INNOVATEUR D'ASSURANCES

GDPR – Politique de gestion des incidents et des violations de données à caractère personnel

Table des matières

1. Préalable

Le groupe Aedes (ci-après « **Aedes** ») a mis en place un ensemble de mesures et de procédures pour garantir le respect du nouveau règlement général sur la protection des données (ci-après « **RGPD** »).

Parmi celles-ci, la présente Politique de gestion des incidents et des violations de données à caractère personnel a pour objectif de réduire l'impact des incidents de sécurité et des violations de données à caractère personnel en veillant à ce qu'un suivi approprié de ces événements ait lieu.

2. Pourquoi cette politique est-elle pertinente pour vous ?

2.1 Objectif

La présente politique vise à fournir au personnel d'Aedes les règles à suivre pour s'assurer qu'Aedes **réagit d'une manière appropriée** à tout **incident de sécurité réel ou suspecté** impliquant des données à caractère personnel ou toute autre information confidentielle classifiée comme données confidentielles conformément à la politique de classification de l'information d'Aedes[1] (conjointement appelées « **Données** »). Aedes doit s'assurer que tout incident de sécurité réel ou suspecté est signalé, enregistré, enquêté et résolu en temps utile.

Quels sont les risques en cas de non-conformité ?

Une mauvaise gestion des **incidents de sécurité** peut entraîner l'incapacité de fournir des services aux clients, des pertes financières, une atteinte à la réputation et la perte de la confiance du public.

En outre, chaque fois qu'un incident de sécurité est qualifié de **violation de données à caractère personnel** au sens de l'art. 4 (12) du Règlement général sur la protection des données ("**RGPD**"), le non-respect des exigences énoncées aux articles 33 et 34 du RGPD peut donner lieu à d'éventuelles enquêtes par les autorités nationales de protection des données, à des amendes et à la possibilité pour les personnes de déposer des plaintes.

Par conséquent, la présente politique **vise à réduire l'impact** des incidents de sécurité et des violations de données à caractère personnel en assurant un suivi approprié.

2.2 Champ d'application

La présente politique s'applique à tout incident de sécurité rencontré par Aedes SA, Aedes IT Sarl (« Aedes IT ») et les autres entités du groupe (ensemble **« le groupe Aedes** », « **Aedes** » ou « **Nous** » et individuellement « **entité du groupe** ») qui sont soumises au RGPD.

[1] Annexe 1 de la Politique de sécurité des données personnelles

Elle s'applique chaque fois que les systèmes d'information ou les Données d'Aedes (y compris les dossiers papier) sont soupçonnés d'être ou sont effectivement affectés par un événement redouté qui a conduit ou est susceptible de conduire à un incident de sécurité.

Elle ne s'applique pas lorsque les données affectées par un incident de sécurité sont traitées pour le compte d'une autre organisation, auquel cas les exigences de notification des incidents de sécurité font partie des accords contractuels avec cette organisation.

2.3 Déclaration de principe

Le respect de la présente politique est un objectif de l'entreprise et nécessite un **effort de collaboration** de la part de tous les employés, actionnaires ou consultants (ci-après « **membres du personnel** », « **Staff** », ou « **utilisateurs** ») qui ont accès à tout type de Données d'Aedes et/ou utilisent les installations ou équipements informatiques d'Aedes.

3. Quelles sont les principales exigences ?

3.1 Définitions

3.1.1 Incident de sécurité

Un incident de sécurité est défini comme tout événement ayant un effet négatif réel sur la sécurité du réseau, des systèmes informatiques et/ou d'autres ressources d'information.

Un incident de sécurité comprend, sans s'y limiter, les éléments suivants :

- Perte ou vol de Données (format papier ou électronique)
- Perte ou vol de matériel (ordinateur portable, téléphone portable)
- Transfert de Données à ceux qui n'ont pas le droit de les recevoir
- Tentative (échouée ou réussie) d'accès non autorisé à des Données ou au stockage d'informations ou à un système informatique
- Perturbation ou déni de service non souhaité d'un système
- Collecte illégitime d'informations (y compris l'espionnage)
- Ordinateur infecté par un virus ou un autre logiciel malveillant
- Succès des attaques de spamming ou de phishing
- L'utilisation non autorisée d'un système de traitement ou de stockage de données par une personne
- Infractions à la sécurité physique

3.1.2 Violations de données à caractère personnel

Une violation de données à caractère personnel 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 (art. 4 (12) RGPD).

