



Cloud Computing et risques

Quelles mesures pour protéger les données personnelles ?

Gianfranco Moi
Directeur Général Adjoint

Organisation de l'administration de l'Etat

L'administration de l'Etat est divisée en 7 départements en tête de chacun desquels est placé un conseiller d'Etat:

- **Département présidentiel (PRE) (incluant la Chancellerie)**
- **Département des finances (DF)**
- **Département de l'instruction publique, de la culture et du sport (DIP)**
- **Département de la sécurité et de l'économie (DSE)**
- **Département de l'aménagement, du logement et de l'énergie (DALE)**
- **Département de l'environnement, des transports et de l'agriculture (DETA)**
- **Département de l'emploi, des affaires sociales et de la santé (DEAS)**

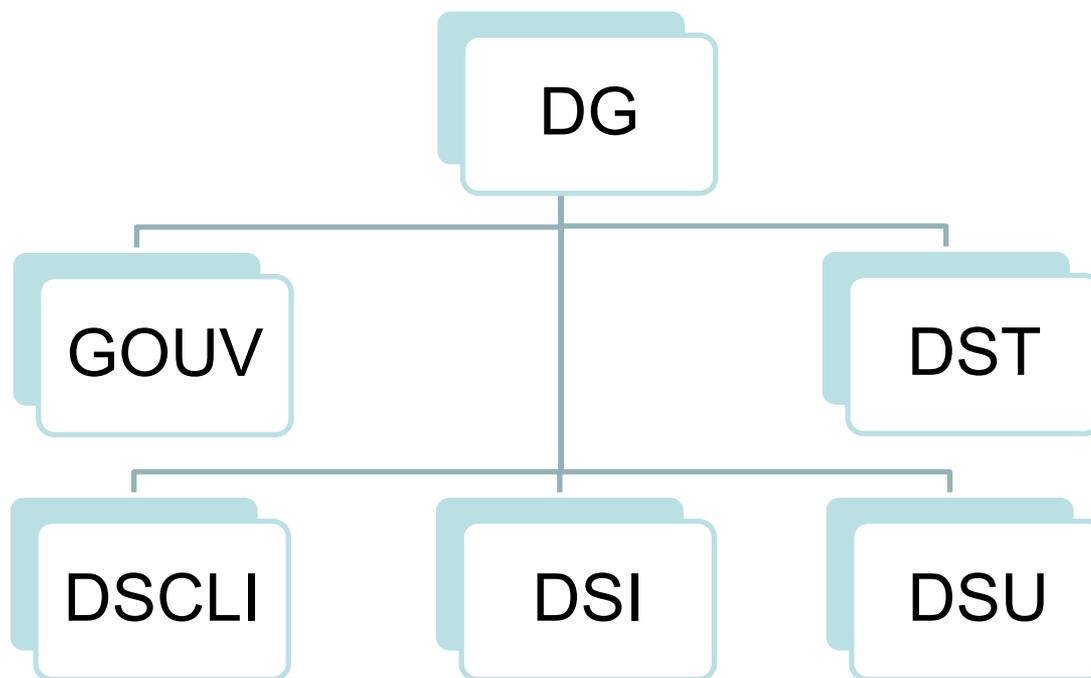
Définition des données personnelles et données personnelles sensibles conformément à la LIPAD

- données personnelles: toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable;
- données personnelles sensibles: les données personnelles sur :
 - 1° les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles,
 - 2° la santé, la sphère intime ou l'appartenance ethnique
 - 3° des mesures d'aide sociale,
 - 4° des poursuites ou sanctions pénales ou administratives;

