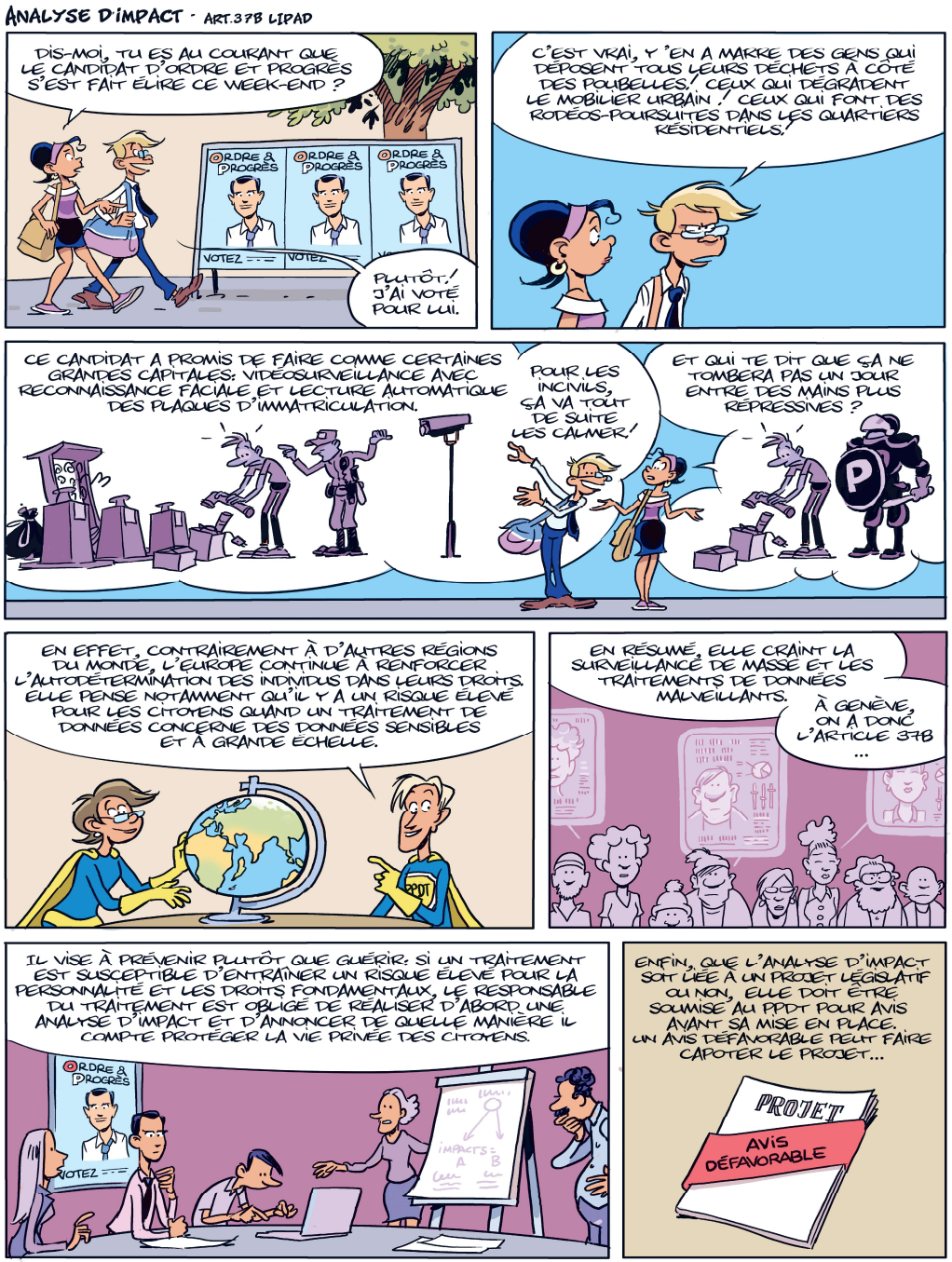
La nouvelle LIPAD, questions choisies

6 mai 2025

Introduction



L'analyse d'impact

Art. 37B LIPAD

L'analyse d'impact (AIPD) - contexte

Origine: Art. 10 al. 2 Convention 108 +

Critère déterminant: impact potentiel du traitement envisagé sur les droits et libertés fondamentales des personnes concernées.