Le RGPD s'applique uniquement lorsqu'il est question de violation de « données à caractère personnel » définies comme étant « tout information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») » (art. 4 (1) RGPD).

Si toutes les violations de données personnelles sont des incidents de sécurité, tous les incidents de sécurité ne sont pas nécessairement des violations de données personnelles.

Les violations de données à caractère personnel peuvent être classées comme suit :

- **Violation de la confidentialité** - lorsqu'il y a une divulgation ou un accès non autorisé ou accidentel à des données à caractère personnel.
- **Violation de l'intégrité** - en cas d'altération non autorisée ou accidentelle de données à caractère personnel.
- **Violation de la disponibilité** - en cas de perte accidentelle ou non autorisée de l'accès à des données à caractère personnel ou de destruction de ces données.

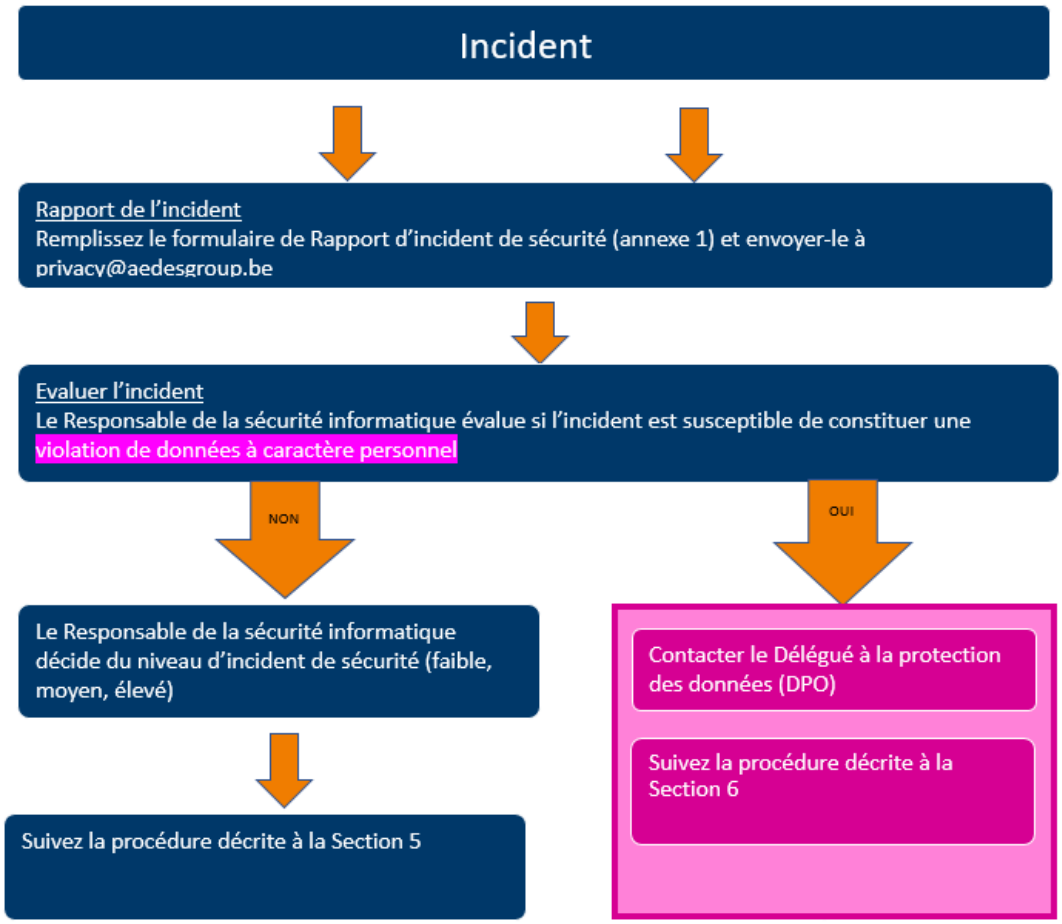
3.2 Procédure à suivre pour la gestion des incidents de sécurité

