niveau de l'école en question.

Deuxième audition de M. Manuel Grandjean, Directeur du service Ecoles-Média au DIP

M. Grandjean indique que depuis le dépôt du projet de loi, plusieurs éléments nouveaux se sont ajoutés au dossier, notamment le développement d'une nouvelle plateforme d'Educa, service qui fournit des solutions informatiques à la Confédération. Concernant le projet de loi, M. Grandjean précise que lorsque l'on fait mention de *Google*, il ne s'agit pas du moteur de recherche en tant que tel, mais d'un environnement collaboratif. Celui-ci comprend un espace de stockage, des outils de bureautique en ligne ainsi que des outils de suivi et de gestion des groupes et des classes. Il note que les discussions ont mentionné largement la messagerie et l'espace de stockage, mais que la plateforme regroupe l'ensemble de ces fonctionnalités.

M. Grandjean ajoute qu'un engagement contractuel avec Google mentionne que les données ne seront pas utilisées à des fins de profilage ou de publicité. La seule possibilité d'utilisation sera à des fins statistiques. Il s'agit d'une différence notable avec l'utilisation des services Google dans le cadre privé.

Parmi les autres éléments nouveaux survenus depuis le dépôt du PL, M. Grandjean cite l'entrée en vigueur dans l'Union européenne du *Règlement européen sur la protection des données* (RGPD). Ce texte pose un cadre plus contraignant au sein de l'Union européenne que la législation suisse en la matière. La Suisse bénéficie de ces mesures de protection accrue, car les grands acteurs du web se sont mis en conformité avec ces nouvelles normes. Il rappelle que le DIP a mis en place des règles contraignantes sur l'utilisation de la plateforme. En effet, il a été spécifié dès le début, que l'usage de la plateforme n'était pas adéquat à des fins administratives de gestion scolaire, ni pour une utilisation privée ou pour le stockage de données personnelles. Lorsque la plateforme a été utilisée au-delà de ce cadre, des contrôles ont permis de rectifier ces pratiques au travers notamment d'un dialogue avec les enseignants.

M. Grandjean ajoute que la thématique de la protection des données n'a jamais été aussi présente dans le débat au sein du DIP depuis la mise en place de la plateforme. Les discussions qui en ont découlé ont été riches et formatrices pour les enseignants et les élèves. Un des principes suivis est de considérer que ces outils informatiques seront immanquablement utilisés par les élèves dans le cadre privé et qu'il est nécessaire de ne pas les extraire du cadre scolaire. Cela permet d'utiliser ces outils dans un encadrement précis, tout en sensibilisant les élèves à une utilisation responsable dans le cadre privé ou dans la vie active.

M. Grandjean explique que le 13 novembre 2018 la Conseillère d'Etat en charge du DIP a présenté sa vision du numérique en introduisant l'importance de la notion de responsabilité et de citoyenneté numérique. A cet égard, il est nécessaire de former les jeunes à une utilisation responsable des outils en ligne. En effet, une utilisation encadrée au sein des écoles est une mesure positive.

M. Grandjean indique que l'entreprise Educa a annoncé qu'elle renoncera à sa plateforme *educanet,* fournie aux élèves depuis une dizaine d'années, au 31 décembre 2020. Parallèlement, l'entreprise poursuit l'établissement de contrats-cadres avec des grands acteurs du marché informatique comme l'entreprise *Microsoft.* Elle a annoncé le 29 novembre 2018 des négociations avec *Google* pour l'établissement d'un nouveau contrat-cadre.

M. Grandjean ajoute que Genève a été pilote dans l'utilisation de la plateforme *educanet*. Au niveau suisse, il existe une volonté d'intégration de ces outils informatiques. Cette intégration doit se faire avec des mesures contractuelles d'accompagnement, qui permettent une utilisation responsable de ces outils.

Un commissaire vert demande dans quelle mesure il est possible de vérifier que *Google* répond aux normes contenues dans les contrats-cadres.

M. Grandjean comprend la préoccupation de ne pas se fier aux simples promesses de l'entreprise. Il rappelle toutefois que ces mesures sont contenues dans des contrats. De plus, il sera possible d'auditer l'institution en charge du respect de ces normes. Il note que les logiciels *Microsoft* sont largement utilisés au sein des entités publiques. Cette utilisation entre dans le cadre d'engagements contractuels. La meilleure méthode pour s'assurer que les engagements sont respectés est d'auditer les fournisseurs de prestations. Dans le cas où l'entreprise *Educa* négocie les contrats-cadres, la responsabilité de la bonne application des engagements leur revient. Il ajoute que le risque d'image pour *Google* dans un cas de non-respect des engagements contractuels est très élevé. Il rappelle que les données stockées seront pour une grande part des travaux d'élèves qui n'auraient qu'une faible valeur pour *Google*, par rapport au risque d'image qu'elle encourt.

Pour répondre au même commissaire vert au sujet de la contrepartie obtenue par Google, M. Grandjean indique tout d'abord que *Google* fournit le service gratuitement. Par ailleurs, *Google* n'applique pas le même modèle économique que pour des utilisateurs privés. En effet, l'entreprise mise davantage sur le fait que l'éducation est une porte d'entrée pour fidéliser les utilisateurs à leurs produits. Il souligne que le DIP tient à offrir une diversité de solutions, le but n'étant pas d'avoir un environnement unique. Toutefois, il n'est pas non plus possible de se baser uniquement sur des logiciels libres. Il ajoute qu'à l'heure actuelle, une partie des ordinateurs fonctionnent avec *Linux* et des logiciels libres, d'autres systèmes d'exploitation sont utilisés comme *Mac, Windows ou Androïd,* pour éviter un attachement spécifique à l'un de ces produits.

Suite à une question complémentaire du même commissaire vert, M. Grandjean répond que la moitié des postes de l'enseignement secondaire est équipée de systèmes d'exploitation *Linux*. Les salles d'informatique sont équipées de postes *Mac* et *Windows*. Il rappelle que le DIP est soucieux d'offrir une diversité, toutefois, pour les travaux en ligne, il est difficile de trouver un service équivalent à celui de *Google*. Un tel service réalisé en interne engendrerait des coûts supplémentaires. Il ajoute qu'une mixité de solutions existe, car tous les sites internet pédagogiques sont déployés sur des

solutions libres comme *Wordpress* ou *Drupal*. La plateforme d'e-learning *Moodle* est également libre. Il rappelle que *Google* n'est qu'un élément de l'ensemble informatique et que, concernant le service fourni par cette entreprise, les coûts de développement interne d'un tel service seraient très élevés.

Suite à une autre interrogation du même député vert, M. Grandjean précise qu'aucune publicité de la société Google ne sera affichée et que les données privées ne seront pas utilisées à des fins publicitaires.

Le même député vert note que le fait d'accoutumer les élèves leur permettra de capter leurs données à des fins publicitaires dans le futur, lorsqu'ils utiliseront ces services de manière privée.

M. Grandjean confirme ce point. Il note que la même problématique se pose pour *Apple* et *Microsoft*. Il ajoute toutefois que les efforts de sensibilisation sont importants. Au cours de l'année dernière, une formation a été donnée à 140 personnes du DIP afin de les sensibiliser à ces questions et pour qu'ils deviennent des relais de ces préoccupations au sein des établissements scolaires. De plus, le DIP organisera une exposition nommée *Data Detox* reprise de l'EPFL. Il ajoute qu'il est difficile de s'affranchir des outils en ligne, dans le cadre privé comme dans le cadre public. Il est donc important de poser un cadre précis.

Pour répondre à l'intervention d'un commissaire socialiste, M. Grandjean expose que la solution proposée respecte le RGPD, car tous les services ont été mis en conformité pour l'ensemble de l'Union européenne. La Suisse fait partie de cette mise en conformité. M. Grandjean indique que le contrat avec Google a été adapté en conséquence. Le contrat en vigueur est un contrat révisé en fonction du RGPD. Il est à noter que si l'entreprise *Educa* négocie un contrat-cadre avec *Google* au niveau fédéral, il n'est plus nécessaire d'entrer en négociation au niveau cantonal. Concernant la manière d'auditer les prestataires de services, il indique que cette question doit être posée à la DGSI. Concernant l'utilisation de solutions libres, M. Grandjean souligne que, bien que de telles solutions existent, il est difficile de trouver l'ensemble des éléments sous une seule plateforme intégrée. Une intégration des services de stockage de données, de messagerie, de bureautique en ligne est possible, mais coûteuse. L'entreprise *Educa* a fait le choix d'investir dans des licences plutôt que dans le développement de proximité. La démarche inverse impliquerait de créer des postes à ces fins au sein du DIP plutôt que de financer des licences.

La discussion porte ensuite sur le droit applicable au contrat.

Un commissaire socialiste note que la première version du contrat mentionne que le droit applicable est celui de l'Etat de Californie. De plus, des échanges de courriels ont mis en exergue le fait que le nouveau contrat est soumis au droit anglais. Il estime que si l'application du RGPD passe par une application du droit anglais, cela risque de poser des problèmes dans le cadre actuel des négociations sur le *Brexit.*

Suite à diverses interventions au sujet du droit applicable, M. Grandjean indique que cette question sera soulevée lors des négociations du contrat-cadre avec *Google* au niveau suisse. En effet, *Educa* négocie des contrats-cadres qui visent à rendre compatible l'utilisation d'outils informatiques avec le droit suisse. C'est le cas pour le contrat avec *Microsoft,* qui est disponible sur le site internet d'*Educa*.

M. Grandjean précise qu'Educa est un organisme soutenu par la Confédération et les cantons. Il est chargé de fournir des solutions informatiques pour les établissements pédagogiques.

Un commissaire socialiste indique que le site *d'Educa* mentionne, par rapport aux contrats-cadre, que *« le droit suisse et la juridiction de la ville de Berne sont applicables aux contrats individuels, qui sont conclus par les écoles lors de leur adhésion au contrat-cadre. Une des exigences juridiques centrales au niveau des contrats-cadres est ainsi remplie ».*

Troisième discussion en commission

Le président (PLR) remarque, au vu des questions qui découlent de l'audition, la peur qui ressort vis-à-vis des GAFA (*Google, Apple, Facebook, Amazon)*. Il rappelle que lors de son audition de la séance du 16 novembre 2018, M. Koch avait invité la commission à s'éloigner de cette inquiétude en démontrant qu'une solution libre et locale n'offrait pas forcément plus de sécurité qu'une solution privée. M. Koch avait insisté sur l'importance de la formation et de la sensibilisation des utilisateurs par rapport aux risques. Il rappelle qu'une solution *home-made* n'est pas plus sûre qu'une solution offerte par *Google*. Il ajoute que l'histoire récente du vote électronique à Genève est une illustration qu'un système « *maison »* peut être défaillant, notamment du fait que, dans le cas d'espèce, l'Etat a refusé le contrôle par « *hacking* » du système. Il rappelle que la DGSI avait annoncé que le devis pour les coûts de mise en place de la messagerie étaient de 7 millions de francs, avec un coût annuel de fonctionnement de 1 million de francs. Ces coûts participent au fonctionnement d'un système qui n'est pas plus sûr qu'un autre. Il partage toutefois la préoccupation sur le lieu d'hébergement des données. A cet égard, si le contrat affiche clairement que les données

seront stockées en Irlande, la solution est satisfaisante. Enfin, il note son intérêt pour le nouveau projet *Educa* qui sera financé par la Confédération et les cantons, qui mérite plus d'approfondissement.

Un commissaire vert indique ne pas partager l'optimisme du président sur les GAFA. Bien qu'il puisse concevoir qu'aucun système n'est sûr à 100%, il rappelle que la capitalisation des données est le premier revenu des géants de l'informatique. Il indique préférer un système qui préserve les données des utilisateurs plutôt qu'un système qui les vend. Il rappelle que la sécurité à proprement dit n'est qu'un volet des questions de protection des données et que la préservation de la sphère privée entre également dans ce cadre.

Un commissaire socialiste indique qu'il ne partage pas la comparaison faite par le président avec la plateforme de vote électronique. Il explique qu'un tel système revêt une sensibilité particulière du fait des processus complexes notamment en terme de vérifiabilité. Le fait de penser que le système genevois est défaillant car un test d'intrusion a révélé des failles est une analyse trop simpliste. Il n'est par ailleurs pas possible de déterminer ce qu'il se serait passé, si le système avait été développé par l'entreprise concurrente qui est une entreprise étrangère et pour laquelle il n'existe pas de vérifiabilité. Cette vision vise à renforcer les acteurs qui disent que le système d'e-voting doit être annulé. Le commissaire socialiste indique qu'à ce stade, il est important de connaître précisément le lieu de stockage des données ainsi que l'application du RGPD. Il ajoute que les questions sur l'audit des sous-traitants sont importantes.

Le président résume les demandes de la commission en trois points :

1. Prendre connaissance du nouveau contrat, du droit applicable, du for et de la localisation des données.
2. Obtenir une prise de position de la DGSI (OCSIN) sur les audits des sous-traitants.
3. Obtenir davantage d'informations sur le projet *Educa.*

Dans la suite des débats, M^{me} Rodriguez indique avoir transmis à la commission un e-mail récapitulant les derniers éléments demandés au DIP et à l'OCSIN (voir annexe). Elle rappelle par ailleurs que le Conseil d'Etat a transmis une lettre qui propose un amendement afin de prévoir uniquement une messagerie pour les élèves.

Une commissaire PLR estime que le texte nécessite un amendement général. Elle propose de laisser le temps aux verts de le formuler.

Quatrième discussion en commission et votes en 2e et 3e débats

Un commissaire vert déclare que ce PL a été déposé par son groupe. Ce dernier pense que l'Etat démocratique doit être vigilant sur les données des jeunes concitoyens que sont les élèves. L'information est la richesse et l'or de l'économie de demain. Il juge irresponsable de la part de l'Etat de laisser des entreprises privées et étrangères capter les données des étudiants. D'une part, cela peut nuire à la protection des données, et d'autre part, le « *big data* » influence sur les perceptions, les mentalités et les portefeuilles des étudiants. Les verts s'opposeront à ce que Google s'introduise dans le DIP.

Un député PLR revient à la genèse de ce projet. Bien que le Pl 12103 soit important, il est rapidement apparu qu'il était irréaliste. Son auteur avait annoncé que son projet de loi coûterait 126 000 francs. Or, toutes les auditions ont démontré le manque de sérieux avec lequel ce PL avait été élaboré. M. Favre de la DGSI a annoncé que la réalisation du projet en interne s'élèverait à 7 millions de francs. Il soulève aussi que le projet de vote électronique a mis au jour le manque de compétence informatique de l'Etat et son incapacité à achever et à mettre en vigueur ses projets d'envergure. Il s'agit du premier motif qui doit conduire au refus de ce PL.

Le second motif de refus réside dans les problèmes que ce PL engendrerait en pratique. Tout d'abord, il rappelle que le DIP a expliqué l'attention qu'il porte à la protection des données et le respect des lieux de stockage des données. De plus, il a fait référence au règlement européen qui fixe des critères très strictes pour la protection des données (le RGPD). A cela s'ajoute que le Préposé fédéral à la protection des données a établi une liste des Etats offrant une garantie similaire à la Suisse, dont font partie tous les pays membres de l'UE. Le DIP a également mis en avant les exigences en matière d'apprentissage. En effet, l'apprentissage des langues se base notamment sur des modules développés en France, en Allemagne ou dans des pays anglo-saxons. L'adoption du PL 12103 empêcherait le recours à de tels outils, pourtant indispensables. Compte tenu de l'application extrêmement large du PL, cela va également poser des problèmes dans les secteurs de recherches des universités et les HES, qui ont un besoin d'échanger les données au niveau mondial. Il insiste sur le fait que la coopération avec d'autres universités est dans l'ADN des universités suisses.

Il pense que les auteurs du projet auraient dû se renseigner sur la réalité du terrain et sur les mesures concrètes du DIP avant de déposer ce PL.

Pour toutes ces raisons, le PLR refusera ce PL. Concernant les amendements, il indique qu'un PL mauvais à l'origine ne peut pas être sauvé par des amendements.

Le député vert indique que les budgets approximatifs donnés par l'OCSIN ne sont pas satisfaisants. Personnellement, il pense que le coût est moins cher que ce que l'OCSIN prétend. Pour un sujet qui touche à la sécurité personnelle et collective, la question du coût est secondaire car on se situe dans le domaine régalien de l'Etat. Concernant les universités, le problème qui se pose est le partage des données par une entreprise privée. Il pense que si ce PL est insuffisant, la commission devrait alors en repenser un autre ou bien déposer une motion. Le sujet n'en demeure pas moins sensible. Il estime que les services offerts par Google ne vont pas dans le sens de l'intérêt collectif des citoyens genevois. Pour ces raisons, les verts s'opposent au DIP et estiment que ce Département doit perdre ses mauvaises habitudes de tout donner au privé.

Un député UDC déclare qu'il souscrit aux propos du groupe PLR et que l'UDC refusera ce PL 12103, malgré le fait qu'un de leur collègue en soit signataire.

Le président (S) revient sur l'intervention du député PLR en lien avec la comparaison du PL 12103 avec le vote électronique. Il ne partage pas l'analyse de son collègue et pense que c'est une question relativement différente, même s'il partage les inquiétudes à l'origine de ce PL sur la protection des données. Il rappelle que bien que le parlement ait donné des signaux clairs sur le vote électronique, le gouvernement peine à l'entendre, ce qui est le réel problème. Enfin, il trouve dommage que les différentes auditions n'aient pas suscité le travail de détail qui aurait dû être fait. Ce PL a peu de chance d'aboutir, ce qui est dommage.

Une commissaire MCG indique que son groupe n'entend pas soutenir ce PL.

Un commissaire socialiste annonce qu'il renonce à participer au vote sur chaque article tant qu'il n'y a pas d'amendements proposés.

Le président propose de passer au **vote article par article en 2e débat**.

Le président procède au vote du titre et du préambule :

Oui :	2 (1 EAG, 1 Ve)
Non :	**3 (2 PLR, 1 MCG)**
Abstentions :	1 (1 UDC)

Le titre et le préambule sont refusés.

Le président procède au vote de l'art. 1 :
Oui : 2 (1 EAG, 1 Ve)
Non : 3 (2 PLR, 1 MCG)
Abstentions : 1 (1 UDC)

L'art. 1 est refusé.

Le président procède au vote de l'art. 37A :
Oui : 2 (1 EAG, 1 Ve)
Non : 3 (2 PLR, 1 MCG)
Abstentions : 1 (1 UDC)

L'art. 37A est refusé.

Le président procède au vote de l'art. 2 :
Oui : 2 (1 EAG, 1 Ve)
Non : 3 (2 PLR, 1 MCG)
Abstentions : 1 (1 UDC)

L'art. 2 est refusé.

Le président clôt le 2e débat et demande s'il y a des remarques pour le **3e débat.**

Mme Toledo Vera, juriste au DIP, rappelle que le Conseil d'Etat a déposé une proposition d'amendement de l'art. 37A :

Art. 37A Sécurité des données personnelles des mineurs et des personnes majeures en formation (nouveau)

Les services de messagerie et d'annuaire des élèves et des autres personnes en formation dans l'enseignement public du canton de Genève, excepté au sein des Hautes écoles genevoises, sont fournis et hébergés par l'Etat.

Une commissaire PLR indique qu'elle ne pense pas que la protection des jeunes se fasse par l'isolation dans une « *bulle* » qui ne correspond pas à la réalité. Au contraire, ces jeunes utilisent les services tels que Google. *De facto*, elle pense que la sensibilisation des jeunes dans le cadre de l'information aux problèmes de protection des données faite par le DIP est plus cohérente que la privation d'un outil efficace. Elle estime que la ligne suivie du DIP est bonne et c'est pour ces raisons que le PLR n'a pas fait d'amendement. Ce n'est en aucune façon de la naïveté. Enfin, pour

l'amendement du DIP, le PLR pense que c'est un autre sujet qui aurait pu faire l'objet d'un PL du Conseil d'Etat destiné à la gestion de ces messageries. Le projet implique également un coût très élevé. Le PLR refusera également cet amendement.

Un commissaire vert estime que cet amendement est un moyen de sortir par le haut pour la commission.

Le président annonce que le groupe socialiste va soutenir cet amendement. Il part du principe que si le Conseil d'Etat le propose et que ça va dans la direction souhaitée, ils vont le soutenir car ils sont là pour faire de la politique.

Un commissaire PLR relève que la commission avait dès le début des travaux considéré que le projet était mal rédigé et les verts avaient indiqué qu'ils allaient faire des propositions, qui ne sont jamais arrivées. Par ailleurs, comme l'a précisé une députée PLR, l'amendement du Conseil d'Etat porte sur un nouveau PL, il est surpris que ce dernier maintienne cet amendement alors que la tendance de la commission se dégage contre ce PL.

Un commissaire vert insiste pour dire que ce projet de loi est bien d'après lui. Il estime que c'est à ceux qui y sont opposés de proposer des amendements. A titre d'exemple, l'alinéa 2 de l'article 37A est inutile et cela surtout sur la mention de « domiciliées en Suisse » qui n'est pas importante. Il insiste sur le fait qu'il faudrait soit un système étatique, soit un système non-privé qui permettent d'avoir des données sécurisées dans lesquelles les élèves ne sont pas « fliqués ». Dans la logique des développements de Google, il n'y aurait plus le besoin de chercher un emploi car Google aura accès aux compétences des étudiants (aux notes par exemple). Il s'inquiète de voir que l'on va vers une société totalitaire qui est menée par les entreprises privées et non pas vers un totalitarisme d'Etat.

Un député PLR souligne que ce projet est vicié à l'origine par nature et qu'il ne voit donc pas d'intérêt à faire des amendements.

Une commissaire MCG trouve étonnante cette proposition d'amendement transformé. Elle affirme qu'elle n'a jamais dit qu'il ne fallait pas se protéger. Elle insiste sur le fait que de dépenser X millions pour la création d'un système protégé à la durée limitée (à partir du moment où les élèves quittent le cycle, ils ne peuvent plus jouir de ces messageries), est incohérent. Au contraire, elle promeut les cours d'information et de sensibilisation plutôt qu'une protection illusoire. Il vaut mieux leur apprendre à être responsable et à ne pas se mettre en danger. Elle n'est pas naïve quant à savoir ce qui est fait avec les données. Elle sait qu'ils sont lus, écoutés, surveillés. Ces entreprises

sont des dangers considérables et ce n'est pas en mettant en place ce PL qu'ils feront mieux. Ce PL ne lui paraît pas utile.

Pour le commissaire vert, il faut penser au monde de demain, ce PL est peut-être « mal fichu » mais il a un caractère visionnaire. Se réfugier derrière l'idée que le monde est tel qu'il est n'est pas une politique. Il insiste sur le fait que la politique est au contraire un moyen pour aller de l'avant et inventer un outil qui protège les données individuelles. Les verts vont continuer à avancer dans un monde vers l'usage collectif et une gouvernance des communs, et non pas un totalitarisme privé ou étatique. Il affirme que la plus grande richesse collective est l'information. Enfin, il conclut que la redistribution des bénéfices de ces « *big data* » aux individus et non pas aux entreprises est un enjeu économique essentiel du siècle prochain. L'ignorer est faire preuve de naïveté.

Le président indique qu'il s'est plongé dans le procès-verbal du 21 juin 2019. Il cite : « *Le président demande si le Conseil d'Etat accepterait un amendement visant à s'assurer que les données demeurent dans une juridiction soumise au RGPD. M. Grandjean répond qu'à l'heure actuelle Google est sur le point d'offrir cette possibilité. Il ignore toutefois si elle est déjà disponible. Le président demande si le Conseil d'Etat peut s'engager à aller dans ce sens, lorsque cette possibilité verra le jour. M. Grandjean confirme* ». Il souhaite aller en ce sens et compléter la proposition du gouvernement en amendant l'alinéa 1 de l'article 37 A. Il pense que l'alinéa 2 peut être laissé de côté, mais que l'alinéa 3 peut être amendé (et deviendrait un alinéa 2).

Une commissaire PLR attire l'attention du président sur le fait qu'à l'issue du 2e débat, le PL 12103 a été vidé de sa substance.

Le président prend note de cet élément. La commission aurait dû voter l'amendement du Conseil d'Etat au 2e débat mais cet amendement sera pour le 3e débat. Il considère qu'il y a un amendement général qui vise à réintroduire les éléments de ce PL avec son article 37A alinéa 1 ainsi qu'un article 37A alinéa 2 libellé en ces termes : « *Les données échangées ou déposées dans les espaces numériques de dépôt et de partage des données, mis à disposition des personnes mentionnées à l'alinéa 1, sont stockées dans un data center, situé dans un territoire dans lequel le règlement général sur la protection des données s'applique* ».

Le but est d'assurer que ces espaces de partage soient soumis à la juridiction du RGPD. Il propose de voter le sous-amendement qu'il a déposé et puis l'amendement amendé ou non d'une manière globale. Il précise que cela réintroduira la loi dans la mesure où il s'agit d'un amendement général.

Une commissaire PLR exprime sa perplexité face à cette méthode qui consiste, pour le président, à déposer en troisième débat un amendement général qui n'a pas été discuté. Elle demande si la commission souhaite vraiment faire un renvoi, dans une loi genevoise, à un règlement européen qui ne s'applique pas sur notre territoire et qui peut être modifié sans l'avis de la Suisse. Cela pose un problème de territorialité.

Le président pense que la loi peut faire un renvoi statique et non pas dynamique.

M. Mangilli, directeur des affaires juridiques, comprend que l'amendement renvoie à la notion de « *data center* ». Sur ce point, il préfère la langue officielle de la République, soit le français. Les « *data center* » seraient situés dans des pays dans lesquels s'applique le RGPD. D'un point de vue juridique, la loi ne fait pas un renvoi au RGPD mais un renvoi qui situe les pays dans lequel ce RGPD s'applique. Il s'opposerait à un renvoi qui dirait que les « *data center* » doivent correspondre aux normes applicables fixées par le RGPD. Il comprend que dans ce cas, la référence est faite au pays d'hébergement.

Le président revient sur son amendement. D'un côté il garderait la base du Conseil d'Etat sur les services de messageries et d'annuaires, d'un autre côté, il adopterait un régime plus large s'agissant des zones sur le stockage des données. Il relit le sous-amendement rédigé comme suit : « *Les données échangées ou déposées dans les espaces numériques de dépôt et de partage de données mis à disposition des personnes mentionnées à l'alinéa 1, sont stockées dans un centre de données, situé en Suisse ou dans un territoire dans lequel le Règlement général sur la protection des données s'applique* ».

Une commissaire PLR comprend que ceux qui sont contre l'alinéa 1 du Conseil d'Etat, ont intérêt à voter contre l'alinéa 2.

Le président revient au dialogue avec la commissaire PLR. Si elle est d'avis de proposer un alinéa 2 sans l'élément de l'alinéa 1, il est ouvert à cette solution. Certes, il pense que cela irait moins loin pour les services de messageries et annuaires, mais cela permettrait de faire un pas dans l'application du RGPD. Il résume en relevant qu'il y a deux niveaux de discussion avec ces amendements. Le premier concerne la proposition voulant que le canton gère un certain nombre de choses. Le second touche le régime de protection des données relatives à ces éléments.

Au sujet du renvoi au RGPD, la commissaire PLR aimerait entendre la position du Département. Elle souhaite savoir s'il y a un risque de bloquer le système actuel et si cela paraît utile.

M. Jean-Luc Corsini (service écoles-médias – DIP) explique que la solution évoquée à l'alinéa 2 poserait problème en lien avec les échanges, notamment dans le domaine de l'apprentissage des langues, qui sont réalisés avec l'Angleterre. En effet, le Royaume-Uni va très prochainement sortir de l'Union européenne, ce qui aura des impacts sur l'application du RGPD.

Un député vert comprend que la commission est en train de bloquer une loi pour la simple raison qu'un logiciel du DIP se situe en Angleterre et ne pourrait donc pas partager les données générées par ce logiciel.

Le président demande s'il est possible de prévoir un stockage de données soumis au RGPD dans le cadre de ces collaborations.

Mme Toledo Vera du DIP estime que pour la langue anglaise, il n'y a pas d'autres choix car les USA et l'Australie ne sont pas inclus dans le champ d'application du RGPD.

Une commissaire PLR déclare que son groupe s'opposera à toutes les propositions d'amendement et refusera ce PL.

Le président invite la commission à voter le sous-amendement, puis l'amendement principal qui constitue à réintroduire ce PL avec uniquement la disposition sur les services de messageries et d'annuaires. Dans le cas d'un refus, il soumettra au 3e débat ce PL vidé de sa substance.

Un commissaire vert exprime sa préoccupation face à l'obstination de la commission à ne pas prendre au sérieux le sujet de la captation des données et à ne pas proposer d'amendements. Pour ces raisons, il va rester sur son vote.

Le sous-amendement à l'al. 2 de l'art. 37A proposé par le président est le suivant : « *Les données échangées ou déposées dans les espaces numériques de dépôt et de partage de données mis à disposition des personnes mentionnées à l'alinéa 1, sont stockées dans un centre de données, situé en Suisse ou dans un territoire dans lequel le Règlement général sur la protection des données s'applique* ».

Vote en 3e débat

Le président procède au vote du sous-amendement de l'al. 2 de l'art. 37A :

Oui :	3 (1 EAG, 1 S, 1 Ve)
Non :	**4 (2 PLR, 1 UDC, 1 MCG)**
Abstentions :	1 (1 S)

Le sous-amendement de l'al. 2 de l'art. 37A est refusé.

L'amendement du Conseil d'Etat à l'art. 37A est le suivant :

Art. 37A Sécurité des données personnelles des mineurs et des personnes majeures en formation (nouveau)

Les services de messagerie et d'annuaire des élèves et des autres personnes en formation dans l'enseignement public du canton de Genève, excepté au sein des Hautes écoles genevoises, sont fournis et hébergés par l'Etat.

Le président procède au vote de l'amendement du Conseil d'Etat :
Oui : 3 (1 EAG, 1 S, 1 Ve)
Non : 4 (2 PLR, 1 UDC, 1 MCG)
Abstentions : 1 (1 S)

L'amendement du Conseil d'Etat est refusé.

Le président met aux voix l'ensemble du PL 12103 ainsi amendé :
Oui : 1 (1 Ve)
Non : **2 (1 PLR, 1 MCG)**
Abstentions : 5 (1 EAG, 2 S, 1 PLR, 1 UDC)

Le PL 12103 ainsi amendé est refusé.

Au vu de ce qui précède, la majorité de la commission vous invite à rejeter le PL 12103, vidé de toute substance au terme du 3e débat.

Projet de loi
(12103-A)

modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)

Le GRAND CONSEIL de la République et canton de Genève
décrète ce qui suit :

Art. 1 Modification

La loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001, est modifiée comme suit :

Art. 37A Sécurité des données personnelles des mineurs et des personnes majeures en formation (nouveau)

[1] Les systèmes de messagerie, ainsi que les espaces numériques de dépôt et de partage de données mis à disposition des élèves, des étudiants et autres personnes en formation, ainsi que des collaborateurs du DIP du canton de Genève doivent être fournis par les services informatiques de l'Etat.

[2] En cas de nécessité, ils peuvent être fournis par des entreprises suisses et domiciliées en Suisse.

[3] L'Etat garantit que les données échangées ou déposées dans l'espace numérique mis à disposition par les personnes mentionnées à l'alinéa 1 sont stockées dans un data center en Suisse et sont uniquement soumises à la loi suisse en matière de protection des données.

Art. 2 Entrée en vigueur

La présente loi entre en vigueur le lendemain de sa promulgation dans la Feuille d'avis officielle.

ANNEXE 1

Projet de loi modifiant la LIPAD

(PL 12103)

Faisabilité technique et coûts

REPUBLIQUE ET CANTON DE GENEVE

Département de la sécurité et de l'économie
Direction générale des systèmes d'information

01/09/2017 - Page 1

Contexte

Périmètre de la DGSI

Le périmètre de la DGSI est défini dans le Règlement du 26 juin 2013 sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC, B 4 23.03).

ROGSIC — Art. 2 Champ d'application

[1] Le présent règlement s'applique à tous les offices, directions et services des départements et de la chancellerie d'Etat, tels que définis par le règlement sur l'organisation de l'administration cantonale, du 11 décembre 2013, à l'exception des organismes placés sous la surveillance des départements.

[2] Le cas échéant, sont réglées par des conventions spéciales les relations entre la direction générale des systèmes d'information (ci-après : la direction générale) et :

a) le pouvoir judiciaire;

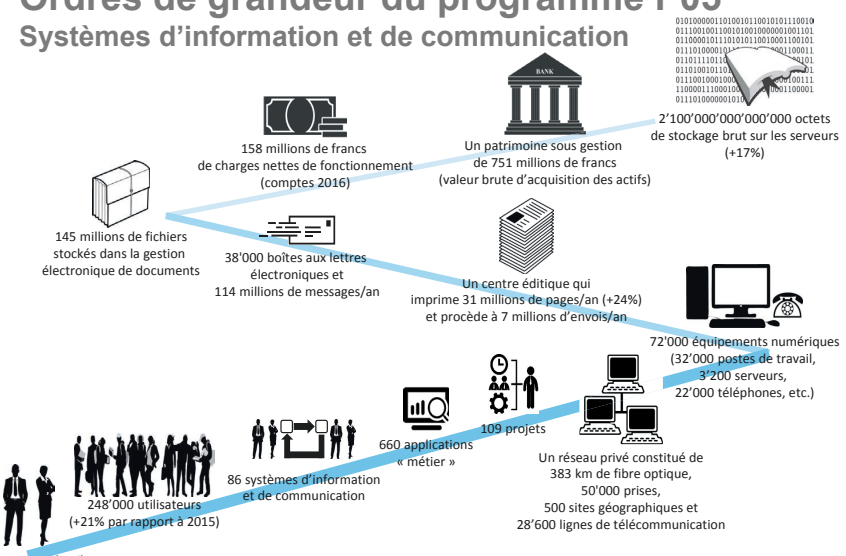
b) le Grand Conseil.

[3] La relation entre la direction générale et le département de l'instruction publique, de la culture et du sport, pour **la part consacrée aux systèmes d'information et de communication pédagogiques, est également réglée par une convention spéciale**.

[4] Toute personne s'intégrant dans un rapport de hiérarchie avec l'Etat et accédant aux systèmes d'information et de communication de l'administration cantonale doit se soumettre aux principes et dispositions du présent règlement, en particulier en matière de sécurité de l'information.

Ordres de grandeur du programme P05

Systèmes d'information et de communication



Données personnelles et sous-traitance

Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD, A 2 08.01), modifié en février 2017.

RIPAD — Art. 13A Sous-traitance (art. 37, al. 2, de la loi)

[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, **prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant**.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] **S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat**.

[6] **Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat**.

Eléments de réponse sur **la faisabilité technique et les coûts** qui seraient induits par la loi

Sécurité des données personnelles des mineurs et des personnes majeures en formation (projet)

Projet de loi modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD, A 2 08)

LIPAD — Art. 37A Sécurité des données personnelles des mineurs et des personnes majeures en formation (nouveau)

[1] Les **systèmes de messagerie**, ainsi que les **espaces numériques de dépôt et de partage de données** mis à disposition **des élèves, des étudiants et autres personnes en formation, ainsi que des collaborateurs du DIP du canton de Genève** doivent être fournis par **les services informatiques de l'Etat**. 1 2 3

[2] En cas de nécessité, ils peuvent être fournis par des **entreprises suisses et domiciliées en Suisse**. 4

[3] L'Etat garantit que les données échangées ou déposées dans l'espace numérique mis à disposition par les personnes mentionnées à l'alinéa 1 sont **stockées dans un data center en Suisse** et sont **uniquement soumises à la loi suisse en matière de protection des données**. 5

Faisabilité technique

Pour procéder à l'exercice dans le délai, nous avons dû formuler quelques hypothèses sur le périmètre du service à fournir, en se basant sur l'exposé des motifs du projet de loi et non sur une expression des besoins formulée par le DIP :

- La brique de base : **Un annuaire pour les élèves et les enseignants**
- Une **messagerie pour les élèves** (les enseignants du DIP en disposent déjà)
- Un **espace de dépôt et de partage de données**
- 45'000 élèves (par conséquent, l'Université, la HES, etc. sont hors périmètre de la présente estimation)

Pour procéder à l'estimation, nous sommes partis de l'hypothèse d'une **extension du service de messagerie d'ores et déjà fourni au sein de l'administration cantonale** (y compris aux enseignants) et **d'un renforcement significatif de l'actuel service de dépôt et de partage de données**, pour en simplifier l'accès à distance (hors des locaux de l'Etat). Nous avons également veillé à la **ségrégation des annuaires des élèves et des fonctionnaires (hors enseignants)**. Enfin, nous sommes partis de l'hypothèse d'un **support** téléphonique fourni uniquement aux enseignants, pendant les heures de bureau, complété cas échéant par des formulaires en ligne pour la déclaration des incidents.

Dans ce cadre, la loi est faisable techniquement.

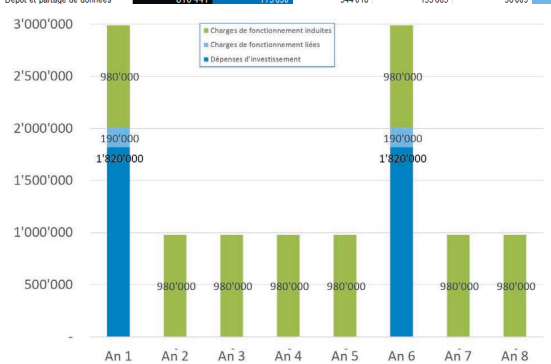
Un mot avant les coûts…

Pour une comparaison entre les services de la DGSI avec ceux fournis par un tiers (Google, Microsoft ou un autre fournisseur de services), il faut également tenir compte des éléments suivants :

- Le service fourni par **Google** est intégré, et **comprend d'autres fonctions que la messagerie et le partage de données** (visés dans le texte du projet de loi)
- La DGSI n'aura pas les moyens de fournir un service avec la même « **expérience utilisateur** » que ce que Google ou Microsoft offrent dans le Cloud
- **Les services fournis par la DGSI s'appuient notamment sur des logiciels achetés chez des éditeurs tels que Microsoft, mais les données sont hébergées sur nos serveurs**, sans connexion avec le Cloud
- **Microsoft** (à l'instar des autres grands éditeurs informatiques) **exerce une forte pression sur l'ensemble de ses clients pour qu'ils utilisent leurs services sur le Cloud**
- Les principaux points forts des services fournis par la DGSI sont :
  - Leur adéquation avec les objectifs de politique publique du Conseil d'Etat et du Grand Conseil
  - La sécurité de l'information et la protection des données
  - Le contrôle opéré par l'autorité politique, et l'obligation pour la DGSI de rendre des comptes à cette même autorité politique

Coûts complets pour la DGSI (estimation)

	Coût du projet à la DGSI					Charges de fonctionnement annuelles induites par le projet		
	Total projet (I+ F)	Investissement (I)			Charges de fonctionnement liées au projet (F)	Total annuel (M + RH)	Maintenance Matériel et Licences (M)	Support et exploitation par la DGSI (RH)
		Total investissement	Matériel et Licences	Prestations sous-traitées	Prestations réalisées par la DGSI			
TOTAL :	**1'998'016**	**1'817'416**	1'146'752	412'106	258'559	**180'600**	**979'938**	384'938	595'000
Gestion de projet et formation	121'726	62'370		62'370		59'356	-		
Centre de services (support)	30'000					30'000	130'000		130'000
Annuaires	283'554	250'844	32'780	87'226	130'838	32'710	162'223	7'223	155'000
Messagerie	752'296	728'512	569'954	126'847	31'712	23'784	280'202	125'202	155'000
Dépôt et partage de données	810'441	775'690	544'018	135'663	96'009	34'751	407'513	252'513	155'000



	Sur 5 ans	
	Total	Coût mensuel moyen par utilisateur
Total	**6'920'000**	**2.60**
Gestion de projet et formation	**130'000**	**-**
Centre de services (support)	**680'000**	**0.30**
Annuaires	**1'100'000**	**0.40**
Messagerie	**2'160'000**	**0.80**
Dépôt et partage des données	**2'850'000**	**1.10**

Eric Favre
eric.favre@etat.ge.ch
+41 22 3880000

Etat: 12 janvier 2017

Etat de la protection des données dans le monde

Liste des Etats ayant une législation assurant un niveau de protection adéquat (art. 6, 1er al., LPD).
Sauf précision, couvre les **traitements de données concernant des personnes physiques**.

