Secrétariat du Grand Conseil **RD 1073**

Date de dépôt : 23 décembre 2014

Rapport
du Préposé cantonal sur l'administration en ligne (AeL)

ATAR ROTO PRESSE – 300 ex. – 01.15

RAPPORT

REPUBLIQUE ET CANTON DE GENEVE
Préposé cantonal à la protection des données et à la transparence

RAPPORT DU PREPOSE CANTONAL SUR L'AeL

Protection des données et transparence • Rue David-Dufour 5 • 1205 Genève
Tél. +41 (22) 546 52 40 • Fax +41 (22) 546 52 49 • E-mail ppdt@etat.ge.ch • www.ge.ch/ppdt
Accès bus : Tram 14, arrêt Jonction, Bus 2,4,11,19,D, arrêt Jonction

Table des matières

1. LISTE DES PRINCIPAUX ACRONYMES UTILISES

AeL	Administration en ligne (programme d'impulsion)
AFC	Administration fiscale cantonale genevoise
CATFICH	Catalogue des fichiers
CCPDTA	Commission consultative en matière de protection des données, de transparence et d'archives publiques
DEAS	Département de l'emploi, des affaires sociales et de la santé
DF	Département des finances
DGSI	Direction générale des systèmes d'information
LArch	Loi sur les archives publiques du 1er décembre 2000 (RSGe B 2 15)
LIPAD	Loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (RSGe A 2 08)
LPD	Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1)
LTrans	Loi fédérale sur le principe de la transparence dans l'administration du 17 décembre 2004 (RS 152.3)
OCDE	Organisation de coopération et de développement économiques
OCEN	Office cantonal de l'énergie
OCPM	Office cantonal de la population de la migration
PFPDT	Préposé fédéral à la protection des données et à la transparence
PPDT	Préposé cantonal à la protection des données et à la transparence
RDU	Revenu déterminant unifié
RF	Registre foncier
SGPD	Système de gestion de la protection des données
SIPD	Système d'information et de protection des données
SITG	Système d'information du territoire à Genève
TIC	Technologies de l'information et de la communication

2. PREAMBULE

Le programme expérimental Administration en Ligne (AeL), initié mi-2008, s'étend jusqu'à la fin de l'année 2015. Il est prévu par l'art. 69 al. 8 de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (LIPAD; RSGe A 2 08) qu'au plus tard fin 2014, trois rapports évaluant ce projet sous différents angles soient remis au Grand Conseil : un rapport du Conseil d'Etat, un rapport de la commission consultative en matière de protection des données, de transparence et d'archives publiques (CCPDTA) et un rapport du Préposé cantonal à la protection des données et à la transparence (PPDT). Selon les termes de l'art. 69 al. 8 let. b, le PPDT doit rédiger un rapport :

> *évaluant l'impact des prestations en ligne offertes sous l'angle des prescriptions exigées à la présente loi, avec des recommandations quant à l'opportunité de modifier ou non la législation pour permettre d'autoriser de manière durable les éventuelles dérogations expérimentées dans le cadre du programme d'administration en ligne*.

Le présent rapport final fait suite au rapport intermédiaire rédigé par la précédente autorité fin 2013. Pour rappel, il s'était agi alors de s'assurer que la mise en œuvre de l'administration en ligne n'entraînait pas de conséquences majeures quant au respect des règles relatives à la protection des données, auquel cas il aurait en effet fallu en informer le législateur suffisamment tôt. Fort heureusement, tel n'a pas été le cas. Dans le présent rapport soumis à l'attention des députés, le PPDT a souhaité étendre le champ de l'analyse en partant d'une notion élargie de l'administration en ligne, soit non seulement les 10 prestations prioritaires définies par le législateur, mais également trois projets transversaux dont l'examen est utile à l'appréciation juridique de la matière. Il s'agit de :

- La mise en œuvre du revenu déterminant unifié (RDU) par le Département de l'emploi, des affaires sociales et de la santé (DEAS);
- L'introduction d'un outil nommé IncaMail, qui permet d'assurer la preuve de l'envoi, respectivement de la réception d'un message électronique, sous l'égide du Département des finances (DF);
- Les projets dits Passerelle et MPI d'interconnexion de différents fichiers informatisés pour répondre aux besoins de l'Office cantonal de l'énergie (OCEN) et du Registre foncier (RF).

Rapport rédigé par M. Romain RIETHER, titulaire d'un master en management public et M. François METRAL, titulaire d'un MBA et d'un diplôme universitaire en gestion des risques, sous la supervision de M. Stéphane WERLY, Préposé cantonal et de Mme Pascale BYRNE-SUTTON, Préposée adjointe.

3. INTRODUCTION

L'AeL peut être définie comme un processus de développement supporté par les technologies de l'information et des communications afin d'orienter plus efficacement l'action de l'Etat. L'approche vise à mieux répondre aux besoins des citoyens, des entreprises et des membres de la société civile en général grâce à un renforcement de la capacité des services de l'Etat en garantissant :

- L'accès des citoyens et des entreprises aux informations que l'Etat détient sur eux et qui les concernent;
- Le recours généralisé aux technologies de l'information et de la communication (TIC) dans les activités de l'Etat;
- Un renforcement de la démocratie en ligne grâce au développement d'espaces partagés, et
- La prestation électronique de services.

a) L'accès des citoyens et des entreprises aux informations que l'Etat détient sur eux

L'Etat est détenteur d'un certain nombre d'informations concernant les citoyens et les entreprises, informations qui leur appartiennent de fait. Ces derniers doivent donc avoir accès à ces informations, et c'est ce que vise l'AeL par une meilleure transparence.

La mise à disposition du portail AeL aux citoyens et aux entreprises leur permet, après s'être correctement identifiés, d'avoir accès à l'information désirée. Le portail AeL doit également leur permettre de transmettre les informations qui les concernent à qui ils le désirent. Finalement, ils peuvent personnaliser la page d'accueil AeL selon leurs préférences afin d'agir à la fois plus rapidement et de manière mieux éclairée.

Cette approche permet ainsi aux citoyens et aux entreprises de mieux partager les données qui les concernent, d'améliorer la qualité des données gérées par l'Etat, et rendre les différents membres de la société civile plus responsables quant à l'utilisation de ces renseignements. Cela favorise donc l'efficacité des services de l'Etat et une meilleure transparence de l'administration publique.

b) Le recours généralisé aux nouvelles technologies dans les activités de l'Etat

L'Etat est le principal responsable de la qualité de ses prestations. Les technologies de l'information et de la communication doivent de ce fait être exploitées au mieux afin lui permettre de se projeter dans une société du savoir, dans laquelle l'information devient la pierre angulaire d'un bon fonctionnement économique.

En effet, les technologies de l'information et de la communication (TIC) contribuent à transformer les services de l'Etat, en vue de les améliorer (obtenir et échanger efficacement des informations de qualité pour favoriser la prise de meilleures décisions) afin de renforcer des démarches plus cohérentes et avec plus de complémentarité, et amener, de façon générale, à une croissance économique concurrentielle et innovante.

Le gouvernement genevois doit ainsi prioriser la mise en œuvre des TIC dans chacun de ses principaux champs d'intervention par des espaces d'information partagés accessibles aux citoyens et aux entreprises via le portail unique de l'AeL.

c) Un renforcement de la démocratie grâce au développement d'espaces partagés

Le portail AeL est également l'occasion d'améliorer le fonctionnement démocratique de la société et de préserver ses valeurs en donnant un droit de regard sur la destinée de l'Etat aux citoyens et aux entreprises, ce qui est important dans une société où l'Etat doit de plus en plus justifier son existence et les actions qu'elle entreprend. Cette approche permet donc de stimuler la participation à la vie démocratique tout en améliorant la transparence des processus constitutifs et partager le savoir et les connaissances propices à une prise de décision plus judicieuse sur les débats de société.

Les technologies de l'information et de la communication permettent ainsi une meilleure transparence de l'information, en facilitant à la fois l'accès aux documents de l'Etat et en amenant le gouvernement à justifier ses choix et ses décisions devant les citoyens. Ces nouvelles possibilités délivrées doivent être complétées par des moyens de communication traditionnels, afin d'offrir aux citoyens la même chance de s'exprimer et d'accéder à l'information, qu'ils aient accès ou non à l'AeL.

d) La prestation électronique de services

Le portail AeL offre aux citoyens et aux entreprises les moyens techniques pour procéder à leurs transactions avec l'administration cantonale, et bénéficier des principaux programmes et services offerts par l'Etat. Etant de plus en plus exigeants avec l'administration publique, les citoyens et les entreprises peuvent se prévaloir de la majorité des services en ligne, en tout temps, et de manière rapide et efficiente.

Les services offerts doivent correspondre à la logique des citoyens et des entreprises, et non à celle de la structure des différents départements et services de l'Etat, en évitant la navigation à travers le dédale de pages Internet existantes pour trouver les informations dont ils ont besoin. Les services proposés doivent ainsi être regroupés par thèmes spécifiques, en pouvant intégrer, à terme, les autres services offerts par les autres paliers étatiques, à savoir ceux de la Confédération et des municipalités.

L'administration doit également continuer à proposer ses services aux citoyens qui, pour diverses raisons, ne peuvent ou ne veulent pas se prévaloir des services de l'AeL. Pour cela, il existe plusieurs formes : outre les solutions déjà existantes, de nouvelles formes de prestation peuvent se développer. La création de centres multiservices semble être une voie à privilégier, afin de tenir compte des préférences de tous les citoyens tout en maintenant la logique d'un panel de services regroupés.

En conclusion, l'approche AeL assure une satisfaction accrue des citoyens et des entreprises quant aux services délivrés par leur administration publique. Cette approche permet au canton de Genève de mettre en œuvre les moyens d'offrir ses services, accessibles en tout temps et partout, permettant notamment:

- A tous les citoyens, quels qu'ils soient, d'améliorer leur niveau de vie;
- Aux entreprises d'augmenter leur compétitivité grâce à des conditions plus attractives et soutenues par une administration allégée et plus efficace;
- Aux membres de la fonction publique d'évoluer dans un environnement de travail revu et corrigé intégrant des éléments de valeur ajoutée, et
- A l'administration elle-même d'offrir des prestations plus innovantes, plus efficaces tout en réduisant les coûts associés au fonctionnement de ses programmes publics. Ces économies pourront être réinvesties par la suite dans des programmes à valeur ajoutée.

4. LES CONDITIONS NECESSAIRES AU SUCCES DE L'AEL

Pour garantir sa réussite, le projet ne doit pas être abordé uniquement sous l'angle technologique, car il soulève également des enjeux d'ordre politique, économique, social et culturel.

a) La gouvernance AeL

La mise en œuvre du projet AeL requiert une direction forte, caractérisée par une structure de gouvernance capable de promouvoir le projet et de concrétiser la vision et les orientations en la matière. C'est à n'en pas douter l'enjeu essentiel de ce projet dans sa phase de déploiement.

Cette structure de gouvernance doit inclure des mécanismes centralisés :

- De planification stratégique globale;
- De coordination d'ensemble;
- De gestion des risques;

- De suivi et d'évaluation des résultats, et
- De reddition de comptes.

Le suivi et l'évaluation des résultats impliquent forcément l'élaboration et la mise en place de standards et de règles encadrant la mise en œuvre des projets de gouvernement en ligne.

Il est donc nécessaire de nommer une personnalité de haut niveau afin d'assurer la direction de l'AeL et d'en faire une des priorités du gouvernement pour engager tous les intervenants concernés dans un processus de renouvellement, selon une vision d'ensemble. En effet, le projet dépasse de loin la simple prestation de services électroniques, car il vise à l'amélioration du processus démocratique dans son ensemble.

Dans une optique de cohérence générale, il est conseillé de créer un poste de dirigeant AeL, chargé de diriger un secrétariat au déploiement AeL. La responsabilité de ce secrétariat serait de développer des stratégies d'intégration et de superviser la pénétration du projet auprès des citoyens et des entreprises genevois. Ce secrétariat devrait bénéficier d'une forte autonomie afin de garder son objectivité et son indépendance auprès des différents intervenants.

Afin de renforcer la mise en œuvre du projet et d'éviter de gérer les services en silo, il serait recommandé de créer un comité d'action, composé des principaux dirigeants des départements et services concernés par l'AeL. Ce comité aurait comme objectif de relier les différents départements et le secrétariat stratégique pour l'application cohérente des politiques et des orientations stratégiques de la gouvernance AeL.

Afin de refléter la priorité du projet AeL et dans le but d'harmonisation d'ensemble des actions des différents départements, des dispositions devraient être prises pour que les différents dossiers soumis aux débats politiques prennent en considération les implications des mesures proposées sur le projet AeL.

Enfin, pour s'assurer que le projet AeL constitue une priorité au sein même des départements et services, il est recommandé que chaque responsable de départements et services concernés s'engage par une convention de performance et d'imputabilité en regard de la gouvernance AeL. Cette convention devra s'appuyer sur un plan d'action annuel ainsi que d'indicateurs permettant de rendre compte des résultats obtenus. Un rapport de gestion devra être produit à la fin de chaque année sur l'atteinte des résultats et transmis au comité stratégique.

b) Établir un environnement de confiance

Afin de garantir l'adhésion des citoyens et des entreprises au projet AeL, il est indispensable d'instaurer un environnement de confiance et de mettre en œuvre les moyens nécessaires associés au déploiement des prestations AeL. Il s'agit d'une condition *sine qua non* de réussite.

L'environnement de confiance repose tout d'abord sur des fondements juridiques adéquats, sur des mesures de protection des données personnelles efficaces, sur l'assurance de la sécurité des systèmes et sur un processus d'identification sûr.

Les fondements juridiques

En premier lieu, la LIPAD constitue le principal fondement juridique qui facilite le recours aux TIC dans la réalisation des services AeL. En mettant l'accent sur les diverses problématiques et possibilités reliées à ces nouvelles technologies, la LIPAD assure les bases juridiques pour mettre en place l'AeL. Cependant, l'AeL ne saurait être validé sans un examen approfondi du corpus législatif afin de respecter les principes mis en avant dans la LIPAD et de permettre l'adoption de lois à caractère transactionnel.

Dans une seconde étape, l'évolution fulgurante des TIC et leurs retombées en matière de protection des données personnelles pose un défi que l'administration publique doit considérer avec le plus grand sérieux, en examinant en permanence l'impact de ces nouvelles évolutions sur le droit à la vie privée. De ce fait, il est impératif que l'Etat continue à se munir de mécanismes réglementaires et légaux clairement définis et qu'il continue à les consolider pour garantir aux citoyens que les données personnelles utilisées par l'AeL soient protégées contre toute atteinte au droit à la vie privée. Ces mécanismes doivent être définis de manière suffisamment souple pour faire face à l'évolution rapide des TIC.

La LIPAD

Dans le contexte AeL, il y a lieu de se demander si le cadre juridique actuel assurant la protection de la vie privée, et la LIPAD en particulier, doit être repensé afin d'encadrer le flux d'informations requises pour assurer le bon fonctionnement et l'efficacité des services AeL. En effet, les services AeL reposent sur l'utilisation et le partage accrus des données personnelles entre différents intervenants. Ce partage est essentiel afin que l'AeL soit en mesure d'optimiser la qualité de ses services.

Il est d'autant plus judicieux de concevoir un cadre juridique où les données personnelles puissent bénéficier de mesures de protection variables selon la sensibilité de l'information et selon les circonstances. Finalement, le cadre juridique doit encadrer l'utilisation des données personnelles afin qu'elles puissent être exploitées pour des services autres que ceux pour lesquels ils ont été initialement collectés.

c) Renforcement des mécanismes organisationnels et technologiques

L'AeL doit garantir une approche où les TIC et les règles organisationnelles mises en œuvre réduisent au maximum les possibilités de violation du droit à la vie privée.

Il est impératif d'exploiter un outil de validation systématique dans le cadre du développement des services AeL et qu'une évaluation des risques relatifs à la vie privée soient contrôlés efficacement, en créant des règles organisationnelles spécifiques ou en incluant de nouvelles fonctionnalités technologiques. Une grille d'évaluation spécifique doit ainsi être développée. Finalement, il est crucial d'impliquer le plus rapidement possible le Préposé cantonal à la protection des données et à la transparence afin qu'il puisse agir directement et activement dès la conception de tout nouveau service AeL.

De plus, quel que soit la qualité des mesures technologiques mises en œuvre, elles sont assujetties au facteur humain, ce que l'administration publique ne peut totalement contrôler. Il est donc primordial de mettre en place des mesures de formation et de sensibilisation à l'attention du personnel pour que les règles et le cadre de gestion des risques soient compris, assimilés et appliqués conformément à la LIPAD.

L'AeL doit également mettre en place des mécanismes organisationnels, voir juridiques, favorisant l'utilisation de technologies spécifiques à la protection des données personnelles et de la vie privée. Ces technologies doivent posséder certaines caractéristiques pouvant garantir et renforcer la protection des données personnelles en réduisant l'utilisation des données personnelles aux seules situations où cela s'avère nécessaire, et ce, sans diminuer la performance des systèmes informatiques et la gestion de l'AeL. Une campagne de promotion est donc nécessaire à l'utilisation de ces technologies et les recherches favorisant leur développement doivent également être encouragées.

d) Vers une culture de la sécurité

La sécurité informatique est un des moyens pour protéger les données personnelles; il prend une importance marquée dans le contexte AeL. Les pare-feux et les logiciels antivirus, entre autres, prennent une importance considérable dans les architectures informatiques et les infrastructures interconnectées. Les risques informatiques ne sont donc pas à négliger (perte d'informations, rupture de confidentialité, etc.) et peuvent rapidement entraîner un manque de confiance des citoyens envers l'AeL. Des coûts financiers non négligeables pour l'économie peuvent être générés par des incidents informatiques.

Il est par conséquent primordial de développer une culture de la sécurité informatique en sensibilisant les différentes parties prenantes en présence, à tous les niveaux, y compris les usagers des services AeL.

e) Identification AeL

L'identification des utilisateurs est un enjeu majeur impliquant autant des éléments de la vie privée que de la sécurité informatique, dans un contexte AeL offrant de plus en plus de services transactionnels et intégrés. En effet, de par la nature de la connexion de l'usager, les services sont délivrés à distance et sans interaction physique, dans un monde virtuel. Un processus d'identification sûr des utilisateurs est donc essentiel pour s'assurer que la bonne personne ait accès aux bonnes données et que la personne derrière l'ordinateur possède les qualités et les droits requis pour disposer d'une prestation électronique appropriée.

Les mesures de contrôle mises en place ne doivent pas porter atteinte au droit de la vie privée tout en empêchant l'usurpation d'identité. L'objectif de ce contrôle est de permettre de déployer un mécanisme permettant l'accès d'un service AeL à un autre, offrant un niveau de certitude acceptable et pouvant évoluer vers des niveaux de certitude élevés.

Cependant, le système mis en œuvre actuellement n'élimine pas totalement les risques encourus liés à la protection des données personnelles. Ces risques peuvent être en partie maîtrisés par l'adoption de mesures organisationnelles additionnelles ou en revoyant la conception du système en vue d'y ajouter des mesures technologiques spécifiques pour améliorer la protection de la vie privée.

f) Simplifier l'accès aux prestations électroniques de l'AeL

Le projet AeL vise à améliorer les prestations de l'Etat aux citoyens et aux entreprises selon une approche simplifiée.

La démocratisation de l'accès à l'AeL

Il est primordial de ne pas réserver l'accès aux nouveaux services regroupés qu'aux personnes disposant d'Internet. C'est pourquoi il est nécessaire de développer, en parallèle au portail AeL, des centres multiservices gouvernementaux permettant l'accès à l'ensemble des services offerts par l'AeL tant par la voie téléphonique que par des offices au guichet. Les fonctionnaires travaillant dans ces centres verront leur rôle enrichi grâce à un travail décloisonné, car ils pourront répondre à des questions et des demandes d'ordre général, dépassant le cadre strict d'un département ou d'un service.

Cette option offerte ne doit en aucun cas perturber la pénétration du portail AeL auprès des usagers. Il est de la responsabilité de l'Etat de combattre la fracture numérique existant entre les individus familiers avec Internet et ceux qui ne le sont pas, en favorisant l'accès à Internet à des coûts modérés et en soutenant les citoyens peu familiers avec les TIC, afin de leur permettre d'acquérir les compétences requises, l'accès à l'information étant considéré comme un droit, au même titre que les autres droits démocratiques.