3.2.1 Rapport

Les incidents de sécurité réels ou présumés doivent être **signalés au Responsable de la sécurité informatique le plus tôt possible.**

Si le rapport d'incident indique que des données personnelles sont concernées, le point 3.3. doit être respecté. Dans le cas contraire, les points 3.2.2 à 3.2.4 s'appliquent.

Le tableau suivant montre comment le signalement de tout incident de sécurité doit être traité :



3.2.2 Evaluer les risques et les mesures à prendre

Le Responsable de la sécurité informatique évalue le niveau d'incident de sécurité sur la base des critères de criticité suivants :

- **Criticité faible** : un incident de sécurité qui peut être géré dans le cadre de procédures d'exploitation normales et avec un faible impact.
- **Criticité moyenne** : un incident de sécurité grave et préjudiciable, nécessitant l'assistance des Responsables techniques ou d'équipes de soutien spécialisées en dehors d'Aedes.
- **Criticité élevée** : un incident de sécurité majeur nécessitant des ressources importantes au-delà des procédures d'exploitation normales, nécessitant une escalade vers l'Equipe de Gestion de Crise et l'activation potentielle du Plan de continuité des opérations.
- **Criticité critique**: un incident de sécurité ayant un impact sérieux sur les services critiques et nécessitant des ressources importantes au-delà des procédures d'exploitation normales, nécessitant une escalade vers l'Equipe de Gestion de Crise, l'activation potentielle du Plan de continuité des opérations, une enquête approfondie et une communication.

Pour plus d'informations sur les critères de criticité, voir l'annexe 2.

Cette évaluation aidera à déterminer :

- Qui doit prendre la direction des opérations de confinement et de récupération après l'incident de sécurité ?
- Qui doit prendre la direction de l'enquête sur l'incident de sécurité ?
- Qui d'autre doit apporter son aide ?
- De quelles ressources a-t-on besoin ?
- Que peut-on faire pour récupérer les pertes éventuelles ?
- Que peut-on faire pour limiter les dommages causés par l'incident de sécurité ?
- L'incident de sécurité doit-il être signalé aux autorités publiques ?

Si un incident de sécurité implique d'autres actes criminels présumés tels que le téléchargement présumé de matériel illégal, le Responsable de la sécurité informatique peut **demander à la police de mener une enquête.**

Si l'enquête sur l'incident de sécurité nécessite l'accès au compte informatique d'un utilisateur, par exemple dans le cas d'un téléchargement présumé de matériel illégal, il faut en référer au département des ressources humaines pour approbation.

3.2.3 Atténuer l'incident de sécurité

Le Responsable de la sécurité informatique et toutes les autres personnes concernées se réuniront pour **s'assurer que toutes les mesures appropriées sont prises** pour en atténuer l'impact et identifier les autres mesures nécessaires pour réduire le risque d'une autre violation de ce type.

3.2.4 Documenter l'incident de sécurité

Le Responsable de la sécurité informatique produira un rapport d'incident de sécurité qui exposera :

- Un résumé de l'incident de sécurité
- Comment et pourquoi l'incident de sécurité s'est produit
- Mesures prises pour résoudre l'incident de sécurité et gérer son impact
- Impact de l'incident de sécurité (opérationnel, financier, juridique, responsabilité, réputation)
- Risques d'autres conséquences négatives de l'incident de sécurité (opérationnelles, financières, juridiques, responsabilité, réputation)
- Toute autre mesure corrective nécessaire pour atténuer l'impact de l'incident
- Actions recommandées pour éviter un renouvellement de l'incident de sécurité
- Implications en termes de ressources ou impacts négatifs, le cas échéant, de ces actions

