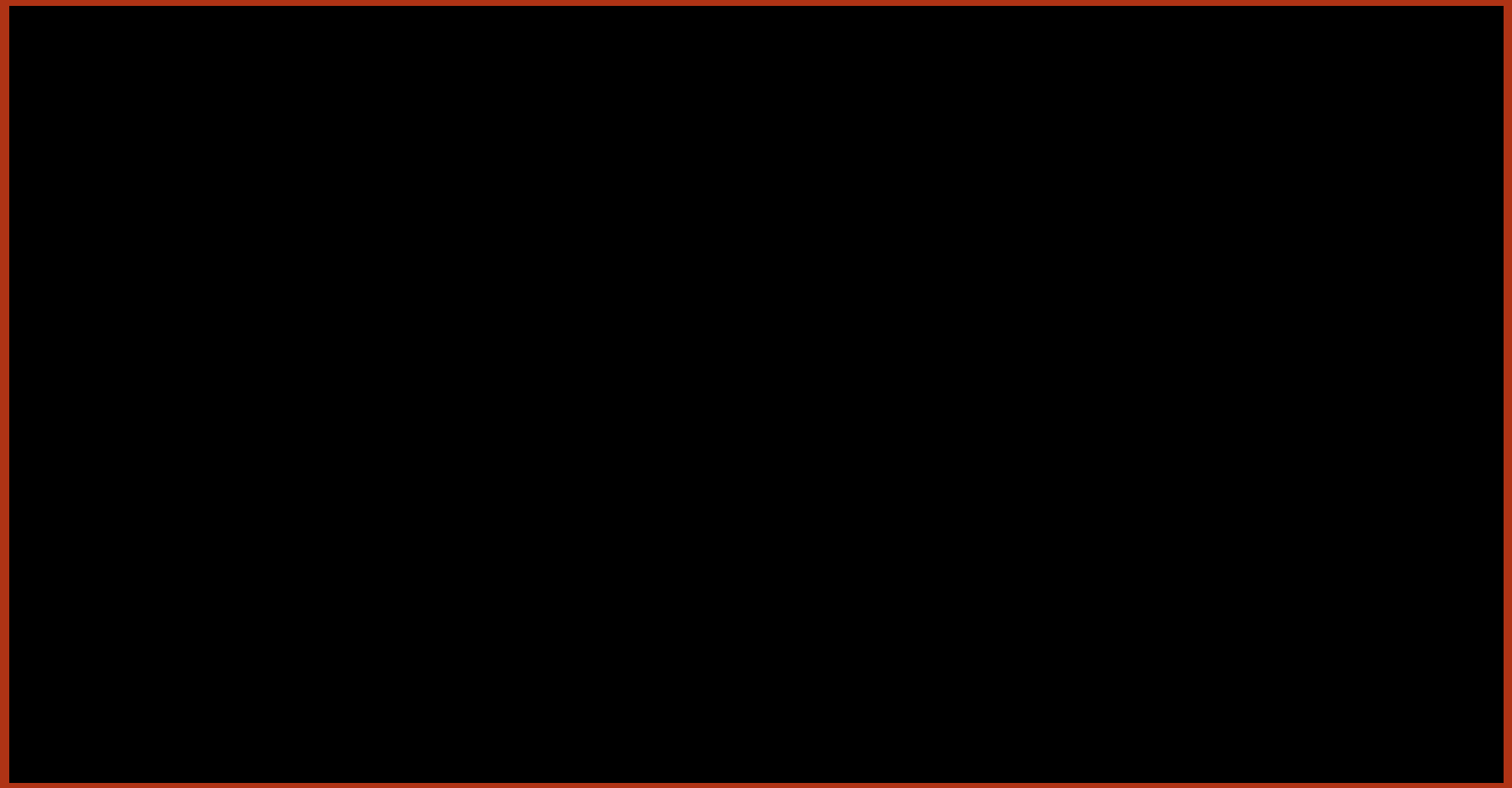
Failles de sécurité:
quelles obligations légales et comment survivre?