Prise en compte des personnes souffrant de limitations motrices, sensorielles ou cognitives

Le projet AeL ne doit pas exclure les personnes souffrant de handicaps, d'autant plus qu'elles peuvent trouver en Internet une source d'information des plus riches, de même qu'un moyen de communication avec des personnes vivant des situations semblables, et ainsi accéder à des possibilités jusque-là inconcevables. Le recours aux sigles et aux images, pour expliciter les démarches par exemple, améliorerait la convivialité des pages Internet. Le langage utilisé doit également être compréhensible par le plus grand nombre. Finalement, l'AeL doit proposer des mesures nécessaires pour garantir une communication rapide, voire instantanée, propre à toute démarche sur Internet.

g) Informer et sensibiliser les usagers aux nouveaux modes de relations avec l'État

Dans le cas où les services AeL ne s'étendent pas, l'argent des contribuables portant sur le développement du projet AeL aura été investi en pure perte. La gouvernance AeL doit donc assurer une communication adéquate auprès des citoyens et des entreprises afin de les informer et de les sensibiliser aux nouvelles techniques AeL. L'Etat doit démontrer les avantages de recourir à une telle solution et les gains réels obtenus. Cette communication doit faire l'objet d'une campagne de grande ampleur. Les départements et services doivent également publier des contenus utiles sur le portail AeL.

h) L'adhésion des collaborateurs de l'administration

Le déploiement AeL crée une occasion unique de valoriser significativement le rôle des collaborateurs de la fonction publique, en leur confiant des tâches à valeur ajoutée faisant davantage appel à leur jugement et à leur capacité de vulgarisation et de formation. Les collaborateurs doivent ressentir le projet AeL comme une opportunité, et non comme une contrainte. Ils doivent donc être intégrés aux changements qui en découlent. Des programmes de formation doivent être développés pour accompagner les collaborateurs tant sur le décloisonnement de leur rôle que sur les innovations technologiques qui leur sont proposées. Une attention toute particulière doit être portée sur les mécanismes de protection des données personnelles.

5. LES PRINCIPES FONDATEURS DE LA PROTECTION DES DONNEES PERSONNELLES

Pour mener à bien cette réflexion, il est bon de rappeler les lignes directrices établies par l'Organisation de coopération et de développement économiques (OCDE) régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel.

Principe de la limitation en matière de collecte : Il conviendrait d'assigner des limites à la collecte des données à caractère personnel; toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Principe de la qualité des données : Les données à caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

Principe de la spécification des finalités : Les finalités en vue desquelles les données à caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

Principe de la limitation de l'utilisation : Les données à caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au principe de spécification des finalités précédemment évoqué, si ce n'est :

- Avec le consentement de la personne concernée; ou
- Lorsqu'une règle de droit le permet.

Principe des garanties de sécurité : Il conviendrait de protéger les données à caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation ou divulgation non autorisés.

Principe de la transparence : Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données à caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données à caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

Principe de la participation individuelle : Toute personne physique devrait avoir le droit :

- D'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;
- De se faire communiquer les données la concernant dans un délai raisonnable, moyennant éventuellement une redevance modérée, selon des modalités raisonnables et sous une forme qui lui soit aisément intelligible;
- D'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet; et

- De contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Principe de la responsabilité : Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

6. LA COMPOSANTE SECURITE

Dans le contexte de la virtualisation des processus et de la mise en place de l'AeL en particulier, la composante sécurité prend une place importante. L'usage intensif des TIC a amené toute une série de risques nouveaux, en raison par exemple du développement de la cybercriminalité et du développement d'architectures et d'infrastructures informatiques toujours plus complexes. Cette réalité doit être assimilée par l'ensemble des intervenants.

Pour rappel, on peut citer les lignes directrices pour la sécurité des systèmes et des réseaux d'information établies par l'OCDE :

Sensibilisation : Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

Responsabilité : Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

Réaction : Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir et détecter les incidents de sécurité et y répondre.

Éthique : Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

Démocratie : La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

Évaluation des risques : Les parties prenantes doivent procéder à des évaluations de risques.

Conception et mise en œuvre de la sécurité : Les parties prenantes doivent intégrer la sécurité en tant qu'élément essentiel des systèmes et réseaux d'information.

Gestion de la sécurité : Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

Réévaluation : Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

L'application de ces principes directeurs dans le cadre de l'AeL est primordiale pour établir et maintenir la confiance des citoyens et des entreprises et leur adhésion aux nouvelles technologies. Ces principes directeurs permettent également de satisfaire les finalités sécuritaires recherchées dans les systèmes d'information :

Confidentialité : Propriété des données ou des informations, comme les renseignements personnels, qui ne sont accessibles qu'aux personnes autorisées.

Intégrité des informations et des systèmes et processus : L'intégrité d'une information est la propriété de ne pas être altérée ou détruite de manière non autorisée, volontairement ou accidentellement.

L'intégrité d'un système ou d'un processus est la propriété de réaliser la fonction désirée de façon complète et selon les attentes, sans être altérée par une intervention non autorisée, volontaire ou accidentelle.

Disponibilité : Propriété d'une information ou d'un système informatique d'être accessible ou disponible en tout temps ou en temps voulu.

Authenticité : Propriété d'une entité d'être bien celle qu'elle prétend être.

L'authenticité s'applique tant aux personnes (utilisateurs) qu'à n'importe quelle autre entité (application, processus, système, etc.). Elle implique une identification, c'est-à-dire la reconnaissance d'une dénomination permettant de désigner l'entité sans équivoque.

Imputabilité : Propriété qui garantit que les actions d'une entité sont tracées et attribuées à cette seule entité.

L'imputabilité assure de pouvoir identifier, pour toutes les actions accomplies, les personnes, les systèmes ou les processus qui les ont initiées (identification) et de garder trace de l'auteur et de l'action (traçabilité).

Irrévocabilité : Propriété d'une information, d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

L'authenticité, l'imputabilité et l'irrévocabilité présentent des défis majeurs dans le cadre de prestations électroniques, où les transactions vont de plus en plus se réaliser dans un espace virtuel dans lequel les contacts physiques sont éliminés. L'Etat doit de ce fait renforcer les

mécanismes permettant d'assurer que ces finalités sont atteintes, pour garantir le bon fonctionnement de l'AeL.

L'Etat se doit de renforcer le domaine sécuritaire de l'information et de la communication via une cellule spécialisée en matière de conseils, d'expertises et de meilleures pratiques dans le domaine de la sécurité de l'information numérique. Cette cellule a pour mission de promouvoir les actions visant à assurer la sécurité de l'information numérique, dans le cadre de l'AeL et des autres prestations électroniques de l'Etat. Son champ d'action porte sur :

- La prévention et la sensibilisation;
- La détection et la réaction en situation de crise;
- La veille et la recherche, ainsi que
- Le soutien aux équipes opérantes.

La sécurité informatique ne garantit toutefois pas à elle seule une protection appropriée des données personnelles et la protection du droit à la vie privée. Le principe de sécurité est nécessaire, mais non suffisant. Il est primordial de considérer également la protection des données personnelles lors de la définition des besoins en architectures informatiques et l'élaboration des infrastructures informatiques.

7. PROTECTION DES DONNEES PERSONNELLES ET TRANSPARENCE

D'une part, il paraît judicieux de s'interroger sur la pertinence du cadre juridique actuel dans l'optique de la protection des données personnelles. En effet, la modernisation apportée par l'approche AeL offre les fondements permettant un meilleur fonctionnement et une plus grande efficacité des services de l'Etat. Elle remet en cause les exigences définies au préalable avant l'apparition de l'AeL, comme par exemple la logique basée sur l'utilisation du papier. Il faut donc vérifier si ces exigences sont toujours d'actualité dans le cadre des nouveaux processus administratifs.

D'autre part, l'adhésion des usagers repose en grande partie sur la présence d'un environnement de confiance associé au déploiement de l'AeL. L'Etat se doit non seulement d'établir cet environnement de confiance, mais aussi de mettre en œuvre les moyens nécessaires pour le maintenir. Il s'agit d'une condition *sine qua non* pour que les citoyens et les entreprises aient recours aux prestations en ligne. Les facteurs influençant cette confiance sont multiples. Néanmoins, on peut relever deux composants essentiels :

- La présence de mécanismes de protection des données personnelles appropriés à la nature du service accédé;

- La présence de mécanismes sûrs et sécuritaires pour empêcher l'interférence d'un tiers dans le processus.

Ces deux éléments doivent être soutenus par un cadre organisationnel, technologique et juridique procurant l'assurance que l'information traitée n'est utilisée et accédée que pour des motifs justifiés, tout en considérant les réalités propres au monde virtuel et la connexion informatique de l'Etat avec son environnement.

Le principe de neutralité technologique : Le principe de neutralité technologique souligne que l'expression d'une norme ne doit pas présupposer de support particulier, que cela soit sous forme papier ou électronique. Or plusieurs éléments dans la législation actuelle ne répondent pas à ce principe.

La législation doit par exemple être précisée quant au droit relatif aux documents :

- Etablissement des documents sur divers supports;
- Transfert de l'information d'un document d'un support à un autre;
- Intégrité des documents électroniques et garantie de leur préservation;
- Identification et authentification des documents électroniques, et
- Certification.

On peut également citer :

- Les dispositions prévoyant des plages horaires précises pour la consultation de documents (consultation d'un registre durant les heures "normales" de bureau….), dispositions remises en cause par la possibilité de consulter des documents en ligne;
- Les dispositions portant sur la référence à des documents annexés ou joints exigeant une certaine concomitance ou simultanéité de l'envoi. La législation doit permettre une mixité des formats de documents joints (papier et/ou électronique) lors d'une formalité;
- Les dispositions requérant le recours à un support technologique spécifique pour transmettre ou recevoir des documents.

Le principe de neutralité technologique doit permettre aux citoyens de s'exprimer sur leurs choix et préférences au moment de la transaction, ce qui garantit une sécurité accrue, puisque l'interchangeabilité permet de recourir à la forme de document papier, en cas de défaillance technologique par exemple.

Il est essentiel de revisiter l'ensemble du corpus législatif pour prendre position sur les dispositions législatives qui ne sont pas neutres sur le plan technologique, pour les conserver, les supprimer ou les modifier sur les principes de neutralité technologique, médiatique, juridique ou d'équivalence fonctionnelle.

La notion de prestation électronique

L'ensemble du corpus législatif doit être révisé afin de prendre en considération les réalités propres au monde virtuel de l'AeL, en considérant les points suivants :

- Les différentes exigences de la signature et des signatures multiples;
- Les modalités de paiement (lorsque le paiement de la carte de crédit n'est pas une option);
- La capacité des personnes physiques ou morales;
- Les documents à fournir;
- Le nombre d'exemplaires à transmettre;
- Le support, la disposition et la forme de la demande;
- La concordance des exigences;
- L'exigence de l'apposition d'un sceau;
- Le mode de transmission de la demande.

a) Niveaux de sensibilité variables des renseignements personnels

Il est primordial de concevoir un cadre juridique où les données personnelles peuvent bénéficier de mesures de protection variables, selon leur sensibilité. Cette sensibilité peut être amenée à évoluer tout au long du cycle de vie de la personne concernée et des circonstances en présence.

Même si toutes les informations relatives à une personne ont un statut semblable, elles ne présentent pas toutes les mêmes risques et enjeux. Par exemple, suivant les circonstances, l'adresse d'une personne spécifique peut comporter des risques pour cette personne et il faut en assurer la protection, alors qu'en général les adresses sont publiées dans des répertoires publics. Les niveaux de sensibilité des informations personnelles sont également fonction du contexte légal dans lequel elles sont exploitées.

Le niveau de sensibilité doit être défini avec le consentement du citoyen, lorsque cela est possible. Dans les autres cas, des mécanismes institutionnels doivent être prévus.

b) Technologies concernant la protection des données personnelles

L'Etat doit également mettre en œuvre des mécanismes institutionnels, voire juridiques, qui puissent favoriser l'utilisation des technologies spécifiques à la protection des données personnelles et du droit à la vie privée et, dans la mesure du possible, favoriser le développement et l'amélioration de la protection des données personnelles.

Dans le contexte AeL, les technologies utilisées semblent posséder certaines caractéristiques pouvant non seulement garantir, mais également renforcer la protection des données personnelles. Elles permettent de réduire l'utilisation des données personnelles aux seules situations où cela s'avère une nécessité, et ce sans diminuer la performance d'ensemble des systèmes informatiques ni la gestion des prestations électroniques.

c) Grille d'évaluation des risques relatifs à la protection des données personnelles

Pour juger de la bonne conformité des mécanismes de protection des données personnelles, il serait pertinent de développer une grille d'évaluation des risques relatifs à la protection de ces données.

Cette évaluation est nécessaire afin de contrôler le niveau de sensibilité des données personnelles à travers les différentes banques de données de l'Etat et de déployer les systèmes informatiques selon ce principe. Les départements et services de l'Etat doivent réaliser ces évaluations, celles-ci devant être rendues publiques selon le principe de transparence.

Cette transparence est un garant essentiel de la confiance de la population, qui doit avoir la possibilité d'en débattre, le cas échéant. L'Etat doit démontrer que les systèmes informatiques utilisés garantissent le droit à la vie privée. Une évaluation insatisfaisante aurait ainsi pour effet d'obliger les responsables à corriger la situation ou à l'améliorer en conséquence.

Le Préposé cantonal à la protection des données et à la transparence aurait une mission de conseil et de soutien auprès des départements et services de l'Etat dans la réalisation des évaluations des risques et la mise en œuvre des moyens pratiques de protection. Il pourrait aussi avoir mandat d'effectuer une vérification de la conformité du processus d'évaluation des risques, selon les critères établis. La responsabilité de la vérification et du contrôle des systèmes d'information doit néanmoins revenir aux responsables opérationnels des départements et services.

La publication de règles claires et l'association du Préposé cantonal à la protection des données et à la transparence permettront de faciliter la tâche de ceux qui ont à développer les systèmes protégeant les données personnelles et la vie privée. Des voies formelles doivent

être établies pour solidifier ces mécanismes organisationnels, dès la conception de tout nouveau projet, et pour faciliter les échanges entre les parties prenantes. Le recours à des experts ou à des informaticiens sur les risques éventuels liés à la protection des données personnelles et de la vie privée sera de plus en plus nécessaire en raison du développement rapide des TIC et de leur impact sur les données.

Il est important d'assurer la gestion et les règles administratives qui orientent forcément les comportements et les décisions encadrant les systèmes informatiques. Les programmes de sensibilisation et de formation jouent alors un rôle important pour le respect du cadre juridique, des règles organisationnelles et le renforcement de la culture sécuritaire des différents départements et services de l'Etat afin que ces règles soient comprises, assimilées et appliquées conformément au corpus juridique.

d) Principe de finalité

Selon le principe de finalité, une donnée ne peut être utilisée que pour les fins pour lesquelles elle a été collectée et non pour d'autres fins. Or, pour éviter des pertes de temps liées aux collectes d'information multiples, les départements et services de l'Etat doivent pouvoir offrir des services en ligne à valeur ajoutée non prévus initialement par leur loi constituante. Dans de tels cas, le principe de finalité n'est pas respecté. Le cadre juridique doit pouvoir statuer sur ce type de possibilités.

Afin de permettre cette situation, il semble judicieux de demander le consentement de l'usager. Ainsi, lorsque les citoyens et les entreprises échangent des données personnelles avec l'Etat, ils pourraient se déterminer afin d'autoriser le département ou service responsable de la collecte de l'information à transmettre l'information à d'autres départements ou services de l'Etat, afin que ceux-ci puissent leur offrir ces nouveaux services à valeur ajoutée.

La mise en place de tels mécanismes permettrait de respecter les principes de protection des données personnelles, et également de tirer profit des possibilités offertes par les TIC afin d'améliorer les services aux citoyens et aux entreprises.

e) L'architecture du système d'informations

L'Etat doit redéfinir un cadre juridique innovateur protégeant mieux ce qui relève de la vie privée sans pour autant empêcher la circulation des renseignements nécessaires au déroulement normal du fonctionnement de l'Etat. Il semble pertinent de promouvoir un échange structuré de données personnelles entre une pluralité de départements et services de l'Etat, tout en assurant une protection optimale de ces informations tout au long de leur transmission, de leur utilisation et de leur conservation.

Le régime actuel des processus de l'Etat duplique ou copie les données personnelles échangées entre les différentes banques de données des départements et services concernés. La duplication de ces données personnelles est nuisible à la qualité même de ces données et augmente le risque de violation de la vie privée. Le régime actuel pourrait être amélioré grâce à un certain nombre d'actions, comme par exemple la réduction du nombre d'endroits où sont conservées les données personnelles. Les départements ou services requérant ces données dans le cadre de l'application de leurs activités pourraient y accéder, sans pour autant les conserver.

Le département ou service devenant ainsi détenteur d'une donnée personnelle serait alors responsable de son utilisation et du respect des critères de confidentialité associés. Le but n'est pas de construire une banque de données centralisée où toutes les données personnelles seraient regroupées, mais, au contraire, de minimiser la duplication de ces données, de limiter leurs collectes excessives, en donnant des droits d'accès justifiés par un cadre réglementaire entre les départements et services concernés.

Ainsi, les données personnelles seraient conservées uniquement là où elles devraient, c'est à dire dans une banque de données, sous la responsabilité d'un département ou service, et non dupliquées ou échangées librement entre les différents départements ou services. Les données personnelles seraient communiquées ou rendues accessibles aux autres départements ou services lorsque cela est permis par la loi. La gestion de l'accès à ces données personnelles serait strictement contrôlée à l'intérieur d'un cadre réglementaire bien défini.

Pour consolider ces fondements légaux et organisationnels, les technologies modernes de cryptologie peuvent offrir des outils grâce auxquels les données personnelles sont échangées de manière sécuritaire, conformément aux règles de protection des données personnelles et de la vie privée.

8. CONTEXTE JURIDIQUE GENEVOIS LIE A LA PROTECTION DES DONNEES PERSONNELLES DANS LE CADRE DE L'AEL

L'AeL a été initiée par la loi 10177[1] votée par le Grand Conseil le 26 juin 2008. Afin de financer le projet, un crédit d'investissement de 26'350'000 F a été voté. Il faisait suite à la loi 8593[2]

[1] Loi ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne, Genève, 26 juin 2008 (http://www.ge.ch/grandconseil/data/loisvotee/L10177.pdf).

[2] Loi ouvrant un crédit d'investissement de 600 000 F pour le projet "Cyber administration – élaboration d'un concept global de l'Etat de Genève", Genève, 14 juin 2002 (http://www.ge.ch/grandconseil/data/loisvotee/L08593.pdf).

adoptée par le Grand Conseil le 14 juin 2002 qui avait ouvert un crédit d'investissement de 600'000 F afin de financer l'élaboration d'un concept global d'administration en ligne pour l'Etat de Genève.

Suite au lancement de l'AeL, la LIPAD a été modifiée par l'adoption, le 24 septembre 2010, de l'art. 69 "Disposition expérimentale relative à l'administration en ligne". Cet article permet à l'AeL de déroger exceptionnellement aux art. 35 à 41 LIPAD, soit les principes régissant le traitement des données personnelles. Conformément aux buts énoncés à l'art. 69 al. 5 LIPAD, cette disposition expérimentale devait permettre d'éviter d'éventuelles entraves au lancement de l'AeL et de déterminer les limites découlant des contraintes techniques et opérationnelles de l'administration. Comme mentionné à l'art. 69 al. 7 LIPAD, les effets de ces dérogations prendront fin le 31 décembre 2015. A ce titre, le rapport intermédiaire du PPDT transmis au Grand Conseil fin 2013 relevait que l'AeL n'avait pas eu besoin de recourir aux dérogations prévues par l'art. 69 LIPAD. En conséquence, dans sa forme actuelle, l'AeL n'exige l'ajout d'aucune dérogation particulière.

8.1 Rappel du droit supérieur

La Suisse fait partie depuis 1963 des Etats membres du Conseil de l'Europe. Cette organisation internationale a pour objectif la promotion de l'Etat de droit, de la démocratie et des droits de l'homme. Sous son égide, nombre d'instruments internationaux d'importance ont été adoptés, comme la Convention européenne des droits de l'homme du 4 novembre 1950 (CEDH; RS 0.101).

Dans ce cadre, la Convention 108 ou "Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel" a été signée à Strasbourg le 28 janvier 1981.

Cet instrument a été le premier - et reste le seul à ce jour - à prévoir des normes internationales juridiquement contraignantes spécifiquement relatives à la protection des données personnelles.

