CORPS GRAND-DUCAL
INCENDIE & SECOURS

doc.2021050-c

Politique de gestion des violations de données à caractère personnel

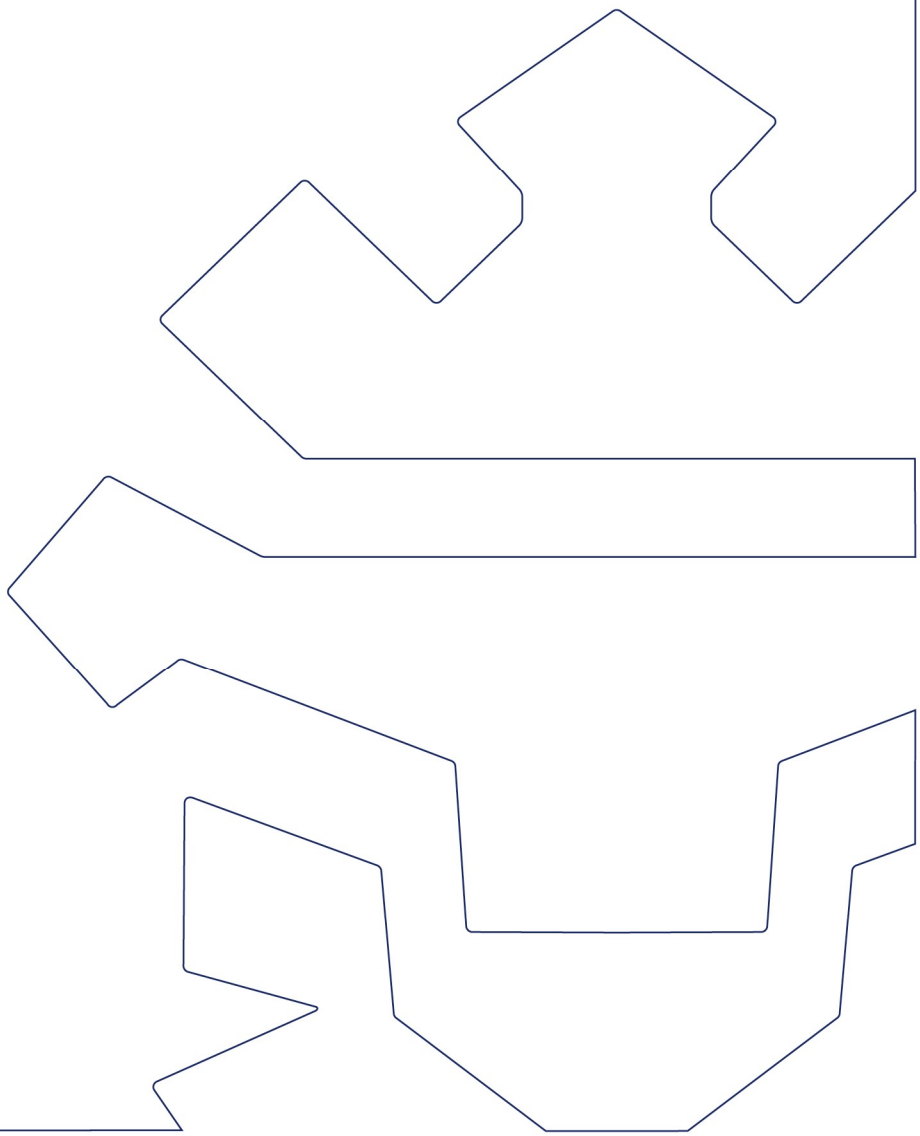

TABLE DES MATIÈRES

1 Définition

Une violation de données personnelles est 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.

2 Signalement d'une violation de données à caractère personnel

Toute personne qui aurait connaissance d'une violation de données à caractère personnel au sens de la présente procédure est tenu de la signaler au Chargé à la protection des données (juridique@cgdis.lu) en indiquant dans la mesure du possible :

- son identité ;
- les catégories de données à caractère personnel concernées ;
- la nature de la violation réelle, potentielle ou suspectée ;
- les personnes physiques concernées par ladite violation des données à caractère personnel ;
- et tout autre information pertinente.

3 Mesures techniques et opérationnelles

Le CGDIS veille à ce que des mesures techniques et organisationnelles appropriées soient prises immédiatement pour minimiser l'impact de toute violation réelle, potentielle ou suspectée de données à caractère personnel et pour éviter qu'une telle situation ne se reproduise.

4 Évaluation des risques

Chaque signalement donne lieu à une évaluation des risques que la violation de données à caractère personnel signalée représente pour les droits et libertés des personnes physiques.

Un risque pour les droits et libertés des personnes physiques existe lorsqu'une violation de données à caractère personnel peut entrainer des dommages physiques, matériels ou immatériels pour les personnes concernées. Lorsque la violation de données à caractère personnel concerne des « catégories particulières de données à caractère personnel » au sens de l'article 9 du règlement européen du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (UE 2016/679), le CGDIS considère automatiquement que ladite violation peut entrainer des dommages physiques, matériels ou immatériels pour les personnes concernées.

Afin d'évaluer le risque, le CGDIS tient compte à la fois de :

- Des circonstances de l'espèce ;

- de la nature, du caractère sensible et du volume des données à caractère personnel concernées ;
- du nombre de personnes physiques concernées ;
- de la gravité de l'impact potentiel que représente une violation de données à caractère personnel sur les droits et libertés des personnes concernées ;
  et
- de la probabilité qu'une telle violation de données à caractère personnel se reproduise ;
- etc.

5 Notification à la CNPD

5.1 Absence de notification

Si l'évaluation du risque indique qu'une violation des données à caractère personnel n'est pas susceptible d'entraîner un risque pour les droits et libertés des personnes physiques, aucune notification à la Commission nationale pour la protection des donnée (CNPD) n'est requise.

5.2 Notification dans les 72 heures

Si l'évaluation du risque indique qu'une violation des données à caractère personnel est susceptible d'entraîner un risque pour les droits et libertés des personnes physiques, le CGDIS en informe la Commission nationale pour la protection des données (databreach@cnpd.lu) au plus tard 72 heures après en avoir eu connaissance au moyen du formulaire prévu à cet effet.

Dans le cas où il ne serait pas possible à la Commission nationale pour la protection des données toutes les informations en même temps, le CGDIS communique ces informations de manière échelonnée.

6 Communication aux personnes concernées

S'il découle de l'analyse de la violation des données à caractère personnel qu'il existe un risque élevé pour les droits et libertés d'une ou de plusieurs personnes physiques déterminées, le CGDIS en informe ces derniers dès que possible.

La notification aux personnes concernées n'est pas requise:

- Lorsque des mesures de protection techniques et organisationnelles 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 (encryptage) ;
- Lorsque le CGDIS a pris des mesures ultérieures pour garantir que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser;
- Lorsqu'une telle communication 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.

7 Registre des violations de données à caractère personnel

Le CGDIS tient un registre de toutes les violations de données à caractère personnel qui lui ont été signalées.

8 Évaluation de la procédure de gestion des violations de données à caractère personnel

Le Chargé à la protection des données à caractère personnel réalise, à intervalles réguliers, une évaluation de la présente procédure de gestion des violations de données à caractère personnel et formule ses propositions à l'attention du comité directeur.