Check-list et processus en cas de violation de la protection des données

État au 30.05.2023

Note pour l'utilisation :

* Il s'agit d'un modèle de règlement interne pour la protection des données d'une organisation, une directive de protection des données.
* Ce modèle est librement mis à disposition par l'[AEM](https://aem.ch/) à ses membres, ses organisations partenaires et les organisations chrétiennes en Suisse.
* Pour les passages marqués en jaune, il s’agit de laisser ce qui est « applicable » et de compléter ce qui manque. Biffer toutes les autres versions de texte. Par exemple, remplacer le terme Nom de l'organisation XY par le nom de l'organisation concernée.

Clause de non-responsabilité :

Malgré un contrôle minutieux, l'AEM décline toute responsabilité quant au contenu et à l'utilisation de ce modèle.

N'hésitez pas à nous contacter pour de plus amples informations :
Lorena Marti, assistante de la présidence de l'AEM, lorena.marti@aem.ch, +41 43 344 72 07
Beat Leuthold, président de l'AEM, beat.leuthold@aem.ch, +41 79 198 83 76

L'AEM

En tant qu'association faîtière suisse alémanique regroupant aujourd'hui 33 œuvres missionnaires et 5 instituts de formation théologique, l'AEM promeut la cause de la diffusion de l'Evangile en paroles et en actes au-delà de toutes les barrières culturelles, au niveau local et mondial. Elle est un réseau et un centre de compétences pour un travail missionnaire global et s'engage pour la mobilisation, la formation, le lobbying, l'encadrement du personnel et l'assurance qualité.

L'association AEM a été créée en 1972 pour renforcer et encourager les œuvres missionnaires et d'entraide protestantes. L'AEM est une communauté de travail de l'Alliance évangélique suisse alémanique.

Lien : www.aem.ch

Définition de la violation de la sécurité des données

Par analogie avec les objectifs de la sécurité de l'information, l'objectif de la sécurité des données consiste à protéger les données personnelles contre toute perte de confidentialité, d'intégrité ou de disponibilité à l'aide de mesures appropriées. Selon la loi sur la protection des données, il y a violation de la sécurité des données,

* lorsque des données personnelles sont perdues, effacées, détruites ou modifiées de manière accidentelle ou illicite ou si elles sont divulguées ou rendues accessibles à des personnes non autorisées, par exemple en cas de perte d'un support de données tel qu'un ordinateur portable, un DVD, une clé USB, etc. ou en cas de destruction de données par un phénomène naturel tel qu'une inondation, un incendie, etc. ou par une attaque de phishing.
* lorsqu’il y a des indices d'une éventuelle violation de la sécurité des données, comme par exemples :
	+ Effraction / vol
	+ Perte d'un ordinateur ou d'un support contenant des données
	+ Incendie

Obligation de signalement

Une violation de la sécurité des données peut entraîner des risques pour les personnes concernées. On distingue ici les risques et les risques élevés. Selon la loi, il y a risque lorsque la violation de la sécurité des données met vraisemblablement en danger les droits fondamentaux ou la personnalité de certaines personnes concernées. La question suivante peut servir à identifier un risque élevé : *Quelle est la probabilité que la violation entraîne une conséquence négative particulière pour la personne concernée (faible, moyenne, élevée) et comment cette conséquence négative serait-elle qualifiée (faible, moyenne, grave) ?*

Si une conséquence négative grave est au moins probable ou si une conséquence négative modérée est très probable, le risque est élevé. Si la violation de la sécurité des données comporte un risque élevé pour les personnes concernées, elle doit être annoncée au Préposé fédéral à la protection des données et à la transparence (PFPDT)[[1]](#footnote-1).

Les exemples possibles d'un risque élevé pourraient être les suivants :

* Les serveurs de l'œuvre missionnaire sont attaqués et l'on pense que les pirates ont eu accès à toutes les données confidentielles des collaborateurs.
* Suite à une panne technique, toutes les données sensibles des collaborateurs sont effacées et le back-up ne peut pas être restauré.

Check-list

La check-list suivante a pour but d'aider à définir les points qui doivent être définis de manière préventive. En cas de violation (présumée) de la sécurité des données, les étapes importantes du processus sont ainsi déjà clarifiées et les décisions pertinentes sont prises.

|  |
| --- |
| Définition de la personne responsable (responsable de la sécurité des données) |
| En cas de violation de la sécurité des données, le responsable de la sécurité des données doit être immédiatement informé et les mesures nécessaires doivent être mises en œuvre avec lui. |
|

|  |
| --- |
| Documentation |

 |
| La loi sur la protection des données prévoit qu'une violation de la sécurité des données doit être documentée par le responsable de la sécurité des données, dans la mesure où la violation doit être déclarée.La documentation contient au moins :* tous les faits liés à la violation de la sécurité des données (cf. processus Violation de la sécurité des données étape du processus « PS-07, Communication au PFPDT »),
* les conséquences de la violation de la sécurité des données et
* les mesures prises pour endiguer ou éliminer la violation de la sécurité des données.