L'Assemblée fédérale a approuvé la ratification de la Convention 108 le 5 juin 1997. Ce texte est entré en vigueur pour la Suisse le 1er février 1998. Il découle de cet instrument l'obligation pour les parties de concrétiser les principes de base contenus dans cette convention dans leur droit interne. Cela se traduit, au niveau fédéral, par la loi fédérale sur la protection des données du 19 juin 1992 (LPD; RS 235.1) ainsi que par la loi fédérale sur le principe de la transparence dans l'administration du 17 décembre 2004 (LTrans; RS 152.3). Sur le plan genevois, cela se concrétise par la LIPAD.

8.2 Notions-clefs

Données à caractère personnel : Il convient de comprendre par données à caractère personnel toute information concernant une personne physique identifiable à partir de ces informations. Par identifiable, il faut entendre le cas de figure où, sans fournir un investissement en temps et en efforts déraisonnables, il serait possible de trouver d'autres informations permettant d'identifier la personne concernée[3]. Dans le cas où la personne n'est pas identifiable, les données sont dites anonymes. Il n'est en effet pas question de données personnelles dans cette hypothèse et les normes de protection ne sont donc pas applicables.

Exemples de données à caractère personnel permettant d'identifier une personne physique : nom et prénom d'un habitant à l'échelle du canton.

Exemple de donnée à caractère personnel ne permettant pas d'identifier une personne physique : prénom d'un habitant à l'échelle du canton.

Données à caractère sensible : Il convient de comprendre par données à caractère sensible, selon l'art. 4 let. b LIPAD et l'art. 6 Convention 108, des données à caractère personnel qui contiennent alternativement à propos d'une personne :

- Les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles;
- La santé, la sphère intime ou l'appartenance ethnique;
- Des mesures d'aide sociale;
- Des poursuites ou des sanctions pénales ou administratives.

Maître de fichier : Défini à l'art. 2 let. d de la Convention 108, le maître de fichier désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du traitement des données à caractère personnel, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées.

Dans une situation où il est difficile d'identifier le responsable du traitement, notamment dans un cas de traitement prétendument illicite, c'est l'entité responsable du traitement de fait qui est considérée comme maître du fichier[4].

---

[3] WALTER Jean-Philippe, La protection des données dans les activités statistiques à la lumière de la recommandation du Conseil de l'Europe n° R (97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins de statistiques, IAOS Statistics, Development and Human Rights, 2000, p. 7 (http://www.portal-stat.admin.ch/iaos2000/walter_final_paper.doc); The European Union Agency for Fundamental Rights, Manuel de droit européen en matière de protection des données, Office des publications de l'Union européenne, Luxembourg, 2014, p. 38.

[4] Voir groupe de travail Article 29, Avis 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant", WP 169, Bruxelles, 16 février 2010, p. 15.

9. PRINCIPES GENERAUX RELATIFS A LA PROTECTION DES DONNEES

Le chapitre II de la Convention 108 énonce les principes généraux minimaux à respecter en matière de protection des données. Ce texte est concrétisé au niveau genevois par la LIPAD qui les reformule aux art. 35 à 40. La loi ne présentant pas lesdits concepts de manière analogue à la convention, un effort de transcription a été réalisé dans le présent rapport afin de les identifier au sein des articles de la LIPAD. Par souci de clarté, le PPDT a également souhaité les définir de manière claire et illustrer certains concepts par des exemples concrets.

L'exigence d'une base légale (art. 35 LIPAD et art. 5 let. a et b Convention 108)
Le principe de légalité restreint le traitement de données à celles, seules, nécessaires dans l'accomplissement de la tâche légale de l'organisme qui les manipule.

Le traitement de données à caractère sensible n'est autorisé que si une loi définit clairement la tâche en question et qu'il est absolument nécessaire, pour la mener à bien, de traiter ces données[5]. Dans le cas où ces données à caractère sensible ne forment pas le cœur même de la tâche de cet organisme mais lui sont nécessaires, alors elles ne peuvent être collectées qu'avec le consentement explicite, libre et éclairé de la personne concernée.

Les données sont pertinentes et nécessaires (art. 36 al. 1 let. a LIPAD et art. 5 let. c Convention 108)
Le principe de proportionnalité, qui comprend la pertinence et la nécessité, implique de s'interroger sur l'importance des données collectées au regard de la tâche à accomplir. Il convient de ne pas collecter plus d'informations que nécessaire.

Exemple d'un cas hypothétique de violation du principe de la proportionnalité : *une collectivité met en place un système de carte magnétique qui permet aux utilisateurs des transports en commun d'acquérir leur ticket de voyage grâce à elle. Les nom et prénom du possesseur de la carte sont enregistrés sous forme électronique dans la puce qu'elle contient.*

A chaque fois que l'utilisateur souhaite faire usage d'un transport public, il doit passer la carte sur une borne magnétique où les données sont lues par l'appareil. Elles font alors l'objet d'une vérification électronique dans la base de données contenant le nom de toutes les personnes ayant acheté la carte de voyage. Ce faisant, cette opération enregistre l'identité de l'usager et l'heure à laquelle il se déplace.

Ce système ne répond pas au critère de la pertinence : il serait possible de vérifier si une personne est autorisée à utiliser des infrastructures de transport sans comparer les données à caractère personnel de la puce de la carte avec celles de la base de données. Un système de

[5] Voir également CourEDH, Rotaru c. Roumanie [GC], n° 28341/95, 4 avril 2000.

code-barres permettrait d'arriver au même résultat, soit la validation ou non de l'utilisation de la carte, sans enregistrer l'heure à laquelle une personne déterminée se déplace[6].

Les données sont exactes et mises à jour (art. 36 al. 1 let. b LIPAD et art. 5 let. d Convention 108)

Le principe de l'exactitude impose à celui qui souhaite faire usage de données à caractère personnel de s'assurer avec un degré de certitude raisonnable que les données sont exactes et à jour. Il convient de mettre en lien le degré de certitude désiré avec l'utilisation qui sera faite des données.

Exemple de situation où il est nécessaire de s'assurer que les données sont à jour : *lorsqu'une personne souhaite conclure avec un établissement bancaire, ce dernier vérifie généralement la solvabilité du client potentiel. Pour ce faire, il existe des bases de données spéciales qui contiennent des données sur les antécédents de crédit de particuliers. Si ces données ne sont pas à jour et se rapportent à une situation aussi dépassée que défavorable, la personne risque de rencontrer de grandes difficultés à obtenir un prêt*[7].

Les données sont sécurisées (art. 37 LIPAD et art. 7 Convention 108)

Le principe de sécurité exige non seulement que les données personnelles doivent être protégées contre tout traitement illicite et être tenues confidentielles, mais également que l'organisme en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou altérées par mégarde. L'art. 14 des lignes directrices adoptées par l'OCDE concernant la protection de la vie privée et les flux transfrontières de données à caractère personnel établit à ce propos que : "*un maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus*"[8].

Les données sont collectées de manière reconnaissable (art. 38 LIPAD et art. 5 let. a et b Convention 108)

Composée des principes de la transparence, de la finalité et de la bonne foi, la collecte des données personnelles implique, pour être reconnaissable, que les personnes sur lesquelles des données à caractère personnel ou sensibles sont collectées soient informées au minimum de :

- L'existence du prélèvement;
- Son but;
- L'organisme qui en a la charge.

---

[6] The European Union Agency for Fundamental Rights, Manuel de droit européen en matière de protection des données, Office des publications de l'Union européenne, Luxembourg, 2014, pp. 77-78.

[7] *Ibid.*, p. 79.

[8] OCDE, Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel du 23 septembre 1980, amendée le 11 juillet 2013 (http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=fr&Book=False).

Font exception à ce principe les enquêtes fondées sur une base légale dont la mention aux personnes concernées pourrait compromettre l'engagement, le déroulement ou l'aboutissement de l'enquête. Par exemple une enquête portant sur une éventuelle obtention indue de prestations sociale.

Transmission de données à caractère personnel ou sensibles
La nécessité d'indiquer le but de la collecte implique que le maître de fichier ne peut, à sa guise, transmettre les données personnelles à d'autres entités intéressées. L'art. 39 LIPAD encadre la transmission en posant comme conditions que :

- L'entité requérante démontre que le traitement des données personnelles satisfera aux principes de la LIPAD;
- Aucune loi ou règlement ne s'oppose à la transmission de ces données personnelles.

Ainsi, la transmission ne permet pas de contourner le cadre légal. La nécessité de respecter les principes contenus dans la LIPAD implique donc que le besoin exprimé par l'entité requérante se déduise de sa tâche légale et que la transmission porte sur des données pertinentes et nécessaires. Il en découle que si l'entité requérante ne s'intéresse qu'au nom et à l'adresse de propriétaires d'immeubles, seules ces données doivent lui être transmises et non pas des informations supplémentaires. Il s'agira donc, pour le maître de fichier, d'extraire les seules données requises et non d'effectuer un transfert "en bloc".

De manière générale, rien ne s'oppose à la transmission lorsqu'il s'agit d'informations aisément accessibles et qu'il serait possible pour la demanderesse de se les procurer elle-même. Entrent également dans ce cas de figure les situations où la loi prévoit un devoir d'entraide ou lorsque l'entraide est nécessaire au bon fonctionnement de l'autorité et que cette dernière pourrait obtenir elle-même les informations en cause. Toutefois, la non-communication est la règle si le secret a été garanti ou si la transmission sert à détourner le but dans lequel ces informations ont été récoltées[9].

Destruction/anonymisation/archivage des données à caractère personnel (art. 40 LIPAD et art. 5 let. e et art. 9 al. 3 Convention 108) :
En lien avec les principes de la proportionnalité et de la finalité, les données à caractère personnel ne doivent pas être conservées sous une forme permettant l'identification de la personne pour une durée supérieure à ce qu'exige la finalité de la collecte.

[9] TANQUEREL Thierry, Manuel de droit administratif, Genève, Zurich, Bâle, 2011, pp. 224-225.

Les données ne portant manifestement pas atteinte à la vie des personnes concernées et conservées à des fins historiques, statistiques ou scientifiques sont exemptées de ce principe[10].

10. DEROGATIONS APPORTEES PAR L'ART. 69 LIPAD POUR LES 10 PRESTATIONS D'IMPULSION PRIORITAIRES DE L'AEL

Adopté par le Grand Conseil le 24 septembre 2010, l'art. 69 LIPAD autorise le fait de déroger aux principes régissant le traitement des données personnelles, exception faite de la sécurité, dans le cadre de l'AeL. Il est ainsi rédigé :

Art. 69 Disposition expérimentale relative à l'administration en ligne

Dérogations

[1] Les institutions publiques sont autorisées à déroger à titre exceptionnel aux articles 35, 36, 38, 39, 40 et 41, dans les limites des alinéas 2 et 3 et dans la mesure nécessaire à la mise en œuvre, à l'exploitation et au développement des 10 prestations d'impulsion prioritaires du programme d'administration en ligne ayant fait l'objet de la loi ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne, du 26 juin 2008.

Sont donc touchés les principes de la légalité, de la proportionnalité, de l'exactitude, de la transparence, de la finalité et de la bonne foi.

Cette dérogation ne constituait pas un blanc-seing et devait n'être utilisé qu'en cas de nécessité[11]. L'importance des dérogations découlait du fait qu'il n'était alors pas possible de déterminer précisément desquelles aurait besoin l'AeL. Dès lors, quelles sont les limites au fonctionnement de l'AeL? Quelle capacité de l'administration à l'adopter? Vu l'importance de ce projet pour l'Etat de Genève, il convenait d'éviter de lui poser des obstacles.

Toutefois, alors que la période d'expérimentation touche à sa fin, il convient de tirer les enseignements de ce projet afin de déterminer si le passage à la téléprocédure doit impliquer une réduction de la protection des données personnelles des citoyennes et des citoyens ou s'il est possible de développer cette voie dans le respect des engagements internationaux de la Suisse.

[10] A ce titre, voir la loi sur les archives publiques du 1er décembre 2000 (LArch; RSGe B 2 15).

[11] Ce principe a été souligné par le PPDT, sous son ancienne autorité, dans sa prise de position du 28 octobre 2011, Mise en œuvre de l'art. 69 LIPAD selon le PPDT dans le cadre de l'Administration en ligne (http://www.ge.ch/ppdt/doc/documentations/PPDT_Prise_de_position_2011_I_013_Art_69_LIPAD_mise_en_oeuvre_selon_PPDT_V.pdf, consulté le 27 novembre 2014).

Concernant les besoins concrets des 10 prestations d'impulsion prioritaires de l'AeL, le PPDT renvoie au rapport intermédiaire établi par la précédente autorité fin 2013 (cf annexe).

11. RAPPEL DES CONCLUSIONS DU RAPPORT INTERMEDIAIRE : MISE EN PERSPECTIVE

Conscient de l'ampleur des tâches effectuées dans le cadre de l'AeL et des enjeux en présence, le PPDT, sous son ancienne autorité, avait réalisé une évaluation de ce projet, fin 2013, sous l'angle de la LIPAD. L'objectif était d'identifier au plus tôt d'éventuelles violations de la LIPAD et de formuler des recommandations réalistes et réalisables afin de permettre la poursuite - si telle est la volonté du législateur - du développement des prestations en ligne au service des citoyennes et des citoyens, dans le respect des règles de protection des données personnelles et de transparence.

Les recommandations étaient les suivantes :

1. Mettre en place un système de gestion "protection des données" (SGPD), sur le modèle du Préposé fédéral à la protection des données et à la transparence (PFPDT), piloté par la Direction générale des systèmes d'information (DGSI).
2. Ancrer l'administration en ligne dans la législation genevoise, par exemple par le biais d'un projet de loi sur l'administration en ligne.
3. Évaluer la conformité, sous l'angle de la protection des données, des systèmes d'information du canton concernés par les prestations en ligne - en particulier le système d'information de l'Office cantonal de la population -, définir un calendrier de mise en conformité; à défaut les remplacer par un système d'information respectueux de la protection des données dès la conception (*privacy by design*); à défaut supprimer les prestations en ligne qui en dépendent.

La troisième recommandation renvoyait indirectement à la première dont l'importance mérite d'être rappelée. Le SGPD prescrit notamment une politique du système de gestion de la protection des données, une sélection de mesures pour le traitement des non-conformités, une déclaration d'applicabilité des mesures implémentées avec justification de celles qui auraient été exclues, un plan de traitement des non-conformités, une revue des violations ou incidents de protection des données et des actions correctives ou préventives pour améliorer le SGPD[12].

[12] Préposé fédéral à la protection des données et à la transparence, Emission des directives du Préposé pour la certification d'organisations (http://www.edoeb.admin.ch/dokumentation/00153/00291/00317/index.html?lang=fr).

Afin de faciliter son adoption au niveau de la Confédération, le PFPDT a développé un dispositif d'accompagnement aux organisations tant privées que publiques afin de répondre de manière concrète aux problématiques posées par la LPD. Il part pour cela notamment du postulat que les systèmes d'information développés antérieurement à la LPD n'ont pas été conçus pour intégrer les exigences apportées par la loi, ce qui implique la nécessité d'adopter une démarche proactive afin d'identifier les aspects problématiques. En outre, le SGPD invite à envisager toute modification d'un système d'information à travers son impact en matière de protection des données, fournissant ainsi un cadre dans lequel développer des projets. Dans la mesure où les principes défendus par la LPD sont très semblables à ceux de la LIPAD, le SGPD serait aisément transposable au contexte genevois. Le PPDT renvoie au rapport du Conseil d'Etat quant à une étude plus approfondie d'une éventuelle adoption d'un SGPD sur le plan cantonal.

12. CHANGEMENT D'AUTORITE : COMPLEMENT D'ANALYSE

Le rapport intermédiaire du PPDT sous sa précédente autorité ayant permis de répondre à la question de l'utilisation des dérogations, le présent document aborde la seconde interrogation découlant de l'art. 69 al. 8 LIPAD, à savoir l'opportunité de modifier ou non la législation.

De là découle la nécessité d'aborder deux points distincts, à savoir les besoins actuels de l'AeL, mais également ceux qui pourraient survenir à moyenne échéance. Pour ce faire, le PPDT se doit d'adopter une vision plus large que l'Administration en Ligne au sens étroit. Dans cette optique, trois projets informatiques menés par l'Etat de Genève ont été étudiés pour leur intérêt tout particulier au regard de la LIPAD.

Le Revenu Déterminant Unifié (RDU)
Le projet du RDU implique la transmission de nombre de données à caractère sensible. Il apparaît pertinent d'analyser la manière dont les services concernés ont encadré ces transferts et élaboré les différents accès pour les collaborateurs. Se pose la question de l'équilibre entre les besoins de l'administration pour la réalisation de ses tâches légales et la protection des données.

L'utilisation d'IncaMail
Ce projet présente l'intérêt de faire intervenir un acteur tiers dans le cadre des prestations de l'AeL. Ainsi, La Poste transmet des messages électroniques de l'AFC aux utilisateurs de l'Administration en Ligne qui ont fait le choix de ce mode de communication.

Les projets Passerelle et MPI
Ces deux projets distincts présentent l'intérêt du lien qui pourrait se créer entre eux du fait de la présence d'un acteur commun. De là découle une série d'interrogations sur le maître du fichier, notamment l'étendue de sa responsabilité.

12.1 AeL : Les prestations initiales de l'AeL et les autres - état des lieux

Le présent chapitre aborde la question de l'Administration en Ligne au sens étroit à travers une présentation de son fonctionnement, un état des lieux et les questions soulevées par son fonctionnement.

A titre liminaire, il convient de noter qu'une prestation AeL se compose de deux éléments cumulatifs :

- La prestation passe par le moteur AeL et
- Elle requiert - parfois uniquement à titre facultatif - un compte AeL.

Ainsi, certains services peuvent utiliser l'un de ces deux composants, mais ils se trouvent alors hors AeL, comme la déclaration de fichier au catalogue des fichiers du Préposé cantonal[13] (CATFICH) qui use uniquement un de ces deux éléments et ne fait, par conséquent, pas partie de l'Administration en Ligne au sens étroit.

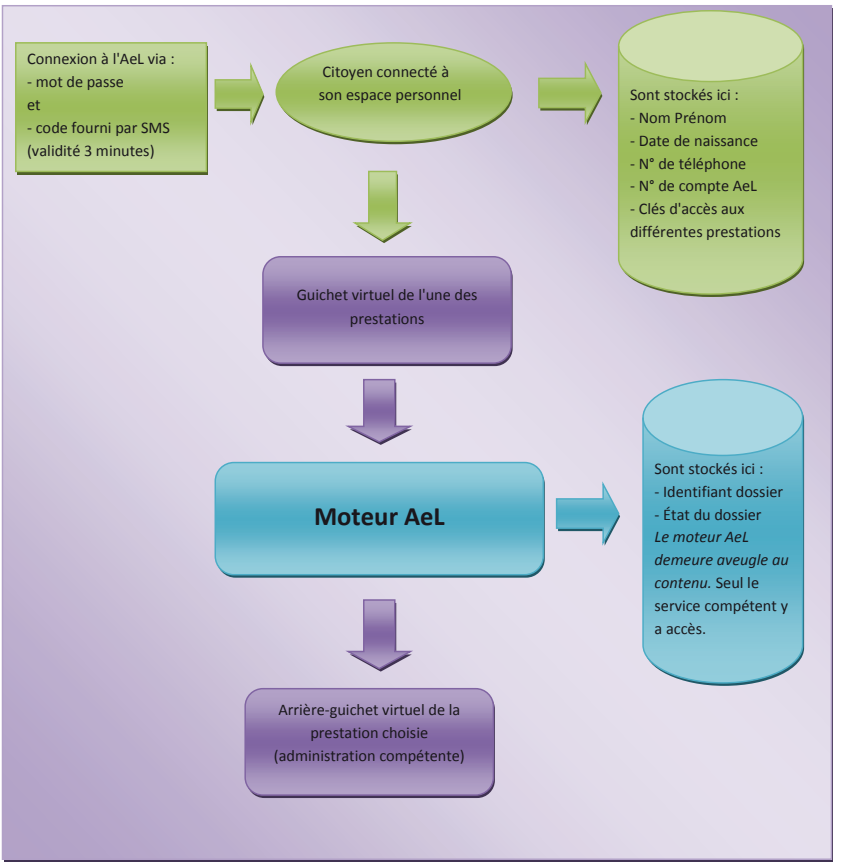
Fonctionnement général de l'AeL
La figure suivante illustre le fonctionnement général de l'Administration en Ligne, de l'impulsion donnée par un citoyen au traitement de sa demande par le service compétent.