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
Europe					
Albanie			X		Data Protection Commissioner Rruga Abdi Toptani, Nr. 4 Katii dyte AL-1000 Tirana Lien
Allemagne	X				Der Bundesbeauftragte für den Datenschutz Husarenstrasse 30 DE-53117 Bonn www.bfdi.bund.de
Andorre	X				Agència Andorrana de Protecció de Dades C/ Prat de la Creu, 59-65 esc. A, 3er. pis despatx 1-A AD-500 Andorra la Vella Principat d'Andorra www.apda.ad

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
Arménie			X		
Autriche	X			La loi s'applique également au traitement de données concernant des personnes morales.	Österreichische Datenschutzbehörde Hohenstaufengasse 3 AT-1010 Wien www.dsb.gv.at
Azerbaïdjan			X		
Bélarus			X		
Belgique	X				Commission de la protection de la vie privée Rue de la Presse 35 BE-Bruxelles 1000 www.privacycommission.be
Bosnie-Herzégovine			X		Personal Data Protection Agency in Bosnia and Herzegovina Vilsonovo šetalište broj 10 BA-71000 Sarajevo www.azlp.gov.ba
Bulgarie	X				Commission for Personal Data Protection 15 Akad. Ivan Ev. Geshov Blvd. BG-Sofia 1431 www.cpdp.bg
Chypre	X				Commissioner for Personal Data Protection 1 Iasonos street CY-1082 Nicosia www.dataprotection.gov.cy
Croatie	X				Personal Data Protection Agency Martićeva 14 HR-10 000 Zagreb www.azop.hr
Danemark	X			A certaines conditions, la loi peut s'appliquer aux traitements	Datatilsynet Borgergade 28, 5

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
				concernant les personnes morales.	DK-1300 Copenhagen www.datatilsynet.dk
Espagne	X				Agencia de Protección de Datos C/Jorge Juan, 6 ES-28001 Madrid www.agpd.es
Estonie	X				Data Protection Inspectorate 19 Väike-Ameerika St. EE-10129 Tallinn www.aki.ee
Finlande	X				Office of the Data Protection Ombudsman Albertinkatu 25 A, P.O. Box 315 FI-00181 Helsinki www.tietosuoja.fi
France	X				Commission Nationale de l'Informatique et des Libertés 8, rue Vivienne CS 30223 FR-75083 Paris cedex 02 www.cnil.fr
Géorgie			X		
Gibraltar			X		Gibraltar Regulatory Authority 2nd floor, Eurotowers 4 1 Europort Road Gibraltar GX11 1AA www.gra.gi
Grèce	X				Hellenic Data Protection Authority Kifissias Av. 1-3 GR-115 23 Athens www.dpa.gr

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
Guernesey	X				Data Protection Office P.O. Box 642 Frances House Sir William Place St. Peter Port Guernsey GY1 3JE www.gov.gg/dataprotection
Hongrie	X				National Authority for Data Protection and Freedom of Information Szilágyi Erzsébet fasor 22/C HU-1125 Budapest www.naih.hu
Île de Man	X				Office of the Data Protection Supervisor P.O. Box 69 Douglas Isle of Man IM99 1EQ www.gov.im/odps
Îles Féroé	X				Dátueftirlitið Tinganes Postboks 300 FO-110 Tórshavn www.datueftirlitid.fo
Irlande	X				Office of the Data Protection Commissioner Canal House, Station Road Portarlington IE-Co. Laois www.dataprivacy.ie
Islande	X				Data Protection Authority Raudararstigur 10 IS-105 Reykjavik

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
					www.personuvernd.is
Italie	X				Garante per la Protezione dei Dati Personali Piazza di Monte Citorio n. 121 IT-00186 Roma www.garanteprivacy.it
Jersey	X				Office of the Data Protection Commissioner Morier House Halkett Place St.Helier Jersey JE1 1DD www.dataprotection.gov.je
Kosovo			X		
Lettonie	X				Data State Inspectorate Blaumana street 11/13-15 LV-1011 Riga www.dvi.gov.lv
Liechtenstein	X			La loi s'applique également au traitement de données concernant des personnes morales.	Datenschutzstelle Kirchstrasse 8 Postfach 684 FL-9490 Vaduz www.dss.llv.li
Lituanie	X				State Data Protection Inspectorate A. Juozapavičiaus str. 6 / Slucko str. 2 LT-09310 Vilnius www.ada.lt
Luxembourg	X				Commission nationale de la protection des données 1, av. du Rock'n Roll LU-4362 Esch-sur-Alzette

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
					www.cnpd.lu
Malte	X				Office of the Information and Data Protection Commissioner 2, Airways House High Street MT-Sliema SLM 1549 www.dataprotection.gov.mt
Macédoine			X		Directorate for Personal Data Protection Samoilova Str. 10 MK-1000 Skopje www.dzlp.mk
Moldavie			X		National Center for Personal Data Protection 48, Serghei Lazo str. MD-2004 Chisinau www.datepersonale.md
Monaco	X				Commission de Contrôle des Informations Nominatives 12, Avenue de Fontvieille MC-98000 Monaco www.ccin.mc
Monténégro			X		Agency for Protection of Personal Data Kralja Nikole 2 ME-81000 Podgorica www.azlp.me
Norvège	X				Datatilsynet P.O. Box 8177 Dep NO-0034 Oslo www.datatilsynet.no
Pays-Bas	X				Data Protection Authority Juliana van Stolberglaan 4-10

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
					P.O. Box 93374 NL-2509 AJ Den Haag www.cbpweb.nl
Pologne	X				Bureau of the Inspector General for the Protection of Personal Data Ul. Stawki 2 PL-00 193 Warsaw www.giodo.gov.pl
Portugal	X				Commissão Nacional de Protecção de Dados Rua de São Bento n.º 148-3º PT-1200-821 Lisboa www.cnpd.pt
République Tchèque	X				Office for Personal Data Protection Pplk. Sochora 27 CZ-170 00 Prague 7 www.uoou.cz
Roumanie	X				National Supervisory Authority for Personal Data Processing Magheru Boulevard 28-30 RO-Bucharest Sector 1 www.dataprotection.ro
Royaume-Uni	X				Information Commissioner's Office Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF www.ico.org.uk
Russie			X		
Saint-Marin			X		
Saint-Siège			X		
Serbie			X		Commissioner for Information of Public

	Niveau adéquat pour des personnes physiques	Niveau adéquat sous certaines conditions	Niveau insuffisant	Remarques	Autorité nationale de protection des données
					Importance and Personal Data Protection 42, Svetozara Markovića str RS-11000 Belgrade www.poverenik.rs
Slovaquie	X				Office for Personal Data Protection Odborárske námestie č. 3 SK-817 60 Bratislava www.dataprotection.gov.sk
Slovénie	X				Information Commissioner Vošnjakova 1 / p.p. 78 SI-1001 Ljubljana www.ip-rs.si
Suède	X				Datainspektionen Drottninggatan 29 Box 8114 SE-104 20 Stockholm www.datainspektionen.se
Suisse	*X*				*Préposé fédéral à la protection des données et à la transparence PFPDT* *Feldeggweg 1* *CH-3003 Berne* *www.leprepose.ch*
Turquie			X		
Ukraine			X		State Service of Ukraine on Personal Data Protection Maryny Raskovoi Str. 15 UA-02660 Kiev www.zpd.gov.ua/dszpd

Amérique du Nord et Central					
Antigua-et-Barbuda			X		
Bahamas			X		
Barbade			X		
Bermudes			X		
Belize			X		
Canada	X			Dans le secteur privé (excepté dans les provinces où une loi sectorielle a été adoptée), la loi fédérale canadienne s'applique aux renseignements personnels, y compris les renseignements personnels sur la santé, recueillis, utilisés ou communiqués dans le cadre d'activités commerciales d'organisations, qu'ils s'agissent d'entreprises fédérales ou non. Les provinces du Québec, de la Colombie-Britannique et de l'Alberta, ainsi que de l'Ontario (pour les renseignements sur la santé) ont adopté des lois similaires à la loi fédérale en matière de protection des renseignements personnels. Même dans les provinces qui ont adopté une loi essentiellement similaire, et partout ailleurs au Canada, la loi fédérale s'applique toujours à tous les renseignements personnels recueillis, utilisés ou communiqués par toutes les entreprises fédérales, y compris les renseignements personnels au sujets des employés de celles-ci. La loi s'applique aussi aux renseigne-	Commissariat à la protection de la vie privée 112, rue Kent, Place de Ville Ottawa (Ontario) K1A 1H3 www.priv.gc.ca

				ments personnels qui circulent d'une province ou d'un pays à l'autre dans le cadre d'activités commerciales.	
Costa Rica			X		
Cuba			X		
Dominique			X		
Etats-Unis d'Amérique		X		Les organismes qui adhèrent au Privacy Shield pour les données provenant de Suisse et qui figurent sur la liste du Département américain du commerce garantissent un niveau de protection adéquat au sens de l'art. 6, al. 1, LPD	Federal Trade Commission FTC 600 Pennsylvania Avenue NW DC – 25080 Washington
Grenade			X		
Guatemala			X		
Haïti			X		
Honduras			X		
Jamaïque			X		
Mexique			X		Federal Institute of Access to Public Information Av México 151, Col Del Carmen Coyoacán México DF 04100 www.ifai.org.mx
Nicaragua			X		
Panama			X		
République dominicaine			X		
Saint-Christophe-et-Niévès			X		
Sainte-Lucie			X		
Saint-Vincent-et-les-Grenadines			X		

Salvador			X		
Trinité-et-Tobago			X		
Amérique du Sud					
Argentine	X			Couvre également le traitement de données concernant des personnes morales ayant un domicile légal dans le pays.	Dirección Nacional de Protección de Datos Personales Sarmiento 1118 – 5º Piso Ciudad Autónoma de Buenos Aires C1041AAX www.jus.gov.ar/datos-personales.aspx
Bolivie			X		
Brésil			X		
Chili			X		
Colombie			X		
Equateur			X		
Guyana			X		
Paraguay			X		
Pérou			X		
Suriname			X		
Uruguay	X				Unidad Reguladora y de Control de Datos Personales Andes N° 1365 piso 7 Montevideo, Uruguay www.datospersonales.gub.uy
Venezuela			X		
Afrique					
Afrique du Sud			X		
Algérie			X		
Angola			X		
Bénin			X		
Botswana			X		
Burkina Faso			X		Commission de l'Informatique et des Libertés

					(CIL)
Burundi			X		
Cameroun			X		
Cap-Vert			X		
Comores			X		
Congo			X		
Côtes d'Ivoire			X		
Djibouti			X		
Egypte			X		
Erythrée			X		
Ethiopie			X		
Gabon			X		
Gambie			X		
Ghana			X		
Guinée			X		
Guinée-Bissau			X		
Guinée équatoriale			X		
Kenya			X		
Lesotho			X		
Libéria			X		
Libye			X		
Madagascar			X		
Malawi			X		
Mali			X		
Maroc			X		
Maurice			X		
Mauritanie			X		
Mozambique			X		
Namibie			X		
Niger			X		
Nigéria			X		
Ouganda			X		

République Centrafricaine			X		
République démocratique de Congo			X		
Rwanda			X		
Sao Tomé-et-Principe			X		
Sénégal			X		
Seychelles			X		
Sierre Leone			X		
Somalie			X		
Soudan			X		
Swaziland			X		
Tanzanie			X		
Tchad			X		
Togo			X		
Tunisie			X		
Zambie			X		
Zimbabwe			X		
Asie					
Afghanistan			X		
Arabie saoudite			X		
Bahreïn			X		
Bangladesh			X		
Bhoutan			X		
Brunéi Darussalam			X		
Cambodge			X		
Chine			X		
Corée du Nord			X		
Corée du Sud			X		Personal Data Protection Center Korea Information Security Agency

					78, Garak-dong, Songpa-Gu Seoul 138-803 www.kisa.or.kr/eng/
Emirats arabes unis			X		
Hong-Kong			X		Privacy Commissioner for Personal Data 12/F, 248 Queen's Road East, Wanchai, Hong Kong. www.pco.org.hk
Inde			X		
Indonésie			X		
Iran			X		
Iraq			X		
Israël	X				Israeli Law, Information & Technology Authority The Government Campus 9th floor, 125 Begin Rd, P.O. Box 7360 Tel Aviv 61072 www.justice.gov.il/MOJEng/ILITA/
Japon			X		Government Information Protection Office Administrative Management 1-2 Kasumigaseki 2-chome, Chiyoda-ku Tokyo 100-8926 www.soumu.go.jp/english/
Jordanie			X		
Kazakhstan			X		
Kirghizistan			X		
Koweït			X		
Laos			X		
Liban			X		
Malaisie			X		

Maldives			X		
Mongolie			X		
Myanmar			X		
Népal			X		
Oman			X		
Ouzbékistan			X		
Pakistan			X		
Philippines			X		
Qatar			X		
Singapour			X		
Sri Lanka			X		
Syrie			X		
Tadjikistan			X		
Taiwan			X		The Ministry of Justice 130, Sec 1, Chung Ching South Road Taipei 100 Taiwan R.O.C. 100 www.moj.gov.tw/mp095.html
Thaïlande			X		Official Information Commission's Office Building Government House Dusit Bangkok Thailand 10300 www.oic.go.th/content_eng/default_eng.asp
Timor-Oriental			X		
Turkménistan			X		
Viêt Nam			X		
Yémen			X		
Océanie					
Australie		X		Avant de transférer des données, il convient de vérifier si le secteur concerné est couvert par la législation australienne régissant le droit à la vie	Federal Privacy Commissioner GPO Box 5218 Sydney NSW 2001 www.privacy.gov.au

				privée, notamment si elle couvre les données des étrangers.	
Fidji			X		
Îles Cook			X		
Kiribati			X		
Marshall			X		
Micronésie			X		
Nauru			X		
Nouvelle-Zélande	X				Privacy Commissioner PO Box 10-094, The Terrace Wellington 6143 www.privacy.org.nz
Palaos			X		
Papouasie-Nouvelle-Guinée			X		
Salomon			X		
Samoa			X		
Tonga			X		
Tuvalu			X		
Vanuatu			X		

ANNEXE 3

Google

Chartes d'autorégulation

Date de la dernière modification : 17 avril 2017

Comme décrit dans notre certification relative au bouclier de protection des données (le "Privacy Shield"), nous nous conformons au cadre défini par le EU-US Privacy Shield Framework et le Swiss-US Privacy Shield Framework mis en place par le ministère du Commerce des États-Unis concernant la collecte, l'utilisation et la conservation des informations personnelles provenant des États membres de l'Union européenne et de la Suisse. Google, y compris Google Inc. et ses filiales américaines en propriété exclusive, certifie son adhésion aux principes du Privacy Shield. Nous demeurons responsables de toutes les informations personnelles transmises à des tiers en vue d'un traitement externe en notre nom, conformément aux principes relatifs à ce type de transfert (Onward Transfer Principle) et tel que décrit dans la section "Données que nous partageons". Pour voir la certification de Google et en savoir plus sur le Privacy Shield, consultez le site Web qui y est consacré.

En cas de question concernant nos pratiques en matière de confidentialité dans le cadre de notre certification relative au bouclier de protection des données UE-États-Unis (Privacy Shield), nous vous invitons à nous contacter. Nous sommes soumis aux pouvoirs d'enquête et d'exécution de la commission fédérale du commerce américaine (Federal Trade Commission). Vous pouvez également soumettre une réclamation à votre autorité locale chargée de la protection des données, avec laquelle nous collaborerons pour résoudre votre problème. Dans certains cas, le cadre défini par le Privacy Shield UE-États-Unis permet d'invoquer un arbitrage exécutoire afin de régler des réclamations non résolues par d'autres moyens, comme décrit dans l'annexe I des principes du Privacy Shield.

Google respecte également les normes de l'industrie en ce qui concerne la transparence des informations et le choix d'annonces en ligne.

ANNEXE 4

educa.ch

PL 12103

modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)

Commission législative du Grand Conseil genevois
Karl Wimmer, educa.ch 12 janvier 2018

educa.ch

Numérisation dans l'éducation

Image: Jannoon028, freepik.com

educa.ch

Introduire les TIC dans l’enseignement et l’école

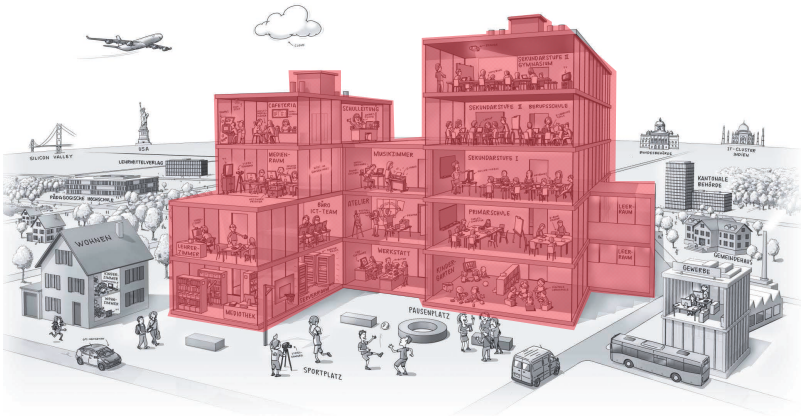


Image: Institut für Medien und Schule – PHZ Schwyz (2011), «Die Schule in der Informationsgesellschaft».
www.schuleinderinformationsgesellschaft.ch

educa.ch

Le paysage numérique de l’apprentissage

Disponibilité de données numérisées de et dans tous les contextes
Ubiquité des appareils mobiles
Omniprésence des médias digitaux et des réseaux sociaux
Applications innombrables pour tous les domaines de la vie

Image: http://sfib.educa.ch/sites/default/files/20141121/tischset_de_web.pdf

educa.ch

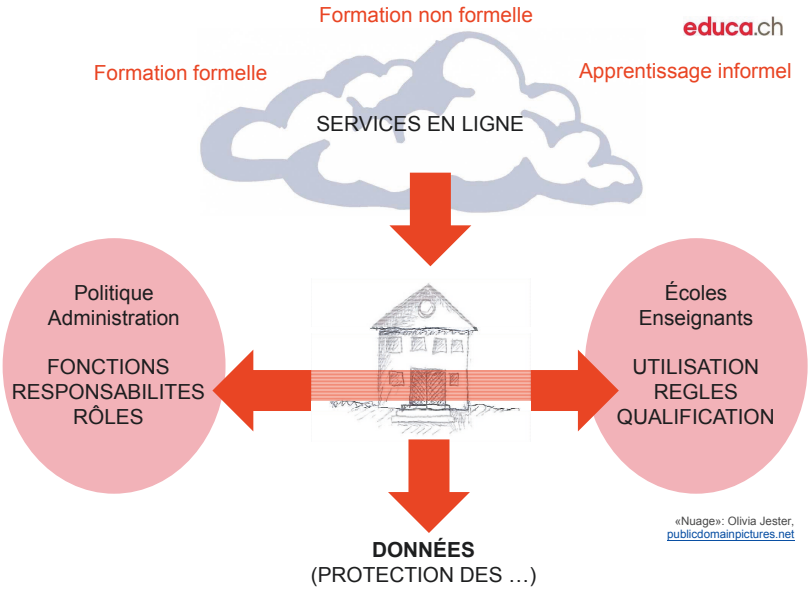
Défis de la transformation numérique

- Gestion des risques au lieu de considérations (i.e. « garantie ») de sécurité
- Utilisation des données
- Vitesse des développements et moments disruptifs
- Modèles économique
- Collaboration, responsabilités et confiance

educa.ch

Monde de travail 4.0 et école

Image: Manpower



educa.ch

Projet de loi 12103

[1] Les systèmes de messagerie, ainsi que les espaces numériques de dépôt et de partage de données mis à disposition des élèves, des étudiants et autres personnes en formation, ainsi que des collaborateurs du DIP du canton de Genève doivent être fournis par les services informatiques de l'Etat.

- Le DIP comme developpeur de services en ligne?
- Éducation aux médias?
- Conséquences financières?

educa.ch

[2] En cas de nécessité, ils peuvent être fournis par des entreprises suisses et domiciliées en Suisse.

- Contrats avec des fournisseurs de services?

educa.ch

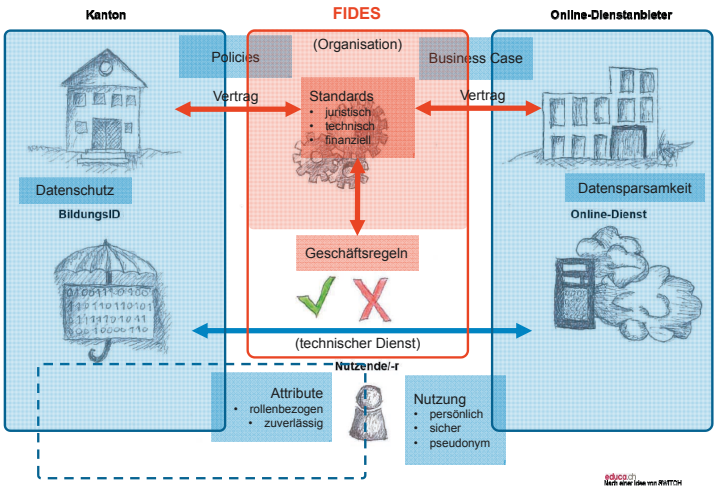
[3] L'Etat garantit que les données échangées ou déposées dans l'espace numérique mis à disposition par les personnes mentionnées à l'alinéa 1 sont stockées dans un data center en Suisse et sont uniquement soumises à la loi suisse en matière de protection des données.

- Lois suisses (et genèvois) en matière de protection des données en vigeur?

educa.ch

Identité numérique pour la formation – et «FIDES»

educa.ch



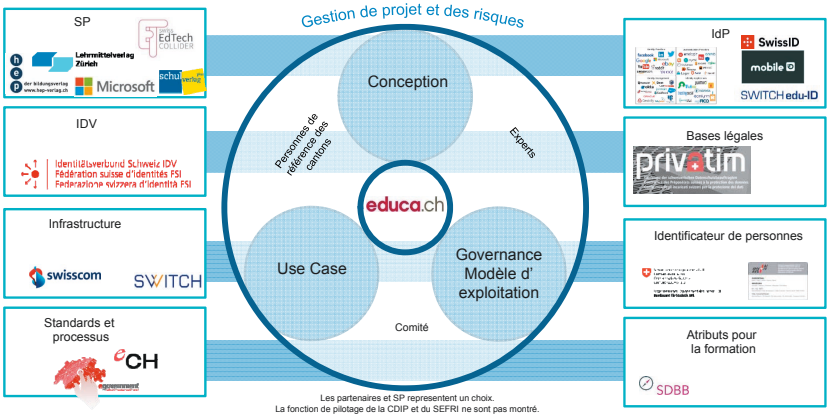
educa.ch

Merci!

Karl Wimmer
031 300 55 40
karl.wimmer@educa.ch

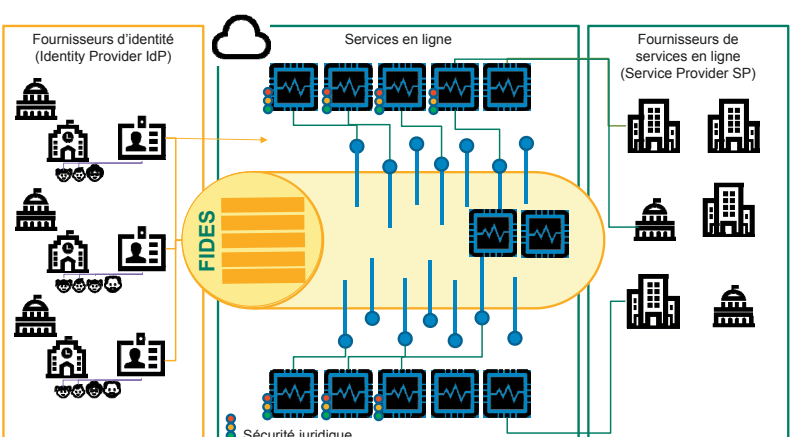
educa.ch

Positionement systémique de la « mise en œuvre de FIDES »

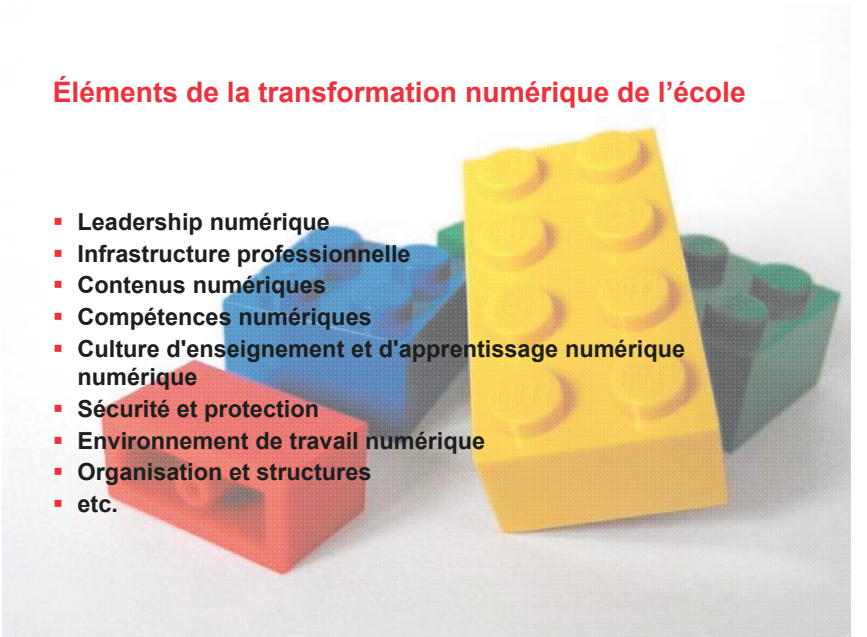


educa.ch

Vers une «cloud pour la formation»



Éléments de la transformation numérique de l'école



- Leadership numérique
- Infrastructure professionnelle
- Contenus numériques
- Compétences numériques
- Culture d'enseignement et d'apprentissage numérique numérique
- Sécurité et protection
- Environnement de travail numérique
- Organisation et structures
- etc.

Brochure
de l'exposition

DATA DETOX

Reprends le contrôle de tes données personnelles !

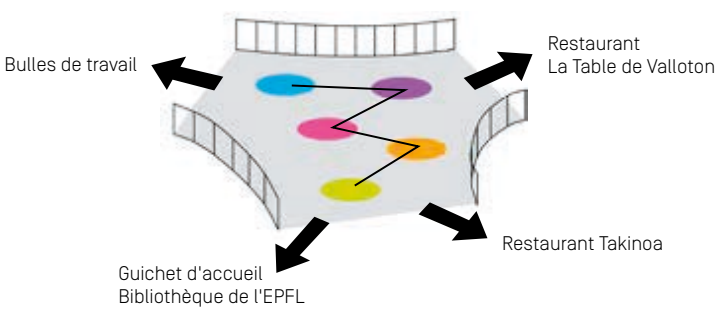
Une exposition de la Bibliothèque de l'EPFL
Rolex Learning Center

Introduction

Dans un contexte où, équipés de smartphones, ordinateurs et tablettes, la plupart d'entre nous créent et diffusent au quotidien un nombre incalculable de données personnelles, la Bibliothèque de l'EPFL traite de ce phénomène à travers l'exposition Data Detox. Il s'agit de faire le point sur les différentes manières dont les données personnelles sont collectées et diffusées lors de l'utilisation de services en ligne.

Cette brochure propose des exercices qui permettent à chacun de tester des outils et des astuces pratiques pour limiter la diffusion incontrôlée de données personnelles. Certains paramètres peuvent être différents en fonction du système d'exploitation, de la marque de l'appareil et de la version.

L'utilisation du genre masculin dans cette exposition et sa brochure est purement formelle et indique aussi bien le genre féminin que masculin.



Géolocalisation

Consulte les localisations que ton smartphone a enregistrées
Empêche la géolocalisation de certaines applications
Désactive la localisation
Supprime les réseaux WiFi sur lesquels tu t'es connecté
Change le nom de ton téléphone

Navigateurs

Consulte et efface l'historique de ton navigateur
Navigue en "mode privé"
Booste ton navigateur sur ton ordinateur

Réseaux sociaux

Cherche ton image sur Internet
Supprime ton image sur Internet
Gère les images sur lesquelles tu n'as pas le contrôle
Active le mode "Conversation secrète" sur Messenger
Demande une copie des données que Facebook a sur toi

Solutions alternatives

Fais le point
Solutions alternatives : navigateurs, moteurs de recherche, messageries électroniques, cartographie, réseaux sociaux, messageries instantanées, espaces de stockage en ligne.

Glossaire
Notes
Bibliographie
Autour de l'exposition

Géolocalisation

Exercices

Sur smartphone et tablette

1 Consulte les localisations que ton smartphone a enregistrées

iOS : Réglages → Confidentialité → Service de localisation → Service système (tout en bas) → Lieux fréquents
Android : Ouvrir Google Maps → Menu → Paramètres → Historique Maps

2 Empêche la géolocalisation de certaines applications

iOS : Réglages → Confidentialité → Service de localisation
Android : Paramètres → Applications → Paramètres → Autoris. des applis → Position

3 Désactive la localisation

iOS : Réglages → Confidentialité → Service de localisation → Désactiver service de localisation
Android : Paramètres → Localisation → Désactivé

4 Supprime les réseaux WiFi sur lesquels tu t'es connecté

iOS : Réglages → Général → Réinitialiser → Réinitialiser les réglages réseaux
Android : Paramètres → WiFi → Menu → Réseaux enregistrés

5 Change le nom de ton téléphone pour ne pas être repéré comme "Alex's phone"

iOS : Réglages → Général → Informations → Clique sur la première ligne, qui contient le nom de ton appareil. Renomme ton appareil, puis clique sur Terminé.
Android : Paramètres → A propos du téléphone → Nom de l'appareil

Conclusion

Pour éviter que ton smartphone ne te suive à la trace, tu peux désactiver les fonctions WiFi, bluetooth et géolocalisation quand tu ne les utilises pas. Mais sache que tu es toujours localisable par les antennes de téléphonie mobile.

L'étape ultime serait d'activer le mode avion quand tu n'as pas besoin de ton smartphone. Dans tous les cas, bravo pour cette première étape de Data Detox !

Navigateurs

Exercices

Avant de débuter cette partie, n'oublie pas de visiter Panopticlick (panopticlick.eff.org/) et clique sur "Test Me" pour savoir si ton navigateur est unique et connaître le niveau de protection de ce dernier.

1 Consulte et efface l'historique de ton navigateur

Lors de ta navigation sur Internet, de nombreuses informations sont conservées dans ton navigateur, dont l'historique des pages visitées. Ces éléments peuvent être étudiés par des sites et applications tiers qui te proposent alors un contenu personnalisé.

Ordinateur

Firefox : Menu (en haut à droite) → Bibliothèque → Historique → Effacer l'historique récent
Chrome et **Safari** : Menu (en haut à droite) → Historique → Historique → Effacer les données de navigation

Smartphone et tablette

Safari : Paramètres → Safari → Effacer historique et données de site
Firefox : Menu → Paramètres → Effacer les données privées
Chrome : Menu (en haut à droite) → Historique → Effacer les données de navigation

2 Navigue en "mode privé"

Utilise cette fonctionnalité complémentaire pour réaliser des recherches sur Internet sans que les traces de navigation comme l'historique de la session ou les cookies soient enregistrés.

Ordinateur
Firefox et Chrome : Menu → Nouvelle fenêtre de nav. privée
Safari : Menu → Historique → Navigation privée

Smartphone
Firefox : Menu → Nouvel onglet privé
Safari : Menu → mettre en relief "privé"
Chrome : Menu → Nouvel onglet nav. privée

3 Booste ton navigateur sur ton ordinateur

Tu es maintenant prêt à installer quelques petits extras connus sous le nom d'extensions ou de modules complémentaires.

Firefox et **Chrome** :
- Pour bloquer les publicités et les traqueurs invisibles, installe Privacy Badger (eff.org/privacybadger).
- Pour t'assurer que tes connexions aux sites Internet sont dans la mesure du possible cryptées, installe HTTPS Everywhere (eff.org/https-everywhere). Il s'agit d'une extension pour naviguer de manière cryptée et protégée. Ces deux extensions sont développées par l'Electronic Frontier Foundation (eff.org/fr).

Conclusion

Vérifie si ta cure de Data Detox fonctionne sur ton ordinateur et retourne sur Panopticlick (panopticlick.eff.org/) avec le navigateur que tu viens de nettoyer et clique sur "Test Me". Compare les nouveaux résultats avec les précédents. Ont-ils changé ?

Parfait ! Tu en as fini avec ton navigateur. A présent, tu as un navigateur mieux paramétré pour protéger tes activités en ligne.

Réseaux sociaux

Exercices

1 Cherche ton image sur Internet

Avec ton nom
Commence par écrire ton nom dans le moteur de recherche que tu utilises. Si tu as un nom très commun, ajoute une autre donnée d'identification, comme ton métier, ta ville ou l'endroit où tu as étudié. Observe les résultats. Sont-ils vraiment liés à toi ?

Avec une photo
Choisis une de tes photos, peut-être une vieille photo de profil à partir d'un compte sur les réseaux sociaux.
Accède à un moteur de recherche de type "Image inversée" comme Tineye (tineye.com/) ou Google Images (images.google.com/), et télécharge l'image pour la rechercher. Sur quels sites apparaît ton image ?

2 Supprime tes images sur Internet

As-tu trouvé des images que tu préfères ne pas afficher sur Internet ? Peut-être est-ce quelque part où tu as un certain contrôle, comme l'un de tes comptes sur les réseaux sociaux ? Dans ce cas, essaie simplement de la supprimer toi-même, de l'écraser avec une nouvelle image ou d'ajuster tes paramètres de confidentialité.

3 Gère les images sur lesquelles tu n'as pas de contrôle

Si l'image se trouve sur l'un des réseaux sociaux de quelqu'un d'autre, tu peux lui demander de la supprimer. Si elle est sur un site Internet, tu peux demander au propriétaire du site de la supprimer ou de la remplacer. Si tu ne parviens pas à obtenir le retrait de l'image, tu peux adresser une requête de "droit à l'oubli" à Google. Pour ce faire, tu peux utiliser le Formulaire de demande de suppression d'informations personnelles (go.epfl.ch/bf2).

Tu devras peut-être attendre un certain temps avant que l'image disparaisse des résultats de recherche. Il vaut la peine de se rappeler que même si l'image n'apparaît plus en ligne, elle est peut-être encore cachée ailleurs :

- sur les appareils d'autres personnes ou dans leurs comptes de réseaux sociaux ;
- sur les sauvegardes de compte (il peut prendre du temps pour que celle-ci soit effacée, selon la plateforme);
- dans un "Cloud" (iCloud, Dropbox, Google Drive).

4 Active le mode conversation secrète sur Messenger

Smartphone et tablette

IOS : Dans l'application Messenger → Paramètres (en haut à droite) → Secret (en haut à droite) → Sélectionne la personne à laquelle tu souhaites envoyer un message. Si tu le souhaites, appuie dans la zone de texte et définis un minuteur pour que les messages disparaissent après un certain temps.

Android : Dans l'application Messenger → Entame une conversation avec la personne avec qui tu souhaites entretenir une conversation secrète → Info (en haut à droite) → Accéder à la conversation secrète. Si tu le souhaites, appuie sur *Minuteur* dans la zone de texte et définis un minuteur pour que les messages disparaissent après un certain temps.

5 Demande une copie des données que Facebook a sur toi

Depuis la version ordinateur de Facebook : Clique sur la petite roue crantée (en haut à droite) → Compte → Général → Télécharger une copie de vos données sur Facebook → Créer mon archive
Après avoir cliqué sur le bouton, un message indique que l'archive est en cours de préparation et qu'un message sera envoyé quand elle sera prête. Sur cette page, un lien permet également de récupérer une archive dite "étendue" qui contient d'autres informations sur ton profil : adresses IP des connexions, cookies...

Cette récupération se fait via le téléchargement d'un fichier d'archive. Etant donné qu'il peut être très volumineux, Facebook t'enverra un email dès que l'archive sera prête à être téléchargée.

Conclusion

Bien joué ! Tu as franchi une nouvelle étape vers ton nouveau Toi numérique.

Il est maintenant temps d'achever ta cure de Data Detox en testant les solutions alternatives qui te sont offertes afin de limiter la diffusion incontrôlée de tes données personnelles.

Solutions alternatives

Fais le point

À qui offres-tu tes données ? Fais ta liste noire !
Qu'utilises-tu comme...

- navigateur ?
- moteur de recherche ?
- messagerie électronique ?
- outil d'orientation et/ou de cartographie ?
- réseaux sociaux ?
- application mobile de messagerie instantanée ?
- cloud pour stocker et partager tes fichiers, tes photos ?

Pour combien de réponses aux questions ci-dessus Google est-il propriétaire de l'outil que tu utilises ?

Pense à tout ce que tu fais en ligne en une journée... Sachant que Google collecte tes données à chaque action, n'as-tu pas l'impression qu'il sait plus de choses sur toi que ton entourage, même le plus proche ?

NAVIGATEURS
Solutions alternatives à Google Chrome

Firefox
mozilla.org/fr/firefox/new/

→ Navigateur libre et gratuit développé et distribué par Mozilla Foundation.
→ Logiciel multi-plateforme compatible avec Windows, MAC OS X, GNU/Linux et Android.
→ L'anonymat n'est pas assuré par défaut, par contre, en paramétrant Firefox, ou en ajoutant certains modules complémentaires, tu peux facilement élever ton niveau de confidentialité et bloquer les traqueurs.

Tor Browser
torproject.org

→ Navigateur développé par The Tor Project et Roger Dingledine, lancé en 2002.
→ L'acronyme signifie "The onion router".
→ En utilisant le Tor Browser, les pistes sont brouillées et ton fournisseur d'accès ne peut pas savoir à quels sites tu t'es connecté. La connexion est chiffrée et les fonctions de géolocalisation désactivées. Tu es complètement anonyme.

MOTEURS DE RECHERCHE
Solutions alternatives à Google Search

Duck Duck Go
duckduckgo.com/about

→ Moteur de recherche lancé en 2008 créé par Gabriel Weinberg dont le propriétaire est DuckDuckGo, Inc.
→ Société éditrice située à Valley Forge, en Pennsylvanie.
→ En utilisant ce moteur de recherche, ta vie privée est préservée. Aucune information personnelle n'est stockée.

SearX
searx.ch/about
- → Métamoteur de recherche développé par Adam Tauber.
- → Disponible sous licence libre AGPLv3.
- → Cet outil de recherche envoie les informations chiffrées. Il ne collecte pas de données personnelles, n'essaie pas de profiler les utilisateurs et n'impose pas de publicité.

MESSAGERIES ELECTRONIQUES
Solutions alternatives à Gmail et Yahoo

Protonmail
protonmail.com/fr/
- → Messagerie chiffrée développée au CERN en 2013, service ouvert à tous depuis mars 2016.
- → Serveurs situés en Suisse.
- → Messagerie gratuite jusqu'à 500 Mo d'e-mails stockés et accessible depuis n'importe quel navigateur.
- → Le niveau de confidentialité est très élevé et il n'y pas de publicité.

Posteo
posteo.de/fr/site/qui_sommes_nous
- → Service de messagerie, calendrier et carnet d'adresses lancé en 2009, dont les propriétaires sont Patrick et Sabrina Löhr.
- → Service payant à hauteur de 1€ par mois.
- → Parmi les avantages offerts, il y a notamment le chiffrement des données, l'inscription et le paiement sans divulgation des données personnelles.

CARTOGRAPHIE
Solutions alternatives à Google Map

Open Street Map
openstreetmap.org/

→ Projet lancé en 2004 et mis en route par Steve Coast au University College de Londres.
→ Service collaboratif de cartographie.
→ L'objectif est de constituer des cartes géographiques libres en utilisant des données GPS et d'autres données libres. Par ailleurs, chacun peut être contributeur de cette carte et corriger des erreurs.

Framacarte
framacarte.org/fr/

→ Logiciel de cartographie développé par Framasoft, un réseau d'éducation populaire créé en 2001, consacré principalement au logiciel libre.
→ Service en ligne libre de création de cartes personnalisées.
→ Permet de dessiner, marquer, annoter les fonds de cartes d'OpenStreetMap et de les afficher ensuite sur un site Internet.

RESEAUX SOCIAUX
Solutions alternatives à Facebook et Twitter

Diaspora*
diasporafoundation.org/

→ Projet initié par quatre étudiants de l'Institut Courant des mathématiques de l'Université de New York et lancé en 2012.
→ Environ 600 000 utilisateurs.
→ Réseau social open source qui propose des fonctions similaires à celles de Facebook.

→ Les données ne sont ni collectées, ni stockées de manière centralisée: au lieu de concentrer tes données dans d'énormes serveurs, propriétés de grandes entreprises, de petits serveurs "pods" locaux peuvent être créés n'importe où dans le monde. Tu choisis le pod auprès duquel tu t'inscris.

Mastodon
mastodon.social/about

→ Réseau social de microblogging décentralisé, créé en 2016.
→ Plus d'un million d'utilisateurs en juin 2018.
→ Le service ne contient pas de publicité et les données des utilisateurs sont préservées.
→ Le journal *Le Monde* possède un compte sur ce réseau social: https://mastodon.social/@lemonde.

MESSAGERIES INSTANTANEES
Solutions alternatives à WhatsApp et Messenger

Signal
signal.org/

→ Messagerie instantanée chiffrée lancée en 2014 et développée par Open Whisper Systems et d'autres contributeurs.
→ Disponible pour Android et iOS.
→ L'application permet de créer des groupes et partager des fichiers multimédia en toute confidentialité.
→ L'application a accès aux contacts et utilise ton numéro de téléphone. Auditée, elle semble irréprochable niveau sécurité. Elle ne vend pas les données.

Wire
wire.com/en/

- → Messagerie instantanée lancée en décembre 2014 par la société WIRE SWISS Gmbh.
- → Wire est disponible sur iOS, Android, Linux, Windows, macOS et sur les navigateurs Internet.
- → Les messages envoyés sont chiffrés.
- → Le service permet d'envoyer des messages, des vidéos, des fichiers, des images.

ESPACES DE STOCKAGE
Solutions alternatives à Google Docs et DropBox

SwitchDrive
switch.ch/fr/drive/

- → Service Cloud proposé par SWITCH qui permet de stocker, synchroniser et partager des fichiers.
- → Toutes les universités et hautes écoles suisses proposent gratuitement à leurs membres un espace de 50 GB sur le cloud SwitchDrive.
- → Les données sont hébergées en Suisse.

OwnCloud
owncloud.org/

- → Première version lancée en 2010 et développée par OwnCloud In.
- → Logiciel libre offrant une plateforme de services de stockage et partage de fichiers et d'applications diverses.
- → Nécessite quelques paramétrages pour créer son propre espace de stockage.
- → Les fonctionnalités sont nombreuses: synchronisation des fichiers entre différents ordinateurs, stockage sécurisé, lecteur de musique, calendrier, etc.

Glossaire

Ce glossaire est fortement inspiré de définitions issues de Wikipédia retravaillées pour l'exposition.

"Accepter les conditions" : Les conditions générales d'utilisation (CGU) sont présentes sur n'importe quel site Internet y compris sur des sites non commerciaux et visent à informer l'internaute des interactions réelles qu'il a avec la plateforme : usage des cookies, suivi du trafic, récupération et utilisation des données récoltées. Tout échange réalisé de manière informatique est concerné par les CGU.

Blockchain : Signifie littéralement "chaîne de blocs". Il s'agit d'une base de données distribuées en blocs. Mis ensemble, les blocs ont un sens, mais séparément ils ne peuvent être lus. En utilisant la technologie du blockchain pour échanger des informations, la traçabilité est empêchée.

Cookies : Fichiers textes de petite taille stockés sur l'ordinateur, qui répertorient chaque action qu'un internaute effectue sur Internet. Ils existent depuis les débuts d'Internet. Grâce à eux, les développeurs de sites Internet peuvent sauvegarder des données sur les utilisateurs afin de faciliter leur navigation et leur proposer certaines fonctionnalités. Les cookies évitent aussi d'avoir à se ré-authentifier à chaque requête. Le navigateur peut également être paramétré pour signaler les cookies déposés sur l'ordinateur et demander de les accepter ou pas. Les cookies sont des traqueurs.

Courtier de données : Grâce à des algorithmes de profilage, ce genre de courtier collecte des informations personnelles disponibles à partir de sources publiques et privées, à propos des habitudes de consommation des internautes. Aussi appelé "data broker" il vend ces informations à des entreprises, des annonceurs ou des prestataires marketing.

Chiffrement : Opération qui consiste à rendre illisibles des données à toute personne qui ne possède pas le code de déchiffrage.

Cryptomonnaie : Monnaie numérique alternative, utilisable sur un réseau informatique. Le Bitcoin est l'une des premières cryptomonnaies. Elle a été introduite en 2009.

Données personnelles : La Loi fédérale suisse sur la Protection des Données (LPD) définit la notion de *Données personnelles* comme "Toutes les informations qui se rapportent à une personne identifiée ou identifiable". (section 1, article 3).

Droit d'accès : Le droit d'accès d'une personne à ses propres données, ainsi que la possibilité de s'informer sur l'origine desdites données est régi en Suisse par les articles 8 à 10 de la section 2 de la LPD. Selon l'article 15 du Règlement Général européen sur la Protection des Données (RGPD), "la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que ses données personnelles sont ou ne sont pas traitées et, lorsqu'elles le sont, elle a le droit d'obtenir l'accès auxdites données ainsi qu'à un certain nombre d'informations complémentaires prévues aux lettres a) à h). Ce droit comprend également celui d'obtenir une copie des données qui font l'objet d'un traitement".

Glossaire

Electronic Frontier Foundation (EFF) : Organisation internationale non gouvernementale de protection des libertés sur Internet, basée à San Francisco. Panopticlick, Privacy Badger et HTTPS Everywhere sont édités par l'EFF.

Empreinte numérique : Trace unique laissée par un dispositif informatique (ordinateur, tablette, smartphone) lors d'une visite sur un site Internet. Il s'agit d'un ensemble de données telles que le numéro de série, l'adresse IP ou encore la configuration des navigateurs Internet. Ces informations collectées permettent de reconnaître l'appareil et donc son utilisateur. Accessible en tout temps, contrairement aux cookies qui peuvent être désactivés, l'empreinte numérique peut être utilisée à des fins publicitaires pour réaliser des campagnes ciblées.

Extension: Module qui complète un logiciel hôte en permettant d'y ajouter des fonctionnalités. Par exemple, il existe des extensions qui complètent les fonctionnalités des navigateurs en bloquant les traqueurs ou les publicités.

GPS : Utilisé par de nombreuses applications, le *Global Positionning System*, est un système de positionnement militaire américain utilisant 24 satellites appartenant au gouvernement des États-Unis. Le GPS a été développé par le département de la Défense des États-Unis à des fins militaires, à partir de 1973. Depuis les années 2000 il est ouvert à tous.

Historique du navigateur : Fonctionnalité présente sur le navigateur qui permet de retrouver les pages précédemment consultées sur Internet. Il est ainsi possible de remonter dans le temps (jusqu'à plusieurs mois) afin de retrouver les adresses de pages consultées. Chaque navigateur fabrique son propre historique.

Métamoteur de recherche : Moteur de recherche agrégeant les résultats de plusieurs moteurs de recherche différents. Les utilisateurs ne saisissent le sujet de leur requête qu'une seule fois et accèdent simultanément aux réponses de plusieurs moteurs de recherche.

Moteur de recherche : Outil permettant de réaliser une requête à partir d'une boîte de recherche et de trouver une ou plusieurs ressources (pages Internet, documents, vidéos, etc).

Navigation privée : Fonctionnalité complémentaire proposée par certains navigateurs Internet, permettant de réaliser des recherches sur Internet sans que les traces de navigation comme l'historique de la session ou les cookies soient enregistrés.

Règlement Général sur la Protection des Données (RGPD) : Entré en vigueur le 25 mai 2018, ce règlement vise à redonner aux citoyens de l'Union Européenne (UE) le contrôle de leurs données. L'article 12 du RGPD oblige les enteprises publiques et privées qui traitent des données personnelles à mettre en place des mesures et des procédures permettant aux citoyens de l'UE d'exercer leurs droits. La LPD s'appuie sur ce même règlement pour renforcer ses mesures.

Glossaire

Système d'exploitation (OS – de l'anglais Operating System) : Ensemble de programmes gérant l'utilisation des ressources d'un appareil informatique par des logiciels applicatifs. Il existe des dizaines de systèmes d'exploitation comme Windows, Mac OS, GNU/Linux ou encore Android.

Traqueur : Logiciel qui piste les utilisateurs, les suit de manière anonyme sur Internet et reconstitue leurs parcours à des fins d'analyse marketing et de relance commerciale. Il est quasiment impossible de savoir comment et où les renseignements personnels sont distribués. Parmis les traqueurs, on trouve les cookies.

WiFi (Wireless Fidelity) : Ensemble de protocoles de communication sans fil, qui permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.) au sein d'un réseau informatique, afin de permettre la transmission de données entre eux.

Notes

Bibliographie

CHARLET, François, 2016. On veut vous faire croire que vous n'avez rien à cacher. In : François Charlet [en ligne]. 18 août 2016. [Consulté le 9 août 2018]. Disponible à l'adresse : https://francoischarlet.ch/2016/rien-a-cacher/.

COLLECTIF, 2017. Guide d'autodéfense numérique. Lyon : Tahin Party. ISBN 978-2-912631-29-9.

DATA GUEULE, 2015. Privés de vie privée ? - #DATAGUEULE 40 [en ligne]. 2015. [Consulté le 9 août 2018].
Disponible à l'adresse : https://www.youtube.com/watch?v=wShQYeH9qJk&feature=youtu.be.

FRAMMERY, Catherine, 2018. Mes données sur Internet, ou le consentement prisonnier. In : Le Temps [en ligne]. 11 février 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.letemps.ch/societe/donnees-internet-consentement-prisonnier.

GIANORA, Tristan et CORNU, Daniel, 2015. Le droit à l'oubli : du mythe à la réalité. Lausanne : Lausanne : CEDIDAC.

KERDELLANT, Christine, 2017. Dans la Google du loup: découvrez le monde que Google nous prépare. Paris : Plon. ISBN 978-2-259-24878-5.