Dr Sylvain Métille

Blackalps, Yverdon, 15 novembre 2017

Equifax: Last Week Tonight with John Oliver (HBO)



Source: https://www.youtube.com/watch?v=mPjgRKW_Jmk

Cadre légal

Plusieurs sources d'obligations

- Suisse
  - Projet de Loi fédérale sur la protection des données (pLPD)
  - Projet de Loi fédérale sur la sécurité de l'information au sein de la Confédération (pLSI)
- Europe
  - Règlement général de protection des données (RGPD)
  - Directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS)
  - Règlement concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE
  - Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (Règlement eIDAS)
  - Directive « Paquet Télécom »
- Obligations contractuelles

Annonce des violations de la sécurité des données (22 pLPD)

1. Le responsable du traitement annonce dans les meilleurs délais au préposé 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 au moins indiquer la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou envisagées pour remédier à la situation.
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 par ailleurs la personne concernée lorsque cela est nécessaire à sa protection ou lorsque le préposé 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. 24 al. 1 let. b ou 2 let. b, ou un devoir légal de garder le secret l'interdit;
   b. Le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés;
   c. L'information de la personne concernée peut être garantie de manière équivalente par une communication publique.
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.

Notification à l'autorité de contrôle d'une violation de données à caractère personnel (33 RGPD)

1. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
2. Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.
3. La notification visée au paragraphe 1 doit, à tout le moins:
   a. décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
   b. communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
   c. décrire les conséquences probables de la violation de données à caractère personnel;
   d. décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
4. Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.
5. Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.

Communication à la personne concernée d'une violation de données à caractère personnel (34 RGPD)

1. Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.
2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).
3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:
   a. le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;
   b. le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;
   c. elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.
4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

Une faille, c’est quoi?

RGPD:
Violation de données à caractère personnel

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données (4 ch. 12 RGPD)

pLPD
Violation de la sécurité des données

Toute violation de la sécurité sans égard au fait qu'elle soit intentionnelle ou illicite, entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données (4 let. g pLPD)

En clair, une faille de sécurité c'est…?

- Incident de sécurité
- Concerne des données personnelles
- Atteinte à
  - la confidentialité
  - la disponibilité
  - l'intégrité des données

Faille de sécurité

=

Obligation d'annonce

Exceptions

- S'il n'y a pas de faille
- S'il n'y a pas de risques pour les personnes concernées (mais il faut documenter)

Par qui?

- Le responsable du traitement
- Le sous-traitant (annonce seulement au responsable du traitement)

A qui?

- Autorité de protection des données
  - Suisse: PFPDT
  - UE: ?

- Personnes concernées
  - si nécessaire à leur protection ou que l'autorité l'exige
  - peut être remplacée par une communication publique
  - peut y renoncer ou différer si intérêts prépondérants

Quand?

- Dans les meilleurs délais (pLPD) ou 72h (RGPD)
- Délai court dès la connaissance de la faille
- Plus le risque et le nombre de personnes concernées sont élevés, plus il faut agir vite

Annoncer quoi?

- Nom et coordonnées du responsable du traitement
- Nature de la violation (effacement ou destruction, perte, modification, communication)
- Conséquences (pour les personnes concernées)
- Mesures prises / envisagées
- Si possible les catégories de données, le nombre de personnes et le nombre de données concernées (RGPD)

Quelles sanctions?