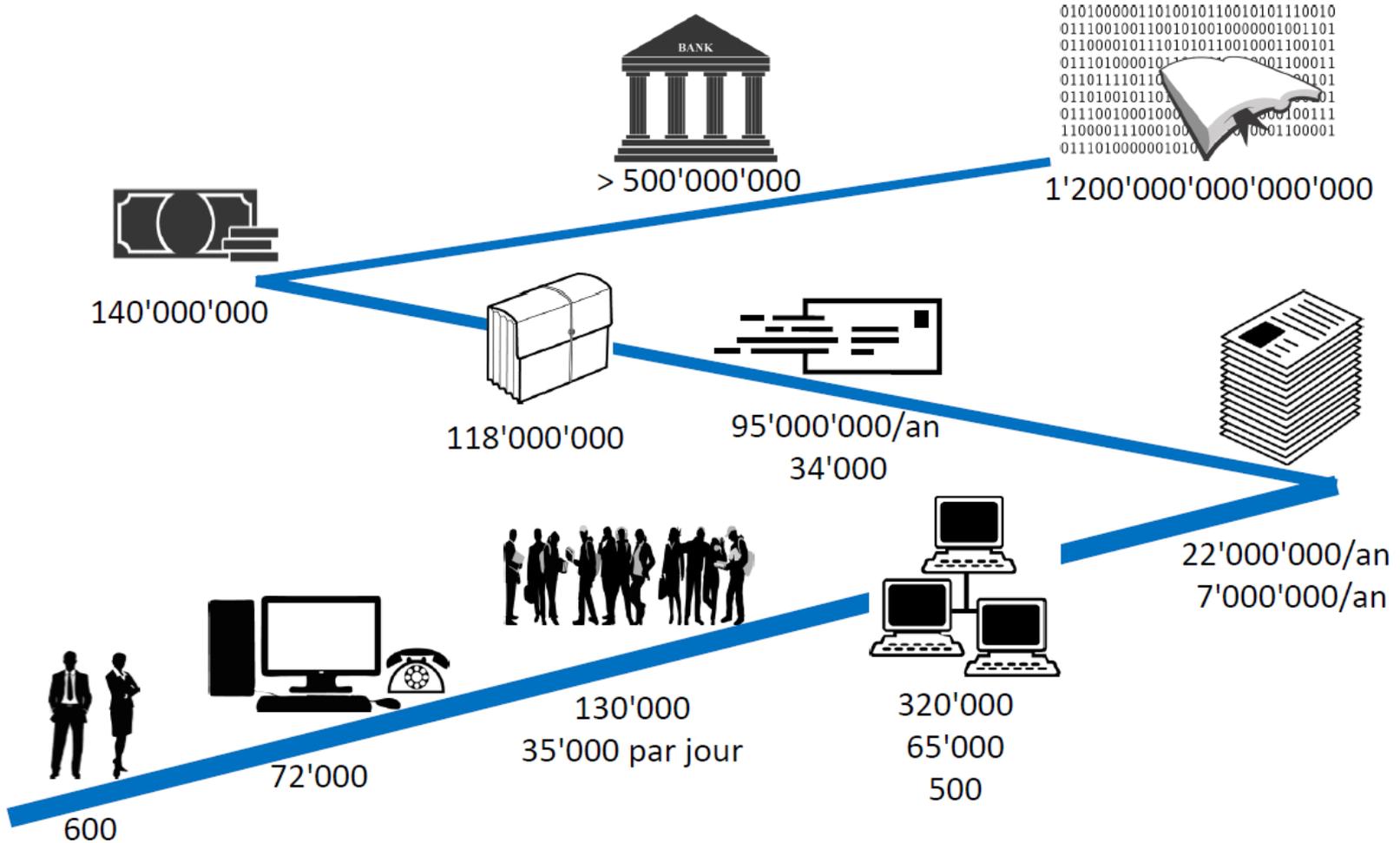
Exemples de données personnelles traitées dans les départements

- **Département présidentiel (PRE) (incluant la Chancellerie)**
 - Le vote
- **Département des finances (DF)**
 - La fiscalité, le personnel, la comptabilité, les poursuites
- **Département de l'instruction publique, de la culture et du sport (DIP)**
 - Les notes, les absences, la santé, les aides financières
- **Département de la sécurité et de l'économie (DSE)**
 - Les personnes, les violences domestiques, la traite des êtres humains, la justice, la police, la détention, le militaire
- **Département de l'aménagement, du logement et de l'énergie (DALE)**
- **Département de l'environnement, des transports et de l'agriculture (DETA)**
- **Département de l'emploi, des affaires sociales et de la santé (DEAS)**
 - Les prestations sociales, les pensions, la santé

Organisation 2015 de la DGSI (rattachée au DSE)