LEBLOGDUHACKER, 2015. Une histoire de vie privée sur Internet [en ligne]. 2015. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.youtube.com/watch?v=q0Ax6m0ff0c&feature=youtu.be.

L'EXPRESS, 2018a. Du risque de la dépendance aux Gafa. In : L'Express [en ligne]. 25 mai 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://lexpansion.lexpress.fr/high-tech/du-risque-de-la-dependance-aux-gafa_2010326.html.

L'EXPRESS, 2018b. États-Unis: Facebook s'intéresse aux données bancaires. In : L'Express [en ligne]. 7 août 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.lexpress.fr/actualite/monde/amerique-nord/etats-unis-facebook-s-interesse-aux-donnees-bancaires_2029749.html

MIMS, Christopher, 2018. Who Has More of Your Personal Data Than Facebook? Try Google. In : Wall Street Journal [en ligne]. 22 avril 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401.

RADIO TÉLÉVISION SUISSE, 2016. La RTS lance Datak, le jeu qui interroge notre gestion des données. In : rts.ch [en ligne]. 13 décembre 2016. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.rts.ch/info/suisse/8235789-la-rts-lance-datak-le-jeu-qui-interroge-notre-gestion-des-donnees.html.

SANNAJUST, Aurélie et MEIER, Olivier, 2018. Comment la blockchain bouleverse les modes de gouvernance traditionnels. In : HBR [en ligne]. 6 mars 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.hbrfrance.fr/chroniques-experts/2018/03/19324-blockchain-bouleverse-modes-de-gouvernance-traditionnels/.

TACTICAL TECH, 2018a. Data Detox Kit, le programme de détox en 8 jours. In : [en ligne]. 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://datadetox.myshadow.org/detox.

TACTICAL TECH, 2018b. Mon ombre et moi : prenez le contrôle de vos données. In : [en ligne]. 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://myshadow.org/.

THE ELECTRONIC FRONTIER FOUNDATION, 2018. Panopticlick. In : [en ligne]. 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://panopticlick.eff.org/.

WU, Tim, 2018. The Tyranny of Convenience. In : The New York Times [en ligne]. 20 février 2018. [Consulté le 9 août 2018]. Disponible à l'adresse : https://www.nytimes.com/2018/02/16/opinion/sunday/tyranny-convenience.html.

Autour de l'exposition

Ateliers Data Detox
"Protégez votre vie privée numérique"
Jeudi 25 octobre 2018
De 10h à 11h30 et de 12h15 à 13h45

Vous souhaitez mieux paramétrer votre smartphone et votre navigateur ? Besoin d'aide pour créer une adresse de messagerie ProtonMail et nettoyer votre historique ?
Après un court bilan de santé de votre identité numérique, mettez en pratique les outils présentés dans l'exposition !

N'oubliez pas votre ordinateur et/ou votre smartphone !
Atelier gratuit et ouvert à tous.
Informations et inscriptions : library.epfl.ch

Verrée de finissage de l'exposition
Jeudi 25 octobre 2018 dès 17h30

Evénements liés à l'exposition

- **MICRO 18 - Big data sous la loupe**
  30-31 août, 1er septembre 2018
  Neuchâtel / unine.ch

- **SWISS DIGITAL DAY**
  Jeudi 25 octobre 2018
  Campus EPFL / digitaltag.swiss/fr/

Inspirations

Le contenu des panneaux d'exposition ainsi que les exercices de cette brochure sont fortement inspirés :

- Du parcours "Data Detox Kit, le programme de détox en 8 jours" par la fondation Mozilla et le Tactical Technology Collective https://datadetox.myshadow.org/fr/detox, consulté le 13.08.2018 CC BY-NC-SA 4.0

- Du site "Me and My Shadow : Take control of your data" https://myshadow.org, consulté le 31.07.2018 CC BY-SA 3.0

Non exhaustivité

L'exposition et cette brochure ne sont pas exhaustives en matière de protection des données et de vie privée sur Internet. N'hésitez pas à contacter la Bibliothèque de l'EPFL pour plus d'informations : library@epfl.ch, +41 21 693 21 56.

Diffusion et licence

DATA DETOX

Reprends le contrôle de tes données personnelles

Une exposition de la Bibliothèque de l'EPFL
Rolex Learning Center

30.08 >>>
25.10.2018
7/7 / 7h-minuit / entrée libre

#datadetox
@EPFLlibrary

BIBLIO THÈQUE

ANNEXE 6


expo
expo
expo
DATA
DETOX
Reprends le contrôle de
tes données personnelles !
Une exposition de la Bibliothèque de l'EPFL
Rolex Learning Center
30.08 >>>
25.10.2018
7/7 / 7h-minuit / entrée libre #datadetox
library.epfl.ch @EPFLlibrary
BIBLIO
THÈQUE
EPFL
ECOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Introduction

As-tu parfois l'impression que ton identité numérique t'échappe ?
As-tu perdu la trace de certains comptes que tu as créés ?
As-tu l'habitude d'installer des applications et de cliquer sur « **Accepter les conditions** » sans les lire ?

L'utilisation faite de tes **données personnelles** peut poser problème. En effet, les appareils connectés que tu utilises (smartphone, ordinateur, tablette, montre, télévision) permettent de collecter tes données. Tes habitudes, déplacements, préférences, relations et même tes croyances sont révélés à des entreprises qui les conservent et en profitent.

Cette exposition est l'occasion de faire le point sur comment et pourquoi tes données sont analysées, partagées et vendues. Reprends le contrôle de ton identité numérique et apprends à mieux la maîtriser grâce à des conseils pratiques et des astuces simples à mettre en place.

C'est parti pour une cure de DATA DETOX !

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Si au fond de toi, tu penses que...

"JE N'AI RIEN À CACHER !"

La protection de la vie privée ne consiste pas à se cacher. Il s'agit de l'autonomie, du pouvoir et du contrôle, de ta capacité à décider comment tu souhaites te présenter au monde.

"JE M'EN MOQUE QUE LES PERSONNES SACHENT QUE JE MANGE UN CROISSANT LE MATIN"

Quand tu regardes plus attentivement les traces numériques que tu laisses, certaines sont très personnelles : où tu vas, ce que tu fais, avec qui. Pense à ce que tu partages avec Google par le biais de tes recherches.
Ce sont peut-être des choses que tu n'as même pas partagées avec ton entourage proche. Ton intimité est dévoilée.

"JE NE SUIS QU'UNE SEULE PERSONNE SUR DES MILLIONS... COMMENT PEUT-ON ME VOIR ?"

Faire partie de la multitude sur Internet n'empêche pas que tu puisses être repéré et suivi en tant qu'individu. Imagines-tu des gens assis derrière un ordinateur quelque part, analysant les traces de données produites par des milliards de personnes ? En réalité, des machines et des algorithmes spécialement conçus pour faire ce travail analysent d'énormes volumes de données. La masse n'est donc pas une protection.

"JE SUIS EN TRAIN D'UTILISER CE SERVICE GRATUITEMENT !"

Un service est rarement gratuit : tu le finances sans le savoir, en fournissant tes données personnelles.

... alors cette exposition est faite pour toi !

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Utilise la brochure de l'exposition !

EXERCICES DE DETOX

Là où tu aperçois le symbole de la brochure dans l'exposition, des exercices pratiques te sont proposés en lien avec le panneau.
Tu trouveras également des conseils à appliquer pour protéger tes données personnelles en ligne sur tes appareils.

LA BROCHURE EST DISPONIBLE TOUT AU LONG DU PARCOURS ! TU PEUX ÉGALEMENT EN DEMANDER AU GUICHET D'ACCUEIL DE LA BIBLIOTHÈQUE.

GLOSSAIRE

Les mots en couleur dans l'exposition comme **métamoteur de recherche** ou **cookies** sont définis dans le glossaire, à la fin de la brochure, par ordre alphabétique.

Sers-toi des tablettes mises à disposition !

ACTIVITÉS EN LIGNE

Là où tu vois le symbole de la tablette, tu peux effectuer les activités directement sur les tablettes mises à ta disposition.

DATA DETOX

Une exposition de la Bibliothèque de l'EPFL

Partage ton expérience de l'exposition sur les réseaux sociaux !

#datadetox
@EPFLlibrary

Jeudi 25 octobre 2018
Ateliers Data Detox
Protégez votre vie privée numérique

Vous souhaitez mieux paramétrer votre smartphone et votre navigateur ? Besoin d'aide pour créer une adresse de messagerie ProtonMail et nettoyer votre historique ? Après un court bilan de santé de votre identité numérique, mettez en pratique les outils présentés dans l'exposition !

N'oubliez pas votre ordinateur et/ou votre smartphone ! Atelier gratuit et ouvert à tous.

Session de 10h à 11h30 et de 12h15 à 13h45
Inscriptions : library.epfl.ch

Jeudi 25 octobre 2018
Verrée de finissage de l'exposition

Rendez-vous dès 17h30 pour visiter une dernière fois l'exposition autour d'une verrée.

Exposition

DATA DETOX
Reprends le contrôle de tes données personnelles
30.08 › 25.10.2018

EPFL
Rolex Learning Center

Entrée libre, 7/7, 7h-minuit

Contact

Bibliothèque de l'EPFL
Rolex Learning Center
Station 20
CH-1015 Lausanne

library.epfl.ch
library@epfl.ch
+41 21 693 21 56

BIBLIOTHÈQUE EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

L'utilisation du genre masculin dans cette exposition et sa brochure est purement formelle et indique aussi bien le genre féminin que masculin.

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Géolocalisation

UN ESPION DANS TA POCHE

La géolocalisation permet de situer une personne ou un objet sur une carte. Elle a un côté très pratique. Par exemple, lorsque tu es perdu dans une grande ville, c'est rassurant de pouvoir te situer sur une carte et de te faire guider par ton smartphone jusqu'à destination. Cependant, si la géolocalisation te permet de repérer ton smartphone en cas de perte, elle enregistre également tous tes déplacements, comme si tu étais espionné en permanence.

Géolocalisation 1/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

A QUEL MOMENT MA LOCALISATION EST-ELLE CONNUE ?

Ton smartphone rend ta géolocalisation possible lorsque le **GPS** (Global Positioning System) est activé. Même si tu désactives la fonction "localisation" de ton téléphone, il existe de nombreux autres moyens pour te localiser sans que tu t'en rendes compte, par exemple lorsque :

- **tu navigues sur Internet avec un appareil connecté**
- **tu envoies un SMS ou que tu passes un appel**
- **tu te connectes à un réseau Wifi**
- **tu postes une photo sur les réseaux sociaux**

COMMENT CELA EST-IL POSSIBLE ?

L'adresse IP

Quand tu te connectes à Internet, que tu envoies un email ou que tu publies sur les réseaux sociaux, le fournisseur d'accès du réseau sur lequel tu navigues associe une adresse IP à ton appareil connecté. Cette adresse IP est un identifiant unique composé d'une suite de chiffres reliés à une antenne dont la localisation est connue.

Les antennes de téléphonie mobile

Pour envoyer et recevoir des appels et des messages, ton téléphone communique tout le temps avec les antennes de téléphonie mobile. Cette activité est suivie et archivée par ton fournisseur de téléphonie mobile et lui permet de savoir depuis quels endroits tu as émis tes communications.

Les réseaux Wifi

Même si tu désactives le Wifi de ton smartphone, ce dernier émet des signaux Wifi régulièrement pour tenter de se connecter à l'un des réseaux. Les traceurs Wifi s'en servent pour suivre tes déplacements, notamment dans les lieux publics tels que les aéroports, les cafés, ou même lorsque tu es chez des amis.

Il existe d'autres moyens de connaître ta localisation. Par exemple avec les métadonnées liées à une photo que tu publies ou les algorithmes permettant de déterminer le lieu où une photo a été prise.

Géolocalisation 2/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Tu travailles à l'EPFL.
Tu t'y rends tous les jours avec le Métro M1 et le bus 25. En général, tu prends ta pause de midi à l'Esplanade.

Tu habites à Lausanne,
dans un quartier chic.

Tu étais au Montreux Jazz Festival
deux soirs en juillet 2018 pour les concerts de Deep Purple et Jamiroquai.

Tu es inscrit
au Centre Sportif Universitaire de Dorigny UNIL-EPFL.

Tu vas fréquemment au Maroc.
Tu y séjournes un week-end tous les trois mois et tu passes par les aéroports de Genève et Marrakech.

Tu passes parfois la soirée et la nuit
au n°65 de la rue de l'Avenir à Renens.

Tu as couru le marathon
de Lausanne en octobre 2017.

Tu étais en voyage à Berlin
du 12 au 15 décembre 2017.

Tu passes souvent la nuit
au labo et tes fins de journée au bar The Great Escape.

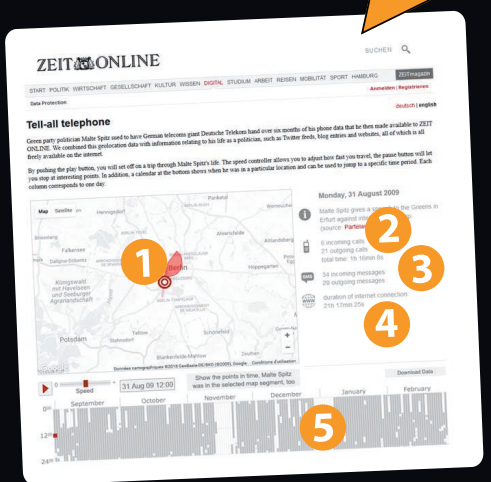
Géolocalisation 3/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

TON SMARTPHONE EST UNE BALANCE !

Avant la mise en place du **RGPD***, Malte Spitz, un politicien du parti écologiste allemand, a intenté un procès pour que le géant des télécommunications Deutsche Telekom lui fournisse plus de six mois de ses données téléphoniques. Il les a ensuite mises à disposition du journal allemand Die Zeit Online, qui a combiné ces données de géolocalisation avec des informations relatives à sa vie politique, comme les flux Twitter, les entrées de blogs et les sites Internet, qui sont tous disponibles gratuitement sur Internet. Die Zeit Online en a fait une animation permettant de connaître, ou déduire :

1 - **ses déplacements sur une carte**
2 - **le nombre, la durée et les horaires de ses appels**
3 - **le nombre de messages envoyés et reçus**
4 - **la durée de ses connections à Internet**
5 - **le lieu où il a fêté le réveillon**



***Bonne nouvelle !**

Depuis l'entrée en vigueur du **Règlement Général sur la Protection des Données**, le 25 mai 2018, les entreprises privées et les institutions publiques ont l'obligation de fournir aux citoyens européens les données personnelles en leur possession. Aujourd'hui, Malte Spitz n'aurait donc plus besoin d'intenter un procès à son opérateur téléphonique.

Géolocalisation 4/4

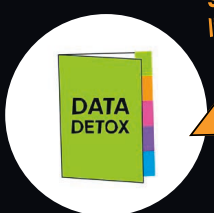
DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Il ne fait aucun doute que la géolocalisation a de nombreux aspects pratiques. Même si elle ne semble pas problématique au premier abord, c'est l'interprétation des données qui peut poser problème.

Prenons l'exemple de l'application Strava qui permet d'enregistrer et de comparer ses performances sportives grâce à son système de géolocalisation. Très utilisée par les soldats américains, elle a notamment révélé, en janvier 2018, l'emplacement de bases militaires secrètes en enregistrant les déplacements des troupes lors de leurs entrainements. C'est l'une des conséquences fâcheuse des objets géolocalisés.

Ton smartphone mémorise les lieux où tu te rends fréquemment afin d'obtenir des données de localisation utiles dans tes applications "plan" et "calendrier". Il est possible de désactiver cette option pour ne pas être suivi à la trace.

Consulte la brochure de l'exposition pour savoir comment limiter les flux de données liées à la géolocalisation que tu émets .



DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Navigateurs

TES DONNÉES À LA DÉRIVE

Un navigateur est un logiciel qui permet de parcourir Internet et de consulter un site web. Les navigateurs les plus connus sont Microsoft Edge, Firefox, Safari et Chrome. Ils sont conçus pour fonctionner avec différents systèmes d'exploitation comme GNU/Linux, Windows, Mac OS, iOS et Android. Mais sais-tu qu'il existe une possibilité de naviguer incognito grâce au mode de navigation privée ?

Navigateurs 1/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

SAIS-TU QUE TON NAVIGATEUR TE SUIT COMME TON OMBRE ?

Tous les sites Internet que tu visites sont stockés dans l'**historique de ton navigateur**. De ce fait, ton navigateur récolte de nombreuses informations sur toi qu'il partage avec d'autres sites que tu visites, ainsi qu'avec les **moteurs** et **métamoteurs de recherche**. Cependant, tu peux empêcher ton navigateur de te traquer en :

- effaçant régulièrement l'historique de ton navigateur
- désactivant la fonction "Historique"
- activant le mode **navigation privée**

COMMENT TON NAVIGATEUR TE TRAHIT-IL EN PERMANENCE ?

De nombreux sites Internet utilisent des **traqueurs** afin de te suivre quand tu navigues dans leurs pages. Certains sites peuvent en dissimuler plus d'une centaine !

Lorsque tu cliques sur "accepter les cookies", tu acceptes d'être traqué par les traqueurs du site, y compris ceux qui transmettent tes informations à des **courtiers de données**.

Navigateurs 2/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

QUI COLLECTE LES DONNEES ET POURQUOI ?

Les traqueurs collectent des données sur tes appareils connectés (smartphone, tablette, ordinateur, télévision) et fournissent au propriétaire du site Internet des informations sur le trafic généré par son site (nombre et fréquence des visites, partages, profils des visiteurs, etc).

Les informations collectées peuvent également être achetées par des courtiers en données qui les revendent à des annonceurs ou à des entreprises. Les activités de ces courtiers en données, comme DoubleClick ou en encore ComScore, reposent donc sur la vente des données qu'ils collectent.

Quant aux entreprises et aux annonceurs, leur but principal est d'établir ton profil afin de cibler l'information et les publicités qu'ils te font parvenir.

COMMENT LES ENTREPRISES SUIVENT-ELLES TES APPAREILS SUR INTERNET ?

Les traqueurs sont capables de collecter un grand nombre d'informations sur tes appareils et de t'identifier, même si tu n'es pas connecté :

- adresse IP
- historique du navigateur
- taille de l'écran
- fuseau horaire
- **système d'exploitation**

Tous ces éléments constituent l'**empreinte numérique** de ton navigateur.

Teste l'empreinte numérique de ton navigateur !

Pour tester ton empreinte numérique, utilise l'outil Panopticlick développé par l'**Electronic Frontier Foundation** (EFF) sur panopticlick.eff.org.

Navigateurs 3/4

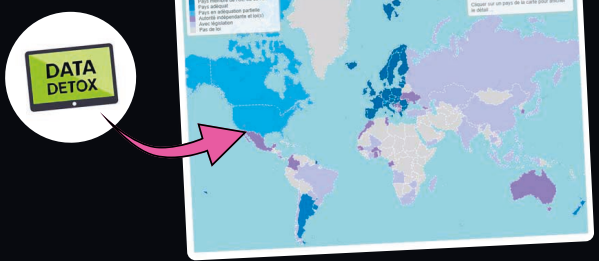
DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

PUIS-JE AVOIR ACCÈS AUX PROFILS QUI ONT ÉTÉ CRÉÉS SUR MOI PAR LES ENTREPRISES ?

Si tu habites dans l'Union Européenne, les entreprises doivent, si tu en fais la demande, te montrer les données qu'elles possèdent sur toi. C'est le principe du "**droit d'accès**" extrait du **Règlement Général sur la Protection des Données** (RGPD) qui s'applique depuis le 25 mai 2018.

En Suisse, le droit d'accès est régi par les articles 8 à 10 de la Loi Fédérale sur la Protection des Données (LPD). Cette dernière s'appuie sur le RGPD pour renforcer ses mesures.

Dans certains pays, il n'existe aucune loi visant à protéger les données personnelles. Utilise la tablette pour comparer les différences entre les législations des pays du monde.



La protection des données dans le monde

Dans quel pays transférer des données personnelles et à quelles conditions ? Quel pays dispose d'une législation spécifique ou d'une autorité de protection des données personnelles ?
Découvre la carte interactive tirée du site Internet de la Commission nationale de l'informatique et des libertés en France (CNIL).

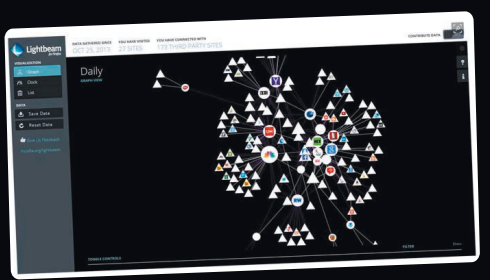
www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Navigateurs 4/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Ton navigateur te suit donc via les traqueurs des sites Internet que tu consultes. Il est grand temps de changer les règles du jeu et de pister les pisteurs avec l'outil **Lightbeam**.

Il s'agit d'une **extension** pour le navigateur Firefox qui permet de visualiser interactivement les requêtes vers les sites tiers, ainsi que les **cookies** déposés par ces derniers.



Il ne fait plus aucun doute que ton navigateur a besoin d'une cure de Data Detox ! Utilise la brochure de l'exposition pour suivre les exercices pratiques.

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Réseaux Sociaux

"JE LIKE DONC JE SUIS"

Incroyable mais vrai ! En moyenne, tu vas passer 5 ans et 4 mois de ta vie sur les réseaux sociaux*. A la fois plateformes d'échanges et lieux d'autopromotion, les réseaux sociaux sont devenus partie intégrante de la vie quotidienne. Mais cela peut avoir des répercussions, notamment sur l'utilisation qui est faite de tes données personnelles.

* BETC, Mediakix et bureau of labor statistics, 2016

Réseaux sociaux 1/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

QUELS SONT LES RÉSEAUX SOCIAUX LES PLUS UTILISÉS CHAQUE JOUR EN SUISSE ?

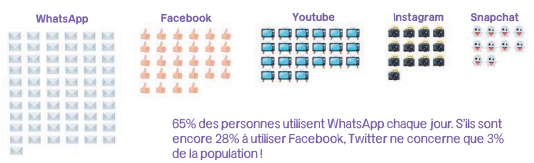
Facebook Snapchat Twitter WhatsApp Instagram Youtube Linkedin

QUELLES DONNÉES SONT RECOLTÉES PAR LES RÉSEAUX SOCIAUX ?

Les réseaux sociaux accumulent beaucoup d'informations sur toi, celles que tu donnes volontairement, mais aussi celles qui sont déductibles d'après ton comportement en ligne. Par exemple, le simple fait de liker un article ou de t'abonner à une page peut en dire long sur ta personnalité. Les réseaux sociaux étant des espaces d'expression personnelle, tu laisses beaucoup de traces te concernant : tes goûts et intérêts, les événements auxquels tu participes, tes photos, tes vidéos, les liens avec ton entourage, les lieux que tu fréquentes, etc. De plus, les réseaux sociaux savent quand et depuis où tu te connectes. Il est très difficile, voire impossible, d'utiliser un réseau social sans laisser de traces.

Top 5 des réseaux sociaux les plus utilisés*

*Utilisation quotidienne en Suisse sur 100 personnes de plus de 15 ans.



65% des personnes utilisent WhatsApp chaque jour. S'ils sont encore 28% à utiliser Facebook, Twitter ne concerne que 3% de la population !

Sondage IGEM digiMONITOR 2017

Réseaux sociaux 2/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

ON N'A QU'UNE SEULE FOIS LA CHANCE DE FAIRE UNE BONNE PREMIÈRE IMPRESSION

En janvier 2018, le parti politique "La République En Marche" d'Emmanuel Macron nomme un nouveau porte-parole, Rayan Nezzar. En acceptant cette fonction, le jeune homme devient un personnage public et suscite l'intérêt de personnes qui prennent le temps de scruter son compte Twitter. Rayan Nezzar avait publié des tweets injurieux à propos de journalistes et de personnes politiques françaises. Par exemple, celui-ci, datant de 2013 :

Ce tweet, visible par tous, est mis en lumière par plusieurs médias et devient viral. Bien que Rayan Nezzar le supprime de son compte, la nouvelle s'est déjà répandue. Quatre jours après sa prise de fonction, il est contraint de démissionner.

Et toi, as-tu publié certains contenus dont tu regrettes la teneur et qui sont toujours en ligne ? Si quelqu'un copie ou fait une capture d'écran d'une de tes publications, tu n'auras plus aucun contrôle sur ton propre contenu.

QUAND FACEBOOK A UNE MEILLEURE MÉMOIRE QUE TOI...

Les réseaux sociaux possèdent suffisamment d'informations sur toi pour te rappeler de bons ou de mauvais souvenirs. Par exemple, Facebook propose régulièrement de republier une photo ou une publication diffusée le même jour, un an, deux ans ou 10 ans auparavant.

Ces suggestions ne sont visibles que par l'utilisateur qui n'est pas obligé de les republier. As-tu vraiment envie qu'un tiers puisse te soumettre un souvenir que tu as peut-être toi-même oublié ou que tu ne souhaites plus te remémorer ?

Si tu as un compte Facebook...

Regarde quels souvenirs sont associés à ce jour sur ton compte : https://www.facebook.com/onthisday/

Facebook te permet de désactiver cette fonctionnalité et même de cacher des souvenirs liés à certaines personnes ou dates.

Réseaux sociaux 3/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

OUI, JE LE VEUX... VRAIMENT ?

Un simple clic pour finaliser l'inscription à un service et ça y est ! Tu as accepté les conditions d'utilisation de la plateforme, ainsi que la politique de confidentialité qui définit comment tes données vont être utilisées.

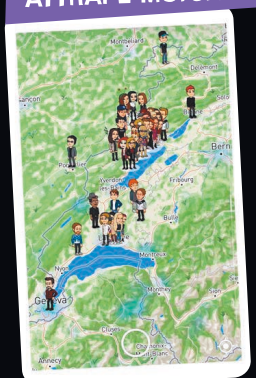
Lire entre les lignes

Qu'est-ce qui se cache derrière les conditions d'utilisation de tes réseaux sociaux préférés ? Découvre les clauses que tu acceptes sans t'en rendre compte au moment où tu cliques sur "**Accepter les conditions**".

Savais-tu par exemple qu'Instagram accède à toutes les photos que tu as sur ton smartphone, même celles que tu n'as pas publiées sur le réseau ?

Sur la tablette, choisis un des réseaux sociaux proposés, clique sur "Reveal" et tu verras les longs pavés de conditions d'utilisation fondre comme neige au soleil pour ne révéler que les informations essentielles.

ATTRAPE-MOI SI TU PEUX !



Snapchat est le réseau social qui pousse l'utilisation de ta géolocalisation le plus loin. As-tu déjà utilisé la fonctionnalité "carte" de Snapchat ? Depuis 2017, Snapchat sait où tu te trouves et partage cette information avec tous tes amis. Si tu ne veux pas être visible sur la carte, tu dois désactiver le champ "Partage des données liées à l'utilisation" dans les paramètres de ton application.

Lorsqu'on y réfléchit, l'application mise sur le sentiment d'appartenance : en voyant ce que tes amis sont en train de faire, tu te sens proche d'eux. Au contraire, en constatant que tes amis passent du temps ensemble sans t'inviter, cela peut vite devenir frustrant.

Réseaux sociaux 4/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

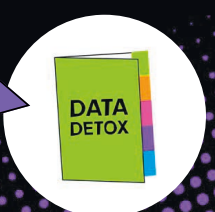
Avec l'entrée en vigueur du **RGPD**, tous les réseaux sociaux ont dû modifier leurs conditions d'utilisation et être plus transparents quant au traitement des **données personnelles**.

Par exemple, Facebook te permet désormais de télécharger l'ensemble des données liées à ton profil et de savoir, notamment, à qui elles ont été vendues.

En téléchargeant ces données, tu risques de découvrir que tu es véritablement fiché et que Facebook scrute tes faits et gestes pour établir un profil numérique qui te ressemble.

Pour télécharger toutes les données que Facebook possède sur toi, suis les instructions de la brochure de l'exposition.

Parmi les données stockées figure l'intégralité des conversations privées que tu as eues avec tes amis, même celles que tu as supprimées ou celles que tu as eues avec des contacts que tu as bloqués.



DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Solutions alternatives

TON KIT DE SURVIE

A ce stade, tu te sens peut-être un peu déconcerté d'avoir offert tes données à de grands groupes commerciaux.
Pas de panique, des alternatives existent !
Elles te permettront d'avoir accès aux mêmes fonctionnalités, tout en gardant la main sur tes données.

Solutions alternatives 1/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

GÉANTS DU WEB : INTOUCHABLES ?

Les géants du web sont tellement puissants et omniprésents dans le quotidien de milliards de citoyens que même les gouvernements semblent désemparés lorsqu'ils veulent lutter contre de telles entreprises. L'un de leurs seuls moyens de pression est de sanctionner financièrement de grands groupes, comme ce fut le cas pour Google en 2018 :

"En juillet 2018, l'Union Européenne a infligé à Google une amende record de 4,34 milliards d'euros dans le dossier antitrust Android. Cette sanction vise à pénaliser le géant pour abus de position dominante relative à Android, son **système d'exploitation** pour smartphone, afin d'asseoir l'hégémonie de son service de recherche en ligne."

"Bruxelles inflige une autre grosse amende à Google", L'Economiste, éd. 5318, 19.07.2018 consulté le 26.07.2018

LADY G.A.F.A.

As-tu déjà entendu parler des GAFA ou plus récemment GAFAM ? C'est le surnom que l'on donne aux géants du web qui monopolisent de manière tentaculaire les marchés.

G oogle
A mazon
F acebook
A pple
M icrosoft

DÉCENTRALISATION DU WEB : UNE SOLUTION ?

Au commencement, Internet était totalement décentralisé. Jusqu'au début des années 2000, la diversité et l'anonymat étaient de mise sur internet. De nos jours, face à l'hégémonie des géants du web, des associations engagées souhaitent proposer aux internautes un web plus libre et décentralisé.

Pour y parvenir, il faudrait que trois critères soient réunis :

1. Que les internautes soient conscients des dérives des géants du web
2. Que des alternatives viables existent
3. Que les internautes aient la possibilité de se former à l'utilisation de ces alternatives

Un exemple de décentralisation est la **blockchain**, une technologie permettant de stocker et transmettre de l'information grâce au **chiffrement**, que seuls l'expéditeur et le destinataire peuvent déchiffrer. Les **cryptomonnaies**, comme le Bitcoin, ont également pour objectif de rendre le web plus décentralisé.

Solutions alternatives 2/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

L'ARAIGNÉE QUI TISSE SA TOILE

Si les applications apparaissent comme des icônes distinctes sur l'écran de ton smartphone, elles peuvent appartenir au même groupe commercial. Par exemple, la plupart des applications de Google affichent clairement leur appartenance, quelle que soit la déclinaison : Google Chrome, Google Photos, Gmail, Google Drive, Google Map, etc. Mais sais-tu que Youtube appartient aussi à Google ?

En revanche, les liens entre les différentes applications que possède Facebook sont moins connus du grand public. Il s'agit notamment de Messenger, mais aussi d'Instagram et de WhatsApp. Facebook possède donc les outils qui sont utilisés tous les jours par au moins 61% de la population suisse.

POURQUOI IL DEVIENT URGENT DE TROUVER UNE SOLUTION...

Depuis un changement de conditions d'utilisation en 2016, WhatsApp peut transmettre les numéros de téléphone que tu utilises à Facebook afin, notamment, de te proposer de nouveaux amis. En tant qu'utilisateur, il n'existe pas de moyen de désactiver le transfert d'informations.

Mais le géant au pouce bleu ne s'arrête pas là. Il a dernièrement acquis "la startup Confirm.io, spécialisée dans l'authentification de documents d'identité officiels."

"Facebook va-t-il vérifier les pièces d'identité de ses utilisateurs ?", Anaïs Cherif, La Tribune, 24.01.2018, consulté le 26.07.2018

UNE JOURNEE SANS GOOGLE & FACEBOOK

Connais-tu quelqu'un qui a fait le choix de ne plus utiliser Facebook ? Pourquoi ne pas lui proposer de te parler des raisons qui l'ont poussé à prendre cette décision ?

Mets-toi au défi ! Dès maintenant et jusqu'à la fin de la journée, n'utilise plus Google, ni aucun de ses dérivés. Si tu es tenté de craquer, regarde quelles solutions alternatives sont disponibles sur les panneaux 3 et 4.

Autre scandale lié à Facebook et qui a fait couler beaucoup d'encre : l'affaire Cambridge Analytica. Cette entreprise "a récupéré, via un questionnaire psychologique auquel ont répondu 270'000 personnes, les données de millions de leurs amis en 2014. Cela a permis à la société britannique de constituer une précieuse base de données, avant d'être embauchée par l'équipe de campagne de Donald Trump."

"Cambridge Analytica a accédé aux données de 87 millions d'utilisateurs de Facebook, dont plus de 200 000 en France" France Info, 04.04.2018, consulté le 26.07.2018.

Solutions alternatives 3/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Il est temps de tester les solutions alternatives proposées par l'équipe de la Bibliothèque de l'EPFL ! Respectueuses de tes données personnelles, ces alternatives sont détaillées dans la brochure de l'exposition !

NAVIGATEURS
Alternatives à Google Chrome :
Firefox et **Tor Browser**

MOTEURS DE RECHERCHE
Alternatives à Google Search :
Duck Duck Go et **SearX**

MESSAGERIES ÉLECTRONIQUES
Alternatives à Gmail et Yahoo :
Protonmail et **Posteo**

CARTOGRAPHIE
Alternatives à Google Maps :
Open Street Map et **Framacarte**

RÉSEAUX SOCIAUX
Alternatives à Facebook et Twitter :
Diaspora et **Mastodon**

MESSAGERIES INSTANTANÉES
Alternatives à WhatsApp et Messenger :
Signal et **Wire**

ESPACES DE STOCKAGE
Alternatives à Google Docs et Dropbox :
SwitchDrive et **OwnCloud**

Solutions alternatives 4/4

DATA DETOX
Une exposition de la Bibliothèque de l'EPFL

Cette exposition a-t-elle éveillé en toi le souhait de reprendre le contrôle de tes **données personnelles** ? Pour aller plus loin, regarde les vidéos diffusées sur la télévision de l'exposition. Tu pourras notamment visionner la conférence TED du journaliste Glenn Greenwald sur "L'importance de la vie privée".

Emporte la brochure de l'exposition chez toi et fais une cure de Data Detox à ton rythme ! Tu y retrouveras toutes les solutions alternatives proposées dans l'exposition, avec de plus amples explications sur chacune d'elles.

Bravo ! Tu viens de prendre conscience des dérives qui peuvent être faites avec tes données sur Internet.

Il est souvent difficile de changer ses habitudes. Prends donc ton temps pour t'adapter aux nouveaux outils et modifier ta manière de naviguer sur Internet.

Et n'hésite pas à contacter la Bibliothèque si tu as des questions ou besoin d'aide !

ANNEXE 7

Rodriguez Tina (SEC-GC)

De: communication <comm@educanet2.ch>
Envoyé: jeudi 29 novembre 2018 14:12
À: Avenir educanet²
Objet: Première information: la plateforme educanet² ne sera plus proposée à partir du 31.12.2020

Chères directrices d'école,
Chers directeurs d'école,
Mesdames et Messieurs,

educa.ch exploite la plateforme d'enseignement, d'apprentissage et de communication educanet² sur mandat de la Confédération et des cantons. Cette plateforme a été lancée en 2004 dans le cadre du Serveur suisse de l'éducation (SSE) comme produit destiné à remplacer educanet (version 1). educanet² est mise gratuitement à disposition des écoles publiques en Suisse. Le financement est assuré à parts égales entre la Confédération et les cantons.

Depuis l'introduction d'educanet², l'offre pour les plateformes de collaboration s'est fortement développée, de sorte qu'une multiplicité d'alternatives similaires est utilisée actuellement dans les écoles. Cela se traduit par une tendance à la baisse du nombre d'utilisateurs d'educanet². Dans cette situation, le passage à un modèle financé par l'utilisateur s'impose. Comme educanet² ne peut, par ailleurs, pas répondre aux demandes croissantes de solutions sur mesure, educa.ch a décidé de ne plus proposer la solution d'educanet² au niveau national à partir du 31 décembre 2020. La fermeture de la plateforme se déroulera dans un processus ordonné avec la participation des cantons et des écoles.

educa.ch analysera les besoins, répondra aux défis et développera avec tous les acteurs impliqués des solutions au cours des deux prochaines années. educa.ch soutient en particulier les écoles en menant des négociations avec divers fournisseurs et en concluant des contrats-cadre. Avec ces contrats, educa.ch crée les conditions préalables à l'utilisation des services en ligne dans le respect de la réglementation sur la protection des données. Les écoles peuvent profiter de conditions contractuelles spécifiques applicables au domaine de l'éducation en Suisse. Des contrats-cadre existent actuellement avec Microsoft et Univention. D'autres contrats sont prévus pour le printemps avec des fournisseurs comme Apple, Google et aussi DigiOnline (développeur d'educanet²).

Nous vous informerons régulièrement sur le site web www.educanet2.ch, ainsi que par ce canal de courrier électronique, des mesures de soutien et d'orientation prévues et mises en œuvre.

Nous sommes à votre disposition via support@educa.ch pour toute question.

Avec nos meilleures salutations

educa.ch
Institut suisse des médias pour la formation et la culture coopérative | Schweizer Medieninstitut für Bildung und Kultur Genossenschaft

Erlachstrasse 21 | 3012 Berne | SUISSE
Téléphone +41 31 300 55 00 | Fax +41 31 300 55 01

comm@educanet2.ch | www.educa.ch

Google for Education

Contrat G Suite for Education

Le présent Contrat G Suite for Education (le "**Contrat**") est établi par et entre Google Ireland Limited, une société de droit irlandais, dont le siège est sis Gordon House, Barrow Street, Dublin 4, Irlande ("**Google**") et le client identifié dans le Bon de commande ("**Client**"). Le présent Contrat entre en vigueur à la date à laquelle le Client clique sur le bouton "J'accepte" ci-dessous ou, le cas échéant, la date à laquelle le Contrat est contresigné (la "**Date d'entrée en vigueur**"). Si vous acceptez les conditions pour le compte du Client, vous déclarez et garantissez que : (i) vous disposez de la pleine capacité juridique de lier votre employeur ou l'entité concernée aux présentes conditions générales ; (ii) vous avez lu et compris le présent Contrat ; et (iii) vous acceptez le présent Contrat pour le compte de la partie que vous représentez. Si vous n'avez pas la capacité juridique d'engager le Client, veuillez ne pas cliquer sur le bouton "J'accepte" ci-dessous (ou, le cas échéant, veuillez vous abstenir de signer le présent Contrat). Le présent Contrat régit l'accès aux Services et leur utilisation par le Client, et prendra effet à la Date d'entrée en vigueur.

1. **Services**.

1.1 Généralités. Google fournira les Services conformément au présent Contrat et au SLA. Google fournira au Client un Compte Administrateur à utiliser pour administrer les Comptes d'Utilisateur final et d'autres fonctionnalités des Services. Le Client devra (a) administrer les Comptes d'Utilisateur final en se servant de la Console d'administration et des Outils d'administration ; et (b) déterminer les Services à fournir aux Utilisateurs finaux.

1.2 Modifications

a. Des Services. Google peut apporter des modifications commercialement raisonnables aux Services de temps à autre. Si Google apporte des modifications significatives aux Services, Google en informera le Client via toute méthode choisie par Google, à condition que le Client ait souscrit auprès de Google l'option permettant d'être informé de ces modifications significatives.

b. Des Conditions d'utilisation des URL. Google peut occasionnellement effectuer des modifications commercialement raisonnables des Conditions d'utilisation des URL. Si Google apporte des modifications significatives aux Conditions d'utilisation des URL, Google en informera le Client, soit en envoyant un e-mail à l'Adresse e-mail de notification ou en alertant le Client via la Console d'administration. Si les modifications ont une incidence négative importante sur le Client et que ce dernier ne consent pas à ces modifications, le Client doit en informer Google via le Centre d'assistance dans les trente (30) jours suivant la réception de l'avis de modification. Si le Client transmet la notification nécessaire à Google, il continuera d'être régi par les conditions en vigueur immédiatement avant les modifications, jusqu'à l'expiration des Conditions des Services alors en vigueur. Si les Services sont renouvelés, ils le seront aux Conditions d'utilisation des URL de Google alors en vigueur.

c. Interruption des Services. Sous réserve de la Clause 1.2(d), Google peut interrompre tous Services, toute(s) portion(s) ou fonctionnalité(s) des Services à tout moment, pour quelque motif que ce soit, sans en répondre au Client.

d. Politique de Dépréciation. Google informera le Client s'il compte effectuer une Dépréciation significative. Google mettra en œuvre les efforts raisonnables afin de continuer à fournir les Services sans Dépréciation Significative pendant au moins un an après cette notification, à moins que (comme Google le détermine de bonne foi et en exerçant un jugement raisonnable) : (i) il en soit interdit par la loi ou par contrat (y compris en cas de modification de la loi ou du contrat applicable) ; ou que (ii) cela crée un risque pour la sécurité ou un fardeau économique ou technique substantiel.

Cette politique est la "Politique de Dépréciation".

1.3 Alias. Le Client est seul responsable du suivi, de la réponse à, et autrement du traitement des e-mails envoyés aux alias "abuse" et "postmaster" pour le ou les Noms de domaine du Client. Le Client accepte que Google puisse contrôler les e-mails envoyés à ces alias pour le ou les Noms de domaine du Client pour permettre à Google d'identifier les abus de Services.

1.4 Publicité. Nonobstant toute autre condition du Contrat, Google ne traitera pas les Données du client à des fins de Publicité et ne proposera pas de Publicité dans le cadre des Services.

1.5 Comptes d'Utilisateur final. Le Client pourra demander des Comptes d'Utilisateurs finaux supplémentaires pendant la Durée en s'adressant à son Gestionnaire de compte Google désigné ou au personnel de support de Google ou au Revendeur (le cas échéant). Pour chaque achat de Comptes d'Utilisateurs finaux supplémentaires pendant la Durée, Google ou le Revendeur (le cas échéant) et le Client signeront un Bon de commande supplémentaire reflétant l'achat.

1.6 Google Vault. Si le Client utilise Google Vault, Google conservera les Données du Client concernées et archivées pour la période retenue dans les Services par l'Administrateur, mais uniquement si le Client renouvelle Google Vault pour la totalité de la période de rétention. Si les Services Google Vault expirent ou sont résiliés conformément aux modalités du Contrat, l'obligation de Google de conserver les Données du Client archivées prendra immédiatement fin.

2. **Traitement des données ; Sécurité.**

2.1 Avenant relatif au Traitement des données. L'Avenant relatif au Traitement des données prévoit les droits et obligations des parties en relation avec le traitement et la sécurité des données des Clients dans le cadre du présent Contrat, et les parties se conformeront à l'Avenant relatif au Traitement des données. De plus, il pourra être demandé au Client d'accepter l'Avenant relatif au Traitement des données via les Services uniquement pour des raisons techniques ou fonctionnelles, mais une telle acceptation n'affectera en rien les droits ou obligations des parties telles que décrites à la Clause 2 de l'Avenant relatif au Traitement des données.

2.2 Mises à jour de l'Avenant relatif au Traitement des données. Sous réserve des Clauses 1.2(a) et 1.2(b), Google peut uniquement mettre à jour ou modifier l'Avenant relatif au traitement des données :

(a) lorsque la modification concernée est nécessaire pour se conformer au droit applicable, à une réglementation applicable, une ordonnance judiciaire ou des directives applicable émise par une autorité administrative indépendante ou une administration ;

(b) lorsque la modification concernée est expressément autorisée par les conditions de l'Avenant relatif au Traitement des données ; ou

(c) lorsque la modification concernée :

(i) est commercialement raisonnable ;

(ii) n'entraîne pas une dégradation de la sécurité générale des Services ;

(iii) n'étend pas la portée, ni ne supprime de restrictions dans le traitement des Données du Client par Google, tel que décrit à la Clause 5 (Traitement des Données du Client) de l'Avenant relatif au Traitement des données ; et

(iv) ne nuit pas de manière significative aux droits du Client au titre de l'Avenant relatif au Traitement des Données.

Si Google effectue des modifications significatives à l'Avenant relatif au Traitement des données conformément à la présente Clause 2.2, Google en informera le Client à l'Adresse électronique de notification ou via la Console d'administration.

3. **Obligations du Client.**

3.1 Conformité. Le Client veillera à ce que le Client et les Utilisateurs finaux utilisent les Services conformément à la Politique d'utilisation autorisée. Google peut occasionnellement mettre à disposition de nouvelles applications, options ou fonctionnalités disponibles via les Services, et dont l'utilisation peut être soumise à l'acceptation par le Client de conditions supplémentaires. En outre, Google mettra à disposition du Client et de ses Utilisateurs finaux d'autres Services complémentaires (outre les Services), conformément aux Conditions d'utilisation supplémentaires des Services complémentaires et aux conditions de services applicables de Google spécifiques aux produits. Si le Client ne souhaite pas activer de Services complémentaires, il peut choisir d'activer ou de désactiver (selon le cas) les Services complémentaires (ou l'un d'entre eux) à tout moment via la Console d'administration. Le Client accepte que son utilisation des API soit soumise aux Conditions d'utilisation des API.