Etape 1 : Le citoyen se rend sur la page d'accueil de l'AeL et se connecte via ses identifiants. Suite à cette action, un SMS contenant un code d'accès est envoyé sur le numéro de téléphone portable qu'il a enregistré sur son profil. La validité de ce code est de trois minutes. Une fois ce code entré, l'utilisateur peut se connecter sur son profil où s'affichent les différentes prestations disponibles. A noter que certaines prestations ne sont pas disponibles dès la création du compte. Le citoyen ne peut qu'en demander l'accès, lequel lui sera donné dans un délai dépendant du service compétent.

Etape 2 : Le citoyen sélectionne la prestation désirée. Cela l'amène auprès du guichet virtuel de celle-ci. Chacun de ces guichets dispose de sa propre base de données, auquel le service en charge de la prestation est le seul à pouvoir accéder. L'utilisateur peut, pour sa part, y stocker les brouillons de ses demandes. L'administration ne peut y accéder, pas plus qu'elle n'est prévenue de la création de brouillons.

[13] Selon l'art. 43 LIPAD, tout traitement de données personnelles doit être annoncé par les institutions publiques cantonales et communales genevoises.

Etape 3 : L'utilisateur finalise son brouillon et transmet sa demande. Pour parvenir à l'administration compétente, elle transite via le moteur AeL.



Services fonctionnels

- Stockage en ligne des demandes administratives;
- Gestion du cycle de vie d'une demande en ligne (état du dossier);
- Contrôle d'accès aux documents AeL : l'accès et la manipulation de chaque dossier AeL se fait sous contrôle des bons droits de l'usager;
- Planification des tâches : possibilité de planifier plusieurs types d'actions selon une fréquence et une durée voulues, à savoir l'envoi de mails à destination d'acteurs (mécanisme de relance) ou encore la mise à jour automatique de l'état d'un dossier (mécanisme d'expiration);
- Envoi d'e-mail : à l'occasion d'un changement d'état de dossier ou à la demande d'une tierce application, un mail peut être émis à destination de tout acteur de la prestation (usager, arrière-guichet). Des modèles de courrier permettant une personnalisation du message sont disponibles (adresse, nom, informations sur le dossier, etc.);
- Transmission aux systèmes métier;
- Paiement en ligne : le moteur prend en charge l'hébergement et le suivi des paiements en ligne des demandes AeL jusqu'à leur terme. Il procède à la mise à jour de la demande métier concernée selon le résultat de la transaction de paiement (succès, échec, etc.).

Services techniques

- Disponibilité 24h/24 et 7j/7 assurée pour l'ensemble des services rendus;
- Hébergement des dossiers AeL : les demandes de toutes les prestations sont stockées dans une base de données unique;
- Statistiques d'activités AeL : diverses statistiques sont publiées hebdomadairement afin de permettre un suivi de l'activité de chaque prestation;
- Hébergement des données de formulaires.

Ces services sont disponibles pour toutes les prestations qui transitent par le moteur AeL, même si elles ne font pas parties des 10 prestations d'impulsion du projet AeL.

Etat des lieux : Pilotage de l'AeL

Le pilotage du projet AeL a connu différentes phases, listées ici par ordre chronologique :

1) Un comité composé de secrétaires généraux départementaux dès le lancement du projet AeL mi-2008
2) Un comité de pilotage descendu au niveau des directions courant 2012
3) Une maintenance opérationnelle au niveau de la DGSI depuis l'été 2014

L'AeL a donc connu plusieurs changements de pilote, aucun acteur ne tenant les rênes du début à la fin du programme. La forme que prendra le pilotage à la fin 2015 demeure inconnue.

Etat des lieux : e-démarches

La direction de l'AeL met actuellement sur pied une plateforme internet qui vise à donner de nouvelles solutions de communication à l'Etat. Cette plateforme, où les prestations feraient office de contenu transactionnel, se voit conférer le rôle d'entrée unique pour accéder à l'ensemble des prestations disponibles en ligne. L'objectif est notamment de faciliter la recherche des différents services proposés pour le citoyen.

Ainsi, l'AeL est désormais intégrée sur la page http://ge.ch/e-demarches/. Elle y côtoie des services qui ne possèdent pas les deux conditions cumulatives de l'AeL (utilisation d'un identifiant AeL et utilisation du moteur AeL).

Les trois tableaux suivants, établis sur la base des documents communiqués au PPDT par la Direction générale des systèmes d'information, présentent l'ensemble des services disponibles divisés selon une base métier.

ANONYMES (AUCUN COMPTE AEL REQUIS)

Métier	e-démarches
AFC / IMPOTS	Délai de déclaration
	Délai de paiement
	Modification d'acomptes
POLICE CANTONALE	Certificat de bonne vie et mœurs
PRESTATIONS COMPLEMENTAIRES FAM	Prendre un rendez-vous
	Modifier un rendez-vous
	Calculer en ligne mes prestations complémentaires familiales
REPERTOIRE ENTREPRISES	Achat de listes d'entreprises
	Demande d'immatriculation d'une nouvelle

	entreprise
SANTE	Acquisition d'un droit de pratique
TERRITOIRE DE GENEVE	Accès à la mensuration officielle du cadastre et consultation des données 3D
VEHICULES	Renseignement détenteurs de plaques et demande de duplicata permis circulation échu
	Enchères fourrière registre du commerce

Total intermédiaire : 13 prestations

PARTICULIERS (PRÉ-REQUIS : CRÉATION DE COMPTE AEL)

Métier	e-démarches	authentification
AFC / IMPOTS	Situation des comptes	Oui avec SMS
	Mes documents	Oui avec SMS
	Déclaration en ligne	Oui avec SMS
	Délai de déclaration	Oui avec SMS
	Délai de paiement	Oui avec SMS
	Modification d'acomptes	Oui avec SMS
	Requête impôt source	Oui avec SMS
ASSURANCE MALADIE	Demande d'attestation des subsides et consultation de situation	Oui avec SMS
MANIFESTATIONS EVENEMENTS	Demande d'autorisation	Oui avec login simple
MOBILITE CHANTIERS	Directives de signalisation de chantiers	Oui avec login simple

POLICE CANTONALE	Certificat de bonne vie et mœurs	Oui avec SMS
POPULATION	Changement d'adresse	Oui avec SMS
	Attestation en ligne	Oui avec SMS
	Gestion de mon rendez-vous biométrique	Oui avec SMS
	Mes données personnelles OPCM	Oui avec SMS
REGISTRE DU COMMERCE	Inscription/modification d'une entreprise individuelle ou d'une société de personnes	Oui avec SMS
	Demande de subvention	Oui avec SMS
	Accès à la mensuration officielle du cadastre et consultation des données 3D	Oui avec SMS

Total intermédiaire : 18 (dont 5 sont disponibles en anonymes également)

ENTREPRISES (PRÉREQUIS : CRÉATION DE COMPTE AEL)

Métier	e-démarches	authentification
AFC / IMPOTS	Accès au dossier fiscal	Oui avec SMS
	Déclaration en ligne	Oui avec SMS
	Délai de déclaration	Oui avec SMS
	Prestation impôt source pour les employeurs	Oui avec SMS
GERANTS D'IMMEUBLES	Echange de données avec l'OCSTAT	Oui avec SMS

	Annonce de déménagement à l'OCPM	Oui avec SMS
PROFESSIONNELS CONSTRUCTION	Facture express	Oui avec SMS

Total intermédiaire : 7

TOTAL E-DEMARCHES : 38

Etat des lieux : taux d'utilisation

Sur la base des documents transmis par la DGSI, le PDDT ressort les chiffres suivants en termes de taux d'utilisation :

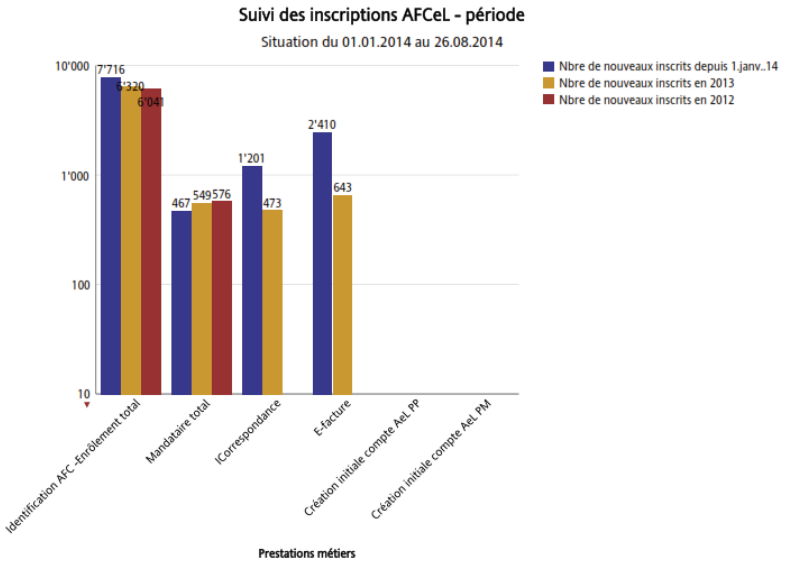
Nombre de particuliers inscrits : 70'000

Nombre d'entreprises actives : 9'500 et 13'000 comptes utilisateurs associés (note : une entreprise peut avoir plusieurs comptes de collaborateurs)

Par prestation :

- 20'000 adhérents aux prestations fiscales
- 2'000 aux prestations du SITG (signalisation de chantiers)
- 4'000 aux prestations relatives aux autorisations de manifester
- 9'000 aux prestations de l'OCPM
- 10'000 aux prestations de l'assurance maladie

Une étude plus approfondie des prestations fiscales, les plus fréquentées, révèle que la progression du nombre d'inscrits a connu une évolution positive entre 2012 et 2014 avec 7'716 nouveaux inscrits en 2014, contre 6040 en 2012.


Suivi des inscriptions AFCeL - période
Situation du 01.01.2014 au 26.08.2014
Nbre de nouveaux inscrits depuis 1.janv..14
Nbre de nouveaux inscrits en 2013
Nbre de nouveaux inscrits en 2012
10'000
1'000
100
10
7'716
6'047
467
549
576
1'201
473
2'410
643
Identification AFC -Enrôlement total
Mandataire total
ICorrespondance
E-facture
Création initiale compte AeL PP
Création initiale compte AeL PM
Prestations métiers
Comparaison aux mêmes périodes 2013 et 2012

La figure suivante illustre le taux de répartition de l'utilisation entre les différentes sous-prestations de l'AFC :

Situation au 26.08.2014

Libellé	Nbre de soumissions au 26.08.2014	Pourcentage par prestation
Demande de modification d'acompte ICC-IFD non authentifié	26'184	14.74%
Dépôt DeclaPP : GeTaxInternet	4'729	2.66%
Dépôt DeclaPP : Téléversement	57'785	32.54%
Dépôt DeclaPM : Téléversement	178	0.10%
Demande de délai de dépôt de déclaration PP et PM non authentifiée	51'806	29.17%
Demande de délais de dépôt de déclaration (personnes physiques) authentifié fort	2'012	1.13%
Demande de délais de dépôt de déclaration (groupée)	7'711	4.34%
Demande de délais de paiement	3'045	1.71%
Gestion IBAN	208	0.12%
IS - Formulaire annonce (Arrivée nouvel employé)	2'971	1.67%
IS - Décompte de paiement	12'975	7.31%
IS - Changement de situation	246	0.14%
IS - Dépôt Liste Récapitulative	6'602	3.72%
Requête Impôt Source	1'154	0.65%
Récapitulatif général	**177'606**	**100.00%**

Le téléversement (versement par internet) des personnes physiques (32,54%), les demandes de délai de dépôt de déclaration des personnes physiques et personnes morales non authentifiées (29,17%) et les demandes de modification d'acompte ICC-IFD non authentifiées (14,74%) représentent plus des trois quarts de l'activité de cette prestation.

Toutefois, il convient de noter qu'au 26 août 2014, 11'721 inscriptions aux prestations AFC avaient été entamées sans jamais être finalisées, sans que la cause en soit connue.

Etat des lieux : perspective

Selon les termes du PL 10177, l'AeL poursuivait un triple objectif de gain d'efficience, d'impulsion et de confort pour le citoyen. Le PPDT n'ayant pas pour tâche d'aborder la question du retour sur investissement, cette dernière n'est pas abordée dans le présent

rapport. Tout au plus pourra-t-on remarquer que, si la littérature scientifique appuie la potentialité de réaliser des gains par ce biais[14], il convient pour ce faire que l'AeL attire un maximum d'usagers tout en misant sur son troisième objectif, le confort pour le citoyen.

La facilité d'utilisation et la création d'une entrée unique pour l'accès à l'ensemble des prestations en ligne est d'ailleurs régulièrement mise en avant comme facteur de succès des projets d'administration en ligne[15].

A ce titre, le projet e-démarches actuellement en cours suit parfaitement cette ligne en s'évertuant à offrir aux usagers une expérience unique pour l'ensemble des prestations fournies par l'Etat. L'AeL a rempli son objectif d'impulsion via la mise sur pied d'une base saine, respectueuse de la LIPAD, comme démontré par le rapport intermédiaire du PPDT, et doit désormais s'atteler à attirer davantage d'usagers afin de remplir ses objectifs.

Dans cette optique, il est à regretter que les directeurs des différentes prestations ne disposent plus de l'espace institutionnel de rencontres et d'échanges que constituait le comité de pilotage de l'AeL, et ce à l'heure où les efforts se dirigent vers une uniformisation des services en ligne.

12.2 Base de données relative au revenu déterminant unifié (RDU)

Présentation du SI RDU

Selon les termes de la convention passée entre le Département des finances et le Département de l'emploi, de l'action sociale et de la santé concernant ce projet, le système d'information du RDU (SI RDU) est un outil informatique qui permet de renforcer et d'assurer l'harmonisation des prestations sociales, le respect de l'égalité de traitement et l'efficience administrative, selon les objectifs de la loi sur le revenu déterminant unifié du 19 mai 2005 (LRDU; RSGe J 4 06), et de la loi 10527 (L 10527) pour le développement du SI RDU. Concrètement, toutes les prestations sociales cantonales soumises à condition de ressources sont délivrées sur la base du montant du revenu déterminant unifié.

---

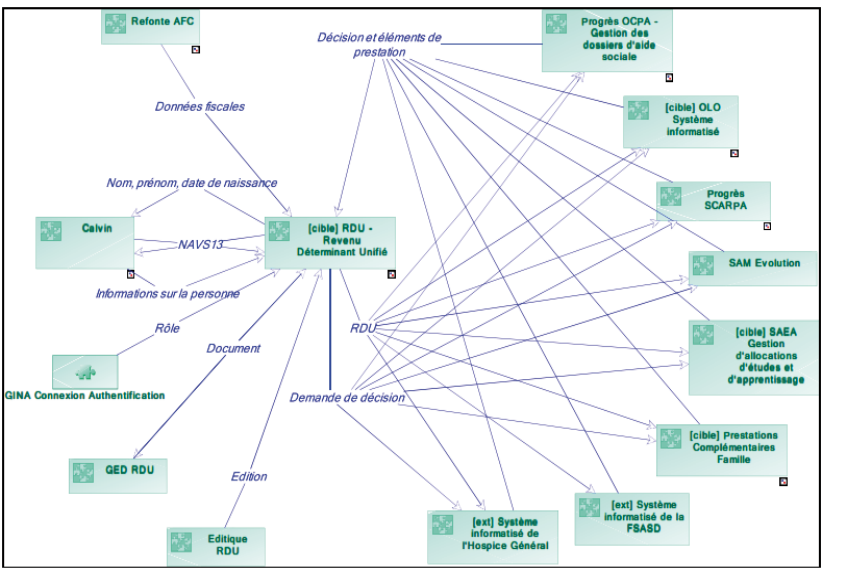
[14] AL-SHAFI Shafi, WEERAKKODY Vishanth, Exploring E-government in the State of Qatar : Benefits, Challenges and Complexities, European and Mediterranean Conference on Information System 2007 (EMCIS 2007), June 24-26 2007, Polytechnic University of Valencia, Spain; FANG Zhiyuan (2002), E-government in digital era : Concept, practice and development, *in* International Journal of the Computer, The internet and Management, 10 (2), 2002, pp. 20-21; KALVET Tarmo, TIITS Marek, HINSBERG Hille (éd.), Impact assessment of the Estonian e-government services, Institute of Baltic Studies & Praxis Center for Policy Studies, Tallinn, 2013.

[15] CORRITORE Cynthia et *al.*, Online Trust and Health information Websites, Association Information Systems Special Interest Group on Human Computer Interaction, 2007 (http://sighci.org/uploads/published_papers/ICIS2007/SIGHCI_2007_Proceedings_paper_2.pdf); REFFAT Rabee, Developing A Successful E-Government, School of Architecture, Design Science and Planning, University of Sydney, Australia, 2003, p. 4.

Le revenu déterminant unifié est un montant composé d'un certain nombre d'éléments de revenus, de fortune et de déductions fixées par la LRDU, fixant ainsi des modalités unifiées et applicables à toutes les prestations sociales soumises à condition de ressources. Les montants des prestations sociales versées viennent ensuite s'ajouter à ce montant, appelé "RDU socle", au fur et à mesure de leur délivrance, et selon l'ordre précis défini par la loi précitée (hiérarchie des prestations).

Pour ce faire, le SI RDU s'est doté d'une base unique de données, qui assure une circulation rapide et actualisée de l'information nécessaire au calcul du RDU. L'alimentation continue en données de revenus et de fortune les plus récentes est un pilier du système.

La figure suivante, tirée du concept SIPD du SI RDU, permet d'obtenir une vue d'ensemble des données concernées :



Etapes de sécurité

Concerné par le nombre important de données personnelles sensibles touchées par ce projet, le PPDT a décidé de s'intéresser aux moyens mis en place afin d'assurer leur sécurité.

1) Concept SIPD

Prévu dans la méthodologie Hermès, le concept SIPD consiste à élaborer une partie des éléments qui constituent le projet, en partant des conditions cadres à respecter en matière de sûreté et protection des données, des exigences exprimées en la matière, des moyens existants et des possibilités technologiques. Ceci dans le but d'élaborer, de spécifier, de planifier et de définir les mesures de protection adéquates afin qu'elles soient intégrées dans le développement et puissent ensuite être mises en œuvre.

Dans le cadre du SIPD, il est procédé à une analyse des risques subdivisée en 3 parties dans le cas d'espèce :

Définition du contexte global : Etablissement des conséquences et des impacts des risques.

Définition du contexte spécifique : Identification des types de données concernées, à savoir:

- Les données personnelles : données sur les personnes de l'ensemble de la population genevoise. Informations détaillées sur la situation familiale, professionnelle, résidentielle et légale. Des identifiants tels que le NAVS 13 sont inclus dans ces données;
- Les données financières : données contenant des éléments de revenus et de fortune. Elles servent à déterminer le droit à une prestation et au calcul RDU;
- Les données des prestations : données relatives aux demandes, décisions et gestion des prestations sociales. Ces données proviennent des bases de données des services délivrant la prestation concernée.

Pour toutes ces données, un ou des propriétaires sont identifiés et trois exigences de sécurité sont systématiquement étudiées et discutées pour les trois groupes de données :

- Confidentialité (composée de la protection des données, d'une gestion des accès établie selon les principes de la proportionnalité et de la finalité, selon les données des mesures organisationnelles comme l'assermentation et enfin le respect des procédures légales quant à l'utilisation du NAVS13);
- Intégrité (données justes et à jour);
- Disponibilité.

Pour les trois catégories de données, ont été retenues comme exigences prioritaires la confidentialité et l'intégrité des données. Ce faisant, la priorité a été donnée au respect des principes généraux en matière de traitement de données.

Scénario des risques : Plusieurs des intervenants du projet se sont réunis afin d'identifier et évaluer les risques les plus critiques dans l'optique d'élaborer et de préconiser des mesures de mitigation. Tous les scénarios ont permis de proposer des mesures de réduction des risques.

2) Newsletter incorporant la protection des données

Le PPDT, sous sa précédente autorité, avait recommandé de mettre en œuvre une sensibilisation des collaborateurs de la Direction générale de l'action sociale à la protection des données. Cela a été fait en conférant à cette problématique un rôle central.

3) Formulaire d'accès au SI RDU

Avant toute création ou suppression d'accès au SI RDU, un formulaire à la teneur suivante doit impérativement être signé par le collaborateur et le responsable du service/entité ou son représentant :

Je, soussigné(e), déclare m'engager à garder le secret le plus absolu sur toutes les données d'ordre fiscal auxquelles j'aurai accès dans le cadre de l'utilisation du système d'information du revenu déterminant unifié (SI RDU).