Approche fondée sur les risques – minimisation des risques.

AIPD: Instrument de travail

L'analyse d'impact – base légale

Art. 37B nLIPAD

Al. 1: Quand une analyse d'impact est-elle nécessaire?

Lorsqu'un traitement de données personnelles est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles. S'il envisage d'effectuer plusieurs opérations de traitement semblables, il peut établir une analyse d'impact commune

L'analyse d'impact

Al. 2: qu'est-ce qu'un "risque élevé"?

L’existence d’un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l’étendue, des circonstances et de la finalité du traitement. Un tel risque existe notamment dans les cas suivants : a) traitements de données personnelles sensibles à grande échelle; b) profilage; c) surveillance systématique de grandes parties du domaine public.

Al. 3 : que contient l'analyse d'impact?

L’analyse d’impact contient notamment : a) une description du traitement envisagé; b) une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée; ainsi que c) les mesures prévues pour protéger la personnalité et les droits fondamentaux de la personne concernée.

L'analyse d'impact

Al 4 et 5: Quand l'analyse d'impact est-elle soumise au Préposé cantonal?

4 Lorsque l’analyse d’impact est requise selon l’alinéa 1 du présent article, elle est jointe au projet d’acte législatif pour avis de la préposée cantonale ou du préposé cantonal au sens de l’article 56A, alinéa 2, lettre e, de la présente loi.

5 Lorsque l’analyse d’impact requise à l’alinéa 1 du présent article n’est pas liée à un projet d’acte législatif, elle est soumise à la préposée cantonale ou au préposé cantonal pour avis avant le début du traitement.

Notion de risque élevé pour la personnalité ou les droits fondamentaux

- **Ce qui est protégé**: la personnalité et les droits fondamentaux de la personne concernée
- Vise principalement
  - Droit au respect de la sphère privée et contre l'emploi abusif des données qui la concerne (art. 13 Cst)

  Mais aussi
  - Droit à l'intégrité physique et psychique et à la liberté de mouvement (art. 10 al. 2 Cst)
  - Liberté de conscience et de croyance (art. 15 Cst)
  - Liberté d'opinion (art. 16 Cst)
  - L'interdiction des discriminations (art. 8 Cst)

Notion de risque élevé pour la personnalité ou les droits fondamentaux

- La simple possibilité d'un risque pour la personnalité ou les droits fondamentaux ne suffit pas à entrainer l'obligation de mener une analyse d'impact.

- La loi impose que ce "risque" soit "élevé"
  - -probabilité de survenance
  - - gravité des conséquences

- Analyse relative au traitement envisagé

Notion de risque élevé pour la personnalité ou les droits fondamentaux

L'art. 37B al. 2 LIPAD prévoit au moins 3 cas de figure lors desquels un tel risque existe :

- traitements de données personnelles sensibles à grande échelle;
- profilage;
- surveillance systématique de grandes parties du domaine public.

Sinon: dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement, en particulier lors du recours à de nouvelles technologies.

Notion de risque élevé pour la personnalité ou les droits fondamentaux

- Indices de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée:
  - Recourir à de nouvelles technologies (Par ex: intelligence artificielle)
  - Interconnexion ou croisement de bases de données
  - Prise de décisions automatisées
  - Finalité du traitement = surveillance
  - Données personnelles accessibles en ligne
  - Activités de prédiction
  - Données sensibles

Notion de risque élevé pour la personnalité ou les droits fondamentaux

Des exemples peuvent être trouvés dans:

- Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679

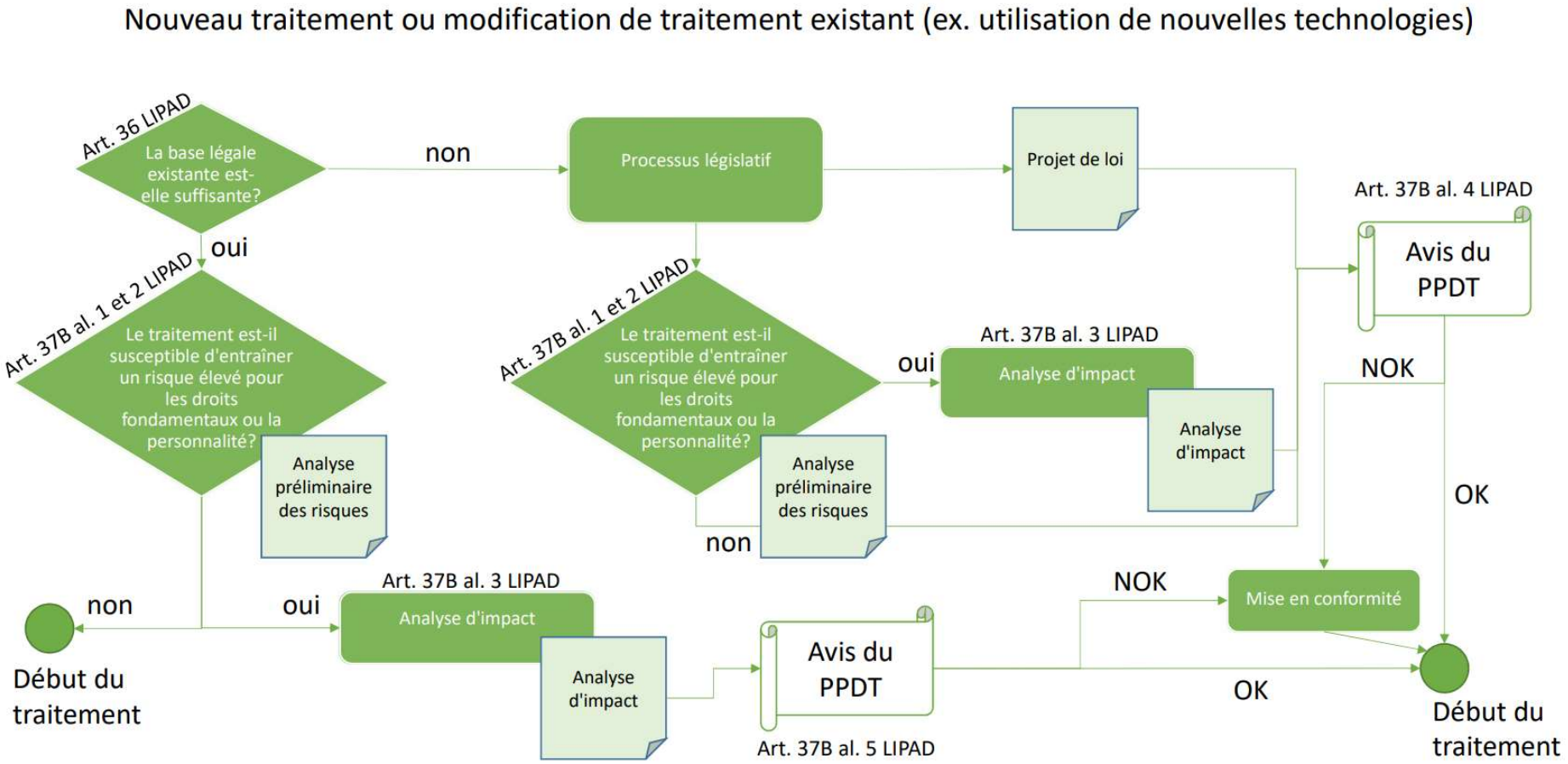
- Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise émise par la CNIL

En pratique comment procéder?

Pour accompagner les institutions publiques dans la mise en œuvre de ces nouvelles obligations, le préposé cantonal émis les publications suivantes:

- fiche-info du PPDT traitant de l'analyse d'impact
- Analyse de risques préliminaire et analyse d'impact (PDF)
- Analyse de risques préliminaire et analyse d'impact (version Word modifiable)
- Guide de l'analyse des risques
- Schéma du processus de l'analyse

Schéma du processus de l'AIPD



Analyse d'impact

Structure du formulaire de l'AIPD

- Première partie – Analyse préliminaires des risques (4 pages)

- Deuxième partie – Analyse d'impact relative à la protection des données personnelles (9 pages)

Première partie – Analyse préliminaire des risques

- Institution concernée
  - Responsable de traitement
  - Personne de contact (si différente du responsable de traitement)
  - Conseiller/conseillère LIPAD
  - RSI
  - Bases légales existantes pour le traitement envisagé

- Chapitre 1 - Description du traitement envisagé
  - Finalité(s) du traitement
  - Catégories de données personnelles