3.2 Administration des Services par le Client. Le Client peut désigner un ou plusieurs Administrateurs, par le biais de la Console d'administration, qui disposeront des droits d'accès au(x) Compte(s) Administrateur afin d'administrer les Comptes d'Utilisateur final. Il appartient au Client : (a) d'assurer la confidentialité du mot de passe et du ou des Comptes Administrateur ; (b) de désigner les personnes qui disposent d'un accès autorisé au(x) Compte(s) Administrateur ; (c) de veiller à ce que toutes les activités effectuées en relation avec le ou les Comptes Administrateur soient conformes au présent Contrat. Le Client reconnaît et accepte que Google n'est pas responsable de la gestion ou administration interne du système de messagerie ou des messages électroniques du Client.

3.3 Revendeur agissant en tant qu'Administrateur. Si le Client commande des Services par l'intermédiaire d'un Revendeur, ce dernier peut disposer d'un accès Administrateur au Compte du client et à ceux de ses Utilisateurs finaux. Pour ce qui ressort de la relation entre Google et le Client, le Client est seul responsable de : (i) tout accès par le Revendeur au Compte du Client et à ceux de ses Utilisateurs finaux ; et (ii) la définition dans le Contrat de revente de tout droit ou obligation existant entre le Revendeur et le Client au regard de cet accès et de ces Services.

3.4 Consentement de l'Utilisateur final. Les Administrateurs du Client ont la capacité d'accéder à, de contrôler, d'utiliser ou de divulguer des données disponibles aux Utilisateurs finaux dans les Comptes d'Utilisateur final via la Console d'administration et/ou les Outils d'administration. Le Client obtiendra et gérera tous les consentements nécessaires de la part des Utilisateurs finaux pour autoriser : (a) ces accès, contrôle, utilisation et divulgation du Client ; et (b) Google à fournir les Services conformément au présent Contrat. Le Client reconnaît et accepte que le Revendeur peut divulguer les données personnelles des Utilisateurs finaux à Google dans la mesure de ce qui est raisonnablement nécessaire pour que le Revendeur puisse traiter des questions relatives à l'assistance que le Client peut choisir de faire remonter à ou via le Revendeur.

3.5 Utilisation non autorisée. Le Client emploiera tout effort raisonnable pour prévenir et faire cesser toute utilisation non autorisée des Services. Le Client notifiera rapidement Google en cas d'utilisation ou d'accès non autorisé aux Services dont il aura connaissance.

3.6 Restrictions d'utilisation. Sous réserve de ce qui est expressément permis dans le présent Contrat ou convenu autrement par Google par écrit, le Client s'abstiendra, et il déploiera tous les efforts raisonnables pour s'assurer que tout tiers s'abstienne de : (a) vendre, revendre, louer les Services à un tiers, ou de

procéder à une opération fonctionnelle équivalente ; (b) tenter de pratiquer de l'ingénierie inverse sur les Services ou tout composant de ceux-ci sous réserve de ce que la loi autorise ; (c) tenter de créer un service de substitution ou équivalent au moyen de l'accès aux Services ou de leur utilisation ; (d) utiliser les Services pour des Activités à haut risque ; ou (e) utiliser les Services pour stocker des Données du client qui font l'objet de contrôles à l'exportation au titre des Lois relatives au contrôle des exportations.

3.7 Demandes de tiers. Il incombe au Client de répondre aux Demandes de tiers. Google devra, dans la mesure permise par la loi et conformément aux conditions de la Demande de tiers : (a) informer rapidement le Client de la réception d'une Demande de tiers ; (b) fournir au Client les informations ou les outils nécessaires pour répondre à la Demande de tiers. Le Client cherchera tout d'abord à obtenir les informations nécessaires pour répondre à la Demande de tiers de sa propre initiative, et contactera Google uniquement s'il ne peut pas raisonnablement obtenir ces informations.

3.8 Utilisations autorisées. L'utilisation des Services est autorisée uniquement si elle est le fait (a) d'institutions pédagogiques à but non lucratif ; et (b) d'autres entités à but non lucratif (tel que défini dans la loi en vigueur).

4. **Paiement.**

4.1 Commandes par l'intermédiaire d'un Revendeur. Si le Client commande les Services par l'intermédiaire d'un Revendeur : a) tous les paiements seront effectués directement au Revendeur conformément au Contrat de revente ; b) les dispositions restantes de la présente Clause 4 (Paiement) ne s'appliqueront pas ; c) Google versera au Revendeur tout remboursement ou crédit dû au regard du Client, et d) toute obligation pesant sur le Revendeur de verser au Client un tel remboursement ou un tel crédit dépendra des conditions du Contrat de revente.

4.2 Commandes directes Sauf indication contraire dans un Bon de commande ou une facture applicables, le Client paiera à Google les frais correspondant aux Services, tel qu'énoncé dans le Bon de commande applicable ("**Frais**"). Tout Frais est payable dans les 30 jours suivant la date de la facture. Tous les paiements dus doivent s'effectuer dans la devise indiquée sur la facture. Les paiements effectués par virement doivent prendre en compte les instructions de virement énoncées dans la facture.

4.3 Retards de paiement Google pourra demander à tout moment le paiement d'intérêts sur tout Frais impayé du au titre des Services au taux de 2 % par an au-dessus du taux de base de la Barclays Bank PLC en vigueur, courant à compter de la date d'échéance jusqu'à la date du paiement effectif, que ce soit avant ou après tout jugement. Il incombera au Client de supporter toutes les dépenses raisonnables (y compris les frais juridiques) engagées par Google aux fins de recouvrer les sommes échues et impayées, sauf dans les cas où ces sommes échues et impayées résultent d'inexactitudes de facturation de Google.

4.4 Contestations de factures Il devra être fait état de tout litige concernant une facture avant l'échéance de la facture. Si les parties déterminent que certaines inexactitudes de facturation sont imputables à Google, Google n'émettra pas de facture corrigée, mais émettra à la place une note de crédit précisant le montant incorrect de la facture affectée. Si la facture contestée n'a pas encore été réglée, Google créditera le montant dans la facture contestée et le Client sera tenu de régler le solde net résultant exigible au titre de cette facture.

4.5 Bons de commande Les parties acceptent qu'aucune des conditions générales d'un quelconque bon de commande émis par le Client ne pourra s'appliquer au présent Contrat ou le modifier, et que toutes les conditions générales dudit bon de commande seront nulles et non avenues.

4.6 Taxes Le Client est responsable de toutes les taxes et paiera à Google les Services toutes taxes comprises. Si Google est obligée de percevoir ou de payer des Taxes, lesdites Taxes seront facturées au Client, sauf si le Client fournit à Google un certificat d'exonération fiscale en cours de validité émanant de

l'autorité fiscale concernée.

5. **Services d'assistance technique.**

5.1 Par le Client. Le Client répondra, à ses propres frais, aux questions et aux réclamations des Utilisateurs finaux ou des tiers liées à l'utilisation des Services par le Client ou les Utilisateurs finaux. Le Client mettra en oeuvre tout effort raisonnable pour résoudre les questions d'assistance avant de les faire remonter à Google conformément à la Clause 5.2.

5.2 Par Google. Si le Client n'est pas en mesure de résoudre une question d'assistance conformément à la Clause 5.1 ci-dessus, alors le Client pourra faire remonter la question à Google conformément aux Instructions SAT. Google y répondra conformément aux Instructions SAT.

6. **Suspension**.

6.1 Des Comptes d'Utilisateur final par Google. Si Google prend connaissance d'une utilisation d'un Compte d'Utilisateur final non conforme au présent Contrat, alors Google pourra demander spécialement à ce que le Client suspende le Compte d'Utilisateur final concerné. Si le Client ne répond pas à la demande de Google de suspendre un Compte d'Utilisateur final, alors Google pourra procéder lui-même à ladite Suspension. La Suspension restera active jusqu'à ce que l'Utilisateur final concerné ait remédié à la violation ayant entraîné la Suspension.

6.2 Problèmes urgents de sécurité. Nonobstant la Clause 6.1 ci-dessus, en cas de Problème urgent de sécurité, Google peut suspendre les Comptes d'Utilisateur final concernés. La portée de la Suspension sera la plus faible possible, et sa durée la plus courte possible, afin d'empêcher ou de mettre fin au Problème urgent de sécurité. Si Google suspend un ou des Comptes d'Utilisateur final sans préavis adressé au Client, sur demande du Client alors, Google fournira une estimation de la durée probable de la Suspension et la raison de ladite Suspension dans les plus brefs délais.

6.3 Suspension pour non-paiement et retard de paiement. Dès la première date à laquelle le paiement de Frais dus par le Client est en retard, le Compte de ce dernier pourra être suspendu jusqu'au paiement complet des arriérés.

6.4 Suspension pour se conformer à la Loi. Google peut suspendre la fourniture de tout Service à tout moment si Google estime, à sa seule discrétion, que cela est nécessaire pour se conformer au droit applicable.

7. **Informations confidentielles.**

7.1 Protection des Informations confidentielles. La partie destinataire ("la Partie Destinataire") d'Informations confidentielles communiquées par l'autre partie (la "Partie Divulgatrice") ne communiquera pas lesdites informations, sauf si la Clause 7.2 le prévoit (Divulgation d'Informations confidentielles). La Partie Destinataire n'utilisera les Informations confidentielles reçues de la Partie Divulgatrice que pour exercer les droits et remplir les obligations énoncés dans le présent Contrat, tout en exerçant une diligence raisonnable pour en préserver la confidentialité.

7.2 Divulgation des Informations confidentielles.

(a) Généralités. Sous réserve des autres dispositions de la présente Clause 7.2, les Informations confidentielles de la Partie Divulgatrice peuvent être divulguées : (i) par la Partie Destinataire à ses Affiliés, au Revendeur (le cas échéant), à ses employés, mandataires, sous-traitants ou conseillers professionnels qui en ont besoin et qui ont l'obligation légale d'en préserver la confidentialité (collectivement, les "Délégués") ; (ii) par la Partie Destinataire ou ses Affiliés dans le cadre d'un Recours juridique ; ou (iii) avec l'accord écrit de la Partie Divulgatrice. La Partie Destinataire veillera à ce

que ses Délégués soient soumis aux mêmes obligations de non-divulgation et d'utilisation qui s'appliquent à lui en vertu de la Clause 7.1 (Protection des Informations confidentielles).

(b) Notification. Avant la divulgation des Informations confidentielles de la Partie Divulgatrice suite à un Recours juridique tel que décrit à la Clause 7.2(a), la Partie Destinataire devra notifier sans délai la Partie Divulgatrice, ou s'assurer que son Affilié le fasse (via l'Adresse électronique de notification, en cas de notifications faites par Google), sous réserve cependant que la Partie Destinataire ou son Affilié puisse divulguer les Informations confidentielles de la Partie Divulgatrice dans le cadre d'un Recours juridique sans préavis si la Partie Destinataire ou son Affilié sont informés que (i) il leur est légalement interdit d'en donner préavis ou (ii) le Recours juridique implique des circonstances exceptionnelles impliquant un danger de mort ou de blessures graves pour quelqu'un.

7.3 Opposition. La Partie Destinataire se conformera aux demandes raisonnables de la Partie Divulgatrice concernant les efforts visant à s'opposer à la divulgation de ses Informations confidentielles.

8. **Droits de Propriété intellectuelle ; Signes distinctifs**

8.1 Droits de propriété intellectuelle. Aucune partie n'acquerra de droit, titre ou intérêt dans les droits de propriété intellectuelle appartenant à l'autre partie ou aux concédants de licence de l'autre partie, sous réserve de stipulations contraires explicites dans le présent Contrat. Pour ce qui ressort de la relation entre les parties, le Client détient l'ensemble des Droits de propriété intellectuelle portant sur les Données du Client et Google détient l'ensemble des Droits de propriété intellectuelle portant sur les Services.

8.2 Affichage des Signes distinctifs. Google peut uniquement afficher les Signes distinctifs du Client autorisés par le Client (cette autorisation est fournie par le Client du fait du téléchargement de ses Signes distinctifs dans les Services) à l'intérieur des zones désignées des Pages de Services. Le Client peut spécifier la nature de cette utilisation en utilisant la Console d'administration. Google peut également afficher les Signes distinctifs Google sur les Pages de Services pour indiquer que les Services sont fournis par Google. Aucune partie ne peut afficher ou utiliser les Signes distinctifs de l'autre partie, sauf si le présent Contrat l'autorise expressément, sans le consentement préalable écrit de l'autre partie.

8.3 Limite relative aux Signes distinctifs. L'intégralité des acquisitions provenant de l'utilisation par le Client des Signes distinctifs de Google appartient à Google. Une partie peut révoquer le droit de l'autre partie à utiliser ses Signes distinctifs conformément au présent Contrat moyennant un avis écrit fourni dans un délai raisonnable.

9. **Garanties.**

9.1 Garanties. Chaque partie déclare qu'elle fera preuve de la diligence et de la compétence raisonnables pour respecter ses obligations dans le cadre du présent Contrat.

9.2 Exclusion de responsabilité. Par les présentes, Google décline toutes conditions, garanties ou autres clauses relatives à tout Service ou tout autre bien ou service ou toutes informations fournis par Google dans le cadre du présent Contrat, sous réserve que ces conditions, garanties ou clauses soient expressément prévues dans le présent Contrat. Par souci de clarté, et sous réserve de la Clause 13.1(b), aucune condition, garantie ou autre clause implicite ne s'appliquera, y compris aucune condition implicite relative à la qualité satisfaisante, l'adaptation à un usage particulier ou la conformité à la description. Le Client reconnaît que les Services ne constituent pas un substitut aux services de téléphonie et que les Services ne sont pas capables d'émettre ou de recevoir

des appels, notamment des appels d'urgence, sur des réseaux téléphoniques publics commutés.

10. **Durée ; Absence de Frais.**

10.1 Durée. Le présent Contrat débutera à la Date d'entrée en vigueur et continuera jusqu'à la fin de la dernière Période de Services, sauf résiliation anticipée conformément à ses clauses ("Durée").

10.2 Période de Services et Achats pendant la Période de Services. Google fournira les Services au Client pendant la Période de Services. Sauf accord contraire des parties par écrit, les Comptes d'Utilisateur final ajoutés pendant des Périodes de Services auront une durée calculée au prorata prenant fin le dernier jour de cette Période de Services.

10.3 Renouvellement automatique. À la fin de la Période de Services, les Services (et l'ensemble des Comptes d'Utilisateur final précédemment commandés) seront automatiquement renouvelés pour une Période de Services supplémentaire de douze (12) mois. Si l'une ou l'autre partie ne souhaite pas le renouvellement des Services, elle doit le notifier à l'autre partie par écrit au moins quinze (15) jours avant la fin de la Période de Services alors en vigueur. Cet avis de non-renouvellement prendra effet au terme de la Période de Services alors en vigueur.

10.4 Frais. Pendant la Période de Services initiale, Google ne facturera au Client aucun Frais pour les Services (autre que le paiement du stockage, le cas échéant). Moyennant l'accord mutuel écrit des parties, (a) Google peut facturer au Client des Frais pour les Services après la Période de Services initiale et (b) Google peut facturer au Client des Frais pour une version premium des Services ou pour une fonctionnalité en option ou des améliorations pouvant être ajoutés aux Services par Google (comme le stockage payé, le cas échéant).

10.5 Révision des tarifs. Pour des Services que le Client a achetés contre des Frais, Google peut réviser ses tarifs pour la Période de Services suivante moyennant un avis écrit adressé au Client (qui peut être envoyé par e-mail) au moins trente (30) jours avant le début de la Période de Services suivante.

11. **Résiliation.**

11.1 Résiliation pour juste motif. L'une ou l'autre partie peut suspendre la mise en œuvre et/ou résilier le présent Contrat (y compris l'ensemble des Bons de commande signés au titre du présent Contrat), avec effet immédiat, si l'autre partie : (a) commet une violation grave du présent Contrat et qu'il ne peut être remédié à cette violation ; (b) commet une violation grave du présent Contrat deux fois ou plus, qu'il soit ou non possible d'y remédier ; ou (c) commet une violation grave du présent Contrat et qu'il peut être remédié à cette violation, mais qu'il n'y remédie pas dans les trente (30) jours après avoir reçu un avis écrit lui notifiant ladite violation.

11.2 Résiliation en cas d'insolvabilité. Sauf en cas d'interdiction prévue par le droit applicable, chaque partie peut résilier le présent Contrat immédiatement après notification écrite si l'autre partie ne peut pas payer ses dettes à échéance, conclut un accord ou une entente avec ses créanciers ou à leur profit, est placée en redressement ou en liquidation judiciaire, est déclarée en faillite ou en cessation de paiement ou est dissoute ou cesse autrement ses activités. Si Google a le droit de résilier le présent Contrat en vertu de la présente Clause, Google peut également suspendre ou résilier tout ou partie des Services tant que ce droit de résiliation s'appliquera.

11.3 Changement de contrôle. L'une ou l'autre partie peut résilier le présent Contrat immédiatement moyennant un avis écrit en cas de Changement de contrôle de l'autre partie, autrement que dans le cadre d'une restructuration ou réorganisation interne de ses Sociétés du Groupe. Dans cette clause, le terme "contrôle" désigne la détention par une ou plusieurs personnes, directement ou indirectement, du pouvoir de donner une instruction ou de faire que des

instructions soient données à une autre personne et "Changement de contrôle" s'interprète en conséquence. La partie qui subit ledit Changement de contrôle en informera l'autre partie par écrit dans les trente (30) jours suivant le Changement de contrôle. Si la partie qui résilie n'a pas exercé son droit de résiliation au titre de la présente clause dans les trente (30) jours suivant la réception de l'avis de Changement de contrôle de l'autre partie, ce droit de résiliation expirera.

11.4 Résiliation liée aux Lois anti-corruption. Google pourra résilier immédiatement le présent Contrat après notification écrite au Client, si Google estime de bonne foi que celui-ci a enfreint, ou a causé la violation par Google d'une quelconque Loi anti-corruption, ou qu'une telle violation est raisonnablement susceptible de se produire.

11.5 Autre résiliation. Le Client peut résilier le présent Contrat pour tout motif (ou sans motif) moyennant un préavis écrit de trente (30) jours remis à Google, à condition toutefois que le Client reste tenu de payer tout Frais au titre des Services qu'il a achetés et applicable au reste de la Période de Services alors en vigueur pour ces Services.

11.6 Effets de la Résiliation. En cas de résiliation ou d'expiration du présent Contrat, alors : (a) les droits accordés par une partie à l'autre cesseront dès la date d'effet de la résiliation ou de l'expiration (sous réserve de ce qui est prévu à la présente Clause 11 et à la Clause 15.15 (Survie)) ; (b) le Client n'aura pas accès aux Données du Client, ni la capacité de les exporter, après la date d'effet de la résiliation ou de l'expiration du Contrat et devra utiliser la fonctionnalité des Services pour supprimer toutes les Données du Client des Services avant cette date ; (c) suite à cette suppression des Données du Client, Google supprimera les Données du Client comme cela est décrit dans l'Avenant relatif au Traitement des données ; et (d) sur demande, chaque partie déploiera sans délai tous les efforts raisonnables pour restituer ou détruire les Informations confidentielles de l'autre partie (à l'exclusion des Données du Client).

12. **Indemnisation.**

12.1 Si le Client reçoit une réclamation émanant d'un tiers alléguant que la technologie de Google ou d'un Affilié Google utilisée pour fournir les Services ou un Signe distinctif de Google enfreignent des droits d'auteur, un secret commercial ou une marque déposée dudit tiers ("Revendication de droits de propriété intellectuelle"), le Client : (a) le notifiera immédiatement à Google ; (b) fournira à Google des informations, une assistance et une coopération raisonnable pour répondre à et, le cas échéant, se défendre contre ladite Revendication de droits de propriété intellectuelle ; et (c) donnera à Google un plein contrôle et une autorité entière sur la défense et le règlement relatifs à ladite Revendication de droits de propriété intellectuelle.

12.2 À condition que le Client respecte la Clause 12.1 et sous réserve de la Clause 12.3, Google acceptera le plein contrôle et l'autorité entière sur la défense et le règlement de ladite Revendication de droits de propriété intellectuelle et indemnisera le Client contre tous dommages-intérêts et frais octroyés au titre de ladite Revendication de droits de propriété intellectuelle, et frais de règlement approuvés par écrit par Google en lien avec ladite Revendication de droits de propriété intellectuelle, ainsi que les honoraires raisonnables d'avocat nécessaires payés par le Client en lien avec ladite Revendication de droits de propriété intellectuelle et les frais raisonnables nécessaires encourus par le Client pour se conformer à la Clause 12.1(b).

12.3 Google n'aura aucune obligation ou responsabilité au titre de la présente Clause 12 en lien avec une Revendication de droits de propriété intellectuelle découlant de : (a) l'utilisation des Services ou des Signes distinctifs de Google en violation du présent Contrat, sous une forme modifiée ou de façon combinée avec des produits de tiers ; et/ou (b) tous contenus, informations ou données fournis à Google par le Client, les Utilisateurs finaux ou tout autre tiers.

12.4 Google peut (à son entière discrétion) suspendre l'utilisation par le Client de tout Service dont Google prétend ou croit qu'il viole les Droits de propriété intellectuelle d'un tiers, ou modifier ces Services afin de les rendre conformes. Si la possibilité qui précède n'est pas raisonnable d'un point de vue commercial, Google peut suspendre ou résilier l'utilisation par le Client des Services impactés. Si une quelconque suspension relevant de la présente clause doit se

prolonger plus de trente (30) jours, le Client pourra, à tout moment et jusqu'à ce que l'utilisation des Services concernés soit rétablie, résilier le présent Contrat immédiatement moyennant un avis écrit. Si les Services sont résiliés conformément à la présente Clause 12.4, alors Google fournira un remboursement au prorata des Frais applicables pour la période consécutive à la résiliation des Services soit au Revendeur (si le Client a commandé les Services auprès du Revendeur) soit au Client (si le Client a commandé les Services directement auprès de Google).

12.5 Si Google reçoit une réclamation d'un tiers indiquant que les Données, le ou les Noms de domaine et/ou les Signes distinctifs du Client enfreignent des Droits de propriété intellectuelle dudit tiers (une "Revendication de droits de propriété intellectuelle contre le Client"), Google : (a) le notifiera rapidement au Client ; (b) fournira au Client des informations, une assistance et une coopération raisonnables pour répondre à et, le cas échéant, se défendre contre ladite Revendication de droits de propriété intellectuelle contre le Client ; et (c) donnera au Client un plein contrôle et une autorité entière sur la défense et le règlement relatifs à ladite Revendication de droits de propriété intellectuelle contre le Client. Google peut désigner, à ses propres frais, son propre avocat principal, à ses propres frais.

12.6 À condition que Google respecte la Clause 12.5, le Client acceptera le plein contrôle et l'autorité entière sur la défense et le règlement de ladite Revendication de droits de propriété intellectuelle contre le Client et indemnisera Google contre tous dommages-intérêts et frais octroyés au titre de ladite Revendication de droits de propriété intellectuelle, et frais de règlement approuvés par écrit par le Client en lien avec ladite Revendication de droits de propriété intellectuelle, ainsi que les honoraires raisonnables d'avocat nécessaires payés par Google en lien avec ladite Revendication de droits de propriété intellectuelle et les frais raisonnables nécessaires encourus par Google pour se conformer à la Clause 12.5(b).

13. **Limitation de responsabilité.**

13.1 Aucune disposition du présent Contrat ne peut exclure ou limiter la responsabilité de l'une des parties en cas de : (a) décès ou dommages corporels résultant de la négligence de l'une des parties ou de ses fonctionnaires, agents ou employés ; (b) fraude ou fausse déclaration ; (c) violation de toute condition prévue concernant le titre de propriété ou la jouissance paisible ; ou (d) utilisation abusive des Informations confidentielles.

13.2 Sauf disposition contraire figurant explicitement dans le présent Contrat, rien dans le présent Contrat n'exclut ou ne limite la responsabilité de chacune des parties au sens de la Clause 12 (Indemnités).

13.3 Sous réserve des Clauses 13.1 et 13.2, aucune des parties ne sera responsable au titre du présent Contrat (que cette responsabilité soit contractuelle, délictuelle ou autre) des pertes suivantes subies ou encourues par l'autre partie (que ces pertes soient ou non envisageables par les parties à la Date d'entrée en vigueur du présent Contrat) :

(a) la perte de profits réels ou anticipés (y compris la perte de profits sur des contrats) ;

(b) la perte d'économies anticipées ;

(c) la perte d'une opportunité d'affaires ;

(d) la perte de notoriété ou l'atteinte à la réputation ; et

(e) les pertes spéciales, indirectes ou consécutives.

13.4 Sous réserve des Clauses 13.1, 13.2 et 13.3, la responsabilité de chacune des parties aux termes du présent Contrat (qu'elle soit contractuelle, délictuelle

ou autre) en lien avec la responsabilité découlant d'un événement ou d'une série d'événements liés, se limitera à : (a) 125 % des Frais totaux payés par le Client au titre du présent Contrat lors des 12 mois précédant immédiatement le mois au cours duquel s'est produit l'événement (ou le premier d'une série d'événements liés) donnant lieu à la responsabilité concernée ; ou (b) 50 000 £, en retenant le montant le plus élevé.

14. **Lois anticorruption.**

En exécutant ses obligations contractuelles au titre du présent Contrat, le Client devra se conformer à l'ensemble de la législation commerciale et anticorruption applicable (la "Loi anticorruption"), y compris, sans s'y limiter, la loi américaine relative aux pratiques de corruption internationales de 1977 (US Foreign Corrupt Practices Act) et la loi britannique anticorruption de 2010 (UK Bribery Act), qui interdisent de corrompre en offrant des objets de valeur, que ce soit directement ou indirectement, à quiconque, notamment les fonctionnaires, en vue d'obtenir ou de conserver des affaires, ou pour obtenir tout autre avantage commercial indu. Par ailleurs, le Client n'effectuera aucun paiement de facilitation, à savoir tout paiement destiné à inciter des fonctionnaires à effectuer des fonctions de routine qu'ils seraient de toute façon tenus d'effectuer. Le terme "fonctionnaires" comprend tout employé gouvernemental, candidat à une fonction publique et employé d'organisations internationales publiques, de partis politiques et d'entreprises publiques ou contrôlées par l'État.

15. **Divers.**

15.1 Notifications. Sauf indication contraire dans le présent Contrat, l'ensemble des notifications de résiliation d'infraction doivent être en anglais, par écrit, adressés au Département juridique de l'autre partie et envoyés à l'adresse postale du Client indiquée dans le présent Contrat ou à legal-notices@google.com (selon le cas) ou à une autre adresse indiquée par l'une des parties à l'autre conformément à la Clause 15.1.Toutes les notifications seront réputées avoir été remises à réception, comme attesté par un accusé de réception écrit ou automatique, ou bien (le cas échéant) un journal électronique. Toutes les autres notifications devront être rédigées en anglais, adressées au contact principal de l'autre partie et envoyées à son adresse postale ou électronique actuelle.

15.2 Cession. Aucune des parties ne peut céder ses droits ou obligations en vertu du présent Contrat sans l'accord préalable écrit de l'autre partie, sauf à un Affilié, mais uniquement si : (a) le cessionnaire a accepté par écrit d'être lié par les termes du présent Contrat ; et (b) le cédant a notifié à l'autre partie ladite cession par écrit. Toute autre tentative de transfert ou de cession est nulle et non avenue.

15.3 Sous-traitance. Sous réserve de toute restriction de l'Avenant relatif au Traitement des données concernant la sous-traitance, chaque partie peut sous-traiter ses obligations au titre du présent Contrat, en tout ou partie, sans le consentement écrit préalable de l'autre, sous réserve que la partie sous-traitante reste pleinement responsable de ces obligations sous-traitées et accepte la pleine responsabilité existant entre les parties pour les actes et/ou omissions de ses sous-traitants, comme si ces actes et/ou omissions étaient les siens.

15.4 Force majeure. Aucune des parties ne pourra être tenue responsable en cas de non-exécution, ou de retard dans l'exécution, de toute obligation au titre du présent Contrat, si ce manquement ou ce retard est dû à des circonstances indépendantes de sa volonté.

15.5 Absence de renonciation. Le non-exercice, ou le retard dans l'exercice, de tout droit ou recours prévu par les présentes ne saurait constituer une renonciation à ce droit ou recours ni à tout autre droit ou recours.

15.6 Autonomie des dispositions contractuelles. Si l'une quelconque des clauses (ou partie d'une clause) du présent Contrat s'avérait nulle, illégale ou inapplicable, les autres stipulations de cette clause (le cas échéant) et le présent Contrat resteraient en vigueur et de plein effet.

15.7 Absence de mandat. Les parties, et le Revendeur (le cas échéant), sont des cocontractants indépendants et le présent Contrat ne crée aucun contrat

d'agence, partenariat ou entreprise commune entre le Client, Google ou le Revendeur (nonobstant l'utilisation des expressions "partenaires", "certifié" ou de toute autre désignation similaire).

15.8 Absence de tiers bénéficiaires. Sauf mention contraire expresse, aucune clause du présent Contrat ne saurait créer ou conférer de quelconques droits ou autres avantages en faveur d'une quelconque personne autre que les parties aux présentes.

15.9 Droit applicable. Le présent Contrat est régi par le droit anglais et les parties se soumettent à la compétence exclusive des tribunaux anglais dans le cadre de tout litige (contractuel ou non contractuel) concernant le présent Contrat, étant entendu que chaque partie pourra demander à toute juridiction une injonction ou tout autre mesure visant à protéger ses droits de propriété intellectuelle. Si le présent Contrat est traduit dans une autre langue, la version anglaise prévaudra en cas d'incohérence.

15.10 Avenants. Tout avenant devra revêtir la forme écrite, et indiquer expressément qu'il modifie le présent Contrat, et devra être signé par les deux parties.

15.11 Intégralité du Contrat. Sous réserve de la Clause 13.1(b), le présent Contrat, qui inclut le ou les Bons de commande, l'Avenant relatif au Traitement des données, les Conditions d'utilisation des URL et toutes les autres clauses incorporées dans les présentes, prévoient l'ensemble des dispositions convenues entre les parties et prévaut sur tous les autres accords entre les parties concernant son objet. En concluant le présent Contrat, aucune partie ne s'est basée sur, et aucune partie ne détiendra de droit ou de recours fondé sur, une déclaration ou une garantie (effectuée de manière négligente ou innocente), à l'exception des déclarations et garanties expressément mentionnées au présent Contrat.

15.12 Interprétation des dispositions contraires. En cas de conflit entre le présent Contrat et les conditions visées dans une quelconque URL, le présent Contrat prévaudra.

15.13 Pluralité d'exemplaires. Les parties pourront signer le présent Contrat en plusieurs exemplaires, y compris par télécopie, au format PDF et autres copies électroniques, et l'ensemble desdits exemplaires constitueront un seul et même instrument.

15.14 Survie. Les clauses suivants survivront à l'expiration ou à la résiliation du présent Contrat : Clauses 4, 7, 8.1, 9.2, 11.6, 12, 13, 15 et 16. L'Avenant relatif au Traitement des données survivra à l'expiration ou à la résiliation du présent Contrat comme cela est exposé dans l'Avenant relatif au Traitement des données.

16. **Définitions**.

16.1 Sauf mention contraire expresse dans le présent Contrat :

"Politique d'utilisation autorisée" désigne la politique d'utilisation autorisée relative aux Services et disponible à l'adresse https://gsuite.google.com/intl/fr/terms/use_policy.html ou à une autre URL fournie par Google.

"Gestionnaire de compte" désigne le professionnel de Google qui travaille avec le Client concernant la commande de Services du Client.

"Compte(s) Administrateur" désigne le ou les comptes administratifs fournis par Google au Client aux fins d'administration des Comptes d'Utilisateur final. L'utilisation d'un ou plusieurs Comptes Administrateur nécessite un mot de passe que Google fournira au Client.

"Console d'administration" désigne l'outil en ligne fourni au Client par Google destiné à être utilisé pour le signalement et d'autres fonctions administratives.

"Outil d'administration" désigne les outils ou API en ligne, ou les deux, fournis par Google au Client pour être utilisés par ce dernier en lien avec son administration des Services pour les Utilisateurs finaux, ce qui peut inclure, entre autres, la maintenance de compte et l'application des politiques d'utilisation du Client.

"Administrateur(s)" désigne le personnel technique désigné par le Client qui administre les Services au profit des Utilisateurs finaux pour le compte du Client.

"Publicité" désigne les publicités en ligne affichées par Google à l'attention des Utilisateurs finaux, à l'exception des publicités dont le Client choisit expressément l'affichage par Google ou tout Affilié de Google en lien avec les Services dans le cadre d'un contrat distinct (par exemple, les publicités Google AdSense déployées par le Client sur un site internet créé par le Client et utilisant la fonctionnalité "Google Sites" dans le cadre des Services).

"Contrat" désigne chaque Bon de commande, le présent Contrat Google Apps for Education et tout document indiqué dans le Bon de commande et le Contrat Google Apps for Education (y compris les Conditions d'utilisation des URL).

"Date de début de facturation" désigne la date à laquelle le Client commencera à payer Google pour les Services.

"Signes distinctifs" désigne les appellations commerciales, marques commerciales, marques de service, logos, noms de domaines et autres Signes distincitfs afférents à chacune des parties, respectivement, tels que protégés à tout moment par cette partie.

" Informations confidentielles" désigne les informations divulguées par une partie à l'autre dans le cadre du présent Contrat, marquées comme étant confidentielles ou qui, de par leur nature, contenu ou des circonstances de leur divulgation, peuvent raisonnablement être présumées confidentielles. Pour lever toute ambiguïté, les conditions générales du présent Contrat sont des Informations confidentielles. Les Informations confidentielles n'incluent pas les informations élaborées de façon autonome par le destinataire, légitimement communiquées à celui-ci par un tiers sans obligation de confidentialité ou devenant accessibles au grand public sans que le destinataire ait commis une faute. Les Données du Client sont des Informations confidentielles du Client.

"Données du Client" désigne les données, y compris les e-mails, fournies, générées, transmises ou affichées via les Services par le Client ou les Utilisateurs finaux.

"Noms de domaine du Client" désigne les noms de domaine détenus ou contrôlés par le Client et utilisés en lien avec les Services. Le Client peut fournir les Services à l'un quelconque de ses sous-domaines (par exemple, si le Nom de domaine du Client est "edu.com", un sous-domaine peut inclure "alumni.edu.com") sans accord écrit de Google.

"Données personnelles du Client" désigne les données personnelles traitées par ou pour le compte de Google dans le cadre du présent Contrat.

"Avenant relatif au traitement des données" désigne la version alors en vigueur de l'avenant de Google au présent Contrat décrivant les obligations de Google relatives à la protection et au traitement des Données du Client, tel que visé à l'URL suivante : https://gsuite.google.com/intl/fr/terms/dpa_terms.html.L'Avenant relatif au Traitement des données et ce lien peuvent être mis à jour ou modifié de temps à autre par Google conformément à la Clause 2.2.

"Problème urgent de sécurité" désigne soit: (a) l'utilisation des Services par le Client ou les Utilisateurs finaux en violation de la Politique d'utilisation autorisée d'une manière perturbant : (i) les Services ; (ii) l'utilisation des Services par d'autres Utilisateurs finaux ou clients ; ou (iii) le réseau ou les serveurs Google utilisés pour fournir les Services ; ou (b) un accès non autorisé d'un tiers aux Services.

"Utilisateurs finaux" désigne les personnes physiques autorisées par le Client à utiliser les Services.

"Compte d'Utilisateur final" désigne un compte hébergé par Google fourni aux Utilisateurs finaux via les Services aux fins de permettre à ces Utilisateurs finaux d'utiliser les Services.

"Lois relatives au contrôle des exportations" désigne toutes les lois et réglementations applicables concernant l'exportation et la réexportation, y compris (i) les sanctions commerciales et économiques administrées par l'Office de contrôle des avoirs étrangers du Département américain au Trésor, et (ii) les Réglementations des transferts internationaux d'armes (Traffic in Arms Regulations, "ITAR") administrées par le Département d'État américain, mais à l'exclusion des réglementations d'administration des exportations (Export Administration Regulations, "EAR") administrées par le Département américain du commerce.

"Frais" a le sens qui lui est donné à la Clause 4.1.

"Politique de confidentialité de Google" désigne la politique de confidentialité consultable à l'adresse http://www.google.com/privacypolicy.html ou à toute autre adresse URL que Google peut à tout moment mettre à jour.

"Affilié" désigne une entité contrôlant une partie, contrôlée par elle ou sous contrôle commun avec elle, le terme "contrôle" étant défini comme a) la détention d'au moins cinquante pourcent (50%) de la participation ou des intérêts bénéficiaires de l'entité; b) le droit de vote ou de désignation d'une majorité au conseil d'administration ou dans tout organe de gouvernance de l'entité; ou c) le pouvoir d'exercer une influence déterminante sur la gestion ou les politiques de l'entité.

"Centre d'aide" désigne le centre d'aide Google accessible à l'adresse http://www.google.com/support/, ou à une autre URL fournie par Google.

"Activités à haut risque" désigne les utilisations telles que les activités d'exploitation des installations nucléaires, du contrôle aérien ou des systèmes de réanimation, lorsque l'utilisation ou la défaillance des Services est susceptible d'entraîner des décès ou de causer des dommages corporels ou environnementaux.

"Période de Services initiale" désigne la période pour les Services concernés commençant à la Date de début des Services et se poursuivant pendant la "Période actuelle des Services" indiquée sur le Bon de commande à partir de la Date de début de facturation (si un Bon de commande s'applique aux Services), ou si aucun Bon de commande ne s'applique aux Services, pour la période commençant à la Date d'entrée en vigueur et continuant pendant.

"Frais de la Période initiale" désigne les frais correspondant aux Services pour la Période de Services initiale (à l'exclusion de tous frais applicables non récurrents), tel qu'indiqué sur le Bon de commande.

"Instructions" désigne les instructions écrites du Client indiquées dans le présent Contrat (tel qu'amendé ou remplacé) et toutes instructions ultérieures écrites du Client à Google et prises en considération par Google.

"Droits de propriété intellectuelle" désigne tous les droits d'auteur, droits moraux, droits en matière de brevets, droits sur les marques, droits sur des dessins ou modèles, droits sur ou relatifs à des bases de données, droits sur ou relatifs à des informations confidentielles, droits afférents à des noms de domaine et tous autres droits de propriété intellectuelle (enregistrés ou non déposés) dans le monde entier.

"Recours juridique" désigne une demande de divulgation des données formulée conformément à une loi, une réglementation gouvernementale, une ordonnance d'un tribunal, une citation à comparaître en qualité de témoin, un mandat, une demande d'une autorité administrative indépendante ou d'une administration, ou formulée conformément à toute autre autorité juridique valide, procédure juridique ou tout autre processus similaire.

"Services complémentaires" désigne des des produits, services et applications de Google qui ne font pas partie des Services, mais auxquels les Utilisateurs finaux peuvent accéder grâce à l'identifiant et au mot de passe de leur Compte d'Utilisateur final. Les Services complémentaires sont indiqués à l'URL suivante : https://support.google.com/a/answer/181865?hl=fr, ou à toute autre URL fournie par Google.

"Conditions d'utilisation supplémentaires des Services complémentaires" désigne les conditions visées à l'URL suivante : https://gsuite.google.com/intl/fr/terms/additional_services.html, ou toute autre URL fournie par Google à tout moment.

"Adresse électronique de notification" désigne l'adresse électronique spécifiée par le Client pour recevoir les notifications par courrier électronique de Google. Le Client peut modifier cette adresse e-mail via la Console d'administration.

"Revendeur" désigne, le cas échéant, le revendeur autorisé qui vend ou fournit les Services au Client dans le cadre du présent Contrat.

"Contrat de revente" désigne le contrat indépendant entre le Client et le Revendeur concernant les Services. Le Contrat de revente est indépendant et en dehors du champ d'application du présent Contrat.

"Services" désigne les Services G Suite for Education fournis par Google et utilisés par le Client dans le cadre du présent Contrat. Les Services sont décrits à l'adresse suivante : https://gsuite.google.com/intl/fr/terms/user_features.html, ou à toute autre URL fournie par Google.

"Date de début des Services" est la date à laquelle Google met les Services à disposition du Client.

"Pages de Services" désigne les pages web affichant les Services pour les Utilisateurs finaux.

"Période de Services" désigne la Période de Services initiale ou la Période de renouvellement, selon le cas.

"Dépréciation significative" désigne le fait d'arrêter ou de réaliser des modifications rétroactives incompatibles au niveau des Services conduisant Google à ne plus fournir à sa base de clients entreprise la possibilité de : (1) envoyer ou recevoir des e-mails ; (2) programmer et gérer des événements ; (3) créer, partager, stocker et synchroniser des fichiers ; (4) communiquer avec d'autres utilisateurs finaux en temps réel ; ou (5) rechercher, archiver et exporter des e-mails.

"SLA" désigne le Contrat de Niveau de Service consultable ici :https://gsuite.google.com/intl/fr/terms/sla.html, ou à toute autre URL fournie par Google.

"Suspendre" ou "suspension" désigne la désactivation immédiate de l'accès aux Services, ou à des éléments des Services, le cas échéant, afin d'empêcher toute utilisation ultérieure des Services.

"Taxes" désigne toute taxe, y compris les taxes de vente, d'utilisation, sur la propriété personnelle, sur la valeur ajoutée, d'accise, les frais et droits de douane, les frais de timbre ou autres taxes et droits imposés par des agences gouvernementales, quelle qu'en soit la nature, relativement à l'ensemble des transactions réalisées dans le cadre du Contrat, y compris les pénalités et les intérêts, mais en excluant expressément les taxes sur le revenu net de Google.

"Directives relatives aux marques" désigne les Instructions de Google relatives à l'utilisation des Signes distinctifs Google par des tierces parties, disponibles à l'adresse URL suivante : http://www.google.com/permissions/guidelines.html, ou à toute autre URL fournie par Google.

"SAT" désigne les services d'assistance technique fournis par Google aux Administrateurs pendant la Durée du Contrat conformément aux Instructions SAT.

"Instructions SAT" désigne les instructions des services d'assistance technique de Google alors en vigueur pour les Services. Les Instructions SAT sont consultables à l'adresse URL suivante : https://gsuite.google.com/intl/fr/terms/tssg.html ou à toute autre URL fournie par Google.

"Conditions d'utilisation des URL" désignent, collectivement, la Politique d'utilisation autorisée, le SLA et les Instructions SAT.

16.2 Dans le présent Contrat, les mots "inclut" et "y compris" ne limiteront pas le caractère général des mots qui les précèdent.

ANNEXE 9

Règles de confidentialité

Date de la dernière modification : 2 octobre 2017 (voir les versions archivées) (Les exemples en liens hypertexte sont disponibles au bas de ce document.)

Vous pouvez avoir recours à nos services pour toutes sortes de raisons : pour rechercher et partager des informations, pour communiquer avec d'autres personnes ou pour créer des contenus. En nous transmettant des informations, par exemple en créant un compte Google, vous nous permettez d'améliorer nos services. Nous pouvons notamment afficher des annonces et des **résultats de recherche plus pertinents** et vous aider à **échanger avec d'autres personnes** ou à **simplifier et accélérer le partage avec d'autres internautes**. Nous souhaitons que vous, en tant qu'utilisateur de nos services, compreniez comment nous utilisons vos données et de quelles manières vous pouvez protéger votre vie privée.

Nos Règles de confidentialité expliquent :

- les données que nous collectons et les raisons de cette collecte.
- la façon dont nous utilisons ces données.
- les fonctionnalités que nous vous proposons, y compris comment accéder à vos données et comment les mettre à jour.

Nous nous efforçons d'être le plus clair possible. Toutefois, si vous n'êtes pas familier, par exemple, des termes "cookies", "adresses IP", "balises pixel" ou "navigateurs", renseignez-vous préalablement sur ces termes clés. Chez Google, nous sommes soucieux de préserver la confidentialité de vos données privées. Ainsi, que vous soyez nouvel utilisateur ou un habitué de Google, prenez le temps de découvrir nos pratiques et, si vous avez des questions, n'hésitez pas à nous contacter.

Données que nous collectons

Les informations que nous collectons servent à améliorer les services proposés à tous nos utilisateurs. Il peut s'agir d'informations de base, telles que la langue que vous utilisez, ou plus complexes, comme les **annonces que vous trouvez les plus utiles**, **les personnes qui vous intéressent le plus sur le Web** ou les vidéos YouTube qui sont susceptibles de vous plaire.

Nous collectons des données des manières suivantes :

- **Informations que vous nous communiquez** : pour accéder à nos services, vous devez souvent créer un compte Google. Dans ce cas, vous fournissez des informations personnelles, telles que votre nom, votre adresse e-mail, votre numéro de téléphone ou votre **carte de paiement**, qui sont enregistrées avec votre compte. Pour pouvoir profiter de toutes les fonctionnalités de partage que nous proposons, vous pouvez également être amené à créer un profil Google public, qui peut comprendre votre nom et votre photo.

- **Informations que nous collectons lorsque vous utilisez nos services** : nous **collectons des informations** relatives aux services que vous utilisez et à l'usage que vous en faites. Exemples : lorsque vous regardez une vidéo sur YouTube, lorsque vous vous rendez sur un site Web sur lequel nos services publicitaires sont utilisés ou lorsque vous **consultez nos contenus et nos annonces, et que vous effectuez des actions sur celles-ci**. Parmi ces informations, on peut citer :

    - **Données relatives à l'appareil utilisé**

      Nous collectons des **données relatives à l'appareil que vous utilisez**, par exemple, le modèle, la version du système d'exploitation, les identifiants uniques de l'appareil et les informations relatives au réseau mobile, y compris votre numéro de téléphone. Nous sommes susceptibles d'associer les **identifiants de votre appareil** ou votre **numéro de téléphone** à votre compte Google.

