L’obligation d’annonce des violations de la sécurité des données

Une nouveauté provenant de la nouvelle loi fédérale sur la protection des données personnelles

Pauline Meyer I 18.10.2022

Au menu

I. Contexte et origine
II. Obligation d'annonce des violations de la sécurité des données
    I. L'annonce au PFPDT
    II. L'information aux personnes concernées
    III. L'annonce au responsable du traitement
III. Non-respect de l'obligation
IV. Perspectives

I. Contexte et origine

- Aucune obligation légale explicite auparavant
- Diverses impulsions
  - Motion, postulats, interpellation
  - Convention 108+ et RGPD

II. Obligation d'annonce

Art. 24 Annonce des violations de la sécurité des données

[1] Le responsable du traitement annonce dans les meilleurs délais au PFPDT les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

[2] L'annonce doit indiquer au moins la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées.

[3] Le sous-traitant annonce dans les meilleurs délais au responsable du traitement tout cas de violation de la sécurité des données.

[4] Le responsable du traitement informe la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le PFPDT l'exige.

[5] Il peut restreindre l'information de la personne concernée, la différer ou y renoncer, dans les cas suivants:

a. il existe un motif au sens de l'art. 26, al. 1, let. b, ou 2, let. b, ou un devoir légal de garder le secret qui l'interdit;

b. l'information est impossible à fournir ou exige des efforts disproportionnés;

c. l'information de la personne concernée peut être garantie de manière équivalente par une communication publique.

([5bis] Le PFPDT peut, avec l'accord du responsable tenu à l'obligation de signalement, transmettre le signalement au Centre national pour la cybersécurité à des fins d'analyse de l'incident. Le signalement peut contenir des données personnelles, y compris des données sensibles relatives à des poursuites ou à des sanctions pénales ou administratives visant le responsable tenu à l'obligation de signalement.)

[6] Une annonce fondée sur le présent article ne peut être utilisée dans le cadre d'une procédure pénale contre la personne tenue d'annoncer qu'avec son consentement.

II. Obligation d'annonce

Art. 15 Annonce des violations de la sécurité des données

[1] L'annonce au PFPDT d'une violation de la sécurité des données comprend les informations suivantes:

a. la nature de la violation;

b. dans la mesure du possible, le moment et la durée;

c. dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées;

d. dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées;

e. les conséquences, y compris les risques éventuels, pour les personnes concernées;

f. les mesures prises ou prévues pour remédier à cette défaillance et atténuer les conséquences, y compris les risques éventuels;

g. le nom et les coordonnées d'une personne de contact.

[2] Si le responsable du traitement n'est pas en mesure d'annoncer simultanément toutes les informations, il fournit les informations manquantes dans les meilleurs délais.

[3] Si le responsable du traitement est tenu d'informer la personne concernée, il lui communique, dans un langage simple et compréhensible, au moins les informations visées à l'al. 1, let. a et e à g.

[4] Le responsable du traitement documente les violations. La documentation contient les faits relatifs aux incidents, à leurs effets et aux mesures prises. Elle est conservée pendant au moins deux ans à compter de la date d'annonce au sens de l'al. 1.

II. Obligation(s) d'annonce

- Trois types distincts de communication:
  i. Annonce au PFPDT (art. 24 al. 1 et 2 LPD ; art. 15 al. 1 OPDo)
  ii. Information des personnes concernées (art. 24 al. 4 LPD ; art. 15 al. 3 OPDo)
  iii. Au responsable du traitement (art. 24 al. 3 LPD)

II.i. Annonce au PFPDT

- Qui ? Le responsable du traitement (art. 5 lit. j LPD) privé ou l'organe fédéral (art. 5 lit. i LPD)
  - Détermine les moyens et les finalités du traitement

- Dans quels cas ?
  - **Violation de la sécurité des données** (art. 5 lit. h LPD)…
    → CIDT (confidentialité, intégrité, disponibilité, traçabilité)
    → Accidentelle / malveillante
  - Entraînant **vraisemblablement**…
    → Probabilité objective
  - …un **risque élevé** pour la personnalité et les droits fondamentaux de la personne concernée
    → Conséquences significatives
    → Différents éléments à prendre en compte

II.i. Annonce au PFPDT

- Quoi annoncer ? (Art. 24 al. 2 LPD ; art. 15 al. 1 OPDo)
  - La nature de la violation
  - Dans la mesure du possible, le moment et la durée
  - Dans la mesure du possible, les catégories et le nombre approximatif de données personnelles concernées
  - Dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées
  - Les conséquences, y compris les risques résiduels, pour les personnes concernées
  - Les mesures prises ou prévues
  - Le nom et les coordonnées de la personne de contact
- Dans quels délais ? « Les meilleurs délais » (art. 24 al. 1 LPD ; art. 15 al. 2 OPDo)
- Comment ?
- Exceptions ?

II.ii. Information aux personnes concernées

- Qui ? Le responsable du traitement
- Dans quels cas ? « Lorsque [l'information] est **nécessaire à [la] protection [de la personne concernée]** ou lorsque le **PFPDT l'exige** » (art. 24 al. 4 LPD)
- Quoi annoncer ? (art. 15 al. 3 OPDo)
  - Au moins la nature de la violation, ses conséquences, les mesures prises et envisagées et les coordonnées d'une personne de contact
- Dans quel délai ?
- Comment ?
- Exceptions (art. 24 al. 5 LPD)

II.i. Annonce au responsable du traitement

- Qui ? Le sous-traitant (art. 5 lit. k LPD)
  - Qui traite des données personnelles pour le compte du responsable du traitement
- Dans quels cas ? « **Tout cas** de violation de la sécurité des données » (art. 24 al. 3 LPD)
- Dans quel délai ? « Les meilleurs délais » (art. 24 al. 3 LPD)
- Comment ?
- Exceptions ?

III. Non-respect de l'obligation

- Enquête et mesure prononcée par le PFPDT (art. 41 al. 1 et 51 al. 3 lit. f LPD)
- Pour le responsable du traitement privé :
  - possibilité d'accompagner la décision de la menace d'une amende (art. 63 LPD)
  - Autres chefs de responsabilité

- Quid pour les organes fédéraux ?
  - Responsabilité de l'Etat
- Quid pour les sous-traitants ?
  - Enquête et mesure prononcée par le PFPDT ? Possibilité d'accompagner la décision de la menace d'une amende ?
  - Autres chefs de responsabilité

- Quid si une autre infraction est découverte par l'annonce ?

IV. Perspectives

- Pour les entités soumises à la LPD
  - Implications au niveau des mesures à prendre
  - Quid en pratique ?

- Au niveau cantonal
  - Adoption de lois cantonales
  - Selon l'entité, double régime

Merci de votre attention !

Sur le sujet : Métille Sylvain/Meyer Pauline, Annonce des violations de la sécurité des données : une nouvelle obligation de la nLPD, RSDA 1/2021, pp. 23-33.

pauline.meyer.3@unil.ch