

## PROCÉDURE À SUIVRE LORS D'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

### 1. INTRODUCTION

En cas de violation, avérée ou présumée, de données à caractère personnel, la présente procédure s'applique. Elle doit garantir que les entreprises BMS sont en mesure de traiter rapidement et, si possible, de limiter les violations éventuelles de données à caractère personnel (telles que définies ci-dessous).

### QUE SONT LES DONNÉES À CARACTÈRE PERSONNEL ?

Sont considérées comme **données à caractère personnelle** toutes les informations concernant une personne physique vivante permettant de l'identifier. Une personne est identifiable lorsque des conclusions peuvent être tirées sur son identité sans grande difficulté. Quelques exemples de données à caractère personnel: Nom, adresse, date de naissance, numéro de téléphone, numéro de compte, titre professionnel, photo, etc.

### 2. QU'EST-CE QU'UNE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL ?

Définition:

*La sécurité des données est violée lorsque des données personnelles sont perdues, effacées, détruites, ou modifiées, ou rendues accessibles ou communiquées à des personnes non autorisées, que ce soit par inadvertance ou illégalement, par une négligence ou une action de tiers ou de collaborateurs/partenaires.*

Exemples:

*La perte ou le vol d'un ordinateur portable ou d'un téléphone mobile contenant des données à caractère personnel, l'envoi à une personne non autorisée d'un fichier Excel (non protégé) ou autre contenant des données à caractère personnel, l'impression d'informations sur les salaires et l'oubli du document sur la photocopieuse, le piratage d'un système contenant des données à caractère personnel et/ou vol ou perte des données, etc.*

Une violation n'est en revanche pas constituée si, lors d'une perte ou d'une dégradation,

- (i) les données à caractère personnel sont cryptées ou anonymisées,
- (ii) il existe une sauvegarde complète et à jour de ces données et
- (iii) l'accès à ces données est contrôlé.

En conséquence, il convient de vérifier, pour chaque incident et selon les circonstances, si une violation est constituée ou non.

### 3. QUAND LA PROCÉDURE S'APPLIQUE-T-ELLE?

Si, des données à caractère personnel sont impliquées dans un incident et que celles-ci ne sont ni cryptées, ni anonymisées, ni intégralement sauvegardées et que leur accès n'est pas contrôlé, il peut y avoir violation des données à caractère personnel et la procédure détaillée ci-dessous s'applique.

### 4. COMMENT UNE VIOLATION DES DONNÉES À CARACTÈRE PERSONNEL EST-ELLE SIGNALÉE EN INTERNE?

#### 4.1 Première notification

Si vous prenez connaissance d'une violation avérée ou présumée de données à caractère personnel, notifiez-la immédiatement aux départements **Legal & Compliance** et **IT** par e-mail aux adresses [dataprotection@bmsuisse.ch](mailto:dataprotection@bmsuisse.ch) et [helpdesk@bmsuisse.ch](mailto:helpdesk@bmsuisse.ch).

Dans un premier temps, vérifiez auprès d'eux qu'il s'agit bien d'une violation.

#### 4.2 Mesures:

Si une violation des données à caractère personnel s'est produite, les points suivants doivent être clarifiés auprès du directeur du département concerné par la violation, sous la conduite du département Legal & Compliance et avec le département IT:

- Catégorie et nombre des données touchées;
- Détermination des mesures nécessaires pour limiter sans délai l'étendue de la violation;
- Nécessité d'informer le Préposé fédéral à la protection des données et à la transparence (PFPDT) de la violation ou, le cas échéant, les personnes concernées;
- Identification des conséquences potentielles pour les personnes concernées et l'entreprise;
- Responsabilité des tiers;
- Mesures appropriées pour l'avenir.

#### 4.3 Est-il nécessaire d'informer le PFPDT?

Seules les violations qui posent un «risque élevé» de conséquences négatives pour les personnes concernées doivent être notifiées au PFPDT. Chaque cas de violation doit donc faire l'objet d'un examen par le département Legal & Compliance, qui le notifie ensuite à l'autorité de protection des données compétente si nécessaire, après consultation du directeur général.

#### 4.4 Est-il nécessaire d'informer la personne concernée?

Il convient de notifier la personne concernée uniquement si la démarche est nécessaire pour sa sécurité, p. ex. si un mot de passe doit être changé pour restaurer la protection d'un compte en ligne parce que des personnes non autorisées ont eu connaissance de ses données d'accès.

## 5. **QUE NOTIFIER AU PFPDT?**

Si une notification au PFPDT est nécessaire, elle doit être faite dans les plus brefs délais et doit comprendre au moins les informations suivantes:

- **Nature de la violation** des données à caractère personnel;
- **Conséquences probables** de la violation;
- **Mesures prises ou envisagées pour remédier à la violation.**

Si vous avez des questions ou que vous avez besoin d'aide, vous pouvez envoyer un e-mail à l'adresse [dataprotection@bmsuisse.ch](mailto:dataprotection@bmsuisse.ch)

## Schéma - Procédure à suivre lors d'une violation de données à caractère personnel