    - **Fichiers journaux**

      Lorsque vous utilisez nos services ou que vous affichez des contenus fournis par Google, nous collectons et

stockons des informations dans les fichiers journaux de nos serveurs. Cela comprend :

- la façon dont vous avez utilisé le service concerné, telles que vos requêtes de recherche.
- des données relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les données de routage des SMS et les types d'appels.
- votre adresse IP.
- des données relatives aux événements liés à l'appareil que vous utilisez, tels que plantages, activité du système, paramètres du matériel, type et langue de votre navigateur, date et heure de la requête et URL de provenance.
- des cookies permettant d'identifier votre navigateur ou votre Compte Google de façon unique.

- **Données de localisation**

  Lorsque vous utilisez des services Google, nous **sommes susceptibles de collecter et traiter des données relatives à votre position exacte**. Nous utilisons différentes technologies pour vous localiser, y compris l'adresse IP, les signaux GPS **et d'autres capteurs** nous permettant notamment d'identifier les appareils, **les points d'accès WiFi et les antennes-relais se trouvant à proximité**.

- **Numéros d'application unique**

  Certains services contiennent un numéro d'application unique. Ce numéro et les informations concernant votre installation (type de système d'exploitation et numéro de version, par exemple) peuvent être envoyés à Google lorsque vous installez ou désinstallez le service, ou lorsque le service contacte régulièrement nos serveurs (par exemple, pour demander des mises à jour automatiques).

- **Stockage en local**

  Nous pouvons être amenés à collecter et à stocker des données (y compris des données personnelles) sur l'appareil que vous utilisez, à l'aide de mécanismes comme le stockage sur le navigateur Web (y compris HTML 5) et les caches de données d'application.

- **Cookies et technologies similaires**

  Nos partenaires et nous-mêmes utilisons différentes technologies pour collecter et stocker des données lorsque vous accédez à un service Google, par exemple en utilisant des cookies ou des technologies similaires pour identifier votre navigateur ou votre appareil. Nous utilisons également ces technologies pour collecter et stocker des informations lorsque vous interagissez avec les services que nous proposons à nos partenaires, comme des **services de publicité** ou les fonctionnalités Google qui peuvent apparaître sur d'autres sites. Notre produit Google Analytics permet aux entreprises et aux propriétaires de sites d'analyser le trafic sur leurs sites Web et sur leurs applications. Lorsqu'il est utilisé parallèlement à nos services publicitaires, tels que ceux utilisant le cookie DoubleClick, les informations Google Analytics sont **associées, par le client Google Analytics ou par Google, à l'aide de la technologie Google, aux informations relatives aux visites sur plusieurs sites**.

Outre les informations vous concernant que nous obtenons par l'intermédiaire de nos partenaires, les données que nous recueillons lorsque vous êtes connecté à Google peuvent être associées à votre compte Google. Nous les traitons alors comme des données personnelles. Pour en savoir plus sur la manière dont vous pouvez accéder aux informations associées à votre compte Google, les gérer ou les supprimer, consultez la section Transparence et liberté de choix des présentes règles.

Comment nous utilisons les données que nous collectons

Les données que nous collectons nous permettent de **fournir**, **gérer**, **protéger** et améliorer nos services, d'en **développer de nouveaux**, et de **protéger aussi bien nos utilisateurs que nous-mêmes**. Ces données nous permettent également de vous proposer des contenus adaptés, tels que des annonces et des résultats de recherche plus pertinents.

Nous sommes susceptibles d'utiliser le nom fourni dans votre Profil Google dans tous nos services qui requièrent l'utilisation d'un Compte Google. Nous pouvons également être amenés à remplacer d'anciens noms associés à votre Compte Google, afin que vous soyez présenté de manière cohérente à travers l'ensemble de nos services. Si d'autres utilisateurs disposent déjà de votre adresse e-mail, ou de toute autre donnée permettant de vous identifier, nous sommes susceptibles de leur montrer les données de votre Profil Google disponibles publiquement, telles que votre nom et votre photo.

Si vous disposez d'un compte Google, nous pouvons afficher le nom et la photo de votre profil, et les actions que vous effectuez sur Google ou sur des applications tierces connectées à votre compte Google (telles que les +1 que vous attribuez, les avis que vous rédigez ou les commentaires que vous postez) au sein de nos services, y compris dans le cadre de la diffusion d'annonces ou dans d'autres contextes commerciaux. Nous nous conformerons aux **paramètres de partage ou de visibilité** que vous définissez dans votre compte Google.

Lorsque vous contactez Google, nous conservons un enregistrement de votre communication afin de mieux résoudre les problèmes que vous rencontrez. Nous pouvons utiliser votre adresse e-mail pour vous tenir informé(e), par exemple, des modifications ou des améliorations à venir de nos services.

Nous utilisons les informations fournies par les cookies et d'autres technologies, comme les balises pixel, pour vous offrir un **meilleur confort d'utilisation** et améliorer la qualité globale de nos services. Google Analytics est un des produits que nous employons à cette fin dans nos propres services. L'enregistrement de vos préférences linguistiques nous permet, par exemple, d'afficher nos services dans la langue que vous utilisez le plus souvent. Lorsque nous vous proposons des annonces personnalisées, nous n'associons aucun identifiant de cookies ou de technologies similaires à des données sensibles, telles que la race, la religion, l'orientation sexuelle ou l'état de santé.

Nos systèmes automatisés analysent vos contenus (y compris les e-mails) afin de vous proposer des fonctionnalités personnalisées sur les produits, telles que des résultats de recherche personnalisés, des publicités sur mesure, et la détection de spams et de logiciels malveillants.

Les informations personnelles que vous fournissez pour l'un de nos services sont susceptibles d'être **recoupées avec celles issues d'autres services Google (y compris des informations personnelles)**, par exemple pour **faciliter le partage de vos informations avec des personnes que vous connaissez**. Selon vos paramètres de compte, **votre activité sur d'autres sites et dans d'autres applications** peut être associée à vos informations personnelles dans le but d'améliorer les services Google et les annonces diffusées par Google.

Toute utilisation de données dans un but autre que ceux qui sont exposés dans les présentes Règles de confidentialité nécessitera votre accord explicite.

Nous traitons vos données personnelles sur des serveurs Google situés dans de nombreux pays à travers le monde. Vos données personnelles sont donc susceptibles d'être traitées sur un serveur situé hors de votre pays de résidence.

Transparence et liberté de choix

Les préoccupations en matière de confidentialité diffèrent d'une personne à l'autre. Nous souhaitons faire preuve de transparence sur la façon dont nous collectons et utilisons les données qui vous concernent, afin que vous disposiez de tous les éléments pour faire des choix informés. Vous pouvez par exemple effectuer les actions ci-dessous :

- Vérifier et mettre à jour les commandes Google relatives à l'activité afin de déterminer les types de données (tels que les vidéos que vous avez regardées sur YouTube ou vos dernières recherches) que vous voulez enregistrer dans votre compte lorsque vous utilisez des services Google. Vous pouvez également consulter ces commandes afin de déterminer si certaines activités sont stockées dans un cookie ou une technologie similaire sur votre appareil mobile lorsque vous utilisez nos services sans être connecté à votre compte.
- Utiliser Google Dashboard pour vérifier et contrôler certains types de données liés à votre Compte Google.
- Grâce aux paramètres des annonces, vous pouvez consulter et modifier vos préférences relatives aux annonces Google qui vous sont présentées sur les sites Google et sur le Web, telles que les catégories susceptibles de vous intéresser. Vous pouvez également vous rendre sur cette page pour désactiver certains services publicitaires Google.
- Ajuster l'affichage du profil associé à votre compte Google.
- Contrôler avec qui vous partagez vos donnés par le biais de votre compte Google.
- Supprimer des données associées à votre compte Google de plusieurs de nos services.
- Choisissez si le nom et la photo de votre profil paraîtront dans les recommandations partagées qui apparaissent dans les annonces.

Vous pouvez également paramétrer votre navigateur de façon à bloquer tous les cookies, y compris les cookies liés à nos services, ou pour être informé lorsque nous vous en envoyons. Il convient toutefois de rappeler que bon nombre de nos services **sont susceptibles de ne pas fonctionner correctement** si vous désactivez les cookies. Ils ne tiendront pas compte, par exemple, de vos préférences linguistiques.

Données que vous partagez

De nombreux services Google vous permettent de partager vos données avec d'autres personnes. Rappelez-vous que lorsque vous partagez des informations publiquement, elles peuvent être indexées par des moteurs de recherche tels que Google. Nos services vous proposent plusieurs façons de **partager** et de **supprimer vos contenus**.

Consultation et mise à jour de vos données personnelles

Lorsque vous utilisez nos services, nous souhaitons que vous ayez **accès à vos informations personnelles**. En cas d'erreur, nous faisons en sorte que vous puissiez les mettre à jour rapidement ou les supprimer, sauf si nous devons les conserver à des fins commerciales légitimes ou si la loi nous l'impose. Avant de répondre à une demande de mise à jour de vos informations personnelles, nous pouvons vous inviter à vous identifier.

Nous nous réservons le droit de décliner toute demande déraisonnable par son caractère répétitif ou systématique, toute demande réclamant des efforts techniques démesurés (par exemple, le développement d'un nouveau système ou une modification majeure d'une procédure existante), compromettant la confidentialité des données de tiers, ou difficilement réalisable (par exemple, des demandes concernant des données stockées sur des systèmes de sauvegarde).

L'accès aux données et leur rectification constituent un service gratuit, sauf dans le cas où ce service impliquerait un effort démesuré. Nous prenons toutes les dispositions pour protéger les données gérées dans le cadre de nos services contre toute destruction accidentelle ou volontaire. Par conséquent, même lorsque vous supprimez des données utilisées par nos services, nous ne supprimons pas immédiatement les copies résiduelles se trouvant sur nos serveurs actifs ni celles stockées dans nos systèmes de sauvegarde.

Données que nous partageons

Nous ne communiquons vos données personnelles à des entreprises, des organisations ou des personnes tierces que dans les circonstances suivantes :

- **Avec votre consentement**

  Nous ne communiquons des données personnelles vous concernant à des entreprises, des organisations ou des personnes tierces qu'avec votre consentement. Nous demandons toujours votre autorisation avant de communiquer à des tiers des données personnelles sensibles.

- **Avec des administrateurs de domaines**

  Si votre Compte Google est géré par un administrateur de domaine (par exemple, s'il s'agit d'un compte Google Apps), l'administrateur de domaine ainsi que tout sous-traitant assurant des services d'aide utilisateur pour votre organisation auront accès aux données de votre Compte Google (y compris, notamment, votre adresse e-mail). Votre administrateur de domaine est susceptible de pouvoir :

  - afficher les statistiques relatives à votre compte, notamment celles concernant les applications que vous installez ;
  - modifier le mot de passe de votre compte ;
  - suspendre ou supprimer l'accès à votre compte ;
  - accéder aux données conservées dans votre compte et les conserver ;
  - recevoir les données propres à votre compte pour satisfaire à des obligations légales, réglementaires, **judiciaires ou administratives** ;
  - restreindre vos droits de suppression ou de modification des données ou des paramètres de confidentialité.

  Pour en savoir plus, veuillez consulter les règles de confidentialité de votre administrateur de domaine.

- **Pour des besoins de traitement externe**

  Nous transmettons des données personnelles à nos filiales ou autres sociétés ou personnes de confiance qui les traitent pour notre compte, selon nos instructions, conformément aux présentes Règles de confidentialité et dans le respect de toute autre mesure appropriée de sécurité et de confidentialité.

- **Pour des raisons juridiques**

  Nous ne partagerons des données personnelles avec des entreprises, des organisations ou des personnes tierces que si nous pensons en toute bonne foi que l'accès, l'utilisation, la protection ou la divulgation de ces données est raisonnablement justifiée pour :

- satisfaire à des obligations légales, réglementaires, **à des procédures judiciaires ou à des demandes gouvernementales ayant force exécutoire** ;
- faire appliquer les conditions d'utilisation en vigueur, y compris pour constater d'éventuels manquements à celles-ci ;
- déceler, éviter ou traiter des activités frauduleuses, les atteintes à la sécurité ou tout problème d'ordre technique ;
- se prémunir contre toute atteinte aux droits, aux biens ou à la sécurité de Google, de ses utilisateurs ou du public, en application et dans le respect de la loi.

Nous pouvons être amenés à partager publiquement, ainsi qu'avec nos partenaires (éditeurs, annonceurs ou sites associés) des informations qui ne permettent pas d'identifier personnellement l'utilisateur. Nous pouvons, par exemple, partager publiquement des **informations relatives aux tendances** d'utilisation de nos services.

Dans le cas où Google prendrait part à une opération de fusion, d'acquisition ou à toute autre forme de cession d'actifs, nous nous engageons à garantir la confidentialité de vos données personnelles et à vous informer avant que celles-ci ne soient transférées ou soumises à de nouvelles règles de confidentialité.

Sécurité des données

Nous mettons en œuvre toutes les mesures de sécurité nécessaires pour protéger Google ainsi que nos utilisateurs contre tout accès et toute modification, divulgation ou destruction non autorisés des données que nous détenons. En particulier :

- Nous chiffrons la plupart de nos services à l'aide de la technologie SSL.
- Nous vous proposons une validation en deux étapes lorsque vous accédez à votre Compte Google et une fonction de Navigation Sécurisée dans Google Chrome.
- Nous menons des audits internes sur la collecte, le stockage et le traitement des données, y compris les mesures de sécurité physiques, afin d'empêcher tout accès non autorisé à nos systèmes.
- L'accès aux données personnelles est strictement réservé aux salariés, sous-traitants et agents de Google qui ont besoin d'y accéder afin de les traiter en notre nom. Ces personnes sont soumises à de strictes obligations de confidentialité et sont susceptibles de faire l'objet de sanctions disciplinaires pouvant aller jusqu'au licenciement en cas de manquement à ces obligations.

Champ d'application des présentes Règles de confidentialité

Les présentes Règles de confidentialité s'appliquent à tous les services proposés par Google LLC et par ses filiales, y compris à YouTube, aux services fournis par Google sur les appareils Android et aux services proposés sur d'autres sites (nos services publicitaires, par exemple), mais excluent les services régis par d'autres règles de confidentialité n'incorporant pas les présentes.

Les présentes Règles de confidentialité ne s'appliquent pas aux services proposés par d'autres sociétés ou personnes, notamment aux produits ou aux sites qui peuvent vous être proposés dans les résultats de recherche, aux sites qui peuvent incorporer des services Google ou aux autres sites accessibles à partir de nos services. Les présentes Règles de confidentialité ne couvrent pas les pratiques en matière de protection des données d'autres sociétés ou organisations qui font la publicité de nos services et qui peuvent utiliser des cookies, des balises pixel ou d'autres technologies pour afficher et proposer des annonces pertinentes.

Respect et coopération avec des organismes de régulation

Nous vérifions régulièrement que nous respectons les présentes Règles de confidentialité. Nous nous conformons par ailleurs à plusieurs chartes d'autorégulation, notamment dans le cadre du bouclier de protection des données EU-US Privacy Shield Framework et Swiss-US Privacy Shield Framework. Lorsque nous recevons une réclamation écrite officielle, nous prenons contact avec l'utilisateur pour donner suite à sa démarche. Nous coopérons avec les autorités compétentes, y compris les autorités locales chargées de la protection des données, pour résoudre tout litige concernant le transfert d'informations personnelles que nous ne pouvons pas régler directement avec l'utilisateur.

Modifications

Les présentes Règles de confidentialité peuvent être amenées à changer. Toute diminution de vos droits dans le cadre des présentes Règles de confidentialité ne saurait être appliquée sans votre consentement exprès. Nous publierons toute

modification des règles de confidentialité sur cette page et, dans le cas où il s'agirait de modifications significatives, nous publierons un avertissement mis en évidence (y compris, pour certains services, par le biais d'une notification par e-mail). Les versions antérieures des présentes Règles de confidentialité seront archivées et mises à la disposition des utilisateurs.

Pratiques spécifiques à certains produits

Les documents suivants exposent des pratiques spécifiques en matière de confidentialité applicables à certains produits ou services Google que vous pouvez utiliser :

- Google Chrome et Chrome OS
- Play Livres
- Payments
- Fiber
- Project Fi
- G Suite for Education
- YouTube Kids
- Comptes Google gérés avec Family Link

Pour obtenir plus d'informations sur certains de nos services les plus populaires, vous pouvez consulter le guide de confidentialité des produits Google.

Autres ressources utiles liées à la confidentialité et à la protection des données

Vous trouverez d'autres ressources utiles liées à la confidentialité et à la protection des données sur les pages Règles et principes de Google, notamment :

- Des informations sur nos technologies et principes, qui comprennent notamment des données complémentaires sur
  - la manière dont nous utilisons les cookies ;
  - les technologies que nous utilisons pour la publicité ;
  - la manière dont nous utilisons la reconnaissance de motifs, tels les visages.
- Une page qui explique quelles données vous nous transmettez lorsque vous consultez des sites Web qui utilisent nos produits publicitaires, d'analyse et sociaux
- L'outil de vérification des paramètres de confidentialité facilite le contrôle de vos principaux paramètres de confidentialité.
- Le Centre de sécurité Google, qui fournit des informations sur la manière de renforcer la sécurité sur Internet

---

"accès à vos données personnelles"

Par exemple, Google Dashboard vous permet de visualiser rapidement et facilement une partie des données associées à votre compte Google.
En savoir plus

"annonces que vous trouvez les plus utiles"

Par exemple, si vous consultez fréquemment des sites Web et des blogs de jardinage, il est possible que des annonces ayant trait à cette activité apparaissent lorsque vous parcourez le Web.
En savoir plus

"services de publicité"

Par exemple, si vous consultez fréquemment des sites Web et des blogs de jardinage sur lesquels nos annonces sont diffusées, il est possible que des annonces ayant trait à cette activité commencent à apparaître lorsque vous parcourez le Web.
En savoir plus

"et d'autres capteurs"

Il se peut que votre appareil soit équipé de capteurs fournissant des informations susceptibles de déterminer votre position avec plus de précision. Par exemple, un accéléromètre permet de mesurer la vitesse, tandis qu'un gyroscope permet de connaître le sens de déplacement.

En savoir plus

"de collecter des informations"

Elles incluent des informations variées : préférences et données liées à votre utilisation des services, messages Gmail, profil G+, photos, vidéos, historique de navigation, recherches sur des cartes, documents ou tout autre contenu hébergé par Google.
En savoir plus

"recoupées avec celles issues d'autres services Google (y compris des informations personnelles)"

Par exemple, lorsque vous êtes connecté à votre compte Google et que vous effectuez une recherche dans Google, vous voyez s'afficher des résultats issus de pages Web publiques, ainsi que des pages, des photos et des posts Google+ émanant de vos amis.
En savoir plus

"échanger avec d'autres personnes"

Par exemple, vous pouvez recevoir des suggestions concernant des personnes que vous êtes susceptible de connaître ou avec lesquelles vous souhaitez vous connecter via Google+, en fonction des contacts dont vous disposez dans d'autres produits Google tels que Gmail. En outre, votre profil peut être proposé aux personnes qui sont en contact avec vous.
En savoir plus

"carte de paiement"

À l'heure actuelle, nous n'exigeons pas de carte de paiement lors de l'inscription. Toutefois, pour vérifier que vous respectez nos critères d'âge, nous vous demandons d'effectuer une transaction d'un faible montant par carte de paiement si votre compte a été désactivé suite à la saisie d'une date de naissance indiquant que vous n'avez pas l'âge minimal requis pour disposer d'un compte Google.
En savoir plus

"développer de nouveaux"

Par exemple, le correcteur orthographique de Google a été développé à partir de l'analyse de recherches précédentes que les internautes avaient eux-mêmes corrigées.
En savoir plus

"identifiants de votre appareil"

Les identifiants d'appareil nous permettent de savoir quel appareil vous utilisez pour accéder à nos services. Nous sommes ainsi en mesure de personnaliser notre service en fonction de votre appareil ou d'analyser tout problème lié à ce dernier dans le cadre de nos services.
En savoir plus

"données relatives à l'appareil que vous utilisez"

Par exemple, lorsque vous consultez le site Google Play à partir de votre ordinateur de bureau, nous pouvons nous servir de ces données pour vous aider à choisir l'appareil sur lequel vous souhaitez utiliser ces achats.
En savoir plus

"meilleur confort d'utilisation"

Par exemple, les cookies nous permettent d'analyser la façon dont les internautes utilisent nos services.
En savoir plus

"judiciaires ou administratives"

Comme d'autres entreprises spécialisées dans les technologies et les communications, nous recevons régulièrement des demandes d'autorités administratives et de tribunaux du monde entier nous invitant à transmettre des informations sur les utilisateurs. Notre équipe juridique analyse chacune de ces demandes, quelle qu'en soit la nature, et nous refusons

fréquemment d'accéder à celles qui nous semblent trop vagues ou qui ne respectent pas la procédure établie.
En savoir plus

"Paramètres de partage ou de visibilité"

Par exemple, vous pouvez définir vos paramètres pour que votre nom et votre photo n'apparaissent pas dans une annonce.
En savoir plus

"associées aux informations relatives aux visites sur plusieurs sites"

Google Analytics repose sur des cookies propriétaires. Les données générées via Google Analytics peuvent être associées, par le client Google Analytics ou par Google, à l'aide de la technologie Google, à des cookies tiers, liés à des visites sur d'autres sites Web, par exemple, lorsqu'un annonceur souhaite utiliser ses données Google Analytics afin de créer des annonces plus pertinentes ou d'analyser son trafic de manière plus approfondie. En savoir plus
En savoir plus

"gérer"

Par exemple, nous surveillons constamment nos systèmes afin de vérifier qu'ils fonctionnent correctement, ainsi que de détecter et de corriger les éventuelles erreurs.
En savoir plus

"sommes susceptibles de collecter et traiter des données relatives à votre position exacte"

Par exemple, Google Maps peut centrer le plan sur votre position actuelle.
En savoir plus

"sont susceptibles de ne pas fonctionner correctement"

Par exemple, nous utilisons un cookie appelé "lbcs" qui vous permet d'ouvrir de nombreux fichiers Google Documents dans un seul navigateur.
En savoir plus

"Nos partenaires"

Nous autorisons les sociétés dignes de confiance à utiliser des cookies ou des technologies similaires à des fins de publicité ou d'étude dans nos services.
En savoir plus

"numéro de téléphone"

Par exemple, si vous ajoutez un numéro de téléphone en tant qu'option de récupération, nous pouvons vous envoyer un SMS contenant un code permettant de réinitialiser votre mot de passe, au cas où vous oublieriez ce dernier.
En savoir plus

"protéger aussi bien nos utilisateurs que nous-mêmes"

Par exemple, si vous soupçonnez que votre messagerie a fait l'objet d'un accès non autorisé, la fonctionnalité "Dernière activité sur le compte" de Gmail permet d'afficher des informations sur l'activité récente de votre compte, notamment les adresses IP utilisées pour accéder à ce dernier, la position géographique associée, ainsi que la date et l'heure correspondantes.
En savoir plus

"protéger"

Par exemple, l'une des raisons pour lesquelles nous collectons et analysons les adresses IP et les cookies consiste à protéger nos services des abus automatisés.
En savoir plus

"fournir"

Par exemple, l'adresse IP attribuée à votre appareil permet d'y renvoyer les données que vous avez demandées.
En savoir plus

"partager"

Par exemple, grâce à Google+, vous disposez de plusieurs options de partage.
En savoir plus

"simplifier et accélérer le partage avec d'autres internautes"

Par exemple, si une personne fait déjà partie de vos contacts, son nom est saisi semi-automatiquement dans Google si vous souhaitez l'ajouter à un message dans Gmail.
En savoir plus

"les personnes qui vous intéressent le plus sur le Web"

Par exemple, lorsque vous saisissez une adresse dans le champ "À", "Cc" ou "Cci" d'un message que vous composez dans Gmail, des adresses vous sont suggérées à partir de votre liste de contacts.
En savoir plus

"faciliter le partage de vos informations avec des personnes que vous connaissez"

Par exemple, si vous avez été en contact avec une personne via Gmail et si vous voulez l'ajouter à un fichier Google Documents ou à un événement Google Agenda, Google vous facilite la tâche grâce à la saisie semi-automatique de son adresse e-mail dès que vous commencez à taper son nom.
En savoir plus

"consultez nos contenus et nos annonces, et que vous effectuez des actions sur celles-ci"

Par exemple, nous signalons régulièrement aux annonceurs si nous avons diffusé leur annonce sur une page et si cette annonce a pu être vue par les internautes (contrairement par exemple, au fait d'être sur une page que les utilisateurs n'ont pas déroulée).
En savoir plus

"Nous sommes susceptibles de partager publiquement, ainsi qu'avec nos partenaires (éditeurs, annonceurs ou sites associés) des informations agrégées"

Le fait qu'un grand nombre de personnes se mettent à effectuer une recherche particulière peut fournir des informations très utiles sur des tendances spécifiques à un instant donné.
En savoir plus

"Points d'accès WiFi et antennes-relais"

Par exemple, nous pouvons déterminer approximativement l'endroit où se trouve votre appareil en fonction de la position connue des antennes-relais situées à proximité.
En savoir plus

"résultats de recherche plus pertinents"

Par exemple, nous pouvons rendre vos recherches plus pertinentes et plus intéressantes en incluant des photos, des posts et d'autres contenus mis en ligne par vous ou vos amis.
En savoir plus

"supprimer vos contenus"

Par exemple, vous pouvez supprimer l'enregistrement de vos activités sur le Web et dans les applications, votre blog, un site Google dont vous êtes propriétaire, votre chaîne YouTube, votre profil Google+ ou votre compte Google dans son intégralité.
En savoir plus

"des informations relatives aux tendances"

Vous pouvez accéder à certaines de ces données sur Google Trends et dans les vidéos populaires sur YouTube.
En savoir plus

"Votre activité sur d'autres sites et dans d'autres applications"

Ces activités peuvent être liées à votre utilisation de produits Google, tels que la synchronisation Chrome, ou de sites et d'applications partenaires. Un grand nombre de propriétaires de sites Web et d'applications travaillent en partenariat avec Google pour améliorer leur contenu et leurs services. Par exemple, un site Web peut utiliser nos services publicitaires (tels qu'AdSense) ou nos outils d'analyse (comme Google Analytics). Ces produits partagent avec Google des informations relatives à vos activités et, selon vos paramètres de compte et les produits que vous employez (par exemple, dans le cas où un partenaire utilise Google Analytics conjointement avec nos services publicitaires), ces données peuvent être associées à vos informations personnelles.
En savoir plus

ANNEXE 10

Google for Education

Avis de confidentialité de G Suite for Education

Cet avis de confidentialité décrit la façon dont Google collecte et utilise les données des comptes G Suite for Education. Il complète les Règles de confidentialité de Google générales, lesquelles s'appliquent également à ces comptes.

Création de comptes par l'administrateur. Le compte G Suite for Education d'un élève est un compte Google créé par l'administrateur du domaine et associé à l'établissement où cet élève est inscrit. Lors de la création d'un tel compte, l'administrateur peut être amené à fournir certaines informations personnelles, y compris, par exemple, le prénom, le nom de famille et l'adresse e-mail de l'élève. Ces informations sont rattachées au compte.

Services principaux de G Suite for Education. Les Services principaux de G Suite for Education sont les suivants : Gmail, Google Agenda, Classroom, Contacts, Drive, Docs, Forms, Google Groupes, Sheets, Google Sites, Slides, Talk/Hangouts et Vault. Ces services sont mis à la disposition de votre établissement d'enseignement dans le cadre du Contrat G Suite for Education et de l'Amendement relatif au traitement des données (vous pouvez demander à votre établissement s'il a accepté ce dernier). Le contrat décrit la manière dont les Données du Client sont utilisées et partagées en vertu de ses dispositions. Il s'applique uniquement aux Services principaux. Google ne diffuse aucune annonce dans les Services principaux, et les dispositions relatives à la confidentialité stipulées dans le contrat limitent le partage des Données du Client avec des tiers dans le cadre des Services principaux.

Restrictions relatives à la publicité. En dehors des Services principaux de G Suite for Education, les produits et services Google peuvent afficher des annonces, comme cela est décrit dans les Règles de confidentialité de Google. Lorsque G Suite for Education est utilisé dans des établissements du primaire et du secondaire, Google n'exploite pas les informations personnelles des utilisateurs (ou toute information associée à un compte Google) pour diffuser des annonces ciblées.

Interprétation des conditions contradictoires. En cas de contradiction, les conditions s'appliquent selon l'ordre suivant : le Contrat G Suite for Education (dans sa version amendée), le présent Avis de confidentialité et les Règles de confidentialité de Google.

ANNEXE 11

Google Cloud

Version 1.6 of the Data Processing Amendment will apply (in relation to G Suite Agreements) until 24 May 2018 inclusive and, as from 25 May 2018 (when the EU's General Data Protection Regulation comes into force), will be replaced by Version 2.0 of the Data Processing Amendment (below).

Current Version (1.6) of Data Processing Amendment

Data Processing Amendment to G Suite Agreement

The Customer agreeing to these terms ("**Customer**") and Google Inc., Google Ireland Limited, Google Commerce Limited, Google Asia Pacific Pte. Ltd., or Google Australia Pty Ltd (as applicable, "**Google**") have entered into a G Suite Agreement, G Suite via Reseller Agreement, G Suite for Education Agreement, G Suite for Education via Reseller Agreement, Google Apps for Work Agreement, Google Apps Enterprise Agreement, Google Apps for Business Agreement, Google Apps for Work via Reseller Agreement, Google Apps Enterprise via Reseller Agreement, Google Apps for Business via Reseller Agreement, Google Apps for Education Agreement or Google Apps for Education via Reseller Agreement, as applicable (as amended to date, the "**G Suite Agreement**"). This amendment (the "**Data Processing Amendment**") is entered into by Customer and Google as of the Amendment Effective Date and amends the G Suite Agreement

The "**Amendment Effective Date**" is: (a) if this Data Processing Amendment is incorporated directly into the G Suite Agreement (whether by reference, or otherwise), the effective date of the G Suite Agreement, as defined in that agreement; or (b) if this Data Processing Amendment is not incorporated directly into the G Suite Agreement, the date Customer accepts this Data Processing Amendment by clicking to accept these terms.

If this Data Processing Amendment is not incorporated into the G Suite Agreement by reference and you are accepting on behalf of Customer, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms; (ii) you have read and understand these terms; and (iii) you agree, on behalf of the party you represent, to this Data Processing Amendment. If you do not have the legal authority to bind Customer, please do not click the "I Accept" button.

1. **Introduction**.

   This Data Processing Amendment reflects the parties' agreement with respect to terms governing the processing of Customer Data under the G Suite Agreement.

2. **Definitions**.

   2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given in the G Suite Agreement. In this Data Processing Amendment, unless expressly stated otherwise:

   "**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

   "**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any Google Affiliate display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using the "Google Sites" functionality within the Services).

   "**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

   "**Agreement**" means the G Suite Agreement, as amended by this Data Processing Amendment and as

may be further amended from time to time in accordance with the G Suite Agreement.

"**Alternative Transfer Solution**" means a solution, other than the Model Contract Clauses, that ensures an adequate level of protection of personal data in a third country within the meaning of Article 25 of the Directive.

"**Customer Data**" means data (which may include personal data and the categories of data referred to in Appendix 1) submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Data Incident**" means (a) any unlawful access to Customer Data stored in the Services or systems, equipment or facilities of Google or its Subprocessors, or (b) unauthorized access to such Services, systems, equipment or facilities that results in loss, disclosure or alteration of Customer Data.

"**Data Privacy Officer**" means Google's Data Privacy Officer for G Suite.

"**Data Protection Legislation**" means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Customer and/or any Customer Affiliates as the controller(s) of the Customer Data; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"**EEA**" means the European Economic Area.

"**Full Activation Date**" means: (a) if this Data Processing Amendment is incorporated directly into the G Suite Agreement (whether by reference or otherwise), the Amendment Effective Date; or (b) if this Data Processing Amendment is not incorporated directly into the G Suite Agreement, the eighth (8th) day after the Amendment Effective Date.

"**Google Group**" means those Google Affiliates involved in provision of the Services to Customer.

"**Instructions**" means Customer's written instructions to Google consisting of the Agreement, including instructions to Google to provide the Services and technical support for the Services as set out in the Agreement; instructions given by Customer, its Affiliates and End Users via the Admin Console and otherwise in its and their use of the Services and related technical support services; and any subsequent written instructions given by Customer to Google and acknowledged by Google.

"**Model Contract Clauses**" or "**MCCs**" means the standard contractual clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Services**" means, for purposes of this Data Processing Amendment, the Core Services for G Suite Basic as described at https://gsuite.google.com/intl/en/terms/user_features.html (as such services and URL link may be updated or modified by Google from time to time in accordance with the G Suite Agreement), and all editions of G Suite that are described at such URL link as comprising or including such Core Services. For clarity, the Services for purposes of this Data Processing Amendment include G Suite Business, G Suite Business (Team Managed) and G Suite for Education but exclude Google Message Encryption.

"**Subprocessors**" means (a) all Google Group entities that have logical access to and process Customer Data (each, a "**Google Group Subprocessor**"); and (b) all third parties (other than Google Group entities) that are engaged to provide services to Customer and that have logical access to and process Customer Data (each, a "**Third Party Subprocessor**").

"**Term**" means the term of the G Suite Agreement, as defined in that agreement.

"**Third Party Auditor**" means a qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

2.2. The terms "personal data", "processing", "data subject", "controller" and "processor" have the meanings given to them in the Directive. The terms "data importer" and "data exporter" have the meanings given to them in the Model Contract Clauses.

3. **Term**.

This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry or termination of the G Suite Agreement, will remain in effect until, and automatically terminate upon, deletion by Google of all data as described in Section 7 (Data Deletion) of this Data Processing Amendment.

4. **Data Protection Legislation**.

The parties agree and acknowledge that the Data Protection Legislation will apply to the processing of Customer Data if, for example, the processing is carried out in the context of the activities of an establishment of the Customer (or of an authorized Customer Affiliate) in the territory of an EU Member State.

5. **Processing of Customer Data**.

5.1. **Controller and Processor**. If the Data Protection Legislation applies to the processing of Customer Data, then as between the parties, the parties acknowledge and agree that: (a) Customer is the controller of Customer Data under the Agreement; (b) Google is a processor of such data; (c) Customer will comply with its obligations as a controller under the Data Protection Legislation; and (d) Google will comply with its obligations as a processor under the Agreement. If under the Data Protection Legislation a Customer Affiliate is considered the controller (either alone or jointly with the Customer) with respect to certain Customer Data, Customer represents and warrants to Google that Customer is authorized (i) to give the Instructions to Google and otherwise act on behalf of such Customer Affiliate in relation to such Customer Data as described in this Data Processing Amendment, and (ii) to bind the Customer Affiliate to the terms of this Data Processing Amendment.

5.2. **Scope of Processing**. As from the Full Activation Date (at the latest), Google will only process Customer Data in accordance with the Instructions, and will not process Customer Data for any other purpose.

5.3. **Processing Restrictions**. Notwithstanding any other term of the Agreement, Google will not process Customer Data for Advertising purposes or serve Advertising in the Services.

5.4. **Additional Products**. Customer acknowledges that if it installs, uses, or enables Additional Products, the Services may allow such Additional Products to access Customer Data as required for the interoperation of those Additional Products with the Services. This Data Processing Amendment does not apply to the processing of data transmitted to or from such Additional Products. Customer can enable or disable Additional Products. Customer is not required to use Additional Products in order to use the

Services.

6. **Data Security; Security Compliance; Audits**.

6.1. **Security Measures**. Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration or unauthorized disclosure or access or other unauthorized processing, as detailed in Appendix 2 (the "**Security Measures**"). Google may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. Customer agrees that it is solely responsible for its use of the Services, including securing its account authentication credentials, and that Google has no obligation to protect Customer Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (e.g., offline or on-premise storage).

6.2. **Security Compliance by Google Staff**. Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance.

6.3. **Data Incidents**. If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by Customer in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring the contact information given for purposes of the Notification Email Address is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

6.4. **Compliance with Security and Privacy Standards; SOC 2 and 3 Reports**. During the Term, Google will maintain the following:

(a) its ISO/IEC 27001:2013 Certification or a comparable certification ("**ISO 27001 Certification**") for the Services;

(b) conformity of the Services with ISO/IEC 27018:2014 or a comparable standard ("**ISO 27018 Conformity**"), as independently verified;

(c) its confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability as related to the Services (the "**SOC 2 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months; and

(d) its Service Organization Control (SOC) 3 Report (or a comparable report) as related to the Services (the "**SOC 3 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months.

6.5. **Auditing Security Compliance**

6.5.1. **Reviews of Security Documentation**. Google will make the following available for review by Customer:

(a) the certificate issued in relation to Google's ISO 27001 Certification;

(b) the then-current SOC 3 Report;

(c) a summary or redacted version of the then-current confidential SOC 2 Report; and

(d) following a request by Customer in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.

6.5.2. **Customer Audits**. If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 of this Data Processing Amendment, Customer or such Customer Affiliate may exercise the audit rights granted under clauses 5(f) and 12(2) of such Model Contract Clauses:

(a) by instructing Google to execute the audit as described in Sections 6.4 and 6.5.1 above; and/or

(b) following a request by Customer in accordance with Section 6.5.4 below, by executing an audit as described in such Model Contract Clauses.

6.5.3. **Additional Business Terms for Reviews and Audits**. Google and Customer (or an authorized Customer Affiliate if applicable) will discuss and agree in advance on:

(a) the reasonable date(s) of and security and confidentiality controls applicable to any Customer review under Section 6.5.1(d); and

(b) the identity of a suitably qualified independent auditor for any audit under Section 6.5.2(b), and the reasonable start date, scope and duration of and security and confidentiality controls applicable to any such audit.

Google reserves the right to charge a fee (based on Google's reasonable costs) for any review under Section 6.5.1(d) and/or audit under Section 6.5.2(b). Google will provide further details of any applicable fee, and the basis of its calculation, to Customer (or an authorized Customer Affiliate) in advance of any such review or audit. For clarity, Google is not responsible for any costs incurred or fees charged by any third party auditor appointed by Customer (or an authorized Customer Affiliate) in connection with an audit under Section 6.5.2(b). Nothing in this Section 6.5 varies or modifies any rights or obligations of Customer (or any authorized Customer Affiliate) or Google Inc. under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA) of this Data Processing Amendment.

6.5.4. **Requests for Reviews and Audits**. Any requests under Section 6.5.1 or 6.5.2 must be sent to the Data Privacy Officer as described in Section 9 (Data Privacy Officer) of this Data Processing Amendment.

7. **Data Deletion**.

7.1. **Deletion by Customer and End Users**. During the Term, Google will provide Customer or End Users with the ability to delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer or End User deletes Customer Data and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash" ("**Customer-Deleted Data**"), Google will delete such data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.2. **Deletion on Standard Termination**. On expiry or termination of the G Suite Agreement (or, if applicable, on expiry of any post-termination period during which Google may agree to continue providing the Services), Google will, subject to Section 7.3 (Deletion on Termination for Non-Payment or No Purchase) below, delete all Customer-Deleted Data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing

so.

7.3. **Deletion on Termination for Non-Payment or No Purchase**. On termination of the G Suite Agreement due to Customer breaching its payment obligations or opting not to purchase the Services at the end of a free trial of the Services, Google will delete all Customer Data from its systems within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

8. **Access to Data**.

8.1. **Access; Export of Data**. During the Term, Google will provide Customer with access to and the ability to correct, block and export Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. To the extent Customer, in its use and administration of the Services during the Term, does not have the ability to correct or block Customer Data as required by applicable law, or to migrate Customer Data to another system or service provider, Google will comply with any reasonable requests from Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the Customer Data.

8.2. **End User Requests**. During the Term, if Google receives any request from an End User for records relating to that End User's personal data included in the Customer Data, Google will advise such End User to submit its request to Customer. Customer will be responsible for responding to any such request using the functionality of the Services.

9. **Data Privacy Officer**.

The Data Privacy Officer can be contacted by Customer Administrators at: https://support.google.com/a/contact/gfw_dpo (or via such other means as may be provided by Google). Administrators must be signed in to their Admin Account to use this address.

10. **Data Transfers**.

10.1. **Data Storage and Processing Facilities**. Google may store and process Customer Data in the United States or any other country in which Google or any of its Subprocessors maintains facilities, subject to Section 10.2 (Transfers of Data Out of the EEA) below.

10.2. **Transfers of Data Out of the EEA**.

10.2.1 **Customer Obligations**. If the storage and/or processing of Customer Data (as set out in Section 10.1 above) involves transfers of Customer personal data out of the EEA and Data Protection Legislation applies to the transfers of such data ("**Transferred Personal Data**"), Customer acknowledges that Data Protection Legislation will require Customer (or an authorized Customer Affiliate) to enter into Model Contract Clauses in respect of such transfers, unless Google has adopted an Alternative Transfer Solution.

10.2.2 **Google Obligations**. In respect of Transferred Personal Data, Google will:

(a) if requested to do so by Customer, ensure that Google Inc. as the data importer of the Transferred Personal Data enters into Model Contract Clauses with Customer (or an authorized Customer Affiliate) as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or

(b) adopt an Alternative Transfer Solution, ensure that transfers are made in accordance with such Alternative Transfer Solution and make information available about adoption of such solution.

10.3. **Data Center Information**. Google will make available to Customer information about the countries in

which data centers used to store Customer Data are located.

10.4 **Disclosure of Confidential Information Containing Personal Data**. If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Google will, notwithstanding any term to the contrary in the Agreement, ensure that any disclosure of Customer's (or, if applicable, an authorized Customer Affiliate's) Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. **Subprocessors**.

11.1. **Subprocessors**. Google may engage Subprocessors to provide parts of the Services and related technical support services, subject to the restrictions in this Data Processing Amendment.

11.2. **Subprocessing Restrictions**. Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required by the following, as applicable pursuant to Section 10.2 (Transfers of Data Out of the EEA): (a) any Model Contract Clauses entered into by Google Inc. and Customer (or an authorized Customer Affiliate); and/or (b) any Alternative Transfer Solution adopted by Google.

11.3. **Consent to Subprocessing**. Customer consents to Google subcontracting the processing of Customer Data to Subprocessors in accordance with the Agreement. If the Model Contract Clauses have been entered into as described above, Customer (or, if applicable, an authorized Customer Affiliate): (a) consents to Google Inc. subcontracting the processing of Customer Data in accordance with the terms of the Model Contract Clauses; and (b) acknowledges that this constitutes the prior written consent of Customer (or the applicable authorized Customer Affiliate) for the purpose of clause 11(1) of the Model Contract Clauses.

11.4. **Additional Information**. Information about Subprocessors including their function and location is available at the following URL: https://gsuite.google.com/intl/en/terms/subprocessors.html, as such URL may be updated by Google from time to time. The information available at the URL is accurate at the time of publication.

11.5. **Termination**. Google will, at least 15 days before appointing any new Third Party Subprocessor, inform Customer of the appointment (including the name and location of such subprocessor and the activities it will perform) either by sending an email to the Notification Email Address or via the Admin Console. If Customer objects to Google's use of any new Third Party Subprocessor, Customer may, as its sole and exclusive remedy, terminate the G Suite Agreement by giving written notice to Google within 30 days of being informed by Google of the appointment of such subprocessor.

12. **Liability Cap**.

If Google Inc. and Customer (or an authorized Customer Affiliate) enter into Model Contract Clauses as described above, then, subject to the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability), the total combined liability of Google and its Affiliates towards Customer and its Affiliates, on the one hand, and Customer and its Affiliates towards Google and its Affiliates, on the other hand, under or in connection with the Agreement and all those MCCs combined will be limited to the maximum monetary or payment-based liability amount set out in the Agreement.

13. **Third Party Beneficiary**.

Notwithstanding anything to the contrary in the Agreement, where Google Inc. is not a party to the

Agreement, Google Inc. will be a third party beneficiary of Section 6.5 (Auditing Security Compliance), Section 11.3 (Consent to Subprocessing) and Section 12 (Liability Cap) of this Data Processing Amendment.

14. **Effect of Amendment**.

To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, the Agreement remains in full force and effect.

Appendix 1: Categories of Data and Data Subjects

Categories of Data

Personal data submitted, stored, sent or received by Customer or End Users via the Services may include the following categories of data: user IDs, email, documents, presentations, images, calendar entries, tasks and other data.

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As of the Amendment Effective Date, Google will take and implement the Security Measures set out in this Appendix to the Data Processing Amendment. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. **Data Center & Network Security**.

(a) **Data Centers**.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) **Networks & Transmission**.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;

2. Employing intelligent detection controls at data entry points; and

3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. **Access and Site Controls**.

(a) **Site Controls**.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data

center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) **Access Control**.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.

3. **Data**.

(a) **Data Storage, Isolation & Authentication**.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google logically isolates each Customer's data, and logically separates each End User's data from the data of other End Users, and data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

The Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to End Users for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use. Google agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) **Decommissioned Disks and Disk Erase Policy**.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy

4. **Personnel Security**.