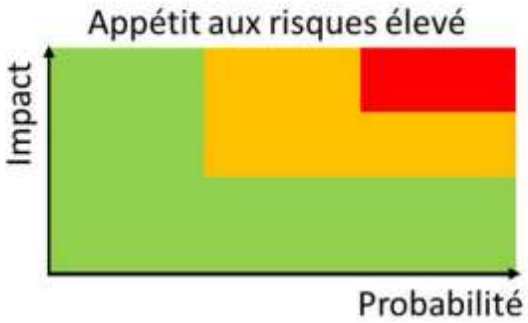
- Chapitre 2 – Analyse préliminaire
  - Principes fondamentaux
  - A. Traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée selon art 37B LIPAD
  - B. Indices de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée

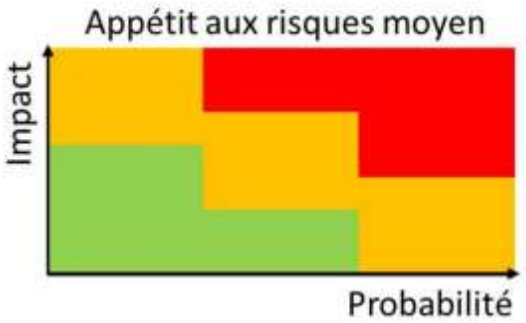
2ème Partie – Analyse d'impact

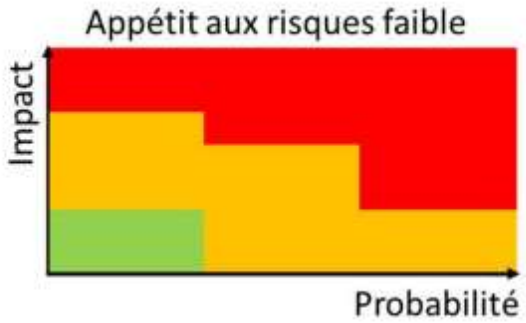
- Première Partie – Analyse détaillée de la base légale
- Deuxième Partie - Description détaillée du traitement envisagé
- Troisième partie – Évaluation du risque pour les droits fondamentaux de la personne concernée
- Quatrième partie – identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée
- Cinquième partie – évaluation des effets des mesures prévues pour protéger les droits fondamentaux de la personne concerné afin de déterminer s'il reste un risque résiduel élevé
- Sixième partie – synthèse et résultats de l'AIPD

Approche basées sur les risques - notions

- Notion de risque: probabilité / impact
- Risques inhérents vs risques résiduels
- Appétit au risque