Je prends bonne note qu'en violant le secret fiscal auquel je m'engage, je m'expose à subir les sanctions prévues par la loi, notamment par le Code Pénal Suisse (CPS).

Un extrait des dispositions légales concernées est reproduit à la suite du document.

4) Assermentation des personnes chargées de manier les données

Les personnes disposant d'accès aux données SI RDU doivent être assermentées. Cela pousse notamment à une réduction du nombre de personnes chargées et ayant la possibilité de manier ces données, en conformité avec le principe de la finalité.

5) Warning dans l'application lorsqu'on accède aux données sensibles

L'accès des collaborateurs aux données est limité à celles que les prestations enregistrées pour leur service leur permettent de consulter. Ainsi, si un collaborateur tente de forcer l'accès, il sera prévenu par un message d'avertissement. Toutefois, dans la mesure où il peut exister des cas où l'accès est en réalité légal et nécessaire, qu'il sera justifié sitôt qu'une mise à jour sera effectuée, alors il demeure possible de forcer l'accès. Cependant, cela doit se faire avec une justification qui sera automatiquement transmise au contrôle interne du service concerné. L'objectif est d'atteindre un juste milieu entre la protection des données et la réalisation de la tâche à effectuer.

6) Surveillance par le contrôle interne
Toute action sur le SI RDU est tracée. Le contrôle interne peut savoir exactement quelle page a été consultée par quel collaborateur. Cette capacité permet de repérer tout accès indu à des données.

Difficultés rencontrées
Il ressort des entretiens menés que, si la législation actuelle permet de répondre aux questions simples comme les conditions pour accéder à des données ou les critères à respecter dans leur collecte, etc., un manque de précision se fait sentir dans les situations complexes où la donnée utilisée concerne l'intéressé et un tiers. Qui peut donner accès à quelles données lorsque ces dernières concernent également un tiers qui n'a pas donné son accord?

Prenons l'exemple d'un couple, A et B, souhaitant divorcer. Madame B obtient une pension alimentaire. Par la suite, elle se remet en couple avec Monsieur C. Elle formule ensuite une demande à l'Office du logement qui, plutôt que de lui demander ses revenus, va accéder au jugement de divorce qui contient tant des informations sur Madame B que sur Monsieur A. Opérationnellement, l'administration peine à caviarder les documents au cas par cas pour ne garder que le strict nécessaire.

Un second problème se posera si Monsieur C, souhaitant accéder au dossier auprès de l'Office du logement, invoque la LIPAD. En effet, le dossier contiendra le jugement de divorce qui concerne également Monsieur A qui, lui, n'a pas donné son accord.

Si le consentement est à la base de la communication d'informations, le redemander ensuite peut s'avérer plus problématique. Dans l'exemple présenté, Monsieur C pourrait refuser pour des raisons chicanières.

12.3 IncaMail

Présentation d'IncaMail dans le cadre de l'AeL
L'objectif d'IncaMail est de transmettre des courriers aux personnes physiques de façon informatique pour des personnes ayant cumulativement fait le choix de s'inscrire aux prestations en ligne de l'Administration fiscale cantonale (AFC) et ayant choisi ce mode de communication.

Afin d'expliquer le fonctionnement de ce système, nous nous référons à l'avis de droit du professeur Werly concernant la signature électronique. Il y relevait que s'il existe de nombreuses techniques baptisées "signatures électroniques", celle fondée sur **la**

cryptographie asymétrique (ou à clé publique)[16] constitue le type de signature le plus répandu et offre les meilleures garanties de sécurité, pour autant que les messages soient cryptés au moyens d'algorithmes utilisant plusieurs dizaines de bits[17].

Le fonctionnement de ce système est le suivant : une fois le message signé par son auteur à l'aide de sa clé privée, il est expédié au destinataire, lequel peut le déchiffrer uniquement avec la clé publique complémentaire à la clé privée de l'émetteur; le destinataire est donc certain que le message émane bien de son auteur dûment identifié.

Si elle permet de vérifier l'authenticité et l'intégrité des données et apporte en conséquence au document numérique les mêmes garanties que la signature manuscrite au document papier, la signature électronique comporte cependant certaines **lacunes**, dès lors qu'elle ne règle pas la question de l'identité de l'expéditeur, de la preuve de l'envoi et de la réception des communications par voie électronique. L'expéditeur d'un message électronique ne peut en effet assurer par ses propres moyens et avec un haut degré de vraisemblance la preuve de l'envoi, respectivement de la réception, car il n'est pas en mesure d'exiger de son destinataire que celui-ci atteste de la réception de son message (le destinataire peut refuser de renvoyer l'accusé de réception demandé). Il est donc indispensable de passer par un tiers de confiance.

La signature électronique repose de la sorte sur une infrastructure de certification gérée par un tiers de confiance appelé fournisseur de services de certification. Cette autorité de certification, qui engage sa responsabilité en cas de problème, est un organisme indépendant habilité à vérifier l'identité des titulaires des clés publiques, à générer des certificats et à assurer la publicité la plus large des certificats ainsi émis**.** En d'autres termes, elle certifie des informations dans un environnement électronique et délivre des certificats électroniques (le résultat de la vérification est incorporé dans un certificat électronique qui contient la clé publique immédiatement exploitable par le destinataire) pour garantir l'identité des utilisateurs d'une signature numérique, titulaires d'une clé secrète[18] Ainsi, grâce au cryptage à clé publique, outre la certitude de l'identité, il est aussi possible d'assurer la preuve du contenu de l'envoi, tout en assurant la confidentialité de la transaction, y compris envers le tiers de confiance.

---

[16] Par clé de signature, il faut comprendre "un ensemble de données uniques telles que des codes ou des clés cryptographiques privées que le titulaire utilise pour composer une signature électronique". Concrètement, il s'agit d'une clé USB contenant un certificat, obtenue auprès du fournisseur. Quant à la clé de vérification de signature, il s'agit d'"un ensemble de données telles que des codes ou des clés cryptographiques publiques utilisées pour vérifier une signature électronique" : DONZALLAZ Yves, Loi sur le Tribunal fédéral, Commentaire, Berne, 2008, n° 691 et 693.

[17] WERLY Stéphane, *Les problématiques juridiques rencontrées, dans le cadre de l'Administration fiscale cantonale en ligne, en matière de idossier, de signature électronique et de notification électronique*, Genève, 2011, pp. 51 s.

[18] DONZALLAZ, *op. cit.*, n° 694. Ce système est décrit dans la Recommandation X.509 de l'Union internationale des télécommunications (UIT).

A cet égard, en parallèle au courrier postal traditionnel, La Poste suisse a mis en place une plateforme baptisée **IncaMail** qui permet d'assurer, moyennant rétribution, la preuve de l'envoi, respectivement de la réception d'un message électronique, en délivrant une quittance horodatée. Son fonctionnement est le suivant :

1. L'expéditeur envoie son message depuis une application web, un e-mail client ou un business software. IncaMail transmet le message de manière sécurisée par une connexion cryptée.
2. Si le destinataire a intégré IncaMail dans son e-mail client ou dans son business software, le courriel sera automatiquement transmis, par le biais d'une liaison sécurisée.
3. Tous les autres destinataires reçoivent le courriel comme pièce jointe cryptée, directement dans leur boîte de réception, et peuvent l'ouvrir au moyen d'un mot de passe ou par double clic (technologie SAFE). Les destinataires qui reçoivent ce courriel pour la première fois doivent s'identifier cette seule fois.
4. L'expéditeur reçoit une attestation de retrait et, pour la variante Recommandé Swiss Post, une quittance d'expédition et de réception sous forme de pdf.

Le recours à la signature numérique est réglé dans des **actes juridiques distincts**, selon que la transaction relève du droit privé ou du droit public. Dans le secteur du droit public, déterminant pour la cyberadministration, il s'agit des normes sur les procédures administratives.

Afin d'éviter aux usagers de l'AeL d'avoir à créer un compte IncaMail en plus de celui qu'ils possèdent déjà auprès de l'administration cantonale, il a été négocié avec La Poste la possibilité d'utiliser le compte AeL dans le cadre d'IncaMail. Concrètement, si un usager fait le choix de recevoir ses courriers de l'AFC par voie électronique, il recevra un message de la manière suivante :

- Un mail "L'administration genevoise vous contacte" est envoyé sur la boîte mail associée au compte AeL. Ce titre générique vise à éviter, dans le cas d'une personne se trouvant dans un lieu public, qu'un tiers puisse savoir que l'intéressé est contacté par l'AFC;
- Afin d'ouvrir le message électronique, l'usager doit se connecter avec son mot de passe AeL (cela passe également par une vérification via un code envoyé par SMS);
- Une fois connecté avec le compte AeL, le message est automatiquement décrypté et s'ouvre directement dans la boîte mail de l'usager.

En terme de sécurité pour l'accès au message, il est nécessaire de posséder le mot de passe de la boîte mail privée, le mot de passe du compte AeL et le code transmis par SMS.

Dans l'éventualité où une erreur survient, elle est traitée par l'AFC comme un retour courrier classique et l'envoi se fera par les moyens papiers traditionnels.

Etat des lieux : taux d'utilisation
A date du 10 novembre 2014, avec un début des inscriptions à cette prestation en 2013, on dénombre :

- 3’202 courriers envoyés électroniquement;
- 2’288 inscrits au domaine AFC Correspondance Personnes Physiques.

Bien que limitée aux personnes physiques, l'utilisation de ce service demeure relativement faible au regard du nombre d'inscrits aux prestations de l'AFC (20'000 dont il convient de retrancher les personnes morales).

Une autre limite provient du fait que le courrier recommandé n'est pas intégré à IncaMail. En effet, ce type de courrier exige la forme traditionnelle, ce qui réduit le champ que cette prestation peut couvrir.

Problématique
Si l'administration cantonale est soumise à la LIPAD, les organes fédéraux et les tiers privés sont eux soumis à la LPD. Par conséquent, il existe un risque de chevauchement entre ces lois. La LIPAD s'applique à la communication de données par l'administration cantonale aux tiers tandis que la LPD s'applique aux tiers, notamment en matière de communication de données d'un administré à l'administration cantonale. Si aucun cas de figure ne s'est présenté à l'heure actuelle, il en découle néanmoins qu'il peut être ardu de déterminer la loi applicable dans un cas d'espèce.

A ce titre, notons que le Conseil d'Etat s'est déterminé fin 2013 en faveur d'une application de la LPD aux administrations cantonales à l'occasion d'une consultation de la Confédération.

12.4 Projets Passerelle et MPI

Le présent chapitre s'intéresse au projet Passerelle entre le RF et l'OCEN et au projet MPI entre le RF et l'AFC. Le choix de coupler leur étude relève du lien qui pourrait se créer entre eux : l'OCEN souhaite obtenir l'accès à des données du RF et ce dernier désire les fiabiliser via celles de l'AFC. De cette situation découlent des interrogations LIPAD en matière de responsabilité concernant les données.

Présentation du projet MPI
Objet : transfert de données de l'AFC au RF

Partant du constat qu'environ 10% des adresses postales de propriétaires possédées par le RF sont obsolètes, le Conseil d'Etat a émis, en 2006, une recommandation visant à accroître la synergie entre le RF et l'AFC. Sur cette base, un projet consistant en la fiabilisation des adresses du RF à travers celles, estimées plus exactes de l'AFC, a été élaboré.

Ce projet, visant à récupérer les adresses postales de l'AFC afin de les transférer de manière automatique, a été lancé et partiellement réalisé côté AFC sous le nom de MPI. La partie RF demeure à l'état de projet à l'heure actuelle. S'il venait à être réalisé, il permettrait de réduire la charge de travail manuel que représentent les demandes auprès de l'AFC à chaque fois que le RF souhaite vérifier ses données.

Présentation du projet Passerelle
Objet : transfert de données du RF à l'OCEN

L'art. 15C de loi sur l'énergie du 18 septembre 1986 (LEn; RSGe L 2 30) ainsi que les art. 14 et 14A du règlement d'application de la loi sur l'énergie du 31 août 1988 (REn; RSGe L 2 30.01) imposent aux propriétaires de bâtiments chauffés de communiquer leur Indice de Dépense de Chaleur (IDC).

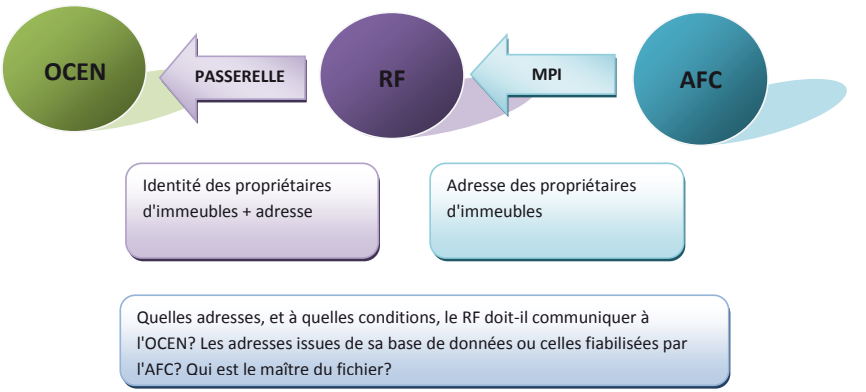
L'OCEN a la charge d'informer les propriétaires de cette législation, de leur envoyer des rappels lorsque les délais ne sont pas respectés et, le cas échéant, de les amender. Toutefois, pour remplir cette tâche, l'OCEN a besoin de deux informations :

- L'identité du propriétaire du bâtiment;
- L'adresse postale du propriétaire.

Pour y parvenir, l'OCEN avait tout d'abord envisagé d'utiliser le fichier des compteurs d'eau SIG. Néanmoins, dans plusieurs cas, la facture d'eau était à la charge des locataires et non du propriétaire. Par conséquent, cette méthode ne se révélait pas optimale. Passer par les données possédées par le RF permet de réduire le nombre de retours de courriers.

Actuellement, la transmission de données du RF à l'OCEN se fait manuellement sur la base d'une convention dont la forme relève du droit fédéral. Le projet Passerelle permettrait d'automatiser le transfert, ce qui se traduirait par un gain de temps pour l'administration. De là découle la question des données que devrait transmettre l'AFC : celles non fiabilisées ou celles ayant fait l'objet d'une vérification à travers celles de l'AFC?

Schéma des projets et problématique :



Si l'art. 39 LIPAD fournit le cadre de la transmission d'une entité A à une entité B, la question d'un second transfert, de l'entité B à une entité C, ne trouve pas de réponse évidente. Quid si l'entité B couple les données fournies par l'entité A à ses propres données ? Relèvent-elles encore de l'entité A? Qui serait alors le maître de fichier ? Jusqu'où s'étendrait la responsabilité de l'entité A dans l'emploi des données ?

13. CONSTATS

Les deux rapports produits par le PPDT sur l'AeL lui permettent de démontrer que ce programme d'impulsion a pu être déployé sans déroger aux engagements internationaux de la Suisse. Par conséquent, la suppression de l'art. 69 LIPAD fin 2015 ne portera pas atteinte aux prestations existantes. Toutefois, cette expérience a également permis d'identifier un certain nombre de zones d'ombre dans la législation qui, sans être propres à ce projet, pourraient entraîner des conséquences dommageables.

Ainsi, si le PPDT ne voit pas la nécessité de rajouter d'autres grands principes à ceux contenus dans la LIPAD, son analyse le pousse néanmoins à préconiser que la législation existante soit précisée afin d'apporter des réponses à des situations qui, à l'heure actuelle, peinent à trouver leur solution dans les textes de loi.

14. CONCLUSIONS

L'impact des nouvelles technologies et leurs retombées en matière de protection du droit à la vie privée doivent être contrôlés en permanence. L'approche AeL nécessite la mise à niveau des lois et des règlements en relation avec l'usage des TIC.

Des mesures doivent également être mises en place afin de renforcer la culture de la sécurité et de la protection des données personnelles. Cette culture repose d'abord sur la sensibilisation et la responsabilisation de toutes les parties prenantes, que cela soient les émetteurs des services (les membres de la fonction publique) ou les destinataires de ces services (les citoyens et les entreprises), et sur le respect des règles de bonne pratique, en distinguant clairement la protection des données personnelles et de la vie privée d'une part, et la sécurité informatique, d'autre part.

Des programmes de sensibilisation et de formation doivent être déployés pour permettre aux usagers de bien assimiler les risques émergeant et les maîtriser en tout temps, en plus du respect des obligations légales telles qu'inscrites dans la législation.

Les mécanismes mis en œuvre doivent être définis de telle manière qu'ils soient suffisamment souples et/ou adaptables face à l'évolution rapide des technologies. Cet assouplissement du corpus législatif ne règle toutefois pas pour autant tous les problèmes d'application des lois, d'autant plus que si les processus administratifs existant sont lourds et complexes, ils ne seront pas facilement adaptés lors de l'introduction des nouvelles technologies.

Finalement, l'AeL doit favoriser une approche où les TIC et les règles organisationnelles mises en œuvre réduisent au minimum les possibilités de violation du droit à la vie privée. Ainsi, plutôt que de contrôler toute violation éventuelle, il est indispensable de prendre les mesures adéquates afin que ces éventualités ne puissent simplement pas survenir.

15. RECOMMANDATIONS

Sur la base du présent rapport et du rapport intermédiaire, le PPDT recommande :

- ➔ D'introduire une disposition, par exemple dans la LIPAD, réglant la question de la responsabilité des acteurs, notamment concernant notamment les "transferts en chaîne" de données personnelles;

- ➔ Dans le cas où le législateur déciderait d'ancrer l'AeL dans une loi spécifique, de s'assurer que la question de la responsabilité renvoie à une disposition dont le champ d'application est le même que celui de la LIPAD. Dans le cas contraire, il ne serait pas exclu que, dans le cadre d'une prestation, tant cette loi spécifique que la LIPAD, voire encore la LPD, soient susceptibles de s'appliquer concurremment, sans qu'il soit aisé de trancher;

- ➔ De poursuivre la mise en œuvre d'un SGPD sur le modèle du Préposé fédéral, piloté par la DGSI;

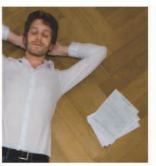
- ➔ D'informer davantage les collaborateurs concernés sur la LIPAD - notamment via le *Code de bonne pratique pour le système de gestion de la protection des données* rédigé en collaboration avec la DGSI dans l'esprit pédagogique d'un "mode d'emploi" - et sur la possibilité de contacter les responsables LIPAD départementaux. Aujourd'hui, le PPDT observe que nombre de questions juridiques, portant sur des aspects de fond, parviennent à l'état brut sur son bureau, sans avoir fait l'objet d'une analyse départementale préalable.

ANNEXE

REPUBLIQUE ET CANTON DE GENÈVE

PPDT

Rapport 2014 du Préposé cantonal concernant l'évaluation du programme AeL



PRÉPOSÉES À LA PROTECTION
DES DONNÉES ET À LA TRANSPARENCE

Table des matières

REPUBLIQUE ET CANTON DE GENEVE

Préposé cantonal à la protection des données et à la transparence

1. Préambule

L'administration en ligne relève de la transparence administrative et comporte de multiples facettes : démarches administratives en ligne sur un guichet unique - publications en ligne des entités publiques - les relations entre les administrations et les entreprises - la mise en œuvre de procédures administratives par voie électronique - les nouveaux modes de travail au sein du secteur public tels que le télétravail ne sont que quelques exemples.

La mission principale du Préposé cantonal consiste à veiller à ce que les droits des particuliers et des personnes morales de droit privé au respect de leurs données personnelles saisies à l'occasion de ces transactions soient protégés.

Le programme expérimental de l'AeL s'étend de la mi 2008 au 31 décembre 2015. En application de l'art 69 al. 8 LIPAD, trois rapports d'évaluation doivent être remis au Grand Conseil, au plus tard à la fin de l'année 2014 :

- Un rapport du Conseil d'Etat
- Un rapport du Préposé cantonal
- Un rapport de la Commission consultative (CCPDTA).

Le préposé cantonal, pour sa part, est chargé d':

«évaluer l'impact des prestations en ligne offertes sous l'angle des prescriptions exigées à la présente loi, avec des recommandations quant à l'opportunité de modifier ou non la législation pour permettre d'autoriser de manière durable les éventuelles dérogations expérimentées dans le cadre du programme d'administration en ligne».