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Google's personnel will not process Customer Data without authorization.

5. **Subprocessor Security**.

Prior to onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.2 (Subprocessing Restrictions) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Version 2.0 of the Data Processing Amendment will take effect from 25 May 2018 (when the EU's General Data Protection Regulation comes into force) and replace Version 1.6 of the Data Processing Amendment (where applicable) on that date.

Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.0)

The Customer agreeing to these terms ("**Customer**") and Google LLC (formerly known as Google Inc.), Google Ireland Limited, Google Commerce Limited, Google Asia Pacific Pte. Ltd or Google Australia Pty Ltd (as applicable, "**Google**") have entered into one or more G Suite Agreement(s) (as defined below) and/or Complementary Product Agreements(s) (as defined below) (each, as amended from time to time, an "**Agreement**").

This Data Processing Amendment to G Suite and/or Complementary Product Agreement including its appendices (the "**Data Processing Amendment**") will, as from the Amendment Effective Date (as defined below), be effective and replace any previously applicable data processing amendment or, in the case of a Complementary Product Agreement, any terms previously applicable to privacy, data processing and/or data security.

1. **Introduction**.

   This Data Processing Amendment reflects the parties' agreement with respect to the terms governing the processing and security of Customer Data under the applicable Agreement.

2. **Definitions**.

   2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given elsewhere in the applicable Agreement. In this Data Processing Amendment, unless stated otherwise:

   "**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

   "**Additional Security Controls**" means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines. "Additional Security Controls" may include the Admin Console and other features and functionality of the Services such as two factor authentication, security key enforcement and monitoring capabilities.

   "**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any of its Affiliates display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using any Google Sites functionality within the Services).

   "**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as: (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

   "**Agreed Liability Cap**" means the maximum monetary or payment-based amount at which a party's liability is capped under the applicable Agreement, either per annual period or event giving rise to liability, as applicable.

   "**Alternative Transfer Solution**" means a solution, other than the Model Contract Clauses, that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).

"**Amendment Effective Date**" means, as applicable:

(a) 25 May 2018, if Customer clicked to accept or the parties otherwise agreed to this Data Processing Amendment in respect of the applicable Agreement prior to or on such date; or

(b) the date on which Customer clicked to accept or the parties otherwise agreed to this Data Processing Amendment in respect of the applicable Agreement, if such date is after 25 May 2018.

"**Audited Services**" means the Services (as defined below), unless the G Suite Services Summary or Complementary Product Services Summary indicates otherwise.

"**Complementary Product Agreement**" means: a Cloud Identity Agreement; Domain Administrator Agreement; any other agreement under which Google agrees to provide identity services as such to Customer; or any other agreement that incorporates this Data Processing Amendment by reference or states that it will apply if accepted by Customer.

"**Complementary Product Services Summary**" means the then-current description of the services provided under a Complementary Product Agreement, as set out in the applicable Agreement.

"**Core Services for G Suite**" means the Core Services for G Suite, as described in the G Suite Services Summary and irrespective of the G Suite edition comprising such services. For clarity, the Core Services for G Suite exclude Google+ to the extent it is used to share content or interact with any persons outside an End User's G Suite Domain, and exclude any "other add-on services" described in the G Suite Services Summary.

"**Customer Data**" means data submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Customer Personal Data**" means personal data contained within the Customer Data.

"**Data Incident**" means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google. "Data Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"**Domain**" means the primary domain and any secondary domains managed together by Customer within a single instance of the Admin Console.

"**EEA**" means the European Economic Area.

"**European Data Protection Legislation**" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Full Activation Date**" means: (a) if this Data Processing Amendment is incorporated into the applicable Agreement by reference, the Amendment Effective Date; or (b) if the parties otherwise agreed to this Data Processing Amendment, the eighth day after the Amendment Effective Date.

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"**Google's Third Party Auditor**" means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

"**G Suite Agreement**" means: one or more Order Form(s) specifying that Google will provide

the Core Services for G Suite under a Master Agreement, combined with a set of General Terms and a G Suite Services Schedule; a G Suite Agreement; a G Suite for Education Agreement; a Google Apps for Work Agreement; a Google Apps Enterprise Agreement; a Google Apps for Business Agreement; a Google Apps for Education Agreement; a Via Reseller version of any of the foregoing agreements; or any other agreement under which Google agrees to provide the Core Services for G Suite to Customer.

"**G Suite Services Summary**" means the then-current description of the Core Services for G Suite and related editions, as set out at https://gsuite.google.com/terms/user_features.html (as may be updated by Google from time to time in accordance with the G Suite Agreement).

"**ISO 27001 Certification**" means ISO/IEC 27001:2013 certification or a comparable certification, as related to the Audited Services.

"**ISO 27017 Certification**" means ISO/IEC 27017:2015 certification or a comparable certification, as related to the Audited Services.

"**ISO 27018 Certification**" means ISO/IEC 27018:2014 certification or a comparable certification, as related to the Audited Services.

"**Model Contract Clauses**" or "MCCs" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

"**Non-European Data Protection Legislation**" means data protection or privacy legislation other than the European Data Protection Legislation.

"**Notification Email Address**" means the email address(es) designated by Customer in the Admin Console or the Order Form to receive certain notifications from Google.

"**Security Documentation**" means all documents and information made available by Google under Section 7.5.1 (Reviews of Security Documentation).

"**Security Measures**" has the meaning given in Section 7.1.1 (Google's Security Measures).

"**Services**" means the following services, as applicable: (a) the Core Services for G Suite; or (b) the services described in the Complementary Product Services Summary.

"**SOC 2 Report**" means a confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability, as produced by Google's Third Party Auditor in relation to the Audited Services.

"**SOC 3 Report**" means a Service Organization Control (SOC) 3 Report (or a comparable report), as produced by Google's Third Party Auditor in relation to the Audited Services.

"**Subprocessors**" means third parties authorized under this Data Processing Amendment to have logical access to and process Customer Data in order to provide parts of the Services and related technical support.

"**Term**" means the period from the Amendment Effective Date until the end of Google's provision of the Services under the applicable Agreement, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.

2.2. The terms "personal data", "data subject", "processing", "controller", "processor" and "supervisory authority" as used in this Data Processing Amendment have the meanings given in the GDPR, and the terms "data importer" and "data exporter" have the meanings given in the Model Contract Clauses, in each case irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies.

3. **Duration of Data Processing Amendment**. This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry of the Term, remain in effect until, and automatically expire upon, deletion of all Customer Data by Google as described in this Data Processing Amendment.

4. **Scope of Data Protection Legislation**.

4.1 Application of European Legislation. The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Personal Data if, for example:

(a) the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA; and/or

(b) the Customer Personal Data is personal data relating to data subjects who are in the EEA and the processing relates to the offering to them of goods or services in the EEA or the monitoring of their behaviour in the EEA.

4.2 Application of Non-European Legislation. The parties acknowledge and agree that Non-European Data Protection Legislation may also apply to the processing of Customer Personal Data.

4.3 Application of Data Processing Amendment. Except to the extent this Data Processing Amendment states otherwise, the terms of this Data Processing Amendment will apply irrespective of whether the European Data Protection Legislation or Non-European Data Protection Legislation applies to the processing of Customer Personal Data.

5. **Processing of Data**.

5.1 **Roles and Regulatory Compliance; Authorization**.

5.1.1. Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

(a) the subject matter and details of the processing are described in Appendix 1;

(b) Google is a processor of that Customer Personal Data under the European Data Protection Legislation;

(c) Customer is a controller or processor, as applicable, of that Customer Personal Data under the European Data Protection Legislation; and

(d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

5.1.2. Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Google that Customer's instructions and actions with respect to that Customer Personal Data, including its appointment of Google as another processor, have been authorized by the relevant controller.

5.1.3. Responsibilities under Non-European Legislation. If Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data.

5.2 **Scope of Processing**.

5.2.1 Customer's Instructions. By entering into this Data Processing Amendment, Customer instructs Google to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services and related technical support; (b) as further specified via Customer's use of the Services (including the Admin Console and other functionality of the Services) and related technical support; (c) as documented in the form of the applicable Agreement, including this Data Processing Amendment; and (d) as further documented in any

other written instructions given by Customer and acknowledged by Google as constituting instructions for purposes of this Data Processing Amendment.

5.2.2 Google's Compliance with Instructions. As from the Full Activation Date, Google will comply with the instructions described in Section 5.2.1 (Customer's Instructions) (including with regard to data transfers) unless EU or EU Member State law to which Google is subject requires other processing of Customer Personal Data by Google, in which case Google will inform Customer (unless that law prohibits Google from doing so on important grounds of public interest) via the Notification Email Address. For clarity, Google will not process Customer Personal Data for Advertising purposes or serve Advertising in the Services.

5.3. **Additional Products**. If Google at its option makes any Additional Products available to Customer in accordance with the Additional Product Terms (if applicable), and if Customer opts to install or use those Additional Products, the Services may allow those Additional Products to access Customer Personal Data as required for the interoperation of the Additional Products with the Services. For clarity, this Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products. Customer may use the functionality of the Services to enable or disable Additional Products, and is not required to use Additional Products in order to use the Services.

6. **Data Deletion**.

6.1. **Deletion During Term**. Google will enable Customer and/or End Users to delete Customer Data during the applicable Term in a manner consistent with the functionality of the Services. If Customer or an End User uses the Services to delete any Customer Data during the applicable Term and the Customer Data cannot be recovered by Customer or an End User (such as from the "trash"), this use will constitute an instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage.

6.2. **Deletion on Term Expiry**. Subject to Section 6.3 (Deferred Deletion Instruction), on expiry of the applicable Term Customer instructs Google to delete all Customer Data (including existing copies) from Google's systems in accordance with applicable law. Google will comply with this instruction as soon as reasonably practicable and within a maximum period of 180 days, unless EU or EU Member State law requires storage. Without prejudice to Section 9.1 (Access; Rectification; Restricted Processing; Portability), Customer acknowledges and agrees that Customer will be responsible for exporting, before the applicable Term expires, any Customer Data it wishes to retain afterwards.

6.3. **Deferred Deletion Instruction**. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Deletion on Term Expiry) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will only take effect with respect to such Customer Data when the continuing Term expires. For clarity, this Data Processing Amendment will continue to apply to such Customer Data until its deletion by Google.

7. **Data Security**.

7.1. **Google's Security Measures, Controls and Assistance**.

7.1.1. Google's Security Measures. Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "Security Measures"). As described in Appendix 2, the Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services; to help restore timely access to personal data following an incident; and for regular testing of effectiveness. Google may update or modify the Security

Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

7.1.2. Security Compliance by Google Staff. Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.1.3. Additional Security Controls. In addition to the Security Measures, Google will make the Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4. Google's Security Assistance. Customer agrees that Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with any of Customer's obligations in respect of security of personal data and personal data breaches, including if applicable Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

(b) making the Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);

(c) complying with the terms of Section 7.2 (Data Incidents); and

(d) providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement including this Data Processing Amendment.

7.2. **Data Incidents**.

7.2.1. Incident Notification. If Google becomes aware of a Data Incident, Google will: (a) notify Customer of the Data Incident promptly and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2. Details of Data Incident. Notifications made pursuant to this section will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps Google recommends Customer take to address the Data Incident.

7.2.3. Delivery of Notification. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address or, at Google's discretion, by direct communication (for example, by phone call or an in-person meeting). Customer is solely responsible for ensuring that the Notification Email Address is current and valid.

7.2.4. No Assessment of Customer Data by Google. Google will not assess the contents of Customer Data in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Data Incident(s).

7.2.5. No Acknowledgment of Fault by Google. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3. **Customer's Security Responsibilities and Assessment**.

7.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Google's obligations under Section 7.1 (Google's Security Measures, Controls and Assistance) and Section 7.2 (Data Incidents):

(a) Customer is solely responsible for its use of the Services, including:

(i) making appropriate use of the Services and the Additional Security Controls to ensure a level of security appropriate to the risk in respect of the Customer Data;

(ii) securing the account authentication credentials, systems and devices Customer uses to access the Services; and

(iii) backing up its Customer Data; and

(b) Google has no obligation to protect Customer Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (for example, offline or on-premise storage), or to protect Customer Data by implementing or maintaining Additional Security Controls except to the extent Customer has opted to use them.

7.3.2. Customer's Security Assessment.

(a) Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures, the Additional Security Controls and Google's commitments under this Section 7 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation and/or Non-European Data Protection Legislation, as applicable.

(b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Google as set out in Section 7.1.1 (Google's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Data.

7.4. **Security Certifications and Reports**. Google will do the following to evaluate and help ensure the continued effectiveness of the Security Measures:

(a) maintain the ISO 27001 Certification, the ISO 27017 Certification and the ISO 27018 Certification; and

(b) update the SOC 2 Report and SOC 3 Report at least once every 18 months.

7.5. **Reviews and Audits of Compliance**.

7.5.1. Reviews of Security Documentation. In addition to the information contained in the applicable Agreement including this Data Processing Amendment, Google will make available for review by Customer the following documents and information to demonstrate compliance by Google with its obligations under this Data Processing Amendment:

(a) the certificates issued in relation to the ISO 27001 Certification, the ISO 27017 Certification and the ISO 27018 Certification;

(b) the then-current SOC 3 Report; and

(c) the then-current SOC 2 Report, following a request by Customer in accordance with Section 7.5.3(a).

7.5.2. Customer's Audit Rights.

(a) If the European Data Protection Legislation applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Data Processing Amendment in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). Google will contribute to such

audits as described in Section 7.4 (Security Certifications and Reports) and this Section 7.5 (Reviews and Audits of Compliance).

(b) If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Google will, without prejudice to any audit rights of a supervisory authority under such Model Contract Clauses, allow Customer or an independent auditor appointed by Customer to conduct audits as described in the Model Contract Clauses in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

(c) Customer may also conduct an audit to verify Google's compliance with its obligations under this Data Processing Amendment by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third Party Auditor).

7.5.3. Additional Business Terms for Reviews and Audits.

(a) Customer must send any requests for reviews of the SOC 2 Report under Section 7.5.1(c) or audits under Section 7.5.2(a) or 7.5.2(b) to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).

(b) Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 Report under Section 7.5.1(c); and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) or 7.5.2(b).

(c) Google may charge a fee (based on Google's reasonable costs) for any review of the SOC 2 Report under Section 7.5.1(c) and/or audit under Section 7.5.2(a) or 7.5.2(b). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such review or audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

(d) Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) or 7.5.2(b) if the auditor is, in Google's reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.

7.5.4. No Modification of MCCs. Nothing in this Section 7.5 (Reviews and Audits of Compliance) varies or modifies any rights or obligations of Customer or Google LLC under any Model Contract Clauses entered into as described in Section 10.2 (Transfers of Data Out of the EEA).

8. **Impact Assessments and Consultations**. Customer agrees that Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with any obligations of Customer in respect of data protection impact assessments and prior consultation, including if applicable Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

(a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation); and

(b) providing the information contained in the applicable Agreement including this Data Processing Amendment.

9. **Data Subject Rights; Data Export**.

9.1. **Access; Rectification; Restricted Processing; Portability**. During the applicable Term, Google will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify

and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion During Term), and to export Customer Data.

9.2. **Data Subject Requests**.

9.2.1. Customer's Responsibility for Requests. During the applicable Term, if Google receives any request from a data subject in relation to Customer Personal Data, Google will advise the data subject to submit his/her request to Customer, and Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2. Google's Data Subject Request Assistance. Customer agrees that (taking into account the nature of the processing of Customer Personal Data) Google will assist Customer in fulfilling any obligation to respond to requests by data subjects, including if applicable Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by:

(a) providing the Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls); and

(b) complying with the commitments set out in Section 9.1 (Access; Rectification; Restricted Processing; Portability) and Section 9.2.1 (Customer's Responsibility for Requests).

10. **Data Transfers**.

10.1. **Data Storage and Processing Facilities**. Customer agrees that Google may, subject to Section 10.2 (Transfers of Data Out of the EEA), store and process Customer Data in the United States and any other country in which Google or any of its Subprocessors maintains facilities.

10.2. **Transfers of Data Out of the EEA**.

10.2.1. Google's Transfer Obligations. If the storage and/or processing of Customer Personal Data (as set out in Section 10.1 (Data Storage and Processing Facilities)) involves transfers of Customer Personal Data out of the EEA and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal Data"), Google will:

(a) if requested to do so by Customer, ensure that Google LLC as the data importer of the Transferred Personal Data enters into Model Contract Clauses with Customer as the data exporter of such data, and that the transfers are made in accordance with such Model Contract Clauses; and/or

(b) offer an Alternative Transfer Solution, ensure that the transfers are made in accordance with such Alternative Transfer Solution, and make information available to Customer about such Alternative Transfer Solution.

10.2.2 Customer's Transfer Obligations. In respect of Transferred Personal Data, Customer agrees that:

(a) if under the European Data Protection Legislation Google reasonably requires Customer to enter into Model Contract Clauses in respect of such transfers, Customer will do so; and

(b) if under the European Data Protection Legislation Google reasonably requires Customer to use an Alternative Transfer Solution offered by Google, and reasonably requests that Customer take any action (which may include execution of documents) strictly required to give full effect to such solution, Customer will do so.

10.3. **Data Center Information**. Information about the locations of Google data centers is available at: https://www.google.com/about/datacenters/inside/locations/index.html (as may be updated by Google from time to time).

10.4 **Disclosure of Confidential Information Containing Personal Data**. If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), Google will, notwithstanding any term to the contrary in the applicable Agreement, ensure that any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, will be made in accordance with such Model Contract Clauses.

11. **Subprocessors**.

11.1. **Consent to Subprocessor Engagement**. Customer specifically authorizes the engagement of Google's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors ("**Third Party Subprocessors**"). If Customer has entered into Model Contract Clauses as described in Section 10.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Google LLC of the processing of Customer Data if such consent is required under the Model Contract Clauses.

11.2. **Information about Subprocessors**. Information about Subprocessors, including their functions and locations, is available at https://gsuite.google.com/intl/en/terms/subprocessors.html (as may be updated by Google from time to time in accordance with this Data Processing Amendment).

11.3. **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, Google will:

(a) ensure via a written contract that:

(i) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Data Processing Amendment) and any Model Contract Clauses entered into or Alternative Transfer Solution adopted by Google as described in Section 10.2 (Transfers of Data Out of the EEA); and

(ii) if the GDPR applies to the processing of Customer Personal Data, the data protection obligations set out in Article 28(3) of the GDPR, as described in this Data Processing Amendment, are imposed on the Subprocessor; and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4. **Opportunity to Object to Subprocessor Changes**.

(a) When any new Third Party Subprocessor is engaged during the applicable Term, Google will, at least 30 days before the new Third Party Subprocessor processes any Customer Data, inform Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform) either by sending an email to the Notification Email Address or via the Admin Console.

(b) Customer may object to any new Third Party Subprocessor by terminating the applicable Agreement immediately upon written notice to Google, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in Section 11.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

12. **Cloud Data Protection Team; Processing Records**.

12.1. **Google's Cloud Data Protection Team**. Google's Cloud Data Protection Team can be contacted by Customer's Administrators at https://support.google.com/a/contact/googlecloud_dpr (while Administrators are signed in to their Admin Account) and/or by Customer by providing a notice to Google as described in the applicable Agreement.

12.2. **Google's Processing Records**. Customer acknowledges that Google is required under the

GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Google is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where requested, provide such information to Google via the Admin Console or other means provided by Google, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

13. **Liability**.

13.1. **Liability Cap**. If Model Contract Clauses have been entered into as described in Section 10.2 (Transfers of Data Out of the EEA), the total combined liability of either party and its Affiliates towards the other party and its Affiliates under or in connection with the applicable Agreement and such Model Contract Clauses combined will be limited to the Agreed Liability Cap for the relevant party, subject to Section 13.2 (Liability Cap Exclusions).

13.2. **Liability Cap Exclusions**. Nothing in Section 13.1 (Liability Cap) will affect the remaining terms of the applicable Agreement relating to liability (including any specific exclusions from any limitation of liability).

14. **Third Party Beneficiary**. Notwithstanding anything to the contrary in the applicable Agreement, where Google LLC is not a party to such Agreement, Google LLC will be a third party beneficiary of Section 7.5 (Reviews and Audits of Compliance), Section 11.1 (Consent to Subprocessor Engagement) and Section 13 (Liability) of this Data Processing Amendment.

15. **Effect of Amendment**. To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the applicable Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, such Agreement remains in full force and effect. For clarity, if Customer has entered more than one Agreement, this Data Processing Amendment will amend each of the Agreements separately.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Services and related technical support to Customer.

Duration of the Processing

The applicable Term plus the period from expiry of such Term until deletion of all Customer Data by Google in accordance with the Data Processing Amendment.

Nature and Purpose of the Processing

Google will process Customer Personal Data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services for the purposes of providing the Services and related technical support to Customer in accordance with the Data Processing Amendment.

Categories of Data

Personal data submitted, stored, sent or received by Customer, its Affiliates or End Users via the Services may include the following categories of data: user IDs, email, documents, presentations, images, calendar entries, tasks and other data.

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As from the Amendment Effective Date, Google will implement and maintain the Security Measures set out in this Appendix 2 to the Data Processing Amendment. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

1. Data Center & Network Security.

(a) Data Centers.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;

2. Employing intelligent detection controls at data entry points; and

3. Employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls.

(a) Site Controls.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for

up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.

3. Data.

(a) Data Storage, Isolation & Authentication.

Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google logically isolates each Customer's data, and logically separates each End User's data from the data of other End Users, and data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to End Users for specific purposes. Customer may choose

to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use. Google agrees that changes to the APIs will not result in the degradation of the overall security of the Services.

(b) Decommissioned Disks and Disk Erase Policy.

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security.

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Google's personnel will not process Customer Data without authorization.

5. Subprocessor Security.

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.3 (Requirements for Subprocessor Engagement) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

ANNEXE 12

REPUBLIQUE ET CANTON DE GENEVE
Département de l'instruction publique, de la culture et du sport
La Conseillère d'Etat

DIP
Case postale 3925
1211 Genève 3

Aux députées et députés de la commission législative

N/réf. : AET/EZ

Genève, le 1er novembre 2017

Concerne : demande de la commission - contrat conclu avec Google pour l'utilisation de l'application « Ecole en ligne »

Mesdames et Messieurs les Députés,

En réponse à votre demande adressée au département de l'instruction publique, de la culture et du sport (ci-après : DIP ou département), je vous prie de trouver ci-joint :

1. le contrat de base G Suite for Education *en ligne* (anciennement Google Apps for Education) ;
2. l'avis de confidentialité qui l'accompagne ;
3. l'amendement au contrat précité relatif au traitement des données (en anglais) ;
4. les règles de confidentialité faisant partie intégrante du contrat ;
5. les garanties formulées par la société Google au DIP, incluant un avis en anglais de commissaires européens à la protection des données.

Comme vous pourrez le lire dans les documents joints, la société Google a confirmé par écrit que la loi américaine ne s'appliquait pas aux écoles suisses. Cette société nous a également communiqué l'avis positif des commissaires à la protection des données d'Irlande, d'Espagne et de Hambourg concernant le cadre contractuel de base applicable à Google Apps (devenu G Suite) (voir annexe 5).

En outre, afin de supprimer le risque que la loi américaine soit appliquée malgré les assurances fournies par la société Google à ce sujet, le DIP a demandé à changer formellement de partenaire contractuel, à savoir que le cocontractant du département ne soit plus la société Google Inc., société enregistrée aux Etats-Unis, mais Google Ireland Limited, une société constituée en vertu du droit irlandais, sise à Dublin. Cette demande vise à ce que les liens de rattachement avec les Etats-Unis d'Amérique soient insuffisants pour qu'une éventuelle requête en justice concernant l'application de la loi nationale de cet État soit admise (voir annexe 5).

Par ailleurs, le DIP appelle votre attention sur le chiffre 2.1 de l'amendement au contrat relatif au traitement des données, G Suite Data Processing Amendment, Version 1.6, qui fait expressément référence à la loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1) et qui est ainsi libellé :

« "Data Protection Legislation" means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Customer and/or any Customer Affiliates as the controller(s) of the Customer Data; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) » (voir annexe 3, p. 2).

En outre, le 25 mai 2018, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, entrera en vigueur et abrogera la directive 95/46/CE (règlement général sur la protection des données). En conséquence, l'amendement susmentionné sera également remplacé par le Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.0). Ce nouvel amendement fera également mention de la loi fédérale sur la protection des données sous la forme suivante :

« "European Data Protection Legislation" means, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) » (voir annexe 3, p. 13).

Par ailleurs, la société Google certifie, dans ses règles de confidentialité, sous la rubrique « Respect et coopération avec des organismes de régulation », qu'elle se conforme au Swiss-US Privacy Shield Framework et qu'elle s'engage à coopérer avec les autorités locales chargées de la protection des données en cas de litige ne pouvant être réglé directement avec l'utilisateur (voir annexe 4, p. 5).

Enfin, il convient de relever qu'un contrat va être prochainement formalisé *par écrit* avec la société Google, lequel se substituera au G Suite for Education *Online* Agreement et contiendra tous les points susmentionnés.

Cette mesure s'inscrit dans un catalogue de mesures mises en œuvre par le DIP, afin de répondre aux obligations lui incombant en matière de protection de la vie privée des élèves qui lui sont confiés, à savoir, outre la conclusion du contrat sous la forme écrite précité, l'instauration d'un cadre réglementaire strict d'utilisation de l'application « Ecole en ligne », une offre comprenant d'autres plates-formes collaboratives, des actions de sensibilisation et prévention auprès des élèves et des établissements concernés.

Tout en réaffirmant l'importance que le DIP accorde à la protection de la vie privée des élèves et sa sensibilité aux préoccupations soulevées par le projet de loi 12103, je vous invite à auditionner le rectorat de l'Université de Genève ou la direction de la HES-SO Genève en regard des incidences que ce projet de loi pourrait avoir sur les hautes écoles, notamment sur la production scientifique et la recherche.

Veuillez agréer, Mesdames et Messieurs les Députés, mes meilleures salutations.

Anne Emery-Torracinta

Annexes : mentionnées

ANNEXE 13

Google for Education

Contrat G Suite for Education (en ligne)

Ce Contrat G Suite for Education (le "**Contrat**") est conclu par et entre Google Inc. ("**Google**") et le client identifié dans le document de commande ("**Client**"). Le présent Contrat entre en vigueur à la date à laquelle le Client clique sur le bouton "J'accepte" ci-dessous ou, le cas échéant, la date à laquelle le Contrat est contresigné (la "**Date d'effet**"). Si vous acceptez les présentes au nom du Client, vous attestez et garantissez (i) que vous disposez de la capacité juridique nécessaire pour engager votre employeur ou l'entité concernée vis-à-vis des présentes conditions d'utilisation, (ii) que vous avez lu et compris le présent Contrat et (iii) que vous acceptez ce dernier au nom de la partie que vous représentez. Si vous ne disposez pas de l'autorité juridique nécessaire, veuillez ne pas cliquer sur le bouton "J'accepte" ci-dessous (ou, le cas échéant, ne signez pas ce Contrat). Le présent Contrat régit l'accès aux Services et leur utilisation par le Client et entrera en vigueur à la Date d'effet.

1. **Services**.

1.1 **Installations et transfert de données.** Toutes les installations utilisées pour stocker et traiter les Données du Client doivent respecter des normes de sécurité raisonnables, assurant une protection au moins équivalente à celle dont bénéficient les installations où Google stocke et traite ses propres informations du même type. Google a mis en œuvre des systèmes et des procédures au moins aussi exigeants que les normes en vigueur dans son secteur d'activité, pour garantir la sécurité et la confidentialité des Données du Client, pour les protéger des menaces ou risques prévisibles visant leur sécurité ou leur intégrité et pour prévenir les accès non autorisés aux Données du Client ou une utilisation non autorisée de celles-ci. Dans le cadre de la fourniture des Services, Google peut stocker et traiter les Données du Client aux États-Unis ou dans tout autre pays dans lequel Google ou ses agents gèrent des installations. En utilisant les Services, le Client consent à ce type de transfert, traitement et stockage de ses Données.

1.2 **Modifications**.

a. **Modification des services.** Google pourra apporter de temps à autre des modifications commercialement raisonnables aux services. Google s'engage à informer le Client de toute modification importante apportée aux Services, dans la mesure où ce dernier s'est inscrit auprès de Google afin d'être averti de telles modifications.

b. **Modification des Conditions d'utilisation hébergées sur des URL.** Google pourra apporter de temps à autre des modifications commercialement raisonnables aux Conditions d'utilisation hébergées sur des URL. Google s'engage à informer le Client de toute modification importante apportée aux Conditions d'utilisation hébergées sur des URL en envoyant un e-mail à l'Adresse e-mail de notification ou une alerte via la Console d'administration. Si la modification a un impact négatif important sur le Client et que ce dernier n'accepte pas ladite modification, il doit le notifier à Google via le Centre d'aide dans les trente jours qui suivent la réception de l'avis de modification. Si le Client notifie dûment Google de son refus, les conditions qui s'appliquaient juste avant la modification sont rétablies, et ce jusqu'à la fin de la Période de validité en vigueur au moment de la notification. Si les Services concernés sont renouvelés, ils le seront conformément aux nouvelles Conditions d'utilisation de Google hébergées sur des URL.

1.3 **Alias.** Le Client est seul responsable du contrôle des e-mails envoyés aux alias "abuse" et "postmaster" associés à ses Noms de domaine, ainsi que de leur traitement et des réponses qui y sont apportées. Toutefois, Google peut effectuer un contrôle des e-mails envoyés aux alias associés aux Noms de domaine du Client afin d'identifier toute utilisation abusive des Services.

1.4 **Annonces.** Google ne diffuse pas d'Annonce dans les Services ni n'utilise les Données du client à des fins publicitaires.

1.5 **Comptes utilisateur final.** Le Client peut demander des Comptes utilisateur final de deux façons : (i) en en faisant la demande en ligne via la Console d'administration ou (ii) après la date d'entrée en vigueur des Services, en contactant le service d'assistance Google. Le Client peut, à tout moment, suspendre ou supprimer des Comptes utilisateur final via la Console d'administration.

1.6 **Google Vault.** Si le Client achète Google Vault, les conditions supplémentaires suivantes s'appliquent :

a. **Conservation**. Google n'a pas l'obligation de conserver les Données archivées du Client au-delà de la période de conservation indiquée par le Client (sauf en cas de préservation de données à titre conservatoire). Si le Client ne renouvelle pas Google Vault, Google n'a pas l'obligation de conserver une archive des Données du Client.

b. **Achat initial de Google Vault**. Lorsque le Client achète Google Vault pour la première fois, il accepte d'acheter un Compte utilisateur final Google Vault pour chacun des membres de son Personnel disposant d'un Compte utilisateur final G Suite for Education. Le Client peut utiliser Google Vault pour les élèves et les Anciens élèves sans frais.

c. **Ajout de Comptes utilisateur final pour le personnel.** Après l'achat initial de Google Vault, dans le cas où, au cours de la période de validité des Services, le Client ajoute au moins 20 % de Comptes utilisateur pour son personnel par rapport au nombre de comptes préalablement achetés pendant cette période de validité des Services, il s'engage à acheter Google Vault pour ces nouveaux Comptes utilisateur final pour la période de validité restante des Services Google Vault. En outre, chaque année, à la date anniversaire de la Date de début de facturation, le Client s'engage à acheter Google Vault pour tous les Comptes utilisateur du personnel qu'il a ajoutés à ceux préalablement achetés, et ce pour le reste de la période de validité en cours des Services Google Vault du Client.

1.7 **Avis de confidentialité**. L'Avis de confidentialité de G Suite for Education régit la collecte et l'utilisation par Google des informations du Client ou des Utilisateurs finaux.

2. **Obligations du Client**.

2.1 **Utilisations autorisées.** Les Services ne peuvent être utilisés que par (a) des établissements d'enseignement à but non lucratif et (b) d'autres entités à but non lucratif (telles que définies par les lois de l'État concerné).

2.2 **Conformité.** Le Client utilisera les Services conformément à la Politique d'utilisation autorisée. Google peut, par le biais des Services, offrir occasionnellement de nouvelles applications, fonctions ou fonctionnalités dont l'utilisation est potentiellement soumise à l'acceptation de conditions supplémentaires par le Client. En outre, Google proposera au Client et à ses Utilisateurs finaux certains Produits complémentaires à G Suite (venant s'ajouter aux Services), soumis aux Conditions d'utilisation des Produits complémentaires à G Suite et aux conditions d'utilisation Google spécifiques à chacun d'entre eux. Le Client peut, à tout moment, utiliser la Console d'administration pour activer ou désactiver des Produits complémentaires à G Suite.

2.3 **Administration des Services par le Client.** Le Client peut utiliser la Console d'administration pour spécifier un ou plusieurs Administrateurs et leur attribuer des droits leur permettant d'accéder au(x) Compte(s) administrateur et d'administrer les Comptes utilisateur final. Il incombe au Client (a) de préserver la confidentialité des mots de passe et des Comptes administrateur, (b) de désigner les individus autorisés à accéder aux Comptes administrateur et (c) de s'assurer que toutes les activités relevant des Comptes administrateur sont conformes au présent Contrat. Le Client accepte que les responsabilités de Google ne s'étendent pas à la gestion ni à l'administration interne des Services destinés au Client, et que Google est uniquement responsable du traitement des données.

2.4 **Consentement de l'Utilisateur final.** Les Administrateurs du Client peuvent être en mesure d'accéder aux données mises à la disposition des Utilisateurs finaux dans les Comptes utilisateur final, de les contrôler, de les utiliser ou de les divulguer. Le Client s'engage à obtenir des Utilisateurs

finaux, pour toute la durée nécessaire, les autorisations requises pour (i) permettre au Client d'afficher, de contrôler, d'utiliser ou de divulguer ces données, et à Google de donner au Client la possibilité d'effectuer ces opérations et (ii) permettre à Google de fournir les Services.

2.5 **Accord parental**. En vertu de la section 10.1 ci-dessous, le Client est responsable du respect de la loi Children's Online Privacy Protection Act (loi relative à la protection de la vie privée des enfants sur Internet) de 1998. Sa responsabilité concerne également l'obtention du consentement parental pour la collecte d'informations personnelles effectuée dans le cadre des Services ou des Produits complémentaires à G Suite dont il autorise l'accès aux Utilisateurs finaux. Le client doit également obtenir l'autorisation des parents des Utilisateurs finaux de moins de 18 ans avant de permettre à ces derniers d'utiliser les Produits complémentaires à G Suite.

2.6 **Utilisation non autorisée**. Le Client s'engage à prendre des mesures commercialement raisonnables pour empêcher toute utilisation non autorisée des Services et mettre fin à d'éventuels abus. Le Client est également tenu d'informer rapidement Google s'il constate que les Services font l'objet d'accès ou d'utilisations non autorisés.

2.7 **Restrictions d'utilisation**. À moins que Google n'y consente expressément par écrit, le Client s'engage à ne pas effectuer les actions qui suivent et à déployer des efforts commercialement raisonnables pour s'assurer qu'aucun tiers ne les réalise : (a) procéder à la vente, revente, location des Services à un tiers ou à toute opération équivalente en pratique (sauf autorisation expresse accordée dans le présent Contrat), (b) tenter d'effectuer la rétro-ingénierie des Services ou de l'un de leurs composants, (c) tenter de créer un service de substitution ou un service similaire via l'utilisation des Services ou l'accès à ces derniers, (d) utiliser les Services pour des Activités à haut risque ou (e) utiliser les Services pour stocker ou transférer des Données du Client dont l'exportation est soumise aux Lois sur le contrôle des exportations. Le Client est seul responsable, le cas échéant, du respect de la loi américaine HIPAA.

2.8 **Demandes de tiers**. Il incombe au Client de répondre aux Demandes de tiers. Dans la limite autorisée par la loi ou par les conditions de la Demande de tiers, Google (a) avertira sans tarder le Client de la réception d'une Demande de tiers, (b) accédera aux demandes raisonnables que lui transmettra le Client dans le cadre d'actions entreprises pour dénoncer une Demande de tiers et (c) fournira au Client les informations ou outils lui permettant de répondre à la Demande de tiers. Le Client s'efforcera d'abord d'obtenir lui-même les informations permettant de répondre à la Demande de tiers, puis contactera Google uniquement s'il ne parvient pas à obtenir raisonnablement ces informations.

3. **Paiement**. Si l'un des Services a fait l'objet d'un achat moyennant paiement de Frais, les conditions de la Section 3 s'appliquent à ce Service.

3.1 **Paiement.** Tous les frais sont dus trente jours après la date de facturation. Tous les frais doivent être réglés en dollars américains (USD), sauf indication contraire dans un Formulaire de commande. Les paiements effectués par virement bancaire doivent comporter les indications suivantes :

Nom de la banque :	Numéro ABA :	Numéro de compte :
Wells Fargo Bank Palo Alto, Californie, États-Unis	121000248 Google Inc.	4375669785

3.2 **Retards de paiement.** En cas de retard de paiement, des pénalités peuvent être calculées par application d'un taux d'intérêt d'un et demi pour cent par mois (ou, si ce taux est inférieur, le taux légal le plus élevé) à compter de la date d'échéance et jusqu'à ce que la totalité de la somme due soit réglée. Le Client prendra à sa charge tous les frais raisonnables (y compris les frais d'avocat) que Google est susceptible d'engager afin de recouvrer les montants impayés, sauf si une telle situation est due à des erreurs de facturation imputables à Google.

3.3 **Bons de commande.**

a. **Requis.** Si le Client souhaite qu'un numéro de Bon de commande soit mentionné sur sa facture, il doit en faire la demande et transmettre un Bon de commande à Google. Si le Client

exige un numéro de Bon de commande, mais ne transmet pas le Bon de commande requis, Google ne sera pas tenu de fournir les Services tant que le Bon de commande n'aura pas été reçu par Google. Les éventuelles conditions d'utilisation figurant sur ledit Bon de commande n'entrent pas dans le cadre du présent Contrat et sont considérées comme nulles et non avenues.

b. **Non requis.** Si le Client n'a pas besoin de numéro de Bon de commande sur sa facture, il devra transmettre à Google une renonciation à cette condition. Celle-ci pourra prendre la forme d'un e-mail. Si le Client renonce au Bon de commande : (a) Google transmettra au Client la facture sans numéro de Bon de commande associé et (b) le Client s'engage à payer les factures sans numéro de Bon de commande associé.

3.4 **Taxes.** Le Client est tenu de régler toute Taxe applicable et doit payer les Services à Google sans aucune déduction liée à ces Taxes. Si Google se trouve dans l'obligation de percevoir ou de payer des Taxes, celles-ci seront facturées au Client, sauf si ce dernier fournit à Google un certificat d'exonération de taxe valide, délivré par l'administration fiscale compétente. Si le Client est contraint par la loi de déduire des Taxes de ses paiements à Google, il doit fournir à Google un reçu fiscal officiel ou tout autre document approprié servant de justificatif.

3.5 **Contestations de facture.** Les contestations de facture doivent être présentées avant la date d'échéance de la facture. Si les parties déterminent que certaines erreurs de facturation sont imputables à Google, Google n'éditera pas de nouvelle facture, mais établira un avoir correspondant au montant incorrect. Si la facture contestée n'a pas encore été réglée, Google déduira le montant de l'avoir de celle-ci et le Client sera alors redevable du solde net dû de cette facture.

4. **Facturation : tarifs**. Si un Service a fait l'objet d'un achat moyennant paiement de Frais, les durées de validité de la présente Section 4 s'appliquent à ce Service. À la Date de début de facturation ou après celle-ci, Google facturera au Client les Frais suivants pour chaque Service applicable : avance sur les Frais mensuels, les Frais annuels ou les Frais correspondant à la période de validité initiale (selon le cas). Tous ces frais seront indiqués dans le Formulaire de commande.

5. **Services d'assistance technique**.

5.1 **Par le Client.** Il incombe au Client de répondre, à ses propres frais, aux questions et aux réclamations des Utilisateurs finaux ou de tiers, concernant l'utilisation des Services par lui-même ou par les Utilisateurs finaux. Le Client s'engage à mettre en œuvre des actions commercialement raisonnables pour résoudre les problèmes d'assistance avant d'en référer à Google.

5.2 **Par Google.** Si le Client est dans l'impossibilité de résoudre un problème d'assistance dans les conditions ci-dessus, il peut le transmettre à Google, conformément aux Instructions des Services d'assistance technique. Google fournira les Services d'assistance technique au Client en accord avec ces instructions.

6. **Suspension**.

6.1 **Des Comptes utilisateur final par Google.** En cas de violation avérée du présent Contrat par un Utilisateur Final, Google peut demander au Client la Suspension du Compte utilisateur final concerné. Si le Client ne se conforme pas à la demande de Google visant à suspendre un Compte utilisateur final, Google est en droit de procéder à cette Suspension. Toute Suspension mise en œuvre par Google reste effective tant que l'Utilisateur final concerné n'a pas remédié à la violation qui en est à l'origine.

6.2 **Problèmes de sécurité urgents.** Nonobstant ce qui précède, en cas de Problème de sécurité urgent, Google se réserve le droit de suspendre les Comptes utilisateur final incriminés. Cette Suspension a la portée et la durée minimales requises pour prévenir ce Problème de sécurité urgent ou y mettre fin. Si Google suspend un Compte utilisateur final pour une raison quelconque sans en aviser préalablement le Client, Google est tenu, à la demande du Client, d'indiquer la raison de cette Suspension dans les plus brefs délais.

7. **Informations confidentielles**.

7.1 **Obligations.** Chaque partie : (a) protégera les Informations confidentielles de l'autre partie comme s'il s'agissait de ses propres informations confidentielles et (b) ne les divulguera pas, sauf aux Sociétés affiliées, aux employés et aux agents qui ont besoin de les connaître et se sont engagés par écrit à les garder confidentielles. Les parties (et l'ensemble des Sociétés affiliées, employés et agents auxquels les Informations confidentielles ont été divulguées) ne peuvent utiliser les Informations confidentielles recueillies que pour exercer leurs droits et remplir leurs obligations en vertu du présent Contrat, en faisant preuve d'une diligence raisonnable pour les protéger. Chaque partie est responsable des éventuelles actions qui pourraient être mises en œuvre par ses Sociétés affiliées, employés et agents en violation de la présente Section.

7.2 **Exceptions**. Les Informations confidentielles ne comprennent pas les informations (a) dont le destinataire avait déjà connaissance, (b) qui sont rendues publiques sans que le destinataire en soit responsable, (c) qui ont été développées indépendamment par le destinataire ou (d) qui ont été transmises légalement au destinataire par une autre partie.

7.3 **Divulgation obligatoire.** Chaque partie peut divulguer les Informations confidentielles de l'autre partie lorsque la loi l'exige, mais uniquement après avoir, dans la mesure où elle peut légalement le faire, (a) entrepris des actions commercialement raisonnables pour notifier l'autre partie de la divulgation et (b) donné à l'autre partie l'occasion de contester cette divulgation.

7.4 **FERPA.** Les parties reconnaissent que (a) les Données du Client peuvent contenir des informations personnelles issues des dossiers d'enseignement soumises à la loi FERPA ("Dossiers FERPA") et, (b) dans la mesure où les Données du Client contiennent des Dossiers FERPA, Google sera considérée comme un "Officiel scolaire" (tel que défini dans la loi FERPA et ses dispositions d'application) et devra se conformer à cette loi.

8. **Droits de propriété intellectuelle et Signes distinctifs des marques**.

8.1 **Droits de propriété intellectuelle.** Sauf disposition contraire expressément énoncée dans le présent Contrat, celui-ci n'accorde à aucune partie des droits, implicites ou autres, sur le contenu ou la propriété intellectuelle de l'autre partie. Comme convenu entre les parties, le Client détient tous les Droits de propriété intellectuelle associés à ses données, et Google détient tous les Droits de propriété intellectuelle afférents aux Services.

8.2 **Affichage des Signes distinctifs des marques.** Google peut afficher les Signes distinctifs des marques autorisés par le Client (celui-ci autorisant un tel affichage en important ces signes distinctifs dans les Services) dans les zones désignées des Pages des services. Le Client peut spécifier la nature de cette utilisation dans la Console d'administration. Google peut également afficher les Signes distinctifs de la marque Google sur les Pages des services pour indiquer qu'elle fournit ces derniers. Aucune des parties ne peut afficher, ni utiliser les Signes distinctifs des marques de l'autre partie en-dehors du cadre du présent Contrat sans obtenir préalablement l'approbation écrite de l'autre partie.

8.3 **Limitations applicables aux Signes distinctifs des marques.** Toute utilisation des Signes distinctifs des marques d'une partie s'appliquera au bénéfice de la partie qui en détient les droits de propriété intellectuelle. Une partie peut révoquer le droit de l'autre partie à utiliser ses Signes distinctifs, dans le cadre du présent Contrat, en adressant à l'autre partie un avis écrit indiquant un délai raisonnable pour cesser cette utilisation.

9. **Publicité**. Le Client accepte que Google puisse inclure le nom et les Signes distinctifs des marques du Client dans une liste de clients Google, sur Internet ou sur des supports de promotion. Le Client autorise également Google à le mentionner verbalement en tant que client des produits ou services Google régis par le présent Contrat. Cette Section est soumise aux dispositions de la Section 8.3.

10. **Déclarations, garanties et clauses de non-responsabilité**.