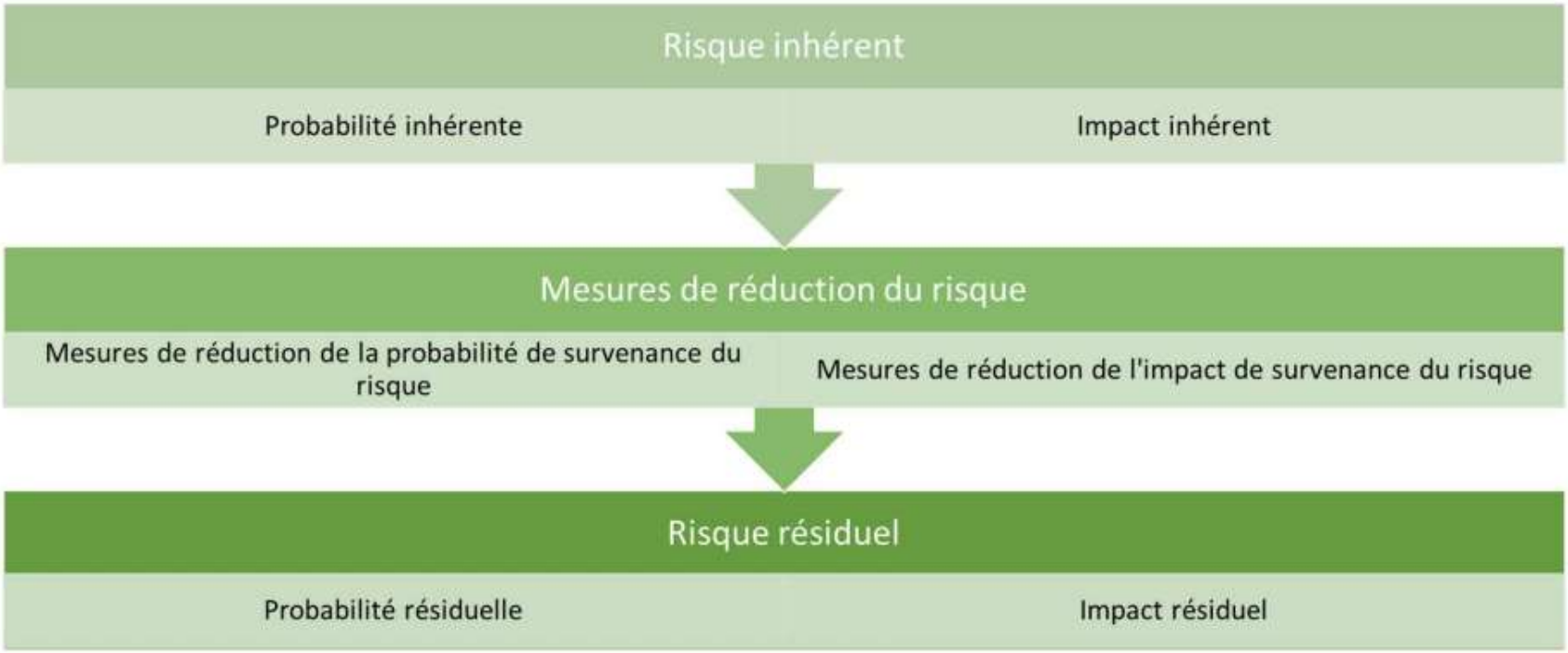






- Mesures de réduction des risques: évitement, réduction, transfert, acceptation

Risques inhérents vs résiduels

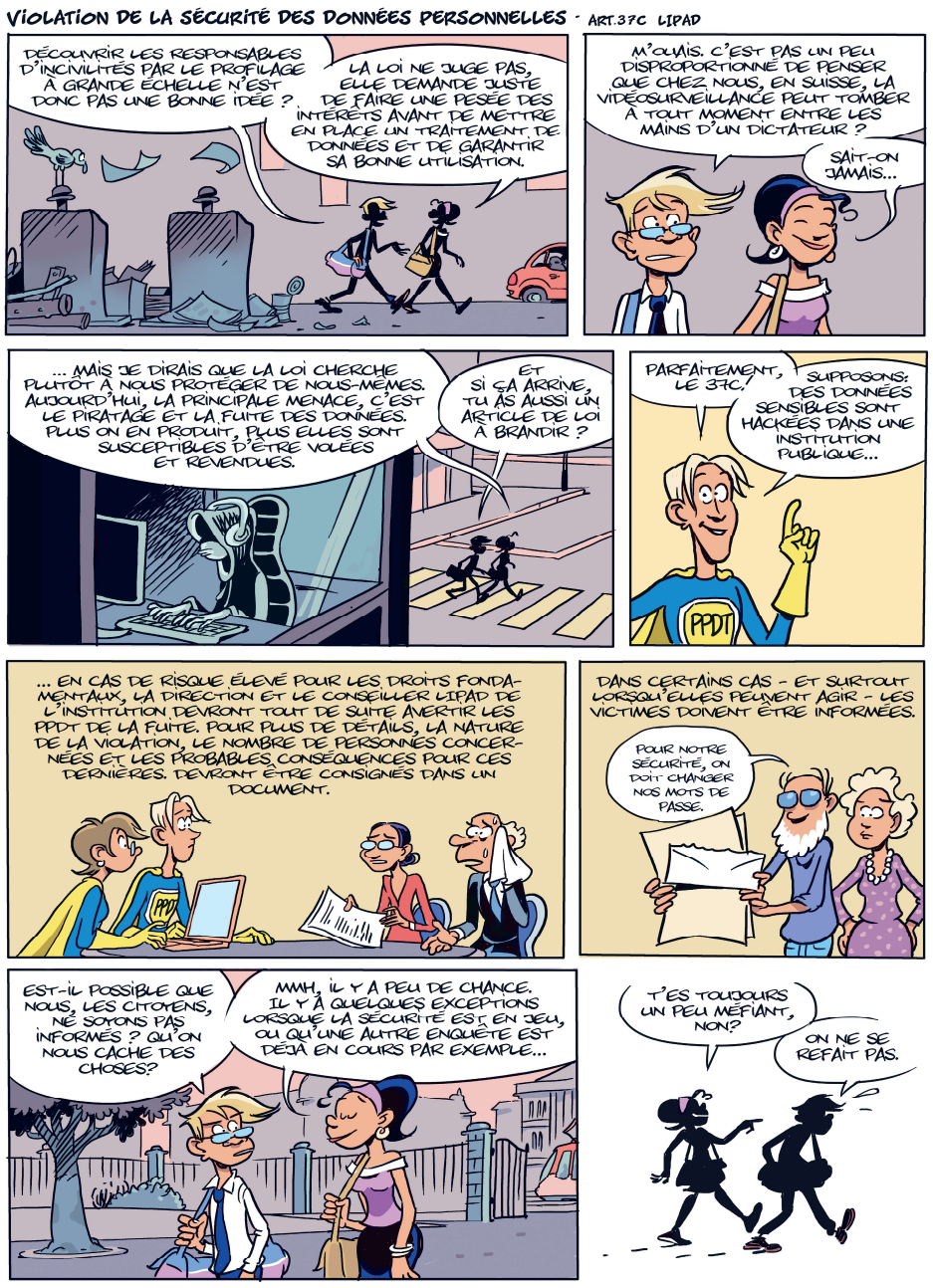


Formulaire d'analyse de risques préliminaire et analyse d'impact

https://www.ge.ch/document/38352/annexe/1

Violation de la sécurité des données

Art. 37C LIPAD



Violation de la sécurité des données (art. 37C LIPAD)

- mesures appropriées afin de mettre fin à la violation et d'en minimiser les effets.
- informe immédiatement sa conseillère ou son conseiller à la protection des données et à la transparence au sens de l'article 50.
- consigne dans un document interne les détails de la violation
- annonce dans les meilleurs délais à la préposée cantonale ou au préposé cantonal les cas de violation de la sécurité des données personnelles entraînant **vraisemblablement un risque élevé** pour la personnalité ou les droits fondamentaux de la personne concernée.
- devoir d'annonce du sous-traitant au responsable du traitement de tout cas de violation de la sécurité des données personnelles

Violation de la sécurité des données (art. 37C LIPAD)

- information à la personne concernée lorsque cela est nécessaire à sa protection ou lorsque la préposée cantonale ou le préposé cantonal l'exige.
- loi prévoit des exceptions lors desquels le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer.

Rappel: Une fiche informative existe déjà sur le sujet, elle sera mise à jour avec la publication de la nouvelle LIPAD et du nouveau RIPAD. (https://www.ge.ch/document/27856/telecharger)