Le rapport sera inclus dans **un registre central des incidents de sécurité** afin d'identifier les leçons à tirer, les types d'incidents de sécurité et les preuves de faiblesse et d'exposition qui doivent être traitées :

- Quelles mesures doivent être prises pour réduire le risque de violations futures et minimiser leur impact ?
- Faut-il améliorer les politiques, les procédures ou les lignes de compte rendu pour accroître l'efficacité de la réponse à la violation ?
- Y a-t-il des points faibles dans les contrôles de sécurité qui doivent être renforcés ?
- Le personnel et les utilisateurs des services sont-ils conscients de leurs responsabilités en matière de sécurité de l'information et sont-ils suffisamment formés ?
- Des investissements supplémentaires sont-ils nécessaires pour réduire l'exposition et, dans l'affirmative, quelles sont les implications en termes de ressources ?

3.3 Comment gérer la réponse à une violation de données à caractère personnel ?

Si vous êtes victime d'une violation de données à caractère personnel, sachez que 9 étapes doivent être accomplies afin de gérer correctement cette situation :

3.3.1 Détecter et signaler

Dès qu'il a connaissance d'une violation de données réelle, potentielle ou présumée, le membre du personnel concerné doit :

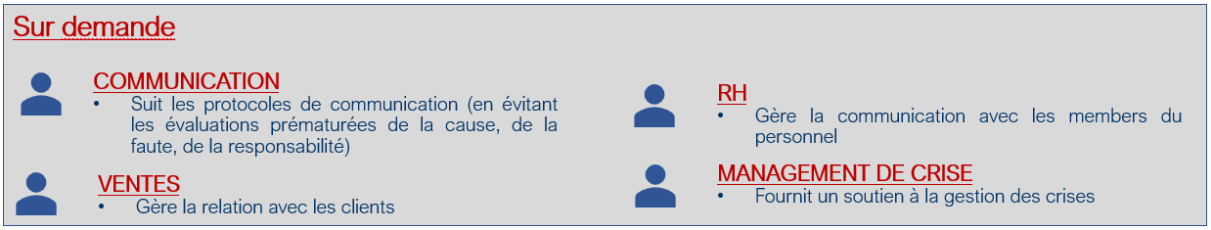
- conformément à la Section 5.1. remplir le "Formulaire de rapport d'incident de sécurité" ci-joint (annexe 1) ;
- et le signaler au Responsable de la sécurité informatique.

3.3.2 Identifier et définir

Après avoir été informée d'une éventuelle violation de données à caractère personnel par le Responsable de la sécurité informatique au moyen du Formulaire de rapport d'incident de sécurité (annexe 1), **l'Equipe de Gestion des Violations de Données** entreprendra une **courte période d'enquête** afin d'établir si une violation s'est effectivement produite ou non.

Pendant cette période d'enquête, Aedes ne peut pas être considéré comme étant "au courant" de la violation des données. Toutefois, il est prévu que cette enquête initiale commence dès que possible et établisse avec un degré raisonnable de certitude si une violation a eu lieu.

L'Equipe de Gestion des Violations de Données est composée de :



Le DPO devrait jouer un rôle clé dans la prévention ou la notification d'une violation en fournissant des conseils et en contrôlant le respect des règles, ainsi que pendant la violation et lors de toute enquête ultérieure de l'autorité de contrôle. Le DPO doit coopérer avec l'autorité de contrôle et agir en tant que point de contact pour celle-ci[2].

[2] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 31.