10.1 **Déclarations et garanties.** Chaque partie atteste disposer des pouvoirs et de l'autorité nécessaires pour conclure ce Contrat. Chaque partie garantit qu'elle se conformera à toutes les lois et réglementations en vigueur concernant la mise à disposition ou l'utilisation des Services, le cas échéant (y compris la loi relative à la notification des violations de sécurité). Google garantit que les Services seront fournis conformément au Contrat de service applicable. Le Client reconnaît être seul responsable du respect de la Children's Online Privacy Protection Act (Loi sur la protection de la confidentialité des données relatives aux enfants sur Internet) de 1998, y compris, mais sans s'y limiter, pour ce qui est de l'obtention du consentement parental pour la collecte de renseignements personnels des étudiants effectuée dans le cadre de la mise à disposition et de l'utilisation des Services par le Client et les Utilisateurs finaux.

10.2 **Clause de non-responsabilité**. DANS LES LIMITES AUTORISÉES PAR LA LOI EN VIGUEUR ET SOUS RÉSERVE DE DISPOSITIONS EXPRESSES DU PRÉSENT CONTRAT, AUCUNE PARTIE N'OFFRE D'AUTRE GARANTIE QUELLE QU'ELLE SOIT (EXPRESSE, IMPLICITE, LÉGALE OU AUTRE), Y COMPRIS, MAIS SANS S'Y LIMITER, DES GARANTIES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER ET DE CONFORMITÉ. GOOGLE N'APPORTE AUCUNE GARANTIE QUANT AU CONTENU OU AUX INFORMATIONS ACCESSIBLES AU MOYEN OU PAR L'INTERMÉDIAIRE DES SERVICES. LE CLIENT RECONNAÎT QUE LES SERVICES PROPOSÉS NE CONSTITUENT PAS UN SERVICE DE TÉLÉPHONIE ET NE PERMETTENT PAS D'EFFECTUER NI DE RECEVOIR DES APPELS, Y COMPRIS DE NUMÉROS D'URGENCE, PAR LE BIAIS DE RÉSEAUX TÉLÉPHONIQUES PUBLICS COMMUTÉS.

11. **Période de validité ; Frais**.

11.1 **Période de validité du Contrat.** Le présent contrat restera en vigueur pendant sa période de validité.

11.2 **Période de validité des Services et achats pendant cette période.** Google s'engage à fournir les Services au Client pendant la Période de validité des Services. En l'absence d'accord contraire écrit entre les parties, les Comptes utilisateur final ajoutés pendant la Période de validité des Services auront une durée de validité calculée au prorata et se terminant le dernier jour de cette période.

11.3 **Renouvellement automatique.** À l'expiration de chaque Période de validité des Services, l'abonnement aux Services (et à tous les Comptes utilisateur final précédemment acquis moyennant paiement de Frais) sont automatiquement renouvelés pour une période de validité supplémentaire de douze mois. Si l'une des parties ne souhaite pas renouveler les Services, elle doit en informer l'autre partie par écrit, au moins 15 jours avant la fin de la période de validité des Services en cours. Cet avis de non-renouvellement prendra effet à la fin de la Période de validité en cours.

11.4 **Frais.** Pendant la Période de validité initiale, Google ne facturera pas les Services au Client (sauf les Frais de Google Vault ou de stockage payant, le cas échéant). En vertu de l'accord mutuel écrit des parties, (a) Google peut facturer des Frais au Client pour les Services une fois la Période de validité initiale échue et (b) Google peut facturer des Frais au Client pour une version Premium des Services ou pour des fonctionnalités ou des améliorations optionnelles pouvant être ajoutées aux Services de Google (par exemple, Google Vault ou un stockage payant, le cas échéant).

11.5 **Utilisation des Services.** Le Client n'est pas tenu d'utiliser les Services et peut interrompre leur utilisation à tout moment, quelle qu'en soit la raison (ou sans raison particulière).

11.6 **Révision des tarifs.** Pour les Services achetés par le Client moyennant paiement de Frais, Google peut réviser ses tarifs pour la prochaine Période de validité des Services à condition d'en informer le Client par écrit (éventuellement par e-mail) au moins trente jours avant le début de la nouvelle période.

12. **Résiliation**.

12.1 **Résiliation suite à un manquement.** L'une ou l'autre des parties peut suspendre l'exécution du présent Contrat ou le résilier si (i) l'autre partie viole substantiellement le Contrat et omet de remédier

à ce manquement dans les trente jours qui suivent la réception de l'avis écrit, (ii) l'autre partie cesse ses activités commerciales ou fait l'objet d'une procédure d'insolvabilité et que cette procédure n'est pas levée dans un délai de quatre-vingt-dix jours ou si (iii) l'autre partie viole substantiellement le présent Contrat plus de deux fois, nonobstant une éventuelle réparation de ces violations.

12.2 **Autre résiliation.** Le Client peut résilier le présent Contrat pour une raison quelconque (ou sans raison particulière) en envoyant un préavis écrit de trente jours à Google, sachant, toutefois, qu'il reste tenu de payer les Frais relatifs aux Services qu'il a achetés jusqu'à la fin de la Période de validité en vigueur pour ces Services.

12.3 **Conséquences de la résiliation.** Si le présent Contrat est résilié, (i) les droits octroyés par une partie à l'autre prendront fin immédiatement (sauf dans les cas décrits dans cette Section), (ii) Google permettra au Client d'accéder à ses Données pendant une période commercialement raisonnable et de les exporter, aux tarifs alors en vigueur pour les Services concernés, (iii) après une période commercialement raisonnable, les Données du client seront supprimées par Google qui retirera les pointeurs associés de ses serveurs actifs et remplacera ces données progressivement, et (iv) chaque partie mettra en œuvre rapidement des actions commercialement raisonnables pour renvoyer ou détruire toutes les autres Informations confidentielles de l'autre partie, si elle en reçoit la demande.

13. **Indemnisation**.

13.1 **Par Google.** Google indemnisera, défendra et dégagera de toute responsabilité le Client vis-à-vis de l'ensemble des responsabilités, dommages et coûts (y compris les frais de justice et les honoraires d'avocat raisonnables) découlant de la réclamation d'un tiers selon laquelle la technologie de Google utilisée pour fournir les Services ou les Signes distinctifs des marques de Google enfreignent ou détournent un brevet, des droits d'auteur, un secret industriel ou une marque de ce tiers. Nonobstant ce qui précède, la responsabilité de Google ne saurait en aucun cas être engagée, en vertu de la présente section, du fait (i) de l'utilisation des Services ou des Signes distinctifs des marques de Google sous une forme modifiée ou en association avec des supports non fournis par Google et (ii) des informations, données ou contenus fournis par le Client, les Utilisateurs finaux ou d'autres tiers.

13.2 **Violation éventuelle.**

(a) **Réparation, remplacement ou modification.** Si Google a de bonnes raisons de penser que les Services enfreignent les Droits de propriété intellectuelle d'un tiers, Google (a) obtiendra, à ses frais, le droit pour le Client de continuer à utiliser les Services, (b) proposera des services de remplacement de même niveau fonctionnel n'enfreignant pas de droits de propriété intellectuelle ou (c) modifiera les Services de sorte qu'ils n'entraînent plus une telle violation.

(b) **Suspension ou résiliation.** Si Google ne pense pas que les solutions précitées sont commercialement raisonnables, elle pourra suspendre l'utilisation par le Client des Services concernés ou y mettre fin. Si Google met fin aux Services concernés, elle procédera à un remboursement au prorata des sommes non dues effectivement versées par le Client (le cas échéant) pour la période suivant la résiliation de ces Services.

13.3 **Généralités.** Le Client avisera immédiatement Google de la réclamation et coopérera avec Google pour assurer la défense contre ladite réclamation. Google exerce un contrôle complet et une pleine autorité sur la défense, excepté que : (a) tout arrangement impliquant que le Client admette une responsabilité ou verse de l'argent nécessitera le consentement écrit préalable de celui-ci, ce consentement ne devant pas être refusé ni retardé de façon non raisonnable, et que (b) le Client peut prendre part à la défense avec son propre avocat, à ses frais. LES INDEMNITÉS CI-DESSUS REPRÉSENTENT LE SEUL RECOURS DU CLIENT, DANS LE CADRE DU PRÉSENT CONTRAT, EN CAS DE VIOLATION PAR GOOGLE DES DROITS DE PROPRIÉTÉ INTELLECTUELLE D'UN TIERS.

14. **Limitation de responsabilité**.

14.1 **Limitation de responsabilité indirecte.** AUCUNE PARTIE NE POURRA ÊTRE TENUE POUR RESPONSABLE, EN VERTU DU PRÉSENT CONTRAT, DE LA PERTE DE REVENUS OU DE DOMMAGES INDIRECTS, SPÉCIAUX, ACCESSOIRES, CONSÉCUTIFS, EXEMPLAIRES OU PUNITIFS, MÊME SI LA PARTIE ÉTAIT INFORMÉE OU ÉTAIT CENSÉE AVOIR EU CONNAISSANCE DE L'ÉVENTUALITÉ DE TELS DOMMAGES ET MÊME SI LES DOMMAGES DIRECTS N'OUVRENT PAS DE VOIE DE RECOURS.

14.2 **Limitation du montant de la responsabilité.** AUCUNE PARTIE NE POURRA ÊTRE TENUE DE VERSER, EN VERTU DU PRÉSENT CONTRAT, UN MONTANT SUPÉRIEUR À (I) MILLE DOLLARS OU (II) CELUI PAYÉ PAR LE CLIENT À GOOGLE DANS LE CADRE DU PRÉSENT CONTRAT AU COURS DES DOUZE MOIS PRÉCÉDANT L'ÉVÉNEMENT AYANT ENGAGÉ CETTE RESPONSABILITÉ.

14.3 **Exceptions aux limitations.** Ces limitations de responsabilité s'appliquent dans la pleine mesure autorisée par la loi applicable, mais ne concernent pas les violations des obligations de confidentialité, les atteintes aux droits de propriété intellectuelle d'une partie par l'autre, ni les obligations d'indemnisation.

15. **Dispositions diverses**.

15.1 **Avis.** Sauf mention contraire figurant dans le présent document, (a) tous les avis doivent être notifiés par écrit et adressés à l'attention du service juridique et du point de contact principal de l'autre partie et (b) un avis est considéré comme remis (i) après confirmation écrite de sa réception en cas d'envoi par coursier personnel ou coursier express, ou à sa réception en cas d'envoi par la poste sans confirmation de réception, ou (ii) après confirmation de sa réception via l'accusé de réception automatique ou des journaux électroniques en cas d'envoi par télécopie ou par e-mail.

15.2 **Cession.** Aucune partie ne peut céder ni transférer une partie du présent Contrat sans le consentement écrit de l'autre partie, sauf à une Société affiliée, et uniquement si (a) le cessionnaire accepte par écrit d'être lié par les conditions du présent Contrat et si (b) la partie cédante demeure responsable des obligations contractées dans le cadre du présent Contrat avant la cession. Toute autre tentative de transfert ou de cession sera considérée comme nulle et non avenue.

14.3 **Changement de contrôle.** En cas de changement de contrôle (par exemple, via une acquisition ou une vente d'actions, une fusion ou une autre forme de transaction d'entreprise), (a) la partie qui fait l'objet du changement de contrôle doit en aviser par écrit l'autre partie dans un délai de trente jours suivant le changement de contrôle et (b) l'autre partie peut résilier avec effet immédiat le présent Contrat à tout moment à compter du changement de contrôle et dans un délai de trente jours après la réception de l'avis par écrit prévu dans la sous-section (a).

15.4 **Force majeure.** Aucune partie ne pourra être tenue responsable d'une mauvaise exécution dans la mesure où elle est causée par une situation qui échappe au contrôle raisonnable de la partie (par exemple, une catastrophe naturelle, un acte de guerre ou de terrorisme, une émeute, des conditions de travail, une mesure des pouvoirs publics ou une perturbation Internet).

14.5 **Absence de renonciation.** L'impossibilité d'appliquer une disposition du présent Contrat ne constitue pas une renonciation à cette disposition.

14.6 **Divisibilité.** Si l'une des dispositions du présent Contrat s'avère inapplicable, les autres dispositions restent en vigueur.

15.7 **Aucune agence.** Les parties sont des entrepreneurs indépendants et le présent Contrat ne crée en aucun cas un(e) quelconque agence, partenariat ou joint venture.

15.8 **Aucun tiers bénéficiaire.** Il n'existe aucun tiers bénéficiaire du présent Contrat.

15.9 **Réparation équitable.** Aucune clause du présent Contrat ne saurait empêcher une partie de solliciter une réparation équitable.

15.10 **Loi applicable.**

a. **Pour les entités publiques d'une ville, d'un comté et d'un État**. Si le Client est une entité publique d'une ville, d'un comté, ou d'un État, les parties conviennent de ne pas faire mention de la loi applicable ni de la juridiction compétente.

b. **Pour toutes les autres entités.** Si le Client est une entité qui n'est pas définie dans la Section 15.10(a), la disposition suivante s'applique : le présent Contrat est régi par la loi de l'État de Californie, exclusion faite des règles sur les conflits de lois de cet État. POUR TOUT LITIGE LIÉ OU RELATIF AU PRÉSENT CONTRAT, LES PARTIES CONSENTENT À SE SOUMETTRE À LA JURIDICTION PERSONNELLE ET EXCLUSIVE DES TRIBUNAUX DU COMTÉ DE SANTA CLARA EN CALIFORNIE.

15.11 **Amendements.** Tout amendement doit être formulé par écrit et doit stipuler expressément qu'il modifie le présent Contrat.

15.12 **Application après la résiliation.** Les sections suivantes continueront à s'appliquer après l'expiration ou la résiliation du présent Contrat : 7 (Informations confidentielles), 8.1 (Droits de propriété intellectuelle), 12.3 (Effets de la résiliation), 13 (Indemnisation), 14 (Limitation de responsabilité), 15 (Divers) et 16 (Définitions).

15.13 **Intégralité du Contrat.** Le présent Contrat, et tous les documents auxquels il fait référence, représentent l'intégralité du contrat en relation avec son objet et remplacent tous les contrats précédents ou tous les contrats contemporains portant sur cet objet. Si le Client se voit présenter un Contrat similaire ayant le même objet en se connectant pour utiliser les Services, le présent Contrat remplace ledit Contrat. Les conditions disponibles via une URL et référencées dans le présent Contrat en font partie intégrante.

15.14 **Interprétation des conditions contradictoires.** En cas de contradiction entre les documents qui constituent le présent Contrat, les documents prévalent dans l'ordre suivant : le Formulaire de commande (le cas échéant), le Contrat et les conditions hébergées sur une URL.

15.15 **Exemplaires identiques.** Les parties peuvent conclure le présent Contrat en signant le Formulaire de commande applicable (le cas échéant) ou le présent Contrat en plusieurs exemplaires, notamment sous forme de télécopies, de fichiers PDF ou d'autres copies électroniques, qui constituent ensemble un seul et même document.

16. **Définitions**.

Politique d'utilisation autorisée : règlement s'appliquant à l'utilisation des Services et accessible à l'adresse https://www.google.com/apps/intl/fr/terms/use_policy.html ou à une autre URL que Google est susceptible de fournir à cette fin.

Compte(s) administrateur : comptes mis à la disposition du Client par Google pour l'administration des Services. L'utilisation des Comptes administrateur nécessite un mot de passe que Google s'engage à fournir au Client.

Console d'administration : outil en ligne fourni par Google au Client, conçu pour la création de rapports et certaines autres fonctions d'administration.

Administrateurs : personnel technique désigné par le Client dont la mission consiste à administrer les Services destinés aux Utilisateurs finaux pour le compte du Client.

Annonces : publicités en ligne affichées par Google et destinées aux Utilisateurs finaux, à l'exclusion de celles fournies par des produits publicitaires ne faisant pas partie des Services (Google AdSense, par exemple) que le Client choisit d'utiliser dans le cadre des Services.

Société affiliée : toute entité qui contrôle directement ou indirectement une partie, est contrôlée par cette partie ou est placée sous le même contrôle que cette dernière.

Contrat : selon le cas, il s'agit du présent Contrat G Suite for Education, ou de la combinaison du Formulaire de commande et du présent Contrat G Suite for Education.

Anciens élèves : diplômés ou anciens élèves du Client.

Frais annuels : frais annuels pour les Services énoncés dans le Formulaire de commande (le cas échéant).

Date de début de facturation : date à laquelle le Client commence à régler Google pour les Services (le cas échéant).

Signes distinctifs des marques : noms commerciaux, marques commerciales, marques de service, logos, noms de domaine et autres signes distinctifs représentant une partie et protégés par cette partie à un moment donné.

Informations confidentielles : informations divulguées par une partie à l'autre partie, dans le cadre du présent Contrat, qui sont signalées comme étant confidentielles ou qui seraient normalement considérées comme telles dans ces circonstances. Les Données du Client sont des Informations confidentielles.

Données du Client : données (y compris les e-mails) fournies, générées, transmises ou affichées via les Services par le Client ou les Utilisateurs finaux.

Noms de domaine du Client : noms de domaine mentionnés dans le Formulaire de commande, appartenant au Client ou contrôlés par lui, et utilisés dans le cadre des Services. Le Client peut fournir les Services à n'importe lequel de ses sous-domaines sans autorisation écrite de Google (par exemple, si le Nom de domaine du Client est "edu.com", un sous-domaine pourrait être "anciens.edu.com").

Date d'effet : date à laquelle le présent Contrat est contresigné.

Problème de sécurité urgent : (a) utilisation des Services par le Client en violation de la politique d'utilisation autorisée et pouvant perturber (i) les Services, (ii) l'utilisation des Services par d'autres clients ou (iii) le réseau ou les serveurs Google utilisés pour fournir lesdits Services ; ou bien (b) accès d'un tiers non autorisé aux Services.

Utilisateurs finaux : personnes autorisées par le Client à utiliser les Services.

Compte utilisateur final : compte hébergé par Google et créé via les Services par le Client, pour un Utilisateur final.

Lois sur le contrôle des exportations : toutes les lois et réglementations applicables en matière de contrôle des exportations et des réexportations, y compris la réglementation sur les exportations (Export Administration Regulations, "EAR") du département du Commerce des États-Unis, les sanctions commerciales et économiques imposées par le Service de contrôle des actifs étrangers (Office of Foreign Assets Control) du Département du Trésor des États-Unis, ainsi que la réglementation sur le commerce international des armes (International Traffic in Arms Regulations, "ITAR") imposée par le Département d'État des États-Unis.

Frais : frais facturés au Client par Google pour les Services (le cas échéant) tels que définis dans le présent Contrat.

FERPA : loi fédérale américaine sur la protection de la vie privée et le droit à l'instruction des familles (Family Educational Rights and Privacy Act, U.S. Code, titre 20, par. 1232g) et règlement de ladite loi (Family Educational Rights and Privacy Act Regulations, Code of Federal Regulations, titre 34, partie 99), dans leurs versions en vigueur amendées, ou modifiées par d'autres biais.

Avis de confidentialité de G Suite for Education : avis disponible à l'adresse https://www.google.com/intl/fr/work/apps/terms/education_privacy.html ou à une autre URL que Google est susceptible de fournir à cette fin.

Centre d'aide : centre d'aide Google accessible à l'adresse https://www.google.com/support/ ou à toute autre URL fournie par Google.

Activités à haut risque : activités, telles que l'exploitation d'installations nucléaires, le contrôle du trafic aérien ou l'utilisation d'équipements de survie, dans le cadre desquelles l'utilisation ou l'échec des Services est susceptible d'entraîner un décès, des préjudices corporels ou des atteintes à l'environnement.

HIPAA : Health Insurance Portability and Accountability Act (loi de 1996 sur la transférabilité et la responsabilité dans le cadre de l'assurance-maladie), dans sa version amendée en vigueur, ainsi que toute réglementation produite dans ce cadre.

Droits de propriété intellectuelle : droits internationaux, actuels et futurs, stipulés dans les lois sur les brevets, les droits d'auteur, le secret industriel, les marques ou dans le droit moral, ainsi que tout autre droit similaire.

Période de validité initiale des Services : période de validité des Services applicables, débutant à la Date d'entrée en vigueur des Services et se poursuivant pendant la "Période de validité des Services en cours" stipulée dans le Formulaire de commande à partir de la Date de début de facturation (si un Formulaire de commande est associé aux Services) ou, si aucun Formulaire de commande n'est associé aux Services, pour une période d'un an à compter de la Date d'effet.

Frais correspondant à la période de validité initiale : frais facturés pour les Services pour la Période de validité initiale (hors frais d'inscription ponctuels, le cas échéant), tels que définis dans le Formulaire de commande (le cas échéant).

Frais mensuels : frais mensuels facturés pour les Services, tels que définis dans le Formulaire de commande (le cas échéant).

Produits complémentaires à G Suite : produits Google ne faisant pas partie des Services, mais auxquels les Utilisateurs finaux peuvent accéder en utilisant l'identifiant et le mot de passe de leur Compte utilisateur final. La liste des Produits complémentaires à G Suite est disponible à l'adresse https://www.google.com/support/a/bin/answer.py?hl=fr&answer=181865 ou à une autre URL que Google est susceptible de fournir à cette fin.

Conditions d'utilisation des Produits complémentaires à G Suite : conditions d'utilisation disponibles à l'adresse https://www.google.com/apps/intl/fr/terms/additional_services.html ou à une autre URL que Google est susceptible de fournir à cette fin.

Adresse e-mail de notification : adresse e-mail indiquée par le Client pour recevoir les notifications de Google. Le Client peut modifier cette adresse dans la Console d'administration.

Formulaire de commande : formulaire de commande sous la forme d'un document écrit fourni par Google et spécifiant les Services commandés à Google par le Client et les Frais associés (le cas échéant) en vertu du Contrat. Le Formulaire de commande comporte : (i) un cadre prévu pour la signature du Client, ou pour la signature du Client et de Google, (ii) les références des services applicables, (iii) les Frais (le cas échéant), (iv) le nombre de Services et la période de validité des Services en cours pour les Comptes utilisateur final.

Bon de commande : bon de commande émis par le Client.

Services : services de la suite principale G Suite for Education, Google Classroom et, le cas échéant, services Google Vault fournis par Google et utilisés par le Client en vertu du présent Contrat. Les Services sont décrits à l'adresse https://www.google.com/apps/intl/fr/terms/user_features.html ou à une autre URL que Google est susceptible de fournir à cette fin.

Date d'entrée en vigueur des Services : date à laquelle Google met les Services à disposition du Client.

Pages des services : pages Web hébergeant les Services destinés aux Utilisateurs finaux.

Période de validité des Services : période initiale de validité des Services et ensemble des périodes de renouvellement des Services applicables.

Contrat de niveau de service : contrat de niveau de service disponible à l'adresse https://www.google.com/apps/intl/fr/terms/sla.html ou à une autre URL que Google est susceptible de fournir à cette fin.

Personnel : personne (y compris les professeurs) qui est ou a été employé par le Client. Tout étudiant ou ancien élève faisant également partie du personnel est considéré comme membre du Personnel en vertu du présent Contrat (et exclu de la catégorie Étudiant ou Ancien élève) s'il a été employé par le Client au cours des douze derniers mois.

Étudiant : personne ayant été inscrite aux cours dispensés par le Client au cours des douze derniers mois.

Suspension : désactivation immédiate de l'accès aux Services ou à certains de leurs composants, selon le cas, afin d'en empêcher l'utilisation.

Taxes : droits, droits de douane et taxes (autres que l'impôt sur les bénéfices payé par Google) relatifs à la vente des Services, y compris les pénalités ou les intérêts connexes.

Période de validité : période débutant à la Date d'effet et se poursuivant jusqu'à la première des dates suivantes : (i) la fin de la dernière période de validité des Services ou (ii) la résiliation du Contrat dans les conditions définies par les présentes.

Demande de tiers : demande d'un tiers visant à obtenir des enregistrements relatifs à l'utilisation des Services par un Utilisateur final. Il peut s'agir d'un mandat de perquisition, d'une ordonnance de tribunal, d'une citation à comparaître, d'une autre ordonnance juridique valide ou d'un consentement écrit de l'Utilisateur final autorisant la divulgation.

Services d'assistance technique : services fournis par Google aux Administrateurs pendant la Période de validité conformément aux Instructions des Services d'assistance technique.

Instructions des Services d'assistance technique : instructions des services d'assistance technique de Google alors en vigueur pour les Services. Ces instructions sont disponibles à l'adresse https://www.google.com/apps/intl/fr/terms/tssg.html ou à une autre URL que Google est susceptible de fournir à cette fin.

Conditions d'utilisation hébergées sur des URL : conditions incluant la Politique d'utilisation autorisée, le Contrat de service et les Instructions des Services d'assistance technique.

ANNEXE 14

UNIVERSITÉ DE GENÈVE
RECTORAT

GRAND CONSEIL
reçu le 27 NOV. 2017

Prof. Denis Hochstrasser
Vice-recteur
Ligne directe: 022 379 79 70
Denis.Hochstrasser@unige.ch

Monsieur Mathias Buschbeck
Président,
Commission législative
Grand Conseil
Rue de l'Hôtel-de-Ville 2
Case postale 3970
1211 Genève 3
Courrier interne : A106E3/GC

Genève, le 24 novembre 2017

Concerne : Projet de loi modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)

Monsieur le Président,
Cher Monsieur,

Suite à notre audition du 17 novembre 2017, nous vous remercions de nous avoir transmis le projet de loi en question afin que nous y apportions nos suggestions. Nous serons bien entendu heureux de collaborer sur ce dossier.

Seulement, après consultation interne, il ressort qu'une revue rapide du PL 12103 par l'UNIGE nous paraît compliquée notamment à cause des points suivants :

- L'article 13A du Règlement d'application de la LIPAD encadre déjà la sous-traitance de données personnelles, et autorise le traitement de données personnelles à l'étranger si la législation de l'Etat destinataire assure un niveau de protection adéquat. Ceci est conforme à l'engagement pris par la Suisse dans la Convention 108. Toute restriction de cet engagement doit être examinée avec soin ;
- La nouvelle LPD, qui s'inspire en grande partie du RGPD européen, va induire une adaptation de la LIPAD. Les évolutions pressenties vont permettre plus de transparence pour les citoyens, plus de protection de leurs données personnelles, et également la possibilité d'établir des codes de conduite par branche ;
- L'ajout d'exigences / contraintes supplémentaires, relatives à la gestion de données personnelles sur des périmètres spécifiques (données des élèves mineurs, données des étudiants, etc.) et l'établissement d'un texte législatif y relatif, nécessite une expertise juridique.

./.

Il nous paraît donc nécessaire de faire appel à une expertise juridique ciblée afin de garantir la pertinence temporelle et la licéité des évolutions proposées par le PL 12103. Nous pensons en particulier à l'implication d'un juriste spécialiste du droit des données personnelles et/ou du droit des technologies de l'information, tel que le responsable juridique de la DGSI, ou d'un professeur de Droit expert en ces domaines.

Je demeure évidemment à votre entière disposition pour toute précision ou renseignement utile et vous prie de croire, Monsieur le Président, cher Monsieur, à l'expression de mes sentiments les meilleurs.

Denis Hochstrasser
Vice-recteur

Copie : Mme Tina Rodriguez, Secrétariat général du Grand Conseil

Uni Dufour - 24 rue Général-Dufour - CH-1211 Genève 4
Tél. 022 379 75 25 - Fax 022 379 11 80 - www.unige.ch/rectorat

ANNEXE 15

RÉPUBLIQUE ET CANTON DE GENÈVE

Genève, le 9 mai 2018

GRAND CONSEIL
reçu le 9 - MAI 2018

Le Conseil d'Etat
2287-2018

Grand Conseil
Commission législative
Monsieur Mathias Buschbeck
Président
Rue de l'Hôtel-de-Ville 2
1204 Genève

Concerne : PL 12103 modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)

Monsieur le Président,

Votre demande de position concernant le projet de loi cité en titre a retenu toute notre attention.

En préambule, le Conseil d'Etat souligne qu'il partage entièrement la préoccupation des auteurs du projet de loi d'offrir aux personnes en formation, en particulier aux mineurs, une protection des données personnelles adéquate.

Le projet de loi PL12103 propose d'adjoindre un article supplémentaire à la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD). Cet article est formulé comme suit :

> **Art. 37A Sécurité des données personnelles des mineurs et des personnes majeures en formation (nouveau)**
>
> [1] Les systèmes de messagerie, ainsi que les espaces numériques de dépôt et de partage de données mis à disposition des élèves, des étudiants et autres personnes en formation, ainsi que des collaborateurs du DIP du canton de Genève doivent être fournis par les services informatiques de l'Etat.
>
> [2] En cas de nécessité, ils peuvent être fournis par des entreprises suisses et domiciliées en Suisse.
>
> [3] L'Etat garantit que les données échangées ou déposées dans l'espace numérique mis à disposition par les personnes mentionnées à l'alinéa 1 sont stockées dans un data center en Suisse et sont uniquement soumises à la loi suisse en matière de protection des données.

Alinéas 2 et 3 de l'article 37A

Les collaboratrices et collaborateurs du département de l'instruction publique, de la culture et du sport (DIP) et du département de la sécurité et de l'économie (DSE) auditionnés par votre commission ont pu exprimer un certain nombre de remarques au sujet du projet de loi dans sa version initiale déposée le 24 avril 2017. Dans ce cadre, il a notamment été relevé que les alinéas 2 et 3 de l'article 37A limiteraient de manière trop importante l'usage des outils numériques.

En effet, par exemple, restreindre au seul territoire suisse le lieu de stockage des données obligerait à renoncer à des services en ligne fournis par des partenaires étrangers et notamment français, comme le Projet Voltaire pour l'apprentissage de l'orthographe ou Compilatio pour la détection du plagiat.

Par conséquent, notre Conseil propose de ne pas retenir les alinéas 2 et 3 de l'article 37A du projet de loi.

Alinéa 1 de l'article 37A

Concernant l'alinéa 1 de l'article 31A, notre Conseil relève les points suivants :

a) Il est nécessaire d'exclure du périmètre de cette disposition les hautes écoles, telles que définies à l'article 4 al. 2 de la LIP. En effet, une restriction de choix des sous-traitants informatiques à ce niveau risquerait d'entraver la recherche et la collaboration internationale.

b) Le projet de loi exige la mise en place d'une messagerie pour le DIP fournie par les services informatiques de l'Etat. Cette condition est déjà réalisée pour les collaborateurs du DIP, mais pas pour les élèves.
Nous sommes d'avis que la messagerie des élèves doit effectivement être fournie par l'Etat. Cette prestation est nécessaire au DIP, non seulement dans le cadre de la relation pédagogique, mais également pour la communication institutionnelle entre les établissements scolaires et les élèves. Partant du principe que la messagerie n'est pertinente pour les élèves qu'à partir du degré secondaire I, il s'agirait de quelque 45 000 adresses à gérer et maintenir.

c) Le projet de loi concerne les élèves, les apprenants et autres personnes en formation (hors hautes écoles), mais également les collaborateurs du DIP. A notre sens, il n'y a pas lieu de mentionner dans ce cadre cette dernière population. En effet, les collaborateurs du DIP sont soumis aux mêmes règles et doivent bénéficier des mêmes prestations que les autres agents de l'Etat.

d) En outre, il ne nous apparaît pas pertinent d'exiger que l'intégralité des données des élèves soit stockée sur des serveurs de l'Etat. Seules les données sensibles devraient être soumises à ce régime. Par ailleurs, le DIP doit pouvoir continuer à utiliser avec ses élèves les applications intercantonales ou nationales, telles que les plateformes mises en place par educa.ch sur mandat de la CIIP ou de la CDIP. De plus, le DIP utilise des services en ligne fournis par des partenaires étrangers et notamment français, comme le Projet Voltaire pour l'apprentissage de l'orthographe ou Compilatio pour la détection du plagiat. La relation avec ces entités, y compris les aspects concernant la protection des données, est réglée contractuellement dans le cadre de la législation actuelle. Formellement, nos sous-traitants ne peuvent utiliser les données personnelles qui leur sont confiées pour faire du profilage de nos utilisateurs, qu'ils soient collaborateurs ou personnes en formation. Le DIP et la DGSI sont garants du respect de la protection des données.
Nous relevons enfin que la notion d' « espace numérique de dépôt et de partage de données » est imprécise et très large. Elle pourrait être comprise comme excluant tout recours à des solutions hors Etat, ce qui n'est pas réaliste et peut représenter un frein important au développement de la formation au numérique et par le numérique. Pour cette raison, nous préconisons de ne pas en faire usage.

e) Le projet de loi ne mentionne pas la question de l'identité numérique des élèves. Ce point est important et devrait être mentionné. L'Etat doit être le fournisseur et le garant d'un emploi correct des informations utilisées par les applications internes ou externes pour authentifier les utilisateurs et donner les autorisations d'accès, via un service d'annuaire. De cette façon, l'Etat est à même de ne transmettre aux

partenaires externes de son choix que les éléments strictement nécessaires à la connexion et peut contrôler l'utilisation des services concernés.

f) La mise en œuvre au sein de l'Etat de services de messagerie et d'annuaire pour 45'000 élèves a un coût évalué et réparti comme suit :

- Des dépenses d'investissement pour environ 1.1 million de francs (pour l'acquisition des licences, du matériel et des prestations, y compris l'activation des charges de personnel) ;
- Des charges de fonctionnement liées au projet d'investissement, estimées à 150'000 F ;
- Des charges de fonctionnement induites de 560'000 F par année, pour assurer la maintenance et l'exploitation du dispositif.

L'investissement devra être reconduit tous les 5 ans, afin de procéder aux mises à jour des versions des logiciels et au renouvellement du matériel, pour un montant globalement similaire à l'investissement initial. Lissé sur 5 ans, le coût complet par élève serait ainsi de 1.50 F par mois.

Proposition du Conseil d'Etat

Compte tenu de ce qui précède, notre Conseil propose d'amender l'article 37A comme suit :

Art. 37A Sécurité des données personnelles des mineurs et des personnes majeures en formation (nouveau)

Les services de messagerie et d'annuaire des élèves et des autres personnes en formation dans l'enseignement public du canton de Genève, excepté au sein des Hautes écoles genevoises, sont fournis et hébergés par l'Etat.

Ainsi formulé, et sous réserve de disposer des moyens nécessaires pour mettre en œuvre ces nouveaux services au sein de l'Etat, nous soutenons le projet de loi 12103.

Si la variante proposée par notre Conseil est retenue par le Grand Conseil, nous déposerons un projet de loi d'investissement et entreprendrons les démarches en vue d'obtenir le budget de fonctionnement complémentaire nécessaire au projet.

En conclusion, nous estimons que l'Etat se doit de proposer aux élèves et autres personnes en formation, excepté au sein des Hautes écoles genevoises, des services de messagerie et d'annuaire leur permettant d'échanger de l'information et de s'identifier sans passer par un tiers. Ces services seraient fournis par la DGSI et gérés administrativement par le DIP, préservant ainsi le lien direct entre les enseignants et les élèves.

En restant à votre disposition pour tout renseignement complémentaire que vous souhaiteriez obtenir, nous vous prions de recevoir, Monsieur le Président, à l'assurance de notre parfaite considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Anja Wyden Guelpa

Le président :

François Longchamp

ANNEXE 16

Chère Madame,

J'ai pris bonne note de votre courriel du 24 octobre dernier et du message qui l'accompagnait, sous la signature de M. le Député Mathias Buschbeck, président de la commission législative du Grand Conseil genevois. Ayant peu d'informations à vous transmettre, je prends la liberté de vous répondre par la même voie électronique, faites-moi savoir si vous souhaitez disposer d'un document en bonne et due forme avec entête de la CIIP.

Voici les trois éléments de réponse qu'il m'est possible de fournir suite à vos questions :

1. Le choix des infrastructures informatiques, des ressources numériques et des outils online utilisés par les établissements scolaires relève exclusivement des autorités locales, soit cantonales soit communales, et de leurs ressources financières et techniques. Cela n'entre pas dans les compétences intercantonales et les conférences intercantonales ne procèdent donc à aucun relevé ou monitorage des choix effectués, ne sachant par exemple pas du tout quels cantons auraient fait un choix de type Google. Il en va de même pour ce qui relève de la protection des données et des critères de sécurité dans l'usage de données et d'adresses individuelles, la législation de chaque canton faisant foi.

2. L'organe disposant de la vue la plus large à ce sujet est le centre de compétences CTIE, Centre suisse des technologies de l'information dans l'éducation (educa.ch https://www.educa.ch/fr), agissant sur mandat de la Confédération et de la CDIP et gérant en leur nom le Serveur suisse de l'éducation et la messagerie educanet2 qui lui est rattachée, choisie par de nombreux cantons. Le CTIE négocie également, pour les besoins des établissements scolaires, des contrats cadre avec de grands fournisseurs de logiciels, dont Microsoft et Adobe, mais pas Google (http://www.educa.ch/fr/contrats-cadre). Lors de sa séance du 27 octobre dernier, la CDIP a adopté un concept cadre et confirmé le mandat attribué au CTIE / educa.ch pour la préparation d'un concept détaillé de "Fédération des services d'identités numériques pour l'espace suisse de la formation" (projet FIDES, voir http://www.educa.ch/fr/acces-ligne et http://www.educa.ch/fr/dossiers/eid). En gros, il s'agirait de créer d'ici 2019/2020 pour les enseignants et les apprenants de la scolarité obligatoire et des filières post-obligatoires, ainsi que pour les HEP, un équivalent de ce qu'est *switch* pour le degré tertiaire, dans une fédération offrant toutes les garanties de sécurité dans les relations électroniques entre acteurs du système éducatif et pour l'accès de ceux-ci à du matériel pédagogique en ligne auprès de fournisseurs publics et privés. Chaque canton devra librement décider, une fois le concept détaillé adopté et les conditions financières et techniques connues, s'il souhaite ou non adhérer à cette fédération, immédiatement ou ultérieurement, ce qui sur le plan romand présenterait de grands avantages au vu des accès aux plans d'études romands et aux ressources en ligne (moyens d'enseignement et ressources documentaires et didactiques disponibles).

3. Au vu de ce qui précède, je vous confirme qu'il n'y a pas de "solution romande" existante ou envisagée, les solutions retenues étant soit cantonale (comme à Genève ou Neuchâtel) soit suisse (educa et ultérieurement FIDES).

Dans l'espoir que ces informations puissent vous être utiles, je vous prie d'agréer, chère Madame, mes salutations les meilleures.
olivier maradan

CONFÉRENCE INTERCANTONALE DE L'INSTRUCTION PUBLIQUE DE

Olivier Maradan
secrétaire général

Secrétariat général de la CIIP
Fbg de l'Hôpital 68 - CP 556 - CH-2002 Neuchâtel
☏ +41 32 889 86 30 - 🖷 +41 32 889 69 73

ANNEXE 17

Tina Rodriguez Commission législative 08.12.2017

Comparaison intercantonale en matière de protection des données personnelles

Canton de Genève

Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)

Art. 37 Sécurité des données personnelles

[1] Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

[2] Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent **ou font traiter.**

[3] Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.

Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD) (A 2 08.01)

Art. 13A Sous-traitance (art. 37, al. 2, de la loi)

[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.

[6] Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.

Canton de Fribourg

Rien de particulier dans la loi sur l'information et l'accès aux documents (LInf) (17.5)

Ordonnance du 17 janvier 2017 ratifiant les statuts de l'Université de Fribourg (431.0.11)

Art. 14 Protection des données

Dans l'accomplissement de leurs tâches ainsi que dans les rapports internes, les membres de la communauté universitaire et les collèges respectent les dispositions relatives à la protection des données et **veillent à la protection des données personnelles.**

Tina Rodriguez Commission législative 08.12.2017

Canton de Vaud

Loi sur la protection des données personnelles (LPrD) (172.65)

Art. 17 Communication transfrontière de données

[1] **La communication vers un pays tiers de données personnelles faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat.**

[2] L'alinéa précédent n'est pas applicable :

a. si la personne concernée a donné son consentement, qui doit dans tous les cas être explicite ;

b. si la communication de données est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures pré-contractuelles prises à la demande de la personne concernée ;

c. si la communication est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;

d. si la communication est, en l'espèce, indispensable soit à la sauvegarde d'un intérêt public, soit à la constatation, l'exercice ou la défense d'un droit en justice ;

e. si la communication est, en l'espèce nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ;

f. si la communication intervient d'un registre public qui, en vertu de dispositions légales ou réglementaires, est destiné à l'information du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier ;

g. si des garanties suffisantes, notamment contractuelles, permettent d'assurer un niveau de protection adéquat à l'étranger.

Art. 18 Traitement des données par un tiers

[1] Le traitement de données peut être confié à un tiers aux conditions cumulatives suivantes :

a. le traitement par un tiers est prévu par la loi ou par un contrat ;

b. le responsable du traitement est légitimé à traiter lui-même les données concernées ;

c. aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

[2] Le tiers est responsable de la sécurité des données qu'il traite.

Canton du Valais

Ordonnance concernant le statut du personnel de la Haute école spécialisée de Suisse occidentale Valais/Wallis (HES-SO Valais/Wallis)

Art. 71 Protection de la personnalité et des données personnelles

[1] La HES-SO Valais/Wallis assure la protection de la personnalité de ses employés.

[2] Dans ce cadre:

a) elle prend les dispositions nécessaires pour empêcher toute discrimination entre les collaborateurs, en particulier en relation avec le sexe, la race, la culture, l'origine, la croyance et le mode de vie, notamment l'orientation sexuelle;

b) elle prend toutes les mesures nécessaires afin d'assurer la protection des employés qui font l'objet de menaces, d'attaques présumées ou d'autres atteintes à la personnalité dans l'exercice de leur fonction;

c) elle soutient, dans la mesure nécessaire, les employés ayant l'obligation de dénoncer d'éventuelles infractions pénales qui se poursuivent d'office;

d) elle prend toute mesure assurant la protection des données personnelles;

e) elle met à disposition une protection juridique pour les employés;

f) elle met à disposition des prestations de soutien, d'aide et de conseil à ses collaborateurs.

[3] L'employé victime d'une atteinte illicite portée par d'autres membres du personnel de la HES-SO Valais/Wallis a, s'il le désire, qualité de partie dans la procédure disciplinaire ouverte contre l'auteur de l'atteinte.

[4] L'autorité d'engagement peut accorder, sur demande formulée dès le début de l'affaire, l'assistance juridique à un employé:

a) en matière civile, si celui-ci est demandeur en raison d'un dommage subi dans l'exercice de ses fonctions ou s'il est intervenant accessoire dans une action ouverte contre la HES-SO Valais/Wallis;

b) en matière pénale, s'il est plaignant en raison d'une atteinte subie dans l'exercice de ses fonctions ou s'il est prévenu en raison d'un fait afférent à l'exercice de ses fonctions.

[5] L'assistance juridique peut être accordée après la cessation des rapports de service.

[6] Les frais d'assistance sont mis, par décision de l'autorité d'engagement, totalement ou partiellement à la charge de l'employé si celui-ci est reconnu coupable, pour autant qu'il ait violé intentionnellement ou par négligence grave ses devoirs de service.

Canton de Neuchâtel

Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel (CPDT-JUNE)

Sécurité des données

Art. 20

[1] Les entités doivent s'assurer que les données sont protégées contre un emploi abusif en prenant des mesures organisationnelles et techniques appropriées.

[2] Les entités veillent à l'intégrité, à la disponibilité et à la confidentialité des données.

Communication transfrontière

Art. 27

[1] Des données ne peuvent être communiquées à l'étranger que si les conditions requises par la législation fédérale sur la protection des données sont remplies.

[2] Les entités informent le préposé des garanties prises en vertu de cette législation avant la communication de données.

ANNEXE 18

RÉPUBLIQUE ET CANTON DE GENÈVE
GRAND CONSEIL
Commission législative

Genève, le 20 décembre 2018

TR

PL 12103 modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)
http://ge.ch/grandconseil/data/texte/PL12103.pdf

Statut juridique d'educa.ch

L'Institut suisse des médias pour la formation et la culture est une coopérative reconnue d'utilité publique. Dans le cadre de ses activités opérationnelles, elle se présente sous le nom d'educa.ch.

Mandat et organe responsable

Spécialisée dans les questions touchant aux technologies de l'information et de la communication (TIC), educa.ch est mandatée par le Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI) et la Conférence suisse des directeurs cantonaux de l'instruction publique (CDIP) pour gérer l'agence spécialisée suisse pour les TIC et l'éducation, depuis le 1er janvier 2017.

En tant qu'agence spécialisée de la Confédération et des cantons, educa.ch veille au développement de la qualité dans le domaine des TIC à l'école obligatoire et au secondaire II. Elle fournit des prestations qui ont pour but :

- d'assurer l'accès aux moyens d'enseignement numériques et aux services en ligne ;
- de garantir aux écoles le respect de leurs intérêts vis-à-vis des fournisseurs privés en négociant des contrats-cadre leur assurant des conditions sûres et équitables ;
- d'apporter l'expertise requise pour analyser les questions techniques, juridiques et éthiques liées à la numérisation dans l'éducation et de fournir des bases décisionnelles aux responsables du système éducatif ;
- de renforcer le dialogue et la collaboration entre les acteurs nationaux et internationaux.