Un formulaire d'annonce de violation de la sécurité des données sera également mis à disposition.

Violation de la sécurité des données (art. 37C LIPAD) – Annonce au PPDT

- Notion de risque élevé pour la personnalité ou les droits fondamentaux:
  - quelle est la probabilité (faible, moyenne, élevée) que la violation ait une conséquence négative déterminée (atteinte à la réputation, humiliation, perte d'emploi, discrimination, dommages corporels par exemple) sur la personne concernée et comment cette conséquence négative serait-elle qualifiée (légère, moyenne, grave)? Il conviendra de prendre en compte, dans l'examen, la nature et le type de données, le type de violation, le nombre de personnes concernées notamment.
  - Exemples selon le PFPDT: données personnelles sensibles concernées (données de santé, données biométriques ou données sur l'aide sociale); accessibilité à un large public sur le darknet; risque d'usurpation d'identité; piratage d'accès informatiques en ligne; informations soumises au secret envoyées au mauvais destinataire.

Formulaire d'annonce de violation de la sécurité des données

Excursus: obligation d'annonce selon la loi sur la sécurité de l'information (LSI)

Le Conseil fédéral a décidé de promulguer au 1er avril 2025 l’obligation de signaler les cyberattaques contre des infrastructures critiques.

Depuis cette date, les exploitants d’infrastructures critiques sont tenus d’annoncer les cyberattaques à l’Office fédéral de la cybersécurité (OFCS) dans les 24 heures suivant leur détection. Si toutes les informations requises ne peuvent pas être fournies dans les 24 heures, le délai pour compléter le signalement est de 14 jours.