3.3.3 Collecter information

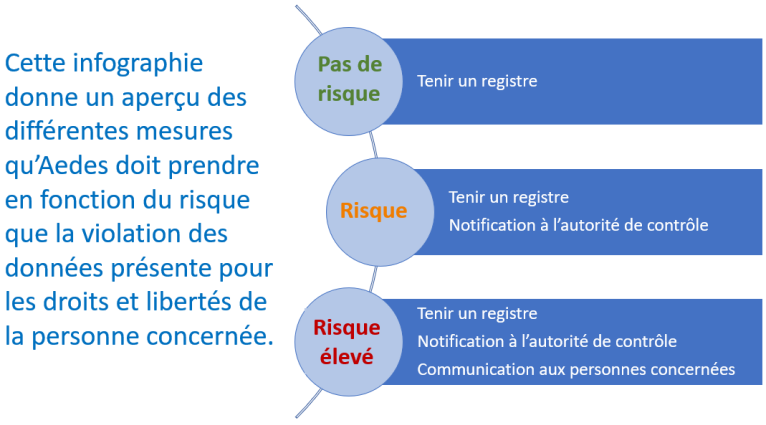
L'Equipe de Gestion des Violations de Données doit utiliser le "**Formulaire de notification de violation de données à caractère personnel**" (Annexe 3) pour recueillir les informations pertinentes concernant la violation, notamment :

- Date et heure de la violation des données ;
- La nature de la violation des données ;
- Les catégories de données à caractère personnel concernées (données ordinaires, données sensibles, catégories spéciales de données) ;
- Le nombre approximatif de données à caractère personnel concernées ;
- Les catégories de personnes concernées ;
- Le nombre approximatif de personnes concernées ;
- Les conséquences probables de la violation ;
- Description des mesures prises pour remédier à la violation des données à caractère personnel ;
- Le nom et les coordonnées du délégué à la protection des données.

Il est important de collecter ces informations, car il s'agit des informations obligatoires que le responsable du traitement doit au minimum notifier à l'autorité de contrôle conformément à l'article 33.3 GDPR (voir étape 6).

3.3.4 Evaluer le risque

Après avoir recueilli suffisamment d'informations sur la violation des données à caractère personnel, l'Equipe de Gestion des Violations de Données doit **évaluer le risque** qui pourrait en résulter.



Il y a un risque lorsque la violation peut entraîner des **dommages physiques, matériels ou immatériels** pour les personnes dont les données ont été violées. Les exemples de tels dommages sont la discrimination, l'usurpation ou la fraude d'identité, les pertes financières et l'atteinte à la réputation. Lorsque la violation concerne des catégories particulières de

données à caractère personnel[3], il convient de considérer que de tels dommages sont susceptibles de se produire.

Lors de l'évaluation du risque, il convient de tenir compte à la fois de la **gravité de l'impact potentiel** sur les droits et libertés de la personne concernée et de la **probabilité** que cela se produise.

Le CEPD[4] et l'ICO[5] recommandent que l'évaluation du risque prenne en compte les critères suivants :

- le **type de violation** ;
- **la nature, la sensibilité et le volume des données à caractère personnel** : de quel type de données s'agit-il ? Quel est le degré de sensibilité ?
- la **facilité d'identification des personnes** : dans quelle mesure sera-t-il facile pour une partie qui a accès à des données à caractère personnel compromises d'identifier des personnes spécifiques ? Existe-t-il un mécanisme de cryptage ?
- la **gravité des conséquences pour les personnes** : quelles sont les conséquences négatives potentielles pour les personnes concernées ? Quelle est leur gravité ou leur importance ? Quelle est la probabilité qu'elles se produisent ?
- **caractéristiques particulières des individus** : les données à caractère personnel concernant des enfants ou d'autres individus vulnérables peuvent être exposées à un risque plus important[6] ;
- **caractéristiques particulières du responsable du traitement** : la nature du responsable du traitement et ses activités peuvent affecter le niveau de risque ;
- le **nombre de personnes concernées** : plus le nombre de personnes concernées est élevé, plus l'impact d'une violation peut être important ;
- le **sort des données** : si des données ont été perdues ou volées, existe-t-il des protections telles que le cryptage ?

Les informations recueillies dans le "Formulaire de notification de violation de données à caractère personnel" (annexe 3) permettront de procéder à cette première évaluation.

3.3.5 Contenir et récupérer

Une fois qu'il a été établi qu'une violation de données à caractère personnel a eu lieu, les mesures appropriées seront prises immédiatement pour **minimiser les effets de la violation**.

Cela implique souvent l'intervention de différents experts tels que