A partir du moment où la sécurité des données a été violée, la documentation doit être conservée pendant au moins **deux ans**, conformément au règlement sur la protection des données. |

**PS-02**
Signalement immédiat

**PS-03**
Évaluation de l'incident de sécurité des données

**PS-04**
Évaluation des mesures

**PS-05**
Mise en œuvre de mesures immédiates

**PS-07**
Communication au PFPDT

**PS-09**
Notification aux personnes concernées

**PS-06**
Obligation de déclara-tion LPD ?

**PS-08**
Information concernés ?

**PS-10**
Autres mesures ?

**PS-12**
Documentation

**PS-11**
Mise en œuvre d'autres mesures

**Collaborateurs**

**Personne responsable de la sécurité des données**

**Oui**

**Non**

**Oui**

**Non**

**Oui**

**Non**

**Processus de violation de la sécurité des données**

|  |  |  |
| --- | --- | --- |
| Étapes du processus | Activités | Description des activités |
| PS-01 | Violation de la sécurité des données | Une violation de la sécurité des données s'est produite et a été identifiée par le responsable de la sécurité des données ou par un collaborateur. |
| PS-02 | Signalement immédiat | Si des collaborateurs ont identifié une violation (potentielle) de la sécurité des données, la personne responsable de la sécurité des données doit en être informée immédiatement. |
| PS-03 | Évaluation de l'incident de sécurité des données | Le responsable de la sécurité des données évalue le signalement ou la violation présumée de la sécurité des données. |
| PS-04 | Évaluation des mesures | Le responsable de la sécurité des données évalue la violation de la sécurité des données sur la base du risque probable et détermine si des mesures sont nécessaires pour traiter la violation, et lesquelles. Lors de la définition des mesures, on peut faire une distinction entre les mesures immédiates visant à endiguer l'incident et les mesures visant à éviter la cause et à traiter l'incident à long terme. |
| PS-05 | Mise en œuvre de mesures immédiates | Si des mesures d'urgence ont été définies dans l'étape PS-04, elles sont directement mises en œuvre afin d'endiguer la violation de la sécurité des données (p. ex. isolement ou mise hors service de certains services ou systèmes). |
| PS-06 | Obligation de déclaration LPD ? | Dans un deuxième temps, le responsable de la sécurité des données examine si la violation de la sécurité des données peut entraîner un risque élevé pour les personnes concernées (cf. « Obligation d’annoncer »). Dans l'affirmative, il en informe la direction, qui décide de l'obligation de déclarer au PFPDT. |
| PS-07 | Communication au PFPDT | S'il existe une obligation de déclaration, la déclaration au PFPDT est préparée. La loi sur la protection des données prévoit à cet égard que la déclaration de violation de la sécurité des données au PFPDT doit contenir au moins les points suivants :* Type de violation de la sécurité des données (par ex. destruction des données, vol des données, etc.) ;
* si elles sont connues, la date et la durée de la violation ;
* dans la mesure du possible, les catégories de données personnelles et le nombre approximatif de données personnelles concernées ;
* dans la mesure du possible, les catégories de personnes concernées et leur nombre approximatif ;
* les conséquences de la violation de la sécurité des données, y compris les risques éventuels pour les personnes concernées (p. ex. mise en danger de la personnalité, interdiction d'entrée sur le territoire, etc.)
* les mesures prises ou prévues pour remédier au manquement ou en atténuer les conséquences (p. ex. restauration de la sauvegarde dans le cas de données numériques),
* le nom et les coordonnées d'une personne de contact.

S'il n'est pas possible de communiquer toutes les informations en même temps, les autres informations peuvent être mises à la disposition du PFPDT progressivement, dans un délai raisonnable.Remarque : Un inventaire des activités de traitement établi au préalable pourrait aider à déterminer quelles catégories de personnes et quelles données sont concernées par la violation de la sécurité des données. |
| PS-08 | Information aux personnes concernées ? | Le responsable de la sécurité des données évalue si les personnes concernées par la violation de la sécurité des données doivent être informées.Les personnes concernées doivent être informées si :* si des mesures de protection à prendre sont nécessaires (p. ex. modification des données d'accès telles que les mots de passe) ou
* le demande le PFPDT.

Le responsable de la sécurité des données peut limiter, différer ou renoncer à l'information des personnes concernées si :* si cela est nécessaire en raison d'intérêts prépondérants ;
* l'information est interdite en raison d'une obligation légale de garder le secret ;
* l'information est impossible ou implique un effort disproportionné ou
* l'information de la personne concernée est assurée de manière comparable par une communication publique.
 |
| PS-09 | Notification aux personnes concernées | S'il est apparu dans PS-08 qu'une information des personnes concernées est nécessaire, une notification de la violation de la sécurité des données doit être préparée. La notification contient au moins les informations suivantes :* Type de violation de la sécurité des données (p. ex. destruction des données, vol des données, etc.)
* Conséquences de la violation de la sécurité des données, y compris les risques éventuels pour les personnes concernées (p. ex. mise en danger de la personnalité des personnes concernées, interdiction d'entrée sur le territoire, etc.)
* Mesures prises ou prévues pour remédier au manquement ou en atténuer les conséquences (p. ex. restauration de la sauvegarde dans le cas de données numériques).
* Nom et coordonnées d'une personne de contact.
 |
| PS-10 | Autres mesures ? | Lorsque les mesures d'urgence ont été mises en œuvre et que l'obligation d'annoncer au PFPDT et aux personnes concernées a été examinée et, le cas échéant, mise en place, il convient de déterminer si d'autres mesures sont nécessaires. Si tel est le cas, d'autres mesures sont nécessaires, mais elles peuvent être mises en œuvre à moyen ou à long terme (voir également PS-04). |
| PS-11 | Mise en œuvre d'autres mesures | Si d'autres besoins de mesures ont été identifiés, la mise en œuvre de celles-ci peut avoir lieu. |
| PS-12 | Documentation | Le responsable de la sécurité des données documente dans tous les cas la violation de la sécurité des données (cf. « Check-list »). |
| PS-13 | Violation de la sécurité des données traitée | Après avoir mis en œuvre les mesures nécessaires, répondu aux éventuelles questions du PFPDT, fait une éventuelle déclaration et documenté la violation de la sécurité des données, le processus est terminé. |

1. <https://www.edoeb.admin.ch/edoeb/fr/home.html> [↑](#footnote-ref-1)