L’OCyS contient les dispositions d’exécution relatives à l’obligation de signalement.

Obligation d'annonce selon la loi sur la sécurité de l'information (LSI)

L'obligation d'annoncer s'applique notamment (art. 74b LSI):

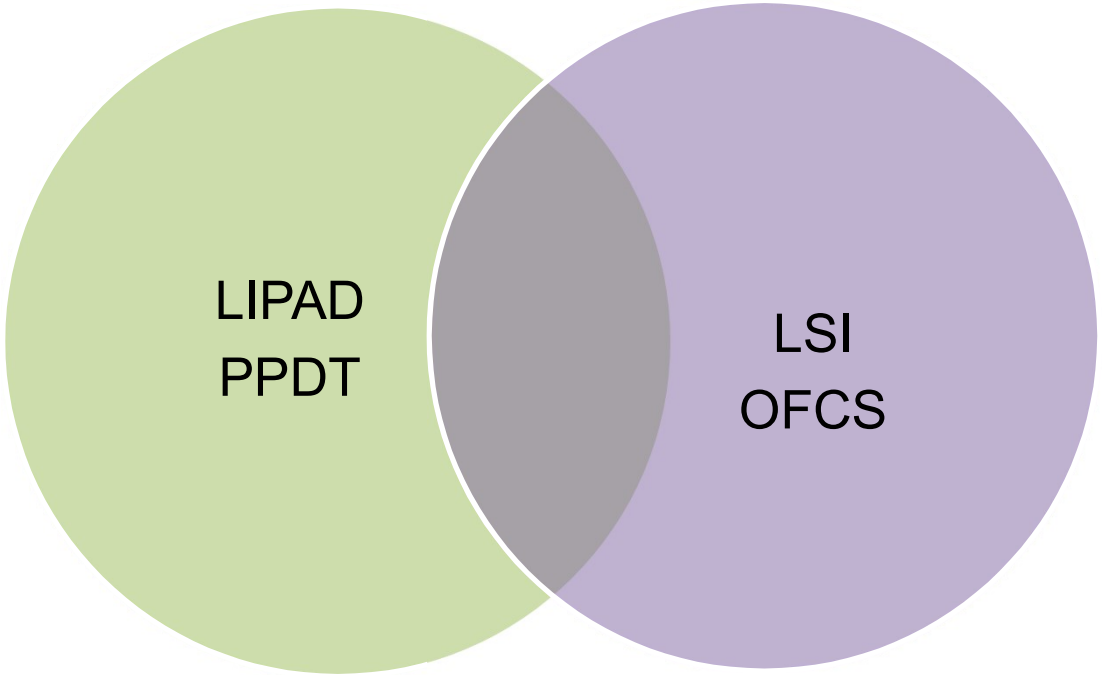
- aux hautes écoles (litt. a)
- aux autorités et organisations cantonales et communales (litt. b)
- aux organisations chargées de tâches de droit public dans les domaines de la sécurité et du sauvetage, de l’approvisionnement en eau potable, du traitement des eaux usées et de l’élimination des déchet (litt. c)
- aux entreprises œuvrant dans les domaines de l’approvisionnement énergétique (litt. d)
- aux établissements de santé figurant sur la liste hospitalière cantonale (litt. f)
- aux entreprises de bus (litt. m), aux aéroports nationaux (litt. n)

Obligation d'annonce selon la loi sur la sécurité de l'information (LSI)

Une cyberattaque doit être signalée, notamment lorsqu'elle met en péril le fonctionnement de l'infrastructure critique concernée, a entraîné une manipulation ou une fuite d'informations, ou s'accompagne d'actes de chantage, de menaces ou de contrainte (art. 74d LSI).

Obligations d'annonces LIPAD / LSI

Le traitement du dossier est effectué séparément par chaque autorité compétente



La LIPAD,
2ème édition

Distribution

REPUBLIQUE
ET CANTON
DE GENEVE

Merci de votre attention

Boulevard Helvétique 27
1207 Genève

Tél. 022/546.52.40
ppdt@etat.ge.ch
https://www.ge.ch/organisation/protection-donnees-transparence