Cette autorité indépendante a ainsi accompagné ce programme dès son entrée en fonction en janvier 2010. Au terme du 1er mandat de quatre ans, l'équipe en place a rendu un premier rapport intermédiaire en décembre 2013 en collaboration étroite avec la direction Sécurité et évènements spéciaux de la direction générale des systèmes d'informations du département de la sécurité et de l'économie.

Le présent rapport est le fruit du travail du Préposé cantonal et la Préposée adjointe entrés en fonction le 1er janvier 2014 ; il complète le rapport intermédiaire en mettant à jour l'état des lieux de l'administration en ligne à ce jour établi fin 2013 et en donnant un éclairage plus spécifiquement juridique conformément à la demande du législateur de recevoir des recommandations relatives à l'opportunité ou non de modifier la législation.

Les recommandations formulées in fine du rapport tiennent compte des expériences faites au plan fédéral et dans d'autres cantons et s'intègre au cadre fixé par la LIPAD quant au respect des principes de protection des données personnelles et de transparence.

Stéphane Werly,

Préposé cantonal à la protection des données et à la transparence

Liste des principales abréviations utilisées

AeL	Administration en Ligne
AFC	Administration Fiscale Cantonale
CCPDTA	Commission consultative en matière de protection des données, de transparence et d'archives publiques.
COPIL	Comité de Pilotage
CTI	Centre des technologies de l'information
DAC	Direction des Autorisations de Construire
DARES	Département des affaires régionales, de l'économie et de la santé
DF	Département des Finances
DGAE	Direction Régionale des Affaires Économiques
DGAS	Direction régionale de l'action sociale
DGS	Direction Générale de la Santé
DGSI	Direction Générale des Systèmes d'Information
DIP	Département de l'Instruction Publique
DS	Département de la Sécurité
DSE	Département de la Solidarité et de l'Emploi
DU	Département de l'Urbanisme
LIPAD	Loi sur l'information du public, l'accès aux documents et la protection des données personnelles
OCPM	Office Cantonal de la Population et des Migrations
OCV	Office Cantonal des Véhicules
PL	Projet de loi
PPDT	Préposé cantonal à la Protection des Données et à la Transparence
SCOM	Service du Commerce
SEM	Service Écoles-Médias
SITG	Système d'Information du Territoire à Genève

2. Rappel législatif

L'Administration en Ligne (ci-après AeL) trouve son fondement dans la loi 10177[1], votée par le Grand Conseil le 26 juin 2008, qui a ouvert un crédit d'investissement de 26'350'000 F pour financer le projet. Cette loi faisait suite à la loi 8593 « Cyberadministration - élaboration d'un concept global à Genève »[2], adoptée par le Grand Conseil le 14 juin 2002, ouvrant un crédit d'investissement de 600'000 F afin de financer l'élaboration d'un concept global d'administration en ligne pour l'Etat de Genève.

En référence à la définition fournie par le projet de loi 10177, l'AeL est l'ensemble des moyens techniques, administratifs, organisationnels et humains mis en œuvre par l'Etat pour permettre de réaliser des interactions transactionnelles complètes avec des correspondants (comprendre ici les citoyens, les entreprises, etc.) en temps réel sur internet. L'objectif est donc, pour l'administration, de s'adapter aux moyens de communication virtuels afin de délivrer des prestations aux destinataires sans que ceux-ci aient à passer par les canaux matériels traditionnels tels que les déplacements, les guichets, les courriers ou le téléphone. Cette adaptation s'insère dans la continuité du mouvement déjà initié par la mise à disposition d'informations sur le site de l'Etat de Genève, du vote électronique, de la gestion des contrôles et des examens de permis de conduire sur le site du Service des automobiles et de la navigation ou encore le système d'information du territoire à Genève (ci-après SITG).

Ainsi, comme indiqué dans les motifs de la loi 8593, il s'agit d'un projet de nature transversale et pluridisciplinaire. Il doit permettre à l'administration de franchir une étape déterminante afin d'être en adéquation avec son temps, à savoir de passer à la phase de la transaction ou téléprocédure, qui permet l'application de procédures à distance par internet.

Ce projet d'AeL se compose de quatre parties distinctes mettant en évidence les différents défis à relever[3] :

I. la construction des composants transversaux techniques nécessaires au déploiement et au fonctionnement des prestations,

II. la réalisation de l'harmonisation des registres conformément à la loi fédérale (ci-après LHR[4]) et, comme conséquence de cette loi, la réalisation des bases métiers transversales comprenant les principaux autres registres de l'Etat,

III. le déploiement de prestations destinées aux usagers des services de l'Etat,

[1] L 10177, loi *ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne*, Genève, 26 juin 2008, (http://www.ge.ch/grandconseil/data/loisvotee/L10177.pdf , site consulté le 9 septembre 2013).
[2] L 8593, loi *ouvrant un crédit d'investissement de 600 000 F pour le projet " Cyber administration - élaboration d'un concept global de l'Etat de Genève"*, Genève, 14 juin 2002, (http://www.ge.ch/grandconseil/data/loisvotee/L08593.pdf , site consulté le 9 septembre 2013).
[3] PL 10177, *projet de loi ouvrant un crédit d'investissement de 30 850 000 F pour le développement de l'administration en ligne*, Genève, 28 novembre 2007, p. 8-9. (http://www.ge.ch/grandconseil/data/texte/PL10177.pdf , site consulté le 9 septembre 2013)
[4] Loi fédérale du 26 juin 2006 sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (LHR; RS 431.02), (http://www.admin.ch/opc/fr/classified-compilation/20052012/index.html , site consulté le 9 septembre 2013)

IV. l'accompagnement de ces prestations auprès de la population et l'accompagnement du changement au sein de l'administration.

Dérogations à la loi en matière de protection des données

Par la révision de la loi sur l'information du public, l'accès aux documents, et la protection des données personnelles[5] (ci-après LIPAD), votée en octobre 2009, un nouveau volet concernant la protection des données a été ajouté au champ d'application matériel de la loi. A cette occasion, l'ancienne loi sur les informations traitées automatiquement par ordinateur du 17 décembre 1981 (LITAO) a été abrogée.

Considérant que les principes posés en matière de protection des données personnelles pourraient soulever des difficultés pratiques quant au développement du projet d'AeL, une disposition spécifique valable durant une période transitoire fut introduite dans la LIPAD. C'est ainsi que la loi 10555[6] a introduit l'article 69 intitulé « Disposition expérimentale relative à l'administration en ligne » précisant :

«Dérogations

[1] Les institutions publiques sont autorisées à déroger à titre exceptionnel aux articles 35, 36, 38, 39, 40 et 41, dans les limites des alinéas 2 et 3 et dans la mesure nécessaire à la mise en œuvre, à l'exploitation et au développement des 10 prestations d'impulsion prioritaires du programme d'administration en ligne ayant fait l'objet de la loi ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne, du 26 juin 2008.

[2] La dérogation visée à l'alinéa 1 concerne :

a) l'exigence de tâches « légales », en application de l'article 35, alinéa 1 in fine;
b) le caractère « nécessaire » du traitement en vue de l'accomplissement des tâches légales, au sens des articles 35, alinéas 1 et 2, 36, alinéa 1, lettre a, et 41, alinéa 1, lettre a;
c) le caractère « absolument indispensable » du traitement pour l'accomplissement de la tâche légale, en application de l'article 35, alinéa 2;
d) l'exigence d'un « lien matériel étroit » entre différentes tâches prévues par des législations différentes en vue de permettre l'utilisation du numéro AVS, au sens de l'article 35, alinéa 4, 2e phrase;
e) le caractère « reconnaissable » de la collecte prévue par l'article 38, alinéa 1;
f) la démonstration par l'institution requérante d'un traitement conforme aux articles 35 à 38 entre institutions publiques soumises à la loi, en application de l'article 39, alinéa 1, lettre a, et sa vérification par l'autorité requise, en application de l'article 39, alinéa 2 ab initio;
g) la communication subséquente au responsable, au sens de l'article 39, alinéa 2;
h) l'obligation de consultation préalable des personnes concernées, au sens de l'article 39, alinéa 10.

[3] Dans le cadre de la mise en œuvre, de l'exploitation et du développement des 10 prestations d'impulsion visées à l'alinéa 1, les institutions publiques soumises tant à la présente loi qu'à la loi sur la gestion administrative et financière de l'Etat de Genève, du 7 octobre 1993, sont également autorisées :

a) à se prévaloir de l'article 2A, alinéa 1, de la loi sur la gestion administrative et financière de l'Etat de Genève, du 7 octobre 1993, même lorsque les informations ou les documents sollicités contiennent des données personnelles;
b) à ne pas appliquer la procédure prévue aux articles 39, alinéas 1, 2, 3, 10 et 11.

[4] Les compétences du préposé cantonal selon l'article 56 sont réservées.

[5] Loi [de la république et canton de Genève] du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD; RSG A 2 08) (http://www.ge.ch/legislation/rsg/f/s/rsg_a2_08.html , site consulté le 9 septembre 2013)

[6] PL 10555, Projet de loi modifiant la loi sur l'information du public, l'accès aux documents et la protection desdonnées personnelles (LIPAD) (A 2 08), Genève, 2 octobre 2009, (http://www.ge.ch/grandconseil/data/texte/PL10555.pdf site consulté le 9 septembre 2013).

But

[5] La présente disposition a un caractère expérimental, au sens de la loi concernant la législation expérimentale, du 14 décembre 1995. Elle a pour but d'évaluer la pertinence des options retenues en matière de traitement et de communication des données personnelles par les institutions publiques en charge de la mise en œuvre du programme d'administration en ligne, ainsi que la justification des dérogations consenties aux alinéas 2 et 3, compte tenu notamment :

a) des contraintes techniques et opérationnelles de l'administration;
b) des buts de la présente loi;
c) des besoins des utilisateurs, de l'utilité et de la fréquence du recours aux solutions offertes au public.

Information

[6] Les utilisateurs sont informés de la présente dérogation.

Durée de validité

[7] La présente disposition est valable pour toute la période postérieure à la loi ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne, du 26 juin 2008, jusqu'au 31 décembre 2015.

Rapports d'évaluation

[8] Un an au plus tard avant l'expiration de la validité de la présente disposition, doivent être remis au bureau du Grand Conseil :

a) un rapport du Conseil d'Etat détaillant pour chacune des 10 prestations visées à l'alinéa 1, si, dans quelle mesure et pourquoi leur développement, leur exploitation ou leur évolution ont impliqué un recours à la présente disposition dérogatoire, ainsi qu'une évaluation des effets de l'expérience conduite en considération des critères visés à l'alinéa 5, accompagné cas échéant d'un projet de loi visant à ancrer durablement dans la législation tout ou partie des éventuelles dérogations qui s'imposent;
b) un rapport du préposé cantonal évaluant l'impact des prestations en ligne offertes sous l'angle des prescriptions exigées à la présente loi, avec des recommandations quant à l'opportunité de modifier ou non la législation pour permettre d'autoriser de manière durable les éventuelles dérogations expérimentées dans le cadre du programme d'administration en ligne;
c) un rapport de la commission consultative en matière de protection des données, de transparence et d'archives publiques prenant position, sous l'angle tant de la présente loi que de la loi sur les archives publiques, du 1er décembre 2000, sur l'expérience conduite en considération des critères visés à l'alinéa 5.

Décision du Grand Conseil

[9] Après réception des rapports prévus à l'alinéa 8, mais avant l'expiration de la validité de la présente disposition, le Grand Conseil vote sur le ou les éventuels projets de loi qui lui sont soumis parallèlement en application de l'alinéa 8, lettre a».

Lors des débats, et comme cela ressort du rapport de la commission judiciaire et de police au PL 10555, il a été jugé important que les compétences ordinaires du préposé cantonal selon l'article 56 LIPAD soient réservées, tout comme il a été considéré nécessaire que les utilisateurs de l'administration en ligne soient informés des dérogations faites à la LIPAD[7].

A ce titre, le Bureau des préposé-es à la protection des données et à la transparence (ci-après PPDT) a jugé nécessaire de clarifier la manière de mettre en œuvre les dérogations

[7] Secrétariat du Grand Conseil (7 septembre 2010), « *rapport de la Commission judiciaire et de la police chargée d'étudier le projet de loi du Conseil d'Etat modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08)* »
(http://www.ge.ch/grandconseil/data/texte/PL10555A.pdf , site consulté le 8 novembre 2013)

prévues aux règles sur la protection des données en publiant une prise de position le 28 octobre 2011[8].

Dans celle-ci, il y est rappelé que cette disposition expérimentale n'est en aucun cas un blanc-seing à l'administration en ligne. Les dérogations sont volontairement larges pour éviter que l'expérience de l'administration en ligne ne soit vouée à l'échec mais doivent n'être utilisées qu'en cas de nécessité. Les données personnelles des citoyennes et des citoyens souhaitant bénéficier de l'une ou de l'autre de ces dix prestations doivent être collectées en tant qu'elles sont nécessaires à l'octroi de l'une ou l'autre de ces prestations, et utilisées par les différents services dans cette même mesure. L'objectif de cette disposition provisoire est donc double : il s'agit de ne pas entraver le développement de l'AeL mais également de déterminer quelles sont les dérogations qui sont réellement nécessaires à sa bonne marche.

Ainsi, au 31 décembre 2015, date de fin de validité de cette disposition expérimentale, il conviendra d'avoir isolé les besoins juridiques réels de l'administration en ligne afin de la doter d'un encadrement qui assure son bon fonctionnement sans pour autant supprimer les droits des citoyennes et des citoyens en matière d'information et de protection des données.

3.Les prestations et les acteurs de l'AeL

3.1 Les dix prestations initiales

Dans le texte accompagnant le projet de loi 10177 (AeL), le Conseil d'Etat expliquait souhaiter mettre en œuvre une AeL efficiente et attractive. Pour ce faire, il désirait développer une dizaine de prestations initiales identifiées comme étant les plus demandées et les plus rentables et ceci : «*pour inciter les usagers à les employer, puis pour les fidéliser et les amener à participer à une communauté active permettant de faire évoluer l`AeL*»[9].

Ces dix prestations et leur définition selon le PL 10177 sont les suivantes :

1. P1. Impôts en ligne
Département responsable de la prestation : Département des finances (DF)
Service responsable : Administration fiscale cantonale (AFC)
Chef de projet : Gaël Le Bourhis

Il s'agit d'offrir au contribuable la possibilité d'interagir directement avec l'administration fiscale notamment pour envoyer sa déclaration, transmettre des documents, demander des

[8] Bureau des préposé-es à la protection des données et à la transparence (2011), « *MISE EN OEUVRE DE L'ART. 69 LIPAD SELON LE PPDT DANS LE CADRE DE L'ADMINISTRATION EN LIGNE*» (http://www.ge.ch/ppdt/doc/documentations/PPDT_Prise_de_position_2011_I_013_Art_69_LIPAD_mise_en_oeuvre_selon_PPDT_V.pdf , site consulté 8 novembre 2013)

[9] PL 10177, *projet de loi ouvrant un crédit d'investissement de 30 850 000 F pour le développement de l'administration en ligne*, Genève, 28 novembre 2007, p. 14.

duplicata ou attestations, consulter ses taxations antérieures (bordereaux, avis de taxation, répartitions intercantonales, relevés de compte, etc.), consulter et imprimer tous les documents tels que relevés de compte, relevés d'intérêt, relevés d'arrangement, payer en ligne, etc.

2. P2. Impôts à la source

Département responsable de la prestation : Département des finances (DF)
Service responsable : Administration fiscale cantonale (AFC)
Chef de projet : Gaël Le Bourhis

Ce projet facilitera sensiblement la gestion de l'impôt à la source pour les personnes morales. Elles pourront notamment remplir ou établir les attestations par téléchargement, annoncer l'arrivée d'un employé à la source, remplir des formulaires, annoncer un changement de situation.

3. P3. L'aide sociale en ligne

Département responsable de la prestation : Département de la solidarité et de l'emploi (DSE)
Service responsable : Direction générale de l'action sociale (DGAS)
Chef de projet : Alexandre Massot

Le portail de l'aide sociale permettra aux citoyens d'avoir accès de façon sécurisée à leur dossier personnel en lien avec l'Etat de Genève. Pour le citoyen, ce dossier revêt deux aspects. En premier lieu pour les personnes ne bénéficiant pas de prestations, l'accès à leur revenu déterminant unifié (RDU) permettra d'orienter leurs demandes de prestations et d'initier virtuellement celles-ci auprès des services sociaux concernés. Par ailleurs, pour les citoyens bénéficiant déjà de prestations sociales, ils pourront suivre celles-ci et auront la possibilité d'échanger des informations par ce canal avec les organismes sociaux. En outre, le bénéficiaire n'aura plus à transmettre les documents et informations déjà connues de l'administration, simplifiant ainsi la tâche de saisie de l'administration.

4. P4. Portail de la population

Département responsable de la prestation : Département de la sécurité (DS)
Service responsable : Office cantonal de la population (OCPM)
Chef de projet : Pedro Carnino

Le portail de la population offrira des prestations tant au citoyen qu'à certaines catégories socioprofessionnelles. Il sera ainsi possible de consulter le « Savoir en ligne » et rechercher l'adresse de toute personne privée. Certains établissements privés (par exemple, les études de notaires) pourront bénéficier d'un accès direct mais ciblé et limité à des informations contenues dans la base de données de la population. Les communes pourront mettre à jour la liste des jurés des tribunaux et les régies pourront communiquer en ligne les changements d'adresses.

5. P5. L'e-service des automobiles

Département responsable de la prestation : Département de la Sécurité (DS)
Service responsable : Office cantonal des véhicules (OCV)
Chef de projet : Jean-Claude Baumann

Concernant les citoyens, le projet permettra à l'office cantonal des véhicules d'offrir de nouvelles prestations électroniques notamment la facturation et le paiement en ligne, la demande d'attestation, la demande d'autorisation spéciale, etc.
Concernant l'administration elle-même, cette prestation permettra d'échanger par voie électronique des informations avec différents secteurs de l'administration (rapports de police / contraventions, réquisitions de poursuite, dossiers au Tribunal administratif, etc).

6. P6. Autorisation de manifestation

Département responsable de la prestation : Département des affaires régionales, de l'économie et de la santé (DARES)
Service responsable : Service du commerce (SCOM)
Chef de projet : Alexande Massot

Il s'agit de permettre à quiconque de déposer une demande d'autorisation de manifestation avec la possibilité de modifier, compléter ou supprimer sa demande en ligne. L'organisateur pourra accéder aux informations pour le suivi et l'historique de sa demande, payer en ligne et imprimer lui-même l'autorisation.

7. P7. PME Genève

Département responsable de la prestation : Département des affaires régionales, de l'économie et de la santé (DARES)
Service responsable : Direction régionale des affaires économiques (DGAE)
Chef de projet : Alexande Massot

Il s'agit d'une plateforme d'information et de gestion des procédures administratives à l'intention des entreprises. Elle permettra de rapprocher les personnes morales et les entreprises de l'administration en intensifiant la simplification de l'interactivité des procédures.
Elles pourront enregistrer les modifications (RC, AVS, TVA, SUVA, statistiques, etc.) qui les concernent directement en ligne (en phase avec la stratégie nationale de la Confédération), accéder aux informations et aux formulaires nécessaires à leur activité (juridique, assurances sociales, permis de travail, fiscalité, aides financières, etc.).
En outre, les pré-requis juridiques pour exercer une profession réglementée sur le canton de Genève (40 professions concernées, par exemple : médecins, pharmaciens, ramoneurs, restaurateurs, vente de seconde main, hôteliers, aides-dentiste, courtiers en assurances, etc.) seront disponibles et l'usager pourra remplir les « formulaires » nécessaires en ligne.

8. P8. Plan d'affectation du sol et autorisations de construire

Département responsable de la prestation : Département de l'urbanisme (DU)
Service responsable : Direction des autorisation de construire (DAC)
Chef de projet : Jean-Michel Just

Ce projet vise à simplifier pour le requérant ou son mandataire le recueil de certaines des informations constitutives des dossiers, notamment par l'accès à des données administratives, la mise au point de formulaires en ligne et la production des extraits du plan du registre foncier et du plan d'ensemble certifiés conformes. Il a également pour objectif de

permettre la numérisation des données (plans, documents et études d'impact sur l'environnement) communiquées à l'administration, pour autant que cette dernière soit de nature à simplifier et accélérer les procédures.
Par ailleurs, le projet doit aboutir à un meilleur et plus rapide échange des informations et données des projets, et des études d'impact sur l'environnement qui les accompagnent le cas échéant, entre les services compétents de l'administration et les instances de préavis.