La DGSI en chiffres



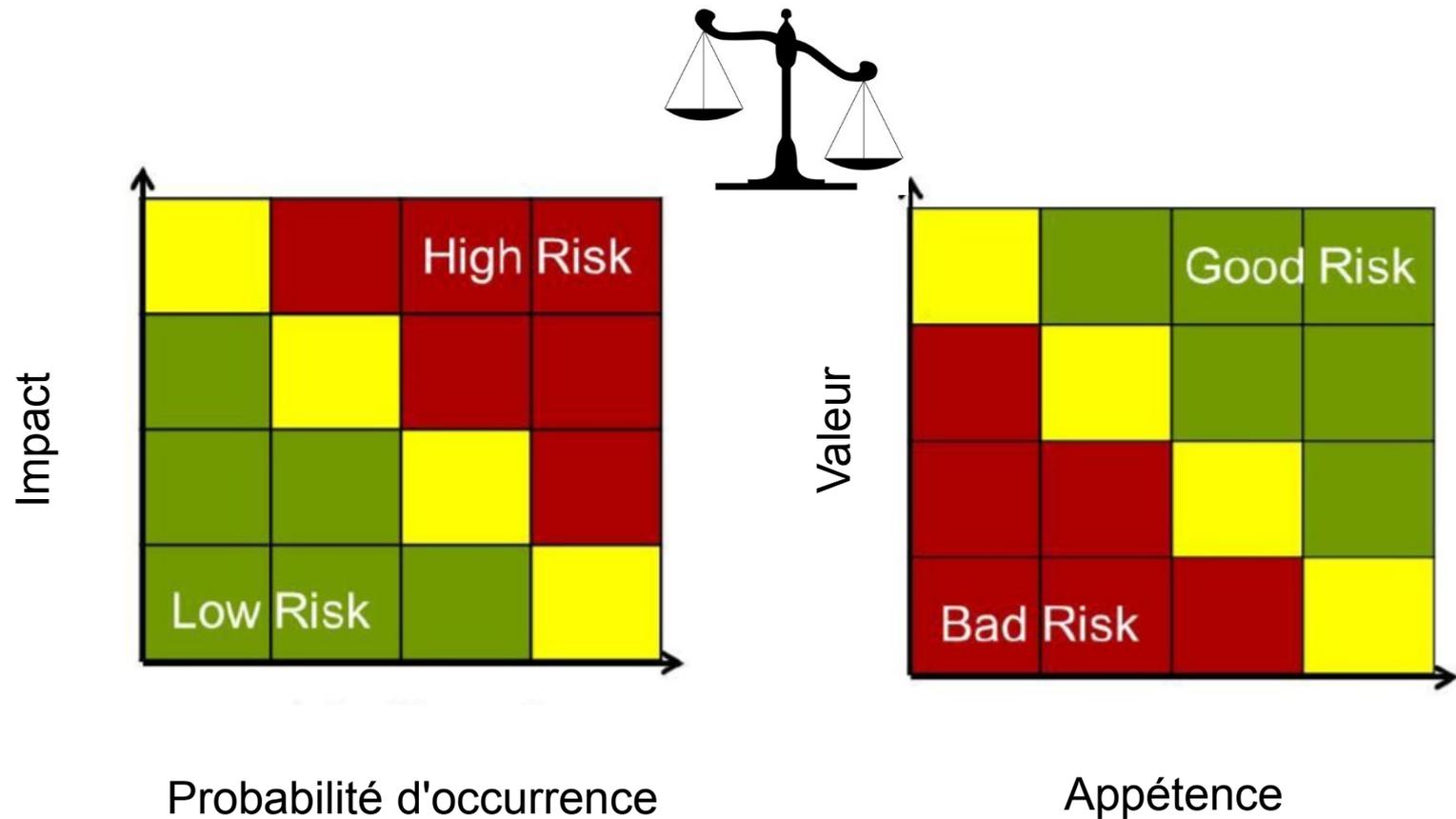
Que dit le rapport 65 de la Cour des Comptes?



Questions sur la sécurité et le Cloud public

- Il est essentiel de bien cerner les problématiques ... en termes de risques et d'opportunités:
- Risques:
 - Est-ce que le risque existe indépendamment de l'utilisation du Cloud public ?
 - Est-ce que l'utilisation du Cloud public permet de mitiger les risques ou au contraire les aggrave
- Opportunités
 - Est-ce que l'opportunité existe indépendamment de l'utilisation du Cloud public ?
 - Est-ce que l'utilisation du Cloud public accroît les opportunités ou au contraire les restreint?