Historique

À la fin des années 1980, l'Office fédéral de l'industrie des arts et métiers et du travail (OFIAMT, actuellement SEFRI) cherchait un partenaire pour la gestion d'un centre de compétences consacré à l'informatique dans la formation. Un contrat de partenariat fut signé en 1989 entre l'OFIAMT et l'Institut suisse du film (actuellement l'Institut suisse des médias pour la formation et la culture) pour la création et l'exploitation du Centre suisse des technologies de l'information dans l'enseignement (CTIE). La CDIP devint rapidement partenaire. La Confédération et les cantons, dans le cadre de leur action coordonnée, se sont ensuite dotés d'un nouvel instrument en 2001 avec le Serveur suisse de l'éducation (SSE). Plateforme nationale d'information, d'enseignement et d'apprentissage en ligne dédiée à la formation, le SSE met à disposition des acteurs du système éducatif des outils favorisant l'intégration des TIC dans l'enseignement et le développement de sa qualité. Depuis le 1er janvier 2017, educa.ch a succédé au CTIE et au SSE en tant qu'agence spécialisée pour les TIC et l'éducation.

ANNEXE 19

REPUBLIQUE ET CANTON DE GENEVE
Département des infrastructures
Office cantonal des systèmes d'information et du numérique

OCSIN
Direction générale
Case postale 2285
1211 Genève 2

N/réf. : PVE/JPG/ERF

République et canton de Genève
Grand Conseil
Commission législative,
A l'attention de M. Edouard Cuendet,
Président
Rue de l'Hôtel-de-Ville, 2
Case postale 3970
1211 Genève 3

Genève, le 11 janvier 2019

Audit des outils informatiques proposés par des fournisseurs externes
PL 12103 modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)

Monsieur le Président, cher Monsieur,

J'ai pris connaissance de votre lettre du 20 décembre 2018 concernant le PL 12103 et y réponds comme suit.

Vous me demandez dans quelle mesure les logiciels et programmes informatiques utilisés au sein de l'Etat de Genève sont audités, et, plus précisément, vous vous interrogez sur les contrôles menés par l'office cantonal des systèmes d'information et du numérique (OCSIN) ou par une autre entité afin de vérifier le respect des engagements contractuels pris par les fournisseurs de services informatiques externes de l'Etat.

En préambule, je souligne que l'OCSIN est particulièrement sensible à la confidentialité et à la protection des données de l'Etat. En particulier, l'OCSIN a pour règle de conserver sur ses propres serveurs les données personnelles qui lui sont confiées, celles-ci étant par conséquent traitées au sein du réseau de l'administration cantonale, également géré et protégé par ses soins.

Cependant, dans certains cas, par exemple lorsqu'un développement est confié tout ou partie à un sous-traitant, il peut s'avérer nécessaire de lui transférer provisoirement des données, notamment à des fins de tests. Lorsqu'il s'agit de données personnelles sensibles, celles-ci sont préalablement rendues anonymes. En outre, lorsque le développement est terminé, l'OCSIN exige du sous-traitant qu'il détruise les données personnelles qui lui auraient été confiées, qu'elles soient sensibles ou non[1].

Au surplus, conformément à ce que stipule l'article 13A, al. 3, RIPAD (RS Ge A 2 08.01)[2], l'OCSIN prévoit dans ses contrats la possibilité d'auditer les fournisseurs à qui des données personnelles sont transmises dans le cadre de sa mission. Ses modèles contractuels prévoient

de manière générique le respect de la LIPAD et de la LPD, et, donc la possibilité d'auditer leurs centres.

Bien qu'elle se réserve le droit d'auditer de tels fournisseurs, l'OCSIN n'audite qu'en cas de doute quant à la bonne exécution par le sous-traitant de ses obligations contractuelles. En effet, la disposition prévue par nos modèles poursuit un but essentiellement préventif. La systématisation de son application requerrait des moyens substantiels.

Concernant la société Google, expressément citée par le PL 12103, je relève qu'elle ne fait pas partie des fournisseurs de l'OCSIN, hormis dans le cadre de l'application « Google Analytics », utilisée sur le site internet officiel de l'Etat pour établir des statistiques d'utilisation du site par les internautes. Un projet est toutefois en cours de réalisation pour la remplacer par une application qui permettra de préserver les données au sein des serveurs de l'administration cantonale. Enfin, je précise que la société Google refuse par principe dans ses conditions générales tout audit de ses serveurs par un de ses clients.

En espérant avoir ainsi répondu à votre question, je vous prie, Monsieur le Président, cher Monsieur, d'agréer l'expression de mes salutations respectueuses.

Eric Favre
Directeur général

[1] Vous trouverez ci-dessous un exemple de clause contractuelle établie par l'OCSIN en matière de protection des données :

Article 19 : Sécurité et protection des données personnelles

Sécurité

1. Le Fournisseur confirme que les modules développés ou modifiés par ses soins ne contreviennent pas aux normes habituelles de sécurité, et qu'ils sont en particulier exempts de tout accès secret aux données de type « porte arrière » (« *back door* ») ou de tout accès qui serait assuré par un code d'identification programmé en dur (« *hardcoded password* ») ; il confirme que les modules livrés ne contiennent ni cheval de Troie ni fonctions non documentées (« *undocumented features* »).

Protection des données personnelles

2. De manière générale, le Fournisseur est conscient de ce que les modules développés par ses soins assurent le traitement de données confidentielles, en particulier d'éventuelles données personnelles au sens de la Loi fédérale sur la Protection des Données personnelles (LFPD – RS 235.1) ou de la Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD – RSGe A 2 08). Il s'engage par conséquent à développer des modules ou des applications répondant aux exigences des lois précitées et de leur règlement d'application.
3. Afin d'éviter toute violation du devoir de confidentialité du Fournisseur, le Client lui transmettra par défaut des données rendues anonymes. En cas de transmission explicite par le Client de données personnelles (non anonymisées), le Fournisseur s'engage à ce que ces données ne sortent pas du territoire suisse.
4. Le Fournisseur s'engage notamment :

- À signaler au Client toute donnée qu'il aurait reçue de lui par erreur sans qu'elles aient été au préalable rendues anonymes ;

- À détruire toute copie de telles données qu'il pourrait détenir dès lors que le motif de leur transmission (tests, correction de défauts…) n'existe plus ;
- À ne pas stocker de telles données dans des machines sises hors de ses locaux professionnels ;
- À ne pas stocker de telles données dans des machines mobiles (sauf accord écrit du Client)
- À ne pas stocker de telles données à l'étranger ;
- À structurer les bases de données contenant des données personnelles de façon à protéger au mieux leur confidentialité à l'égard d'accès indus de tiers ("Privacy by design") et à assurer une gestion des accès compatible avec les exigences légales.
- À ce que les données personnelles gérées par le Produit puissent être traitées (modification, suppression) de manière individuelle et non en paquets, afin de permettre une gestion circonstanciée de chacune d'entre elles ;
- À ce que le Produit permette d'effectuer un contrôle des accès de sorte que les données confidentielles ne puissent pas être consultées dans le cadre d'une utilisation régulière par des tiers non autorisés ;
- À ce que les accès aux données personnelles permettent de distinguer strictement les accès en lecture seule (simple consultation) des accès en écriture (droit de créer, modifier, supprimer les données) ;
- À ce que les modules développés prévoient d'associer aux données personnelles qu'ils gèrent, lorsque ces dernières sont destinées à être échangées entre différents offices ou services, l'indication de leur source ;
- À ce que les modules développés permettent au Client – notamment par des procédures de tri adéquates – de gérer aisément le cycle de vie des données personnelles et de supprimer les données répondant à la notion de « données inutilisées ou inutiles ».

[2] Pour mémoire, l'article 13A RIPAD, adopté à la demande de l'OCSIN et du collège LIPAD-RIPAD de l'administration cantonale, a la teneur suivante :

Art. 13A Sous-traitance (art. 37, al. 2, de la loi)

[1] Le traitement de données personnelles peut être confié à un tiers pour autant qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

[2] L'institution demeure responsable des données personnelles qu'elle fait traiter au même titre que si elle les traitait elle-même.

[3] La sous-traitance de données personnelles fait l'objet d'un contrat de droit privé ou de droit public avec le prestataire tiers, prévoyant pour chaque étape du traitement le respect des prescriptions de la loi et du présent règlement ainsi que la possibilité d'effectuer des audits sur le site du sous-traitant.

[4] Le recours par un sous-traitant à un autre sous-traitant (sous-traitance en cascade) n'est possible qu'avec l'accord préalable écrit de l'institution et moyennant le respect, à chaque niveau de substitution, de toutes les prescriptions du présent article.

[5] S'il implique un traitement à l'étranger, le recours à un prestataire tiers n'est possible que si la législation de l'Etat destinataire assure un niveau de protection adéquat.

[6] Le préposé cantonal publie une liste des Etats qui disposent d'une législation assurant un niveau de protection adéquat.

ANNEXE 20

Monsieur le Président,

Mesdames et Messieurs les député-e-s,

En vue de la séance de vendredi, je vous transmets les compléments de Mme Toledo du DIP sur le PL « Google » (PL 12103) :

Afin de répondre aux questions de la commission législative, dans sa nouvelle composition, concernant l'objet cité sous rubrique, je vous transmets à l'intention des nouveaux commissaires le courriel du DIP du 2 novembre 2017, lequel contient le contrat dont il est question et les amendements à celui-ci, y compris ceux entrés en vigueur le 25 mai 2018. ***Ce sont ces documents qui font foi à l'exclusion des conditions d'utilisation qui lient uniquement les personnes privées et la société Google.***

J'appelle respectueusement l'attention des membres de la commission sur le document intitulé **"Amendement relatif au traitement des données_annexe 3" et en particulier sur ses pages 12 et suivantes**.

L'amendement considéré porte le titre "*Version 2.0 of the Data Processing Amendment will take effect from 25 May 2018 (when the EU's General Data Protection Regulation comes into force) and replace Version 1.6 of the Data Processing Amendment (where applicable) on that date" (ci-après: Version 2.0 of the Data Processing Amendment; voir annexe 3, pages 12 et ss).*

Cet amendement venant compléter le contrat *Contrat G Suite for Education (en ligne)*, ci-joint, permet de préciser les éléments suivants :

- **Le droit applicable et l'application du RGPD** :

  Non, le droit anglais n'est pas applicable entre le DIP et Google, au contraire de ce qui est généralement prévu pour les particuliers.

  A ce sujet, je prie les membres de la commission de bien vouloir se référer à ***la définition figurant à la page 13 du document intitulé Version 2.0 of the Data Processing Amendment*** où il est précisé que : ***"European Data Protection Legislation" means,*** as applicable: (a) the GDPR; **and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland), ainsi qu'à *l'article 4.1, lettre a, de l'amendement précité***, lequel prévoit que :

  "4.1 Application of European Legislation. ***The parties acknowledge and agree that the European Data Protection Legislation will apply to the processing of Customer Personal Data if, for example: (a) the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA***".

  Ainsi, en matière de protection de données, ce sont le règlement européen sur la protection des données (RGPD) et ("and") la loi fédérale sur la protection des données (LPD) qui s'appliquent, conformément à l'article 4.1 de l'amendement précité, entré en vigueur le 25 mai 2018; le DIP exerçant son activité sur le territoire suisse, territoire bénéficiant des mêmes clauses contractuelles que celles prévues, par l'entreprise Google, pour les pays de l'Espace économique européen et le droit suisse ayant en outre été expressément mentionné.

- **Le for :**

  Contrairement à ce qui se fait avec des particuliers, le DIP n'a conclu aucune élection de for en faveur des tribunaux anglais mais au contraire ***la société Google s'est engagée à collaborer avec les autorités nationales de protection de données, conformément à la législation européenne applicable et à la LPD***.

- **Le lieu de stockage des données :**

  En principe, les données devraient être stockées au sein de l'Espace économique européen (voir les articles 10.2 de la *Version 2.0 of the Data Processing Amendment will take effect from 25 May 2018*). Néanmoins, en raison de

l'emploi du Cloud, la société Google ne s'est pas engagée à ne pas transférer des données vers les Etats-Unis, pays jusqu'à ce jour reconnu par les autorités fédérales comme présentant, en matière de protection des données, un niveau de protection équivalent à celui de la Suisse à condition que l'entreprise considérée se soit engagée à appliquer le ***Swiss-US Privacy Shield***, ce que l'entreprise Google a fait. Voir la liste du préposé fédéral à la protection des données :
https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/04/staatenliste.pdf.download.pdf/liste_des_etats.pdf
.

J'appelle également l'attention des membres de la commission sur l'article suivant de la "*Version 2.0 of the Data Processing Amendment will take effect from 25 May 2018" :*

"7.5.2. Customer's Audit Rights.

(a) ***If the European Data Protection Legislation applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Data Processing Amendment in accordance with Section 7.5.3*** (Additional Business Terms for Reviews and Audits). Google will contribute to such audits as described in Section 7.4 (Security Certifications and Reports) and this Section 7.5 (Reviews and Audits of Compliance)."

Ainsi, conformément aux exigences du RGPD, la société Google s'est bien engagée à permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le contrat Google et ses amendements n'étant pas simples à lire pour des personnes qui ne sont pas familières avec ce type de contrat, je me tiens bien volontiers à disposition pour tout complément d'information que la commission législative ou vous-même estimeriez utile.

Avec mes meilleurs messages,

Giselle Toledo Vera
Juriste, titulaire du brevet d'avocat

REPUBLIQUE ET CANTON DE GENEVE

Département de l'instruction publique, de la formation et de la jeunesse

Direction des affaires juridiques

Rue de l'Hôtel-de-Ville 6

Case postale 3925 - 1211 Genève 3

Tél. +41 (0)22 546 69 20 - Fax +41 (0)22 546 69 49

Tél. DAJ +41 (0)22 546 69 22/40

Code d'acheminement interne : A104ER

Absente les lundis et mardis

Date de dépôt : 10 août 2020

RAPPORT DE LA MINORITÉ

Rapport de M. Jean Rossiaud

Mesdames et
Messieurs les députés,

Le PL a été déposé lors de la dernière législature par le groupe des Verts. Il aborde pour la première fois à Genève un sujet d'une très grande importance.

A la lecture de l'exposé des motifs, on comprend qu'il vise à protéger les écoles genevoises des grandes entreprises du numérique, notamment les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), et plus particulièrement Google, qui a infiltré les écoles genevoises (comme partout ailleurs dans le monde, du reste, avec une plus grande efficacité que ses concurrents Apple et Microsoft).

Le projet de loi vise à introduire un nouvel article dans la *Loi sur l'information du public, l'accès aux données et la protection des données personnelles (LIPAD)* : L'art. 37A *Sécurité des données personnelles des mineurs et des personnes majeures en formation*.

Cette modification de la LIPAD vise à protéger les élèves, non seulement pendant leur parcours scolaire dans une école publique sous la responsabilité de l'Etat, puisque leurs données pourraient être captées à des fins de profilage commercial ou politique, mais également une fois leur parcours scolaire terminé, puisque les données produites alors que les élèves étaient sous la protection de l'Etat, pourraient être utilisées contre leur intérêt après leur sortie du système scolaire.

En tant que tel, le PL 12103 ne vise pas frontalement à protéger les élèves des GAFAM, mais il le fait de manière indirecte, en légiférant sur les adresses e-mail des élèves (al. 1 et al. 2 de l'art. 37A du PL) et sur le stockage des données (al. 3 de l'art. 37A du PL). Une majorité de commissaires a prétendu que le libellé de ce projet de loi était imprécis, voire inapplicable. Il pouvait être amendé et c'est ce qu'a proposé le Conseil d'Etat, dont la position a évolué dans le bon sens, au fur et à mesure que nos débats démontraient la nécessité absolue de légiférer en la matière.

L'amendement du Conseil d'Etat a été refusé par la majorité de la commission. Même le Conseil d'Etat ne prend pas, à notre avis, toute la mesure du risque encouru par les élèves quant à la protection de leurs données personnelles et évalue mal les responsabilités de l'Etat en la matière. Cependant, son amendement va dans le sens de ce projet de loi, et la minorité pourrait reconnaître que son adoption constituerait une première étape. Il est donc encore temps de rectifier le tir et d'accepter l'amendement du Conseil d'Etat ; puis il s'agira de remettre l'ouvrage sur le métier pour compléter la réflexion et les mesures à prendre en la matière, en convainquant les enseignant.e.s, qui aujourd'hui poussent à un usage imprudent des outils « offerts » par Google ou d'autres géants du Net, que l'utilisation d'un outil pédagogique ne justifie pas une prise de risque inconsidérée sur la protection des données personnelles des élèves dont nous avons collectivement la responsabilité.

Que dit le PL 12103 ?

La messagerie. Le premier alinéa de l'art. 37A (nouveau) oblige l'Etat à donner une adresse électronique administrative et officielle à chaque élève (comme dans les universités, les EPF et les HES), pour éviter, ce qui est le cas aujourd'hui, que ce service soit fourni par une entreprise privée, en l'occurrence Google, qui a un intérêt immédiat et concret à la captation des données produites par les élèves via leur adresse électronique Google. Le deuxième alinéa propose qu'« en cas de nécessité » la messagerie puisse être fournie par des entreprises suisses et domiciliées en Suisse. Cet alinéa 2 a été jugé, par une majorité de la commission, difficile à mettre en œuvre sur le long terme. En effet, qu'est-ce qu'une « entreprise suisse » ? Que fait-on si elle est rachetée par une entreprise étrangère ?

Le stockage. Le troisième alinéa traite quant à lui des espaces personnels de stockage mis à disposition des élèves pour leurs travaux scolaires, et précise qu'ils doivent être fournis par un centre de données en Suisse et soumis à la loi suisse. L'idée est d'empêcher que les Etats, notamment les Etat-Unis avec le *Patriot Act*, obligent les entreprises ayant leur siège sur leur territoire à fournir toutes leurs données, même si celles-ci sont produites hors du territoire de l'Etat en question, et même si elles sont protégées par des conventions *ad hoc*. Il est vrai que toutes les GAFAM ont leur siège aux Etats-Unis, et que les Etats-Unis font généreusement appel à la procédure d'extra-territorialité. Il est donc impératif de se protéger.

Le travail en commission nous a démontré que l'ampleur du problème posé par les GAFAM est bien plus importante que ce que la majorité des

député.e.s avait soupçonné. Il est vrai également que depuis que ce projet de loi a été déposé, en avril 2017, le pouvoir des GAFAM n'a cessé d'augmenter, les scandales sur leur utilisation abusive des données personnelles à des fins commerciales ou délictueuses se sont multipliés.

L'objet de ce projet de loi est donc plus que jamais d'actualité, même si techniquement il ne traite que de la pointe de l'iceberg (l'adressage électronique et le stockage). La crise sanitaire de la Covid19, et surtout les mesures massives de confinement mises en place sur tous les continents, ont développé de manière inédite le télétravail, le télé-enseignement et la téléformation ; ils ont fait se croiser également sur un même lieu, le foyer familial, utilisant souvent la même adresse IP, les données des entreprises, des administrations, des ONG et des partis avec les données personnelles des membres du foyer, élèves y compris. Les GAFAM (auxquelles nous devrions adjoindre aujourd'hui Netflix) ont vu leur chiffre d'affaire et leurs bénéfices exploser alors que la crise économique frappait de manière indiscriminée le reste de l'économie mondiale. Leur renforcement relatif dans l'économie mondiale en fait aujourd'hui un acteur « politique » extrêmement puissant, et bien plus important que la majeure partie des Etats, non seulement financièrement mais aussi puisque leur emprise et leur impact est planétaire. Quand nous entendons en commission « le DIP a négocié avec Google », nous ne pouvons que sourire.

En attendant une *gouvernance mondiale du Net* qui permettrait à la fois de protéger les personnes et de faire bénéficier chacun.e et tout le monde de l'énorme manne que constitue l'intelligence artificielle produite avec les données personnelles, les Etats qui désirent rester souverains devraient être amenés à une stricte prudence. En l'occurrence, brader les fondements de notre Etat de droit et de notre démocratie fondée sur les libertés publiques pour quelques outils pédagogiques – dont l'intérêt n'a nullement été démontré – relèvent de la pure inconscience des enjeux contemporains, ainsi que de l'aventurisme politique.

Avant de détailler la pratique actuelle du DIP et en quoi elle est problématique, intéressons-nous à l'enjeu sociétal posé par les GAFAM.

Les GAFAM : un empire mondial

Le développement de ces cinq géants du Web s'inscrit dans le cadre de la révolution numérique ou de la troisième révolution industrielle du début du XXIe siècle. Il s'agit pour ce qui deviendra les GAFAM de prendre possession mondialement des données des personnes, pour les revendre à des acteurs économiques (à travers la publicité ciblée par exemple) ou politiques

(voir par exemple le scandale *Cambridge Analytica*, qui a manipulé contre rémunération des élections et votations dans une vingtaine d'Etats, sur la base du profilage des comptes Facebook des électeurs et électrices).

Depuis une dizaine d'années en tout cas, on enseigne dans le post-obligatoire genevois, dans des cours de géographie ou d'histoire, ainsi que dans les formations aux médias, que dès le début des années 2000, les GAFAM forment un oligopole qui se partage le marché de l'Internet. Cet oligopole est concentré « verticalement » (centres de données, systèmes d'exploitation, navigateurs web, infrastructures de réseaux, etc.) et « horizontalement » (messageries, communication, réseaux sociaux, etc.). Tous les aspects de la vie publique et privée sont potentiellement ciblés et tracés par ces entreprises.

On enseigne aussi dans ces cours que les Big 5 (comme on les appelle également) font régulièrement l'objet de critiques sévères voire de poursuites judiciaires sur le non-respect de la vie privée des internautes, sur des abus de position dominante, ainsi que sur le plan fiscal (selon un rapport de 2017 de Moody's – société active dans l'analyse financière des entreprises –, cité par le journal *Le Temps* du 12 octobre 2017, Google/Alphabet possédait 51 milliards de dollars américains de fortune placée dans les paradis fiscaux).

Le DIP n'aurait-il pas une attitude schizophrénique à laisser enseigner, avec objectivité et sérieux les dégâts actuels et les risques potentiels que font porter les GAFAM sur le respect de la vie privée des individus et plus généralement sur les libertés publiques, tout en livrant, dans le même mouvement, les élèves en pâture au plus vorace d'entre eux, Google, qui se nourrit de ce qui est la plus précieuse valeur marchande au monde aujourd'hui, l'information que nous produisons nous-même à chaque fois que nous nous connectons. Comment l'Etat de Genève peut-il continuer à passer des accords avec des entreprises considérées à juste titre comme des délinquantes fiscales ?

Comme le relève de nombreuses ONG défendant les droits humains (dont Amnesty international et Oxfam International), la collecte disproportionnée de données personnelles est incompatible avec le droit à la vie privée ; la perte de ce dernier portant atteinte à d'autres droits : la liberté d'expression, la liberté d'opinion, la liberté de pensée ainsi que le droit à la non-discrimination.

Nous savons que le modèle économique des GAFAM est basé sur le ciblage et le traçage des personnes, c'est-à-dire sur leur surveillance permanente. En effet, en même temps que l'oligopole se déploie sur la planète de manière globale, chaque individu est *ciblé* à la fois dans des

caractéristiques (toujours plus nombreuses) les plus personnelles (âge, sexe, localisation, reconnaissance faciale, vocale, habitudes de consommation, méthode de travail, relations familiales et amicales, préférences sexuelles, analyses de contenu permettant de discerner ses opinions politiques, son « entregent », son « savoir-vivre » ou son « savoir-être », *etc*.), et « *tracé* » dans l'espace (déplacements) et dans le temps (histoire de vie). L'ensemble des informations que chacun.e d'entre nous transmet sans y prêter attention aux GAFAM, constitue pour les géants du Net, une mémoire sur nous-mêmes, qui est bien plus précise, plus systématique et plus objective – et donc moins sélective et moins subjective – que nos propres souvenirs. *L'anonymisation, dans ces conditions, est un vœu pieu*. Dans le domaine scolaire, il ne s'agit pas seulement de protéger les données, mais bien également de permettre aux élèves d'apprendre et de dépasser leurs difficultés, sans qu'ils n'aient à se soucier de la façon dont leurs préférences, talents, habitudes d'apprentissage précoces, analysés par les algorithmes pourraient donner des indications sur les opportunités de développement personnel que leur réserve l'avenir. Aucun utopiste des systèmes totalitaires n'a jamais rêvé d'un tel pouvoir de surveillance et de contrôle sur les personnes. Aucune entreprise n'a rêvé d'une telle exploitation des ressources individuelles et collectives, d'une telle captation de marché sur les plans local et global, de la création de nouveaux produits ciblés tant au niveau des individus, des groupes, des communautés, des sociétés, que sur le plan universel. Aujourd'hui les GAFAM réunissent en leurs mains à la fois le pouvoir de domination des personnes, historiquement le fait de l'Etat, et le pouvoir d'exploitation des ressources (l'information et le Big Data), moteur moderne de la vie économique. Elles ne manqueront pas d'imposer leur vision du monde, qui était l'apanage des religieux et des idéologues, tant il leur sera facile de contrôler et de manipuler les esprits. Il est de notre devoir collectif d'opposer une résistance à ce phénomène. Certes nous n'avons pas les moyens, en tant qu'Etat de Genève, de changer seuls le cours des choses, mais nous pouvons dire à la manière des dissidents « not in my name », et participer à la mise en place de solutions collectives.

Le DIP instrumentalisé par Google

Les commissaires à la Commission législative partageaient unanimement le point de vue que le DIP a pour mission de rester innovant et d'utiliser les outils pédagogiques de notre temps. Il existe donc un large accord pour que le DIP poursuive son programme d'*école en ligne*, qu'il prépare les élèves à la production collaborative, au partage de données et des savoirs, aux apprentissages autodidacte et collectif, au télé-enseignement, à la recherche

en ligne, à la téléformation, au télétravail, à la valeur et à la valorisation (pourquoi pas) de leurs données personnelles, et bien sûr aux risques de captation de leur données par des acteurs économiques poursuivant leur intérêt d'entreprise, c'est-à-dire leur propre profit.

Cette politique éducative n'est pas compatible selon la minorité avec l'utilisation des services d'une entreprise privée telle que Google (ou toute autre GAFAM), car ces entreprises n'offrent pas le minimum de garantie que nous exigeons sur la protection des données personnelles, et que par les outils, c'est toute une philosophie de l'éducation qui est véhiculée et qu'il faudrait prendre le temps d'interroger.

La stratégie de Google/Alphabet (depuis 2018 le consortium Alphabet regroupe toutes les activités de Google, ainsi que notamment Gmail et YouTube) n'est pas spécifique à la Suisse, ni même à Genève, même si nous devons regretter que Genève a fait figure de pionnière dans le domaine, en installant parmi les premières, ce cheval de Troie dans les classes et les cerveaux des élèves.

Au fil des années, Google s'est révélé pouvoir produire le service le plus complet et le plus facile d'utilisation. Aux Etats-Unis d'abord, en commençant par Chicago, puis en Europe (dont en Suisse et à Genève en particulier), Google a mis en place une stratégie commerciale agressive ciblée sur les enseignant.e.s et les pédagogues, et un lobbying politique important, principalement auprès de l'Union Européenne, notamment au moment des discussions autour du RGDP.

Dès 2014, le DIP utilise « *Google Suite for Education* », un logiciel intégré qui comprend à la fois une suite bureautique, un service de mail, un espace de stockage limité et une plateforme d'interaction entre l'élève et l'enseignant, ainsi que d'autres logiciels permettant notamment l'apprentissage des langues.

La suite bureautique par exemple (très proche des outils word ou excel, développés par Microsoft) permet à plusieurs élèves et à leur enseignant.e., de travailler en même temps sur les mêmes documents. Pour le DIP, c'est ainsi une philosophie de l'apprentissage collaboratif et de la philosophie du partage qui est encouragée, notamment parce qu'elle ouvre les élèves à davantage de co-construction des connaissances.

Cependant, sur le plan du rapport à la connaissance et au savoir, il s'agit d'un changement de paradigme dont nous ne sommes pas certains que le DIP (la FAPSE a-t-elle été au moins consultée ?) n'ait mesuré toute l'ampleur.

La préférence systématique donnée à la fois au travail en équipe et à la résolution de problème, que proposent les outils pédagogiques de Google,

peut se faire insidieusement au détriment de l'apprentissage individuel, théorique ou conceptuel, et à l'esprit critique. En effet, surtout dans le post-obligatoire, développer l'esprit critique est l'enseignement le plus important à apporter. Il est le socle de la citoyenneté, et la garantie de la meilleure adaptation au monde qui change. Cela se manifeste le plus souvent par le fait qu'il est parfois préférable de reconfigurer le problème et de questionner ses présupposés, avant de prétendre vouloir le résoudre (penser « en dehors de la boîte »). L'approche par la résolution de problèmes est utile, certes, c'est la pensée pragmatique de l'ingénieur, du médecin ou du juriste, dont le métier est précisément de résoudre les problèmes qu'on lui pose. Mais dans le processus d'apprentissage, il ne s'agit pas tant d'apprendre à résoudre des problèmes spécifiques, mais principalement de se faire une compréhension personnelle et intime des phénomènes, et plus fondamentalement de ce que sont la technique, la science, la santé ou la justice et leur rapport au savoir, à l'éthique personnelle ou aux rapports de force politique, économique, sociaux qui sous-tendent la société… et les problèmes qu'elle nous pose.

Pour *l'apprentissage des langues* avec les outils de Google, notamment l'anglais et le français, les *plateformes interactives* entre élèves et entre les enseignants et les élèves sont, d'après le DIP, tellement supérieure aux autres méthodes, qu'on se demande un peu comment pouvait-on enseigner ses matières avant, comment les enseigne-t-on ailleurs. N'y aurait-il vraiment pas des solutions finalement moins coûteuses à terme, si l'on prend une évaluation globale des risques, non seulement pour les élèves, mais aussi pour l'Etat, en cas de mise en cause de sa responsabilité ? N'existe-t-il pas de possibilités de construire sur le plan suisse ou européen des outils pédagogiques performants ? Est-on obligé de foncer dans la première opportunité venue, alors que les risques sont mal évalués ? Pour la minorité, le jeu n'en vaut pas la chandelle.

Une adresse et un lieu de stockage chez Google. Enfin, et voilà le point central et problématique du dossier, pour utiliser la plateforme Google, et tous ses logiciels, les élèves, qu'ils travaillent en classe ou à la maison, sont obligés de passer, pour travailler en ligne et pour stocker leurs documents, par une adresse e-mail que Google leur offre « gratuitement (?!) », par l'intermédiaire du DIP. Le format de l'adresse est trompeur « @eduge.ch », car il est presque identique au » @edu.ge.ch » (avec points entre « edu » et « ch ») créé par l'Etat pour le personnel enseignant et administratif du DIP. Les libellés des adresses instillent ainsi auprès des élèves et des parents une confusion (voire une tromperie), puisque, écrite sous cette forme, l'adresse Google se voit conférée une apparence officielle (presque la même adresse

que celle utilisée par les enseignants dans leur correspondance administrative avec les parents et les élèves).

Le stockage des données par Google est une condition sine qua non de l'utilisation de la plateforme, et *l'adresse électronique chez Google* est ce qui garantit à Google que toutes les données lui seront bien transmises. Comme ses données sont évidemment déposées sur le *cloud* de Google, c'est-à-dire partagées à différents endroits de la planète numérique, la question de la localisation en Suisse ou dans des entreprises suisses de ses données, nous semble très difficile à exiger et à contrôler.

La captation systématique des données des élèves par cette entreprise commerciale pose immédiatement deux problèmes politiques et juridiques.

Premièrement, comme on l'a vu, ces adresses peuvent très difficilement être anomymisées. Jusqu'à peu de temps en arrière, la politique d'anonymisation du DIP consistait à supprimer les voyelles (!) des noms des élèves. Pour les géants du Net, la reconstitution des identités est un jeu d'enfant. Une telle naïveté de la part du DIP prêterait à sourire, si elle ne démontrait pas une méconnaissance des potentialités techniques des algorithmes créés par les GAFAM, et surtout du potentiel de nuisance que permet la reconstitution des identités et le profilage (psychologique, commercial, politique), d'autant plus quand on les croise avec la géolocalisation, et notamment celles des parents quand l'élève se connecte depuis l'adresse IP de l'ordinateur familial, pour terminer ses devoirs, notamment par temps de confinement.

Deuxièmement, le DIP ne nous a pas convaincu sur le fait qu'il demandait suffisamment *formellement* l'autorisation aux parents des élèves mineur.e.s de pouvoir se connecter à une plateforme privée, voire d'élèves majeur.e.s vivant chez eux et utilisant un ordinateur familial. A titre personnel, je n'ai aucun souvenir d'avoir dû signer une autorisation pour mes trois enfants mineur.e.s, lors de leur passage dans le post-obligatoire, pour la création et l'utilisation d'une telle adresse ; encore moins avons-nous reçu une explication claire pour promouvoir la sécurité ou prévenir les risques liés à la protection des données, ni à l'école, ni depuis la maison. Le DIP est-il bien certain que son devoir d'information et de formation auprès des élèves et de leurs parents est réellement effectif ?

Des mouvements de contestations contre ces pratiques grondent et commencent à se faire entendre. Que ferait un enseignant si les parents refusaient que leur enfant possède une adresse Google ou s'opposaient au travail en collaboration ou au dépôt d'exercices scolaires personnels sur des plateformes *privées*, dont l'objectif avéré est la captation d'un maximum de

données personnelles à des fins lucratives ? Ces élèves seraient-ils exclu.e.s du cours ? L'Etat de Genève pourrait-il faire face financièrement à des plaintes de parents pour violation de la sphère privée (de leur enfant ou de la leur via l'adresse Google/DIP de leur enfant), s'il s'avérait que malgré les protocoles signés, le système mis en place ait permis le profilage de leur enfant ou d'eux-mêmes, à des fins commerciales ou politiques et engendré des conséquences dommageables (le refus d'entrée sur le territoire d'un pays qui aurait été critiqué dans des dissertations ou exercices ; le refus de l'obtention d'une bourse d'étude ou de l'entrée dans une école ou une université ou une disqualification pour un poste de travail, sur la base de difficultés orthographiques, sur un profilage comportemental ou idéologique jugé inadéquat par l'établissement universitaire ou par l'employeur, ou sur le fait que son parcours scolaire puisse être relié à des séjours en clinique psychiatrique, ou encore le refus d'une assurance de l'accepter comme assuré sur la base de données collectées pendant toute sa scolarité, par exemple ?).

Au-delà du DIP, l'Etat a-t-il mesuré ce risque de manière adéquate et avons-nous en tant que parlement budgété suffisamment de fonds pour faire face le cas échéant à une avalanche de plaintes en responsabilité parce que le DIP n'aurait pas suffisamment protégé les élèves ?

Le risque de violation de la sphère privée et ses conséquences en termes de responsabilité pour l'Etat vaut-il la peine d'être encouru, en regard de l'avantage – à démontrer (le DIP a été peu convainquant en la matière) – que procurerait l'utilisation d'un outil pédagogique spécifique proposé par une plateforme commerciale ?

Bien sûr, Google peut assurer vouloir respecter toutes les lois et réglementations en vigueur et, notamment pour ce qui nous concerne, la loi suisse sur la protection des données et la LIPAD genevoise, et le RGPD de l'Union Européenne (un peu plus contraignant), mais Google se permet *contractuellement* (c'est stipulé dans les contrats et avis de confidentialité validés par le DIP) de changer unilatéralement ses conditions et, quels seraient les moyens politiques ou financiers que le DIP devrait déployer pour sortir du système, récupérer les données et, le cas échéant, intenter un procès à Google, au cas où l'entreprise violerait la protection des données personnelles des élèves ou si elle était obligée par les Etats-Unis de livrer ces données à la NSA, au FBI ou à la CIA au nom du principe d'extra-territorialité (Patriot Act).

Effectivement, « sur le marché de l'éducation » aujourd'hui, le DIP nous a convaincu que rien n'existe d'aussi concurrentiel que Google. Si nous pensons à courte vue, nous ne pouvons qu'en convenir, notamment parce que Google est « presque gratuit ». Or nous savons que selon l'expression « si

c'est gratuit, c'est toi le produit » que le modèle d'affaires de Google est loin d'être gratuit, puisqu'il rapporte très gros.

Premièrement, l'acquisition de fait des données (même anonymisées) par Google constitue un paiement en nature.

Apple ou Microsoft par exemple ont construit leur modèle d'affaires principalement en vendant des appareils ou des services logiciels. Au contraire, Google gagne principalement de l'argent de la publicité en ligne. Même si le DIP a choisi un produit Google en partie payant pour éviter que les élèves ne reçoivent de la publicité en ligne, les données collectées par Google permettent de mieux cibler la publicité pour d'autres personnes au profil similaire, ou sur ces mêmes personnes quand elles seront sorties du contexte scolaire, mais resteront traçables au moment de la connexion à d'autres applications (notamment YouTube, Gmail ou Google Chrome). Bien sûr, Google n'accepte de rendre public ni les détails des informations récoltées, ni l'objectif de cette récolte, ni la manière dont ces données sont utilisées. Mais cela rapporte gros, indéniablement.

Si l'on convient que le chiffre d'affaires de Google était, bon an, mal an, avant la Covid-19, de 40 milliards de dollars par an (dont 20 milliards de bénéfice !), la valeur de la « gratuité » offerte par les internautes à Google est donc de 20 milliards (ce qui est une somme colossale) par année. Une fondation qui gèrerait cette somme comme un bien commun au service de la connaissance et de la construction d'outils pédagogiques universels règlerait définitivement la question de la protection des données.

Deuxièmement, même si l'argument précédent est écarté et que Google ne revend pas les données personnelles des élèves (ce dont nous doutons fortement), le fait même que l'environnement pédagogique de Google soit privilégié par le DIP, donne à Google un avantage concurrentiel important par rapport à ses concurrents dans le domaine de l'éducation (notamment Apple et Microsoft). En étant pionnier en la matière, Google dispose dans chaque pays, dans chaque système éducatif, d'utilisateurs privilégiés, les pédagogues et les enseignants, dont le retour permanent d'expérience permet d'améliorer continuellement les outils et les rendant encore plus compétitifs. Les élèves et les enseignants participent ainsi au renforcement de l'entreprise commerciale Google, en affaiblissant *ipso facto* ses concurrents et en diminuant les possibilités d'émergence d'outils éducatifs publics ou en main de fondations à but non lucratif, qui partent très handicapés dans cette concurrence déloyale. Dans la guerre commerciale planétaire que se livrent entre elles les GAFAM, mettre la main sur l'école est un enjeu géopolitique de la plus grande importance, tant nous savons que formater les outils, c'est

formater les esprits. Donner un tel avantage concurrentiel à une entreprise privée particulière devrait également se monnayer.

Troisièmement, les élèves qui se seront habitués à travailler avec l'environnement Google seront tentés de poursuivre dans le même environnement de travail une fois qu'ils auront quitté l'école. Ils deviendront ainsi des ambassadeurs permanents de Google. Google est très offensif dans la poursuite de cette stratégie : alors qu'il est toujours assez compliqué de récupérer ses données stockées par Google le temps de sa scolarité, Google propose aux élèves qui ont terminé leur cursus de basculer de leur adresse scolaire, « @eduge.ch » par exemple, sur une adresse @gmail.com. L'élève ne perd ainsi rien de ses données scolaires personnelles (ce qui le rassure) ; Google récupère l'ensemble des données historiques de l'élève, tout en pouvant préciser son ciblage et renforcer son traçage, maintenant que les conditions spécifiques des accords de confidentialités signées avec le DIP ne s'appliquent plus et que ce sont les conditions générales de Google qui s'appliquent désormais. Le poisson, canalisé par le DIP vers le chalutier Google, a mordu à l'hameçon. Là encore, l'avantage offert par le DIP à Google a une valeur qu'il faudrait savoir évaluer et, le cas échéant, faire payer.

Le DIP a-t-il calculé le coût réel de ce qu'il offre à Google en contrepartie de la gratuité ? Non. A-t-il l'intention de le faire ? Non. Si cette contrepartie était évaluée, nous arriverions peut-être à la conclusion que quitte à monnayer les données des élèves (même anonymisées, ce qui semble presque impossible), le DIP pourrait au moins les vendre à un meilleur prix et augmenter les bourses d'études, voire développer ses propres outils informatiques. Produire sa propre intelligence collective peut rapporter gros ! Inciter les autres cantons et les autres Etats à en faire de même pourrait être un défi digne de l'esprit de Genève et du rôle de promotion de la Genève internationale en matière de gouvernance du bien commun formidable que constitue le Big Data, quand il n'est pas utilisé à des fins commerciales ou anti-démocratiques.

Voter l'amendement du Conseil d'Etat et remettre l'ouvrage sur le métier

La majorité de la Commission législative n'a pas été en mesure de comprendre l'ampleur du problème, et par conséquent, elle n'a pas su saisir l'opportunité d'être créative en la matière. Le parlement a encore la possibilité de redresser la barre.

La situation est grave et ce projet de loi, par une trop grande prudence peut-être, ne s'attaquait pourtant qu'à la pointe de l'iceberg.

Et pourtant encore, au fil des 15 séances de commission sur deux ans, le DIP et le Conseil d'Etat ont mieux compris les enjeux, notamment sur le fait d'offrir une adresse électronique à chaque élève. Seule une telle option pourrait *séparer les données personnelles strictes et les données administratives des élèves*, d'une part, *des données pédagogiques,* d'autre part. Les premières comprennent les bulletins scolaires, les notes, les communications avec les parents sur les absences et sur le comportement des élèves, et toutes les données personnelles des élèves, sauf les données pédagogiques. Elles ne peuvent en aucun cas être délivrées par une entreprises commerciale quelle qu'elle soit, encore moins par un des géants de l'Internet, comme Google. Les secondes ne concernent que les données pédagogiques (cours, travaux et exercices), qui constituent à nos yeux également des données personnelles d'élèves qu'il faudrait protéger car leur contenu est utile au profilage malveillant, mais qui demande une protection peut-être moins stricte. Ces dernières pourraient être accessibles par une adresse privée *ad hoc*, mais là encore, il faudrait éviter les suites proposées par les GAFAM, en raison des risques qui ont été décrits plus haut. Il faudra pour cela convaincre certains pédagogues et enseignant.e.s, qui ne regardent le problème que par le bout de leur lorgnette pédagogique, et continuent à défendre un système délétère.

Le Conseil d'Etat a proposé un amendement très raisonnable pour la mise en place par l'Etat d'une adresse électronique pour chaque élève. Cet amendement a été refusé à une très faible majorité en commission. Il est encore temps de le voter ce soir. L'Art. 37A nouveau deviendrait : Les services de messagerie et d'annuaire des élèves et des autres personnes en formation dans l'enseignement public du canton de Genève, excepté au sein des Hautes écoles genevoises, sont fournis et hébergés par l'Etat ». En attendant une *identité numérique*, publique et sécurisée, pour chaque résident.e, cette modification législative pourrait être considérée comme un premier pas.

Le coût de cette opération, qui devrait s'élever à environ 2.50 F par mois pour chaque élève, est minime par rapport à la sécurité que l'Etat doit à ses élèves.

Le Conseil d'Etat est d'avis que les alinéas 2 et 3 de l'art. 37A du projet de loi « limiteraient de manière trop importante l'usage des outils numériques ». Nous ne partageons pas ce point de vue. Cependant, nous avons admis que ces deux alinéas posent un certain nombre de problèmes, car ils sont difficiles à mettre en œuvre sur le long terme. En effet, qu'est-ce

qu'une entreprise suisse ? Que fait-on si elle est rachetée par une entreprise étrangère ? Comment garantir qu'un centre de données suisse ou situé en Suisse offre davantage de sécurité qu'un centre de données détenu en Suisse ou même hors de Suisse par une société « non suisse » ?

Le projet de loi 12103 n'a pas osé s'attaquer de front aux GAFAM – et à Google en particulier – et n'a pas osé demander que l'Etat de Genève adopte une forme de « laïcité numérique » car il serait impératif de « sortir les marchands du temple de la connaissance », et pourtant c'est le devoir qui nous incombe aujourd'hui collectivement. Il existe aujourd'hui de très nombreux outils de partage de documents, dans des environnements « libres » et non commerciaux, qui offrent une grande sécurité quant à la protection des données personnelles, et qui remplissent un bon nombre de fonctionnalités « offertes » par la suite Google. Bien sûr, ces outils ne sont peut-être pas aussi performants, et pour cause, que leur concurrent hégémonique ! Mais c'est le devoir des collectivités publiques de les co-développer en mettant à profit l'expérience d'utilisateur des pédagogues, des enseignant.e.s et des élèves. Apprendre à travailler dans un univers numérique libre et ouvert a également une valeur importante dans le monde contemporain, alors qu'il faudra sans cesse s'adapter à des outils numériques mouvants. Savoir les modifier et les actualiser en fonction des questions spécifiques à résoudre fera bien vite partie de la « *littératie numérique* » élémentaire.

Nous demandons donc à la *commission de contrôle de gestion* de s'autosaisir de cet objet pour s'assurer que l'Etat évalue correctement les risques personnels pour les élèves et les risques financiers pour le DIP, si des plaintes de parents aboutissaient à des demandes en réparation pour violation de la sphère privée (de leur enfant ou de la leur *via* l'adresse Google/DIP de leur enfant), s'il s'avérait que malgré les protocoles signés, le système mis en place ait permis le profilage de leur enfant ou d'eux-mêmes à des fins commerciales ou politiques et que des conséquences dommageables en auraient découlé pour leur enfant, alors sous protection de l'école publique.

Plus généralement, la commission de contrôle de gestion pourrait également demander au Conseil d'Etat d'évaluer précisément les risques de l'utilisation des GAFAM, au DIP, mais également dans toute l'administration cantonale.