9. P9. Gestion administrative des praticiens

Département responsable de la prestation : Département des affaires régionales, de l'économie et de la santé (DARES)
Service responsable : Direction générale de la santé (DGS)
Chef de projet : Alexandre Massot

Les médecins, pharmaciens, droguistes et autres laborantins sont quelque 20'000 à Genève.
Le projet leur permettra de soumettre une demande de droit de pratique ou d'autorisation d'exploiter et de suivre leur dossier en ligne, de modifier et mettre à jour les informations les concernant.
Il permettra également d'informer les internautes sur les types et localisation des différents praticiens.

10. P10. Espace école en ligne

Département responsable de la prestation : Département de l'instruction publique (DIP)
Service responsable : Service écoles-médias (SEM)
Chef de projet : Nicolas Deprez

Cet ambitieux projet vise à permettre l'enseignement à distance (e-learning), à ouvrir des espaces collaboratifs d'enseignement à disposition des élèves et des enseignants et à fournir des ressources d'enseignement en ligne et des services Web pour l'ensemble des disciplines.
Il permettra des échanges et des interactions en ligne avec des écoles distantes (par exemple, interaction orale entre des élèves genevois et étrangers dans le cadre de l'apprentissage d'une langue) et fournira un support en ligne aux enseignants et aux élèves.

3.2 Les autres prestations en ligne développées

3.3 Les acteurs de l'AeL

3.3.1 Comité de pilotage (Copil) :

Au lancement du programme, selon l'arrêté départemental du DCTI[10] du 31 octobre 2008,, le Copil était en charge du pilotage stratégique du projet AeL et occupait le rôle d'organe décisionnel. Ses responsabilités étaient les suivantes :

- traduire la politique du Conseil d'Etat en objectifs opérationnels
- décider de l'affectation du budget annuel de l'AeL

[10] Devenu DU pour les constructions et DS pour les systèmes d'information (SI)

- conduire le programme, et en particulier maintenir le portefeuille des projets AeL dans le canton de Genève
- coordonner les actions du Centre des technologies de l'information (CTI) et des structures transversales en la matière
- fixer les priorités
- prioriser les prestations à réaliser en ligne sur la base des propositions départementales
- valider les analyses relevant de plusieurs départements
- valider l'ordre de réalisation des prestations
- définir les stratégies de développement et de déploiement de l'AeL
- définir les développements de l'infrastructure
- élaborer les modifications législatives nécessaires en partenariat avec les instances concernées
- mesurer l'avancement du programme et proposer des options stratégiques au Conseil d'Etat
- tenir le conseiller d'Etat en charge du DCTI (aujourd'hui DS) informé de l'avancement des travaux par un rapport trimestriel

Sous l'impulsion de son président, le Copil a pris, depuis fin 2010, une orientation plus opérationnelle et moins stratégique. Ainsi, les secrétaires généraux, à l'exception de celui du DS, ont été remplacés par les directeurs généraux en charge des prestations à réaliser. Aujourd'hui, la composition du Copil est la suivante:

- Le secrétaire général adjoint du département de la sécurité, actuellement président du Copil
- Le directeur général de l'administration fiscale cantonale
- Le directeur général du département de la solidarité et de l'emploi
- Le directeur général du département de la sécurité
- Le directeur général du département des affaires régionales, de l'économie et de la santé
- La directrice des autorisations de construire
- Le médecin cantonal
- Le directeur du service écoles-médias du département de l'instruction publique, de la culture et du sport.
- Le directeur général de l'office du personnel de l'Etat (OPE)
- Le directeur des finances, logistique, systèmes d'information et opérations de vote de la chancellerie d'Etat (place pour l'heure vacante depuis le départ du titulaire)
- Le directeur des systèmes d'information, de la logistique et de l'organisation (DS)
- Le directeur général des systèmes d'information (DS)
- Le juriste de l'état-major de la Direction générale des systèmes d'information (DGSI)
- Le directeur du programme AeL

3.3.2 La direction du programme :

Elle a pour tâche de rapporter au comité de pilotage afin d'assurer la livraison du programme. Son orientation est purement opérationnelle et elle chapeaute les différents projets. Son directeur est également membre du Copil. Sa composition est la suivante :

- Le directeur du programme AeL
- Le directeur adjoint de l'AeL
- Un project management officer
- La responsable de la communication
- La responsable de l'accompagnement au changement
- Du responsable de l'accessibilité

3.3.3 Groupe "point de cohérence" :

Prévu par la méthodologie HERMES[11], ce groupe vise à aider les projets à s'insérer dans le paysage des systèmes d'information de l'Etat. Il représente une étape incontournable avant le lancement d'une nouvelle prestation. Son objectif consiste en la vérification d'un développement harmonieux des prestations, respectueuses de l'architecture globale. Ce groupe formule des recommandations à l'attention des chefs de projet qui s'expriment devant lui. Ces chefs de projet sont ensuite appelés à prendre position et déclarer la suite qu'ils ont donné aux recommandations lors d'un second passage devant le point de cohérence. Ce dernier est composé de représentants de différents corps de métiers en informatique :

- Présidente du groupe : la responsable du Centre d'expertise des systèmes d'information (CESI) de la DGSI
- Un responsable de service, représentant de la direction Services Clients de la DGSI
- Un responsable du service Architecture et composants transversaux, du Service Clients de la DGSI
- Deux représentants de la Direction de la sécurité de l'information et des évènements spéciaux de la DGSI
- Un représentant de la Gestion des données et des informations, de la Direction Infrastructure de la DGSI
-

3.3.3 Datatrans :

Datatrans[12] est une société privée, domiciliée en Suisse, spécialisée dans le paiement en ligne. Elle occupe la position de leader sur le marché helvétique et compte notamment parmi ses clients les chemins de fer fédéraux (CFF), le Touring club suisse (TCS), Kuoni Voyages SA ou encore Swiss International Airlines SA[13]. Elle occupe également un rôle de partenaire de l'Etat de Genève en prenant en charge les paiements en ligne réalisés dans le cadre de l'AeL.

Le chapitre sur le fonctionnement de l'AeL détaille plus précisément son rôle dans le cadre de ce projet.

[11] HERMES, «***Conduite et déroulement de projets dans ledomaine des technologies de l'information et de la communication (TIC)*** **», Édition 2003, p. 13.**
[12] Datatrans SA, Stadelhoferstrasse 33, 8001 Zurich, Tél. +41 44 256 81 91, Fax +41 44 256 81 98
[13] Datatrans, « *Travel, tourisme, transport* » (http://www.datatrans.ch/en/References/Travel-tourism-transport/ , site consulté le 2 octobre 2013)

3.3.4 Postfinance :

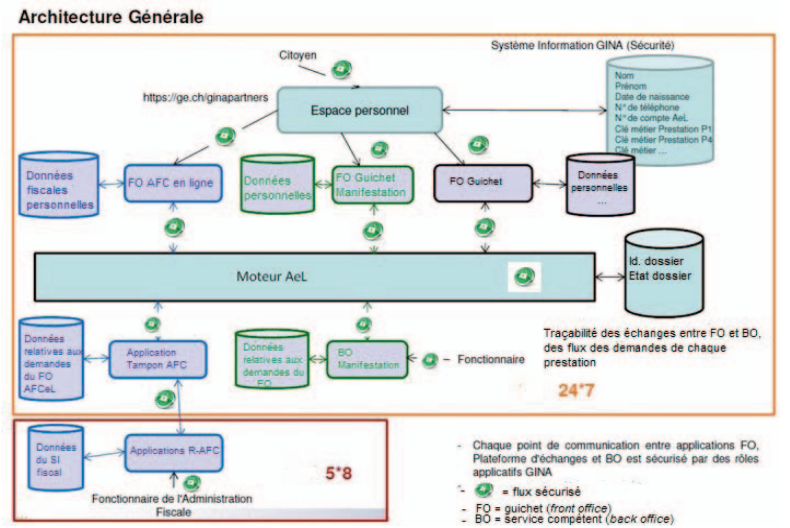
4. Fonctionnement de l'AeL

Ce chapitre a pour but de présenter le fonctionnement de l'AeL en termes de flux, de mettre en évidence ceux qui sont sécurisés (représentés par un cadenas vert sur les illustrations) et quelles données sont transmises à quels acteurs.
Les trois graphiques commentés ici sont : le fonctionnement général de l'AeL, le cas des formulaires électroniques soumis sans authentification préalable du citoyen et l'Architecture ePaiement. Ils ont été produits et élaborés à l'attention du PPDT par M. Barrès, Responsable de secteur administration des composants transversaux,

4.1 Architecture générale

Le graphique "Architecture Générale" illustre le fonctionnement de l'AeL en terme de flux, de l'impulsion du citoyen au traitement de sa demande par le service compétent.

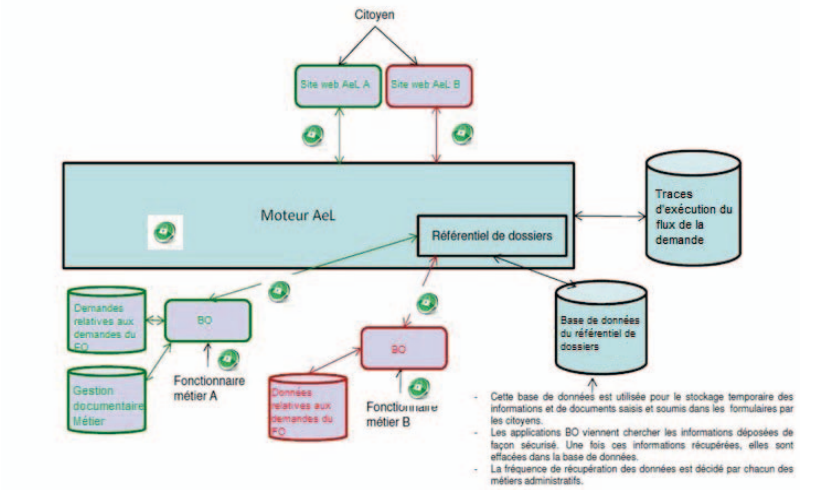
1) La première étape consiste donc en la connexion du citoyen à son espace personnel. Pour cela, il se rend sur la page d'accueil de l'AeL et utilise ses identifiants ainsi que le code qui lui est alors transmis par SMS. La durée de validité de ce code est de trois minutes. Les informations contenues sur cet espace (nom, prénom, date de naissance, numéro de téléphone, numéro de compte AeL ainsi que les différentes clés métiers des prestations) sont stockées sur le système d'information GINA, qui gère la sécurité au sein de la DGSI.
2) En second lieu, le citoyen sélectionne la prestation désirée, ce qui l'amène auprès du guichet (*front office*, abrégé FO) de celle-ci. Chacun de ces *front offices* dispose de sa propre base de données à laquelle il est le seul à pouvoir accéder. C'est à ce niveau que sont stockés les brouillons des demandes. Concernant les éventuelles pièces-jointes, si l'administration concernée ne dispose pas de l'infrastructure nécessaire, elles sont temporairement stockées sur le moteur AeL. Seul le rédacteur du brouillon peut y accéder et l'existence de demande en état brouillon est inconnue de l'administration. Lors du passage en état soumis du formulaire par le citoyen, ces fichiers sont envoyés dans l'application du service compétent (*back office*, abrégé BO) et supprimés du moteur AeL.
3) La communication entre le *front office* et *le back office* se fait à travers le moteur AeL qui, lui, stocke un identifiant dossier et un état du dossier, ce qui permet la traçabilité des échanges entre le *front* et le *back office*. Le moteur AeL est "aveugle" au contenu de ce qui transite à travers lui, ce afin de garantir que seuls les services compétents ont accès aux informations transmises.
4) L'AeL est disponible sur une base de 24h sur 24 et 7 jours sur 7 (24/7). Toutefois, certains *back offices* comme l'administration fiscale ne disposent pas de la même disponibilité (8/5). Pour assurer la continuité du service, des tampons sous responsabilité métier sont établis pour stocker les demandes survenues durant une période d'indisponibilité. Seule l'administration compétente peut accéder à ces tampons.



4.2 Formulaires électroniques soumis sans authentification préalable du citoyen

1) La demande du citoyen n'est pas entreposée en brouillon sur le guichet (*front office*) mais sur le moteur AeL lui-même.
2) Lors de l'envoi de la demande, le service compétent (*back office*) vient télécharger le dossier de façon sécurisée avant de le supprimer du moteur AeL. L'administration compétente établit la régularité à laquelle elle vient récupérer les demandes stockées sur le moteur AeL.

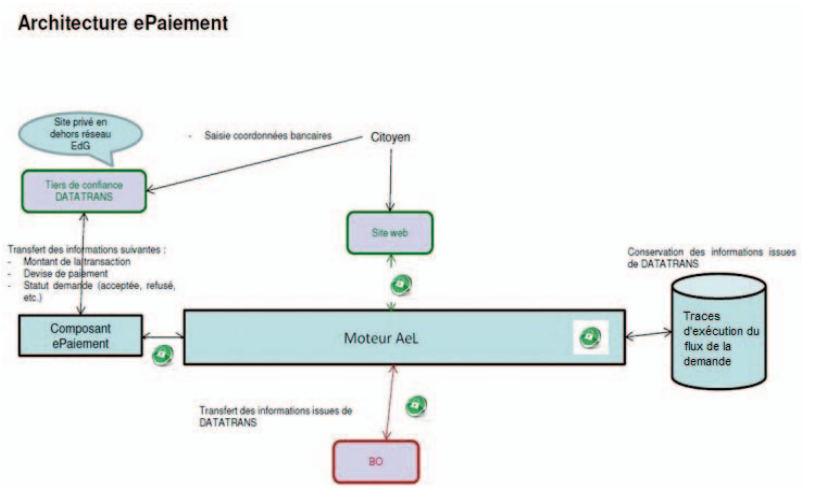
Architecture : cas des formulaires électroniques sans authentification préalable du citoyen



4.3 Architecture ePaiement

Dans le cas d'un formulaire payant sans authentification préalable:

1) Le citoyen est automatiquement envoyé sur le site internet de Datatrans lorsqu'il lui est demandé de saisir ses coordonnées bancaires. La saisie des coordonnées bancaires ne se déroule donc pas sur le site de l'Etat de Genève mais celui de Datatrans, qui est un partenaire privé de l'Etat.
2) Les seules informations renvoyées à l'AeL par Datatrans sont le montant de la transaction, la devise de paiement et le statut de la demande (acceptée, refusée, etc.). Ces informations sont stockées sur le moteur AeL.
3) Le service métier compétent (BO) vient récupérer ces données sur le moteur AeL, d'où elles sont ensuite effacées.



5. Les enjeux et les risques

Tout l'enjeu de l'AeL réside dans sa capacité à faire de sorte que l'administration soit efficiente, apporte des réponses techniques conformes à l'évolution de la société en garantissant que les droits de personnes soient protégés. Les inquiétudes des particuliers d'atteinte à leur vie privée sont parfaitement légitimes. Souvenons-nous que les législations relatives à la protection des données sont nées du souci de protéger les personnes physiques face au développement des grands fichiers informatisés recueillant maintes informations sur la population. En Suisse, à la fin des années 80, la révélation de l'affaire dite des fiches tenues par la police fédérale avait fait grand bruit[14]. A l'heure actuelle, toute personne fait l'objet d'un traitement de données dans de multiples domaines de la vie quotidienne : en tant qu'élève, apprenti ou étudiant, puis en tant que salarié ou indépendant, contribuable, assuré, personne au bénéfice d'aides sociales, chômeur, auteur d'une infraction, détenteur d'un abonnement auprès d'une institution publique, etc.

L'objectif du présent rapport est de réaliser un état des lieux, sous l'angle de la conformité à la LIPAD. A ce titre, un certain nombre d'écueils, classés selon leur degré de risque, avaient été identifiés par le PPDT lors de sa prise de position de 2011. En ayant à l'esprit que les dérogations à la LIPAD prévues par son article 69 s'achèvent à la fin de l'année 2015, il

[14] Les autorités fédérales suisses ainsi que les polices cantonales avaient observé environ 900 000 personnes sur le territoire suisse (700 000 personnes et organisations selon les sources officielles) de façon plus ou moins active et avaient ainsi produit des fiches d'information sur ces personnes. Voir le point final du 10 janvier 2001 fait par le Conseil fédéral sur http://www.admin.ch/aktuell/00089/index.html?lang=fr&msg-id=23132. Une affaire qualifiée d'anecdote aujourd'hui par le Préposé fédéral Hans-Peter Thür face aux révélations concernant le programme d'espionnage américain sur les réseaux informatiques du monde entier, Hebdo, 13 juin 2013. .

convient d'identifier *ex ante* le degré des risques pouvant découler d'un non respect des autres articles de la LIPAD. Cette démarche présente un double intérêt. Tout d'abord, c'est un moyen d'ouvrir des pistes de réflexion quant à la suite législative à donner à l'AeL. En outre, elle permet de déterminer dans quelle mesure certaines dérogations se révèlent pertinentes et/ou nécessaires et quelles frontières ne devraient pas être franchies. En ayant à l'esprit ces mises en garde, on peut alors tracer les lignes d'une AeL à la fois efficace, fonctionnelle et protégeant de manière satisfaisante les données personnelles des citoyennes et des citoyens.

Ainsi, à titre illustratif, le non respect de l'article 35 al.1 in fine de la LIPAD[15] présente un risque faible, puisque cela permet d'aller plus loin que les seules tâches strictement mentionnées par la loi, ce qui peut se concevoir alors que l'administration cherche à offrir, dans le cadre de cette expérience, de nouvelles prestations. Cependant, il n'en va pas de même pour l'article 35 al.2[16] concernant les données sensibles. Soit leur traitement est absolument indispensable, soit il est nécessaire mais alors autorisé par la personne concernée. Cette dérogation là ne devrait donc pas trouver d'application concrète dans l'AeL.

[15] Art. 35 al. 1 LIPAD (http://www.ge.ch/legislation/rsg/f/s/rsg_a2_08.html , site consulté le 9 septembre 2013)
[16] Art 35 al. 2 LIPAD (http://www.ge.ch/legislation/rsg/f/s/rsg_a2_08.html , site consulté le 9 septembre 2013)

Articles de la LIPAD concernés par la dérogation légale	Description de la dérogation	Mise en oeuvre concrète (dérogation appliquée)	Degré de risque (**F**aible, **M**oyen, **E**levé)
Article 35 al. 1 in fine	Exigences d'une tâche légale	Permet d'aller plus loin que les seules tâches strictement mentionnées par la loi, d° aug-menter le service au citoyen. Ex : disposer d'un dossier fiscal dématérialisé	**F**
Article 35 al. 1 et 2 36 al. 1 let. A 41 al. 1 let. A	Caractère nécessaire du traitement pour l'accomplissement d'une tâche légale	Dérogation purement théorique, qui ne devrait pas trouver d°application concrète : le caractère nécessaire du traitement pour livrer une prestation X est à la base de la protection des données (partie du principe de proportionnalité)	**E**
Article 35 al. 2	Caractère absolument indispensable du traitement pour l'accomplissement d'une tâche légale	Dérogation purement théorique, qui ne devrait pas trouver d°application concrète : pour les d.p.sensibles, soit le traitement est absolument indispensable, soit il est nécessaire et autorisé par la personne concernée	**E**
Article 35 al. 4, 2ème phrase	Exigence d'un lien matériel étroit entre les tâches pour l'utilisation du NAVS13	Dérogation purement théorique, qui ne devrait pas trouver d°application concrète : pas de base légale a une utilisation généralisée du NAVS13 par l'administration. La législation à venir va dans ce sens (numéro d'identification commun)	**M**
Article 38 al. 1	Caractère reconnaissable de la collecte	Dérogation purement théorique, qui ne devrait pas trouver d°application concrète : la transparence de la collecte est à la base de la protection des données. Cette condition est par ailleurs facile à mettre en œuvre dans l'AeL. Le principe de l'exactitude des données (pas de dérogation prévue) justifie que les gestionnaires vérifient les d.p. en leurs mains avec le citoyen, et l'informe de l'usage fait de ses d.p.	**M**
Article 39 al. 1 let. a	Preuve d'un traitement conforme par l'institution requérante	Une procédure simplifiée pour la communication des d.p. entre institutions découle directement de l'AeL, puisque les d.p. sont mises à disposition de celles-ci via un socle commun. La sécurité des données ne peut faire l'objet d'aucune dérogation, l'art. 69 LIPAD ne le prévoit d'ailleurs pas : toutes les institutions doivent garantir la disponibilité, l'intégrité et la confidentialité des d.p.	**F** (avec gestion des droits d'accès) à **E** (absence de gestion des droits d'accès)
Article 39 al. 2	Communication subséquente au responsable LIPAD(après communication entre institutions publiques)	Vu la communication automatique par le biais du socle, on peut renoncer à la communication systématique au responsable LIPAD	**F**
Article 39 al. 10	Obligation de consultation préalable des personnes concernées	Dérogation purement théorique, qui ne devrait pas trouver d°application concrète : la communication de données personnelles à un tiers de droit privé n'est pas une prestation de l'AeL. Si elle devait le devenir, les règles prévues à l'art. 39 al. 10 (notamment consultation du tiers ou saisine du PPDT) devraient continuer de s'ap-pliquer. En tous les cas ces demandes devraient être traitées par les responsables LIPAD, et non les gestionnaires AeL.	**M**

Pour veiller au respect de la protection des données, la loi genevoise a institué une approche double, à savoir d'une part, un contrôle d'une autorité indépendante et neutre ayant la vocation de veiller à la transparence des traitements de données personnelles effectués par les institutions publiques - annonce des fichiers dans le catalogue des fichiers - contrôles a posteriori par le biais de visites sur le terrain et, d'autre part, les contrôles qui peuvent être effectués directement par les personnes concernées :

- Le contrôle par le particulier suppose la connaissance préalable des traitements existants
- Le droit d'accès permet de connaître les données personnelles saisies
- Le droit de rectification ou de suppression est le corollaire du droit d'accès.