Changement de paradigme dans la gestion des risques



Enjeux et problématiques sur le Cloud *public*

- **Problématiques**

- Agilité
- Conformité
- Fournisseur
- Disponibilité
- Sécurité

- **Enjeux**

- Les responsables de la sécurité qui tenteraient de bloquer les accès au Cloud public sans considération pour les besoins de l'organisation ...
- Les dirigeants qui s'engageraient dans le Cloud public sans considération sur les risques encourus ...
- Les acheteurs qui ne seraient pas capables de positionner les offres du Cloud public du point de vue des coûts et des risques ...

Interrogations typiques sur la protection de données privées...

- La localisation des données et les personnes ayant accès
- La localisation des traitements et les personnes traitant
- Les réseaux sociaux et la frontière entre la sphère publique et sphère privée
- Les lois et règlements sur la protection des données en Suisse et à Genève
- Les mesures à prendre pour garantir la protection des données

Exemple de questions sur la localisation des données...

- En matière d'utilisation d'outils ou de bases de données qui impliquent le transfert de données personnelles à l'étranger, en dehors de l'Europe, aux Etats-Unis (par exemple avec Google Analytics - qui utilise l'outil à l'Etat et pourquoi ?)
- Pourrait-on faire autrement?

Exemple de questions sur la localisation des traitements...

- Lorsque nous travaillons avec des mandataires extérieurs sur des bases de données (par exemple des données personnelles sensibles fiscales, de santé, d'aide sociale) de l'Etat de Genève, comment vous assurons-nous que les données sont protégées?
- Que se passe-t-il quand le mandataire est à l'étranger?

Exemple de questions sur les réseaux sociaux...

- Nous savons que des données personnelles d'élèves ou de professeurs sont sur Facebook – Est-ce un problème?
- Quels conseils de principe faut-il rappeler?

Exemple de questions sur les lois et règlements sur la protection des données personnelles en Suisse ...

- Au Colloque du Clusis où Mme Perrinjaquet, Conseillère d'Etat, disait en ouverture que les entreprises privées étrangères venaient protéger leurs données personnelles en Suisse, qu'évidemment c'est plus cher dans notre pays mais que la Suisse a la réputation d'être un pays très fiable dans ce domaine. Est-ce correct?
- Si le règlement genevois - qui interdit tout traitement en dehors de Suisse – est modifié, alors, que faudra-t-il envisager pour pouvoir assurer aux citoyennes et citoyens genevois que la protection de leurs données restera garantie ?

Lois et le règlement d'application sur les données personnelles à Genève

- Loi sur la protection des données (loi fédérale)
- Loi sur la transparence (loi fédérale)
- Loi sur l'information du public et l'accès aux documents (LIPAD loi genevoise)
- Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD règlement genevois)

Traitement transfrontières de données

RIPAD Art. 13 al. 5: Sécurité des données personnelles (art. 37, al. 2, de la loi)

- "Les systèmes d'information et les systèmes informatiques d'une institution soumise au présent règlement permettant le traitement des données sensibles, des données fiscales, des données relatives à des élèves ou à des mineurs, ainsi que des données relatives au personnel, doivent garantir que, **quelle que soit la technologie utilisée, aucun traitement de données ne survienne hors du territoire suisse**".

Systemes informatiques délocalisés

RIPAD Art. 13 al. 6: Sécurité des données personnelles (art. 37, al. 2, de la loi)

- "Le recours à des systèmes informatiques délocalisés ou dématérialisés (informatique en nuage) permettant l'exportation sur des **serveurs distants** de traitements **traditionnellement** localisés sur des **serveurs locaux** ou sur le poste de l'utilisateur, notamment par la fourniture d'une plateforme technique adaptée fournie par un hébergeur tiers :
 - a) est **interdit pour toutes les données personnelles sensibles**, quel que le soit le type de traitement envisagé;
 - b) n'est possible pour les autres données que pour autant que **l'intégralité du traitement survienne sur territoire suisse** et que les institutions soumises au présent règlement concluent un contrat de droit public ou de droit privé tendant au traitement de données placées sous leur responsabilité. Il incombe alors à l'institution de veiller au respect de toutes les prescriptions visées aux alinéas 1 à 6."

Exemple de questions sur les mesures à prendre pour garantir la protection des données...

- Que faut-il envisager pour pouvoir assurer aux citoyennes et citoyens genevois que la protection de leurs données est garantie ?

Merci pour votre attention!

Gianfranco Moi

Gianfranco.Moi@etat.ge.ch



REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX

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