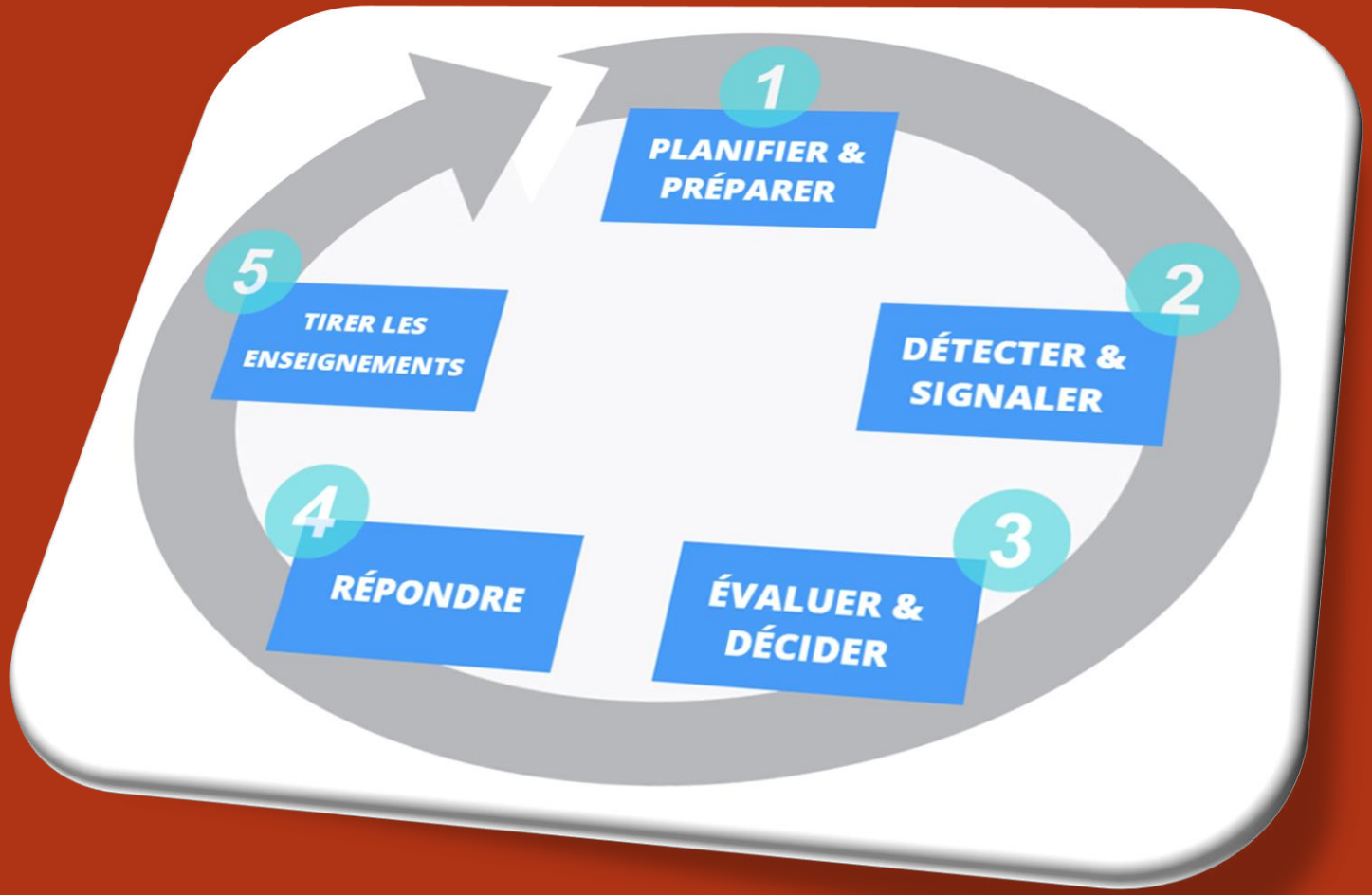
- RGPD
  - Amendes administratives jusqu'à EUR 10 mios ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent

- pLPD
  - Pas de sanction
  - Sauf si notification ordonnée par le PFPDT sous menace d'amende (max. CHF 250'000.-)

Anticiper

Les délais sont courts, il faut être prêt avant la faille!

Processus de gestion des incidents



Source: CNIL, https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser

1. Planifier et préparer (s'entraîner)

- Prévoir des procédures de gestion des incidents
- Avoir un annuaire à jour des personnes à contacter (internes et externes)
- Tester les procédures et (in)former tous les collaborateurs

2. Détecter et signaler (alerter)

- Veille (générale) des menaces actuelles
- Détection technique et remontée d'alertes
- Dispositif humain permettant de signaler sans crainte les failles

3. Évaluer et décider (réunir et analyser)

- Identifier analyser les informations transmises
- Impliquer les bonnes personnes (internes et externes)
- Qualifier l'incident et les obligations qui y sont liées
- Documenter

4. Résoudre et notifier (prendre des mesures et communiquer)

- Prendre les premières mesures de protection et de continuité
- Sauvegarder les preuves
- Notifier l'autorité
- Assurer la communication interne et publique
- Impliquer les autorités judiciaires et policières (?)

5. Apprendre et corriger (gérer et améliorer)

- Comprendre l'origine de la faille et ses conséquences
- Améliorer la sécurité
- Engager les procédures judiciaires éventuelles, soigner la réputation
- Evaluer la gestion de crise
- Améliorer les processus

Conclusion

- Pour réagir correctement en cas de faille, il faut:
  - s'y préparer
  - la collaboration de toutes les personnes concernées
  - comprendre et identifier ce qui se passe
  - bien communiquer
  - sauvegarder ses droits

LAW FIRM
ÉTUDE D'AVOCATS

Sylvain Métille
Dr, avocat, chargé de
cours à l'Université

Av. Auguste Tissot 2bis
CP 851
1001 Lausanne

T 021 310 73 10
F 021 310 73 11

metille@hdclegal.ch
www.hdclegal.ch
www.smetille.ch/blog
@smetille