Les fichiers connectés ensemble
Les numéros d'identification communs
Les modalités d'authentification des usagers
Le recours à la signature électronique

Les données cryptées
L'accompagnement des usagers - sécurité juridique, exercice des droits
Maîtriser les données personnelles
Une fonction de pilotage, d'encadrement et de coordination capitale
Sécuriser les échanges

6. Démarches d'évaluation à la conformité et outils

Dans le but d'évaluer la conformité LIPAD de l'AeL, le PPDT a fait usage tant de sources primaires que secondaires. A ce titre, le PPDT a réalisé de multiples entretiens semi-directifs[17] avec les différents acteurs impliqués dans le projet. En outre, un questionnaire visant à déterminer l'état atteint par rapport à l'état dans lequel le projet devrait être au plan de la conformité à la LIPAD (ci-après le degré de maturité LIPAD) au sein des différentes prestations a été transmis à l'ensemble des chefs de projet. Le tableau des risques issu de la prise de position du PPDT de 2011 était annexé à ce questionnaire. De plus, un tableau visant à établir le cheminement des données a également été établi pour chaque prestation. Le rédacteur a également recouru à une approche *client mystère* afin de tester concrètement l'AeL et d'identifier, en l'état, ses forces et ses faiblesses. Enfin, en partenariat avec le président du COPIL de l'AeL, une réunion d'échanges et de réflexion a été organisée le 27 novembre 2013. Étaient conviés les membres du COPIL AeL, les responsables LIPAD départementaux concernés, les membres du Collège spécialisé des systèmes d'information (ci-après CSSI), les responsables sécurité des systèmes d'informations (ci-après responsables sécurité SI), les responsables de prestations, les chefs de projet et le groupe "Point de cohérence". A cette occasion, l'objectif et le canevas du présent rapport ont été présentés.

A l'exception des personnes approchées dans le cadre de l'approche *client mystère*, chaque acteur contacté par les PPDT dans le cadre de ce rapport a été informé de la volonté de fournir un accompagnement au projet afin d'identifier, au plus tôt, les aspects problématiques et les moyens de réponse pouvant être mobilisés.

La suite de ce chapitre présente succinctement le questionnaire ainsi que le tableau de cheminement des données.

6.1 Questionnaires

Les questionnaires élaborés par les PPDT[18] se présentaient sous la forme d'un tableau à double entrée, la ligne horizontale se divisant selon les 10 prestations de base ainsi que le moteur AeL tandis que la ligne verticale comprenait les différentes questions. Il était indiqué sur le questionnaire lui-même que 5 réponses différentes pouvaient être fournies pour déterminer le niveau de maturité des prestations, à savoir :

0 = Non existant

[17] Technique de recueil d'informations qualitatives permettant de rassembler des faits et opinions des personnes interrogées sur un sujet donné (définition fournie par Euréval, Centre Européen d'Expertise et d'Evaluation, http://www.eureval.fr/IMG/File/FT_Entretien.pdf , site consulté le 28 novembre 2013)
[18] Voir modèle ci-annexé.

1 = En projet
2 = En cours de mise en œuvre
3 = Partiellement implémenté
4 = Totalement implémenté

En fin de document, possibilité était offerte de joindre un commentaire à chacune des questions posées.

Ces questions s'élevaient au nombre de 34, classées dans 9 catégories distinctes. Elles comprenaient une partie concernant la protection des données en générale et les 8 risques concernant les dérogations identifiés par les PPDT lors de leur prise de position de 2011. Par souci de clarté, le tableau des risques établi par le PPDT était annexé au questionnaire. La liste des 9 catégories était donc la suivante :

1. *Protection des données en général*
2. *Dérogation à : Exigences d'une tâche légale (article 35 al. 1 in fine)*
3. *Dérogation à : Caractère nécessaire du traitement pour l'accomplissement d'une tâche légale (article 35 al 1 et 2, 36 al. 1 let. A, 41 al. 1 let. A)*
4. *Dérogation à: Caractère absolument indispensable du traitement pour l'accomplissement d'une tâche légale (article 35 al. 2)*
5. *Dérogation à : Exigence d'un lien matériel étroit entre les tâches pour l'utilisation du NAVS13 (article 35 al. 4 2ème phase)*
6. *Dérogation à : Caractère reconnaissable de la collecte (article 38 al. 1.)*
7. *Dérogation à : Preuve d'un traitement conforme par l'institution requérante (article 39 al. 1 let. A.)*
8. *Dérogation à : Communication subséquente au responsable LIPAD (après communication entre institutions publiques) (article 39 al. 2.)*
9. *Dérogation à : Obligation de consultation préalable des personnes concernées (article 39. al. 10.)*

L'objectif, annoncé dans la lettre d'accompagnement, était de déterminer le degré de conformité au cadre réglementaire LIPAD.

Les questionnaires furent, à titre préalable, transmis à la commission consultative en matière de protection des données, de transparence et d'archives publiques (CCPDTA) ainsi qu'aux responsables LIPAD départementaux concernés, afin qu'ils formulent d'éventuelles remarques. Faute de commentaire de ces deux instances, les questionnaires furent ensuite transmis le 26 avril 2013 par le Directeur du Programme AeL aux différents chefs de produit (membres de la DGSI). Il était précisé qu'afin de répondre à certaines des questions il leur serait nécessaire de prendre contact tant avec les chefs de prestation (membres des départements concernés par les prestations) qu'avec les responsables LIPAD départementaux. Le retour pour les questionnaires seuls était fixé au 21 mai 2013, un délai supplémentaire jusqu'au 18 juin était fixé pour les documents demandés en annexe.

6.2 Tableau de cheminement des données

Le tableau de cheminement des données vise à suivre chaque élément ou groupe d'information, depuis la collecte jusqu'à son utilisation en déterminant :

1) Les catégories de données
2) Qui se charge de les collecter
3) Quels sont les droits d'accès au données
4) A quelle(s) fin(s) elles sont collectées
5) A qui les données sont éventuellement communiquées
6) Quel est leur lieu de conservation

Cette méthode s'inspire de celle pratiquée par le gouvernement canadien lors de ses évaluations des facteurs relatifs à la vie privée (ÉFVP) pour lesquelles il déclare que : «*…les détails nécessaires à la réalisation d'une évaluation des facteurs relatifs à la vie privée s'obtiennent en dressant un tableau détaillé du cheminement des données.*»[19]. Selon les propres termes du Secrétariat du Conseil du Trésor du Canada : «*L'ÉFVP est un processus qui aide les ministères et les organismes à déterminer si les nouvelles technologies, les systèmes d'information, les initiatives, ainsi que les politiques et les programmes proposés sont conformes aux exigences élémentaires en matière de protection de la vie privée. De plus, elle aide les organisations gouvernementales à prévoir la réaction du public face aux répercussions d'une proposition sur le respect de la vie privée, ce qui pourrait permettre d'éviter une coûteuse refonte des programmes, des services ou des processus*»[20]. Dans la mesure où le rapport intermédiaire élaboré par les PPDT vise à apporter un soutien au programme afin qu'à son terme, fin 2015, il soit possible de conclure à un succès, la méthode utilisée par le gouvernement canadien se révèle extrêmement pertinente dans le cas d'espèce.
Le tableau utilisé dans ce cadre par les autorités canadiennes a été modifié dans sa forme par le PPDT afin que la dénomination de ses catégories corresponde davantage au contexte genevois.

Catégorie de données personnelles y.c sensibles	**Collectées par**	**Utilisées par (droit d'accès)**	**But de la collecte**	**Communiquées à**	**Lieu de conservation**

[19] Secrétariat du Conseil du Trésor du Canada (2012), «*Archivée - Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée - Cadre de gestion des risques d'entrave à la vie privée*» (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12451&section=text , site consulté le 17 octobre 2013).
[20] Secrétariat du Conseil du Trésor du Canada (2012), «*Archivée - Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée - Cadre de gestion des risques d'entrave à la vie privée*» (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12451&section=text , site consulté le 17 octobre 2013).

Ce tableau a ensuite été transmis à M. Viganò, de la direction de la sécurité de l'information et des évènements spéciaux de la DGSI, qui a été à la rencontre des différents chefs de projet afin de le remplir avec eux, tout en apportant les éventuelles précisions nécessaires. Il était préconisé d'utiliser les sous catégories du catalogue des fichiers (Catfich) pour remplir le tableau. Dans certains cas, les chefs de projet ont également ajouté au tableau la référence à la déclaration de fichier concernant la prestation.

6.3 Résultats de l'analyse

a) Les questionnaires
Sur les 11 questionnaires envoyés, les 10 prestations de base et le moteur AeL, 8 ont été retournés au PPDT. Sur les questionnaires retournés, seuls 5 le sont de manière sûre et complète, 4 si l'on exclut le moteur AeL pour se focaliser sur les prestations. Il ressort de l'étude de ces documents que, malgré les indications contenues dans la lettre d'accompagnement, les réponses sont le fait des seuls chefs de produits (DGSI) sans participation des chefs de prestation (métier) ou des responsables LIPAD départementaux.
En particulier, les réponses apportées ne permettent pas de déterminer quelles dérogations sont concrètement utilisées *in fine* dans la mise en œuvre des différentes prestations. En effet, comme illustré dans le chapitre sur le fonctionnement de l'AeL, aucun acteur ne dispose, seul, d'une vue d'ensemble du processus des différentes prestations. La révolution initiée par l'AeL, en visant à établir l'administration de demain, implique la mise sur pied de nouvelles collaborations au sein de l'Etat. Par conséquent, parvenir à isoler les dérogations qui se révèlent pertinentes ou encore analyser la manière dont elles sont implémentées ne saurait être réalisé par l'étude de ces documents.

Malgré l'insuccès de la démarche ambitionnée, les informations ainsi collectées permettent tout de même de répondre partiellement à la question qui était posée, à savoir le degré de conformité LIPAD. En effet, les réponses obtenues mettent en évidence un manque de connaissance concernant le cadre posé par la LIPAD ainsi qu'un manque de communication au sein même des prestations entre les chefs de produit (DGSI), les chefs de prestation (métier) et les responsables LIPAD départementaux. Cette démarche a ainsi permis d'identifier un besoin de renforcer et la collaboration entre ces différents acteurs aux tâches extrêmement imbriquées et les ressources cognitives en matière de cadre réglementaire LIPAD. La rencontre du 27 novembre 2013 est le résultat de ce constat.

b) client mystère
Une autre approche utilisée dans le cadre du rapport intermédiaire fut celle dite du *client mystère*. Cette approche qui vise, pour l'évaluateur, à endosser les habits d'un simple utilisateur de l'AeL, avait pour but de permettre de réunir des informations sur le projet en identifiant ses forces et ses faiblesses. De par le nombre moins élevé qu'escompté des informations collectées via les questionnaires, il s'agissait également de découvrir quelles

données personnelles étaient effectivement demandées dans le cadre des différentes prestations.

Cette approche a un intérêt limité, en l'occurrence, vu le nombre des prestations concrètement mises en œuvre. En effet, pour une citoyenne ou un citoyen qui ne fait ni partie des quelques professionnels sélectionnés dans le cadre de la prestation P8 portant sur les autorisations de construire ou du corps enseignant de la P10 sur l'espace école en ligne et qui n'est pas concerné par les prescripteurs dans le domaine de la santé, peu de prestations sont disponibles. A la création d'un compte AeL, les deux seules prestations directement disponibles après authentification sont la P6 sur les autorisations de manifestation et l'inscription au registre du commerce. Sur demande, il est également possible d'obtenir un lien menant à la page web SITG[21], à laquelle on peut accéder sans authentification AeL en faisant, par exemple, usage d'un moteur de recherche. Enfin, sur demande d'un code supplémentaire envoyé par courrier recommandé, il est aussi possible d'obtenir accès aux prestations P1 et P2 portant respectivement sur l'impôt en ligne et l'impôt à la source ainsi qu'à deux prestations de l'OCPM, à savoir l'accès à son iDossier et la gestion de son éventuel rendez-vous biométrique. Cette gestion ne comprend pas la prise du rendez-vous lui-même.

Sous l'angle de la LIPAD, point de mire du présent rapport, on doit constater l'absence d'information claire au citoyen sur les dérogations et une charte d'utilisation peu visible. En effet, si conformément à la prise de position des PPDT de 2011 concernant le caractère reconnaissable de la collecte[22] l'information est désormais donnée aux citoyens que la mise en œuvre de l'AeL peut nécessiter des dérogations aux règles de la LIPAD, elle est relativement difficile d'accès. En effet, les conditions générales d'utilisation (ci-après CGU) ne sont accessibles qu'au bas du document d'inscription à l'AeL. Ce n'est donc qu'une fois le processus d'inscription entamé que les utilisateurs les découvrent et peuvent en prendre connaissance. Ainsi, la page d'accueil de l'AeL ne nous propose aucun accès direct aux CGU pas plus qu'elle ne précise quelles prestations sont effectivement disponibles via l'AeL que cela soit avec ou sans identification préalable[23].

c) Tableaux de cheminement des données

Ces tableaux ambitionnaient de clarifier la situation en permettant d'offrir une vision claire du parcours des données, la raison de leur collecte, les acteurs impliqués et le lieu de conservation final des données. Le taux de réponse fut ici très satisfaisant, un tableau ayant été rempli pour toutes les prestations, à l'exception de la P8 (autorisations de construire), prestation d'ailleurs retirée à la fin du mois de novembre 2013.

Les réponses ainsi obtenues révèlent des résultats très satisfaisants pour les prestations 1, 2, 3,6,7,9 et 10. Les données collectées le sont car nécessaires à la prestation, elles sont récoltées par le service compétent et les droits d'accès sont limités aux personnes responsables du dossier. En outre, rien n'est communiqué au-delà du service concerné à

[21] SITG, «*Le territoire genevois à la carte*» (http://ge.ch/sitg/ , site consulté le 29 octobre 2013)
[22] Préposé-es à la protection des données et à la transparence, *MISE EN OEUVRE DE L'ART. 69 LIPAD SELON LE PPDT DANS LE CADRE DE L'ADMINISTRATION EN LIGNE*, Prise de position, 28 octobre 2011, p. 4.
[23] Etat de Genève, «*Administration en ligne*» (http://www.ge.ch/ael/welcome.asp , site consulté le 30 octobre 2013)

l'exception de ce qui est requis par la loi ou nécessaire à la bonne marche de la prestation. Ainsi, la P7 concernant les PME publie les seules données publiques au sens de l'ordonnance sur le registre du commerce. La P9, concernant les droits de pratique, ne transmet les données qu'au registre fédéral des droits de pratique (MEDREG). La P10, sur l'espace école en ligne, fait usage de GoogleApps à qui les données sont donc transmises. Toutefois, les données sont préalablement anonymisées et en principe seul l'utilisateur en possède l'accès. En outre, le DIP a bénéficiée de l'accompagnement du PPDT pour une mise en œuvre conforme à la LIPAD de ce projet.

Concernant la P4, le portail population de l'OCPM, les réponses concernant les droits d'accès mettent en lumière un problème déjà soulevé par la Cour des Comptes dans un rapport du mois de décembre 2011[24] et dont le suivi du 30 juin 2013 relevait comme non résolu[25]. En effet, l'accès aux données n'est pas limité aux seules personnes ayant besoin, afin d'exécuter leur tâche, de les consulter. A ce titre, dans le suivi du rapport susmentionné, l'OCPM se déclarait conscient du problème et annonçait que sa politique de sécurité en matière documentaire serait définie sur la base de travaux d'analyse en cours. Le délai prévu est fixé au 31 décembre 2013.

A propos de la P5, relevant de l'office cantonal des véhicules, on ne peut que regretter que les citoyennes et les citoyens ne soit pas clairement informés du partenariat avec le site web ricardo.ch[26]. Ce dernier est en effet chargé de la vente de la vente aux enchères des véhicules en fourrière, l'OCV occupant le rôle de tiers à qui les données sont communiquées. L'utilisateur passe d'un site de l'Etat de Genève à celui d'une entité privée sans pour autant être informé sur ce dernier.

8. Protection des données personnelles et droits des particuliers

9. Conclusion

Pour rappel, le projet AeL ambitionne de permettre à l'administration genevoise de franchir une étape déterminante afin d'être en adéquation avec son temps. Cet objectif se divise en quatre parties distinctes[27], constituant toutes autant de défis à relever. Les résultats obtenus dans le cadre de la présente évaluation intermédiaire sont encourageants. En particulier le constat qu'il n'est guère nécessaire de déroger aux principes de la LIPAD pour livrer des prestations en ligne. C'est dire que moyennant la prise de certaines mesures, figurant ci-dessous sous forme de recommandations, le projet expérimental de l'AeL pourra, si tel est le

[24] Cour des Comptes, *Mise en œuvre de la loi 9332 concernant la gestion électronique des dossiers (GED)*, audit de légalité et de gestion, rapport n°46, décembre 2011, p. 32. (http://www.cdc-ge.ch/Htdocs/Files/v/5881.pdf/Rapportsdaudit/2011/20111214rapportno46.pdf?download=1 , consulté le 21 novembre 2013)

[25] Cour des Comptes, *Mise en œuvre de la loi 9332 concernant la gestion électronique des dossiers (GED)*, suivi du rapport n°46, juin 2013, p. 7. (http://www.cdc-ge.ch/Htdocs/Files/v/6303.pdf/Rapportsdaudit/2013/suivirapport462013.pdf?download=1 , consulté le 21 novembre 2013)

[26] ricardo.ch (http://www.ricardo.ch/ , site consulté le 24 novembre 2013)

[27] Voir chapitre «*Rappel législatif*».

désir du législateur, devenir une véritable politique publique. En l'état, nous constatons que le moteur AeL, au cœur de l'architecture globale, est sûr et offre une base solide pour envisager le développement de nouvelles prestations. En outre, les prestations qui ont été développées sont respectueuses des données des citoyennes et des citoyens ou, lorsque la situation est moins satisfaisante, le problème dépasse le cadre de l'AeL seule, et concerne la configuration des applications informatiques elles-mêmes.

Recommandations du préposé cantonal

Vu les constats effectués dans le cadre de la présente évaluation et la séance d'information commune du 27 novembre 2013, dispensée par la direction sécurité et événements spéciaux et le PPDT à l'attention des acteurs de l'AeL, le préposé cantonal recommande de prendre les mesures suivantes :

1. Mettre en place un système de gestion « protection des données » (SGPD), sur le modèle du préposé fédéral, piloté par la direction générale des systèmes d'information.

2. Ancrer l'administration en ligne dans la législation genevoise, par exemple par le biais d'un projet de loi sur l'administration en ligne.

3. Évaluer la conformité sous l'angle de la protection des données des systèmes d'information du canton, concernés par les prestations en ligne -en particulier le système d'information de l'Office cantonal de la population - , définir un calendrier de mise en conformité; à défaut les remplacer par un système d'information respectueux de la protection des données dès la conception (privacy by design); à défaut supprimer les prestations en ligne qui en dépendent.

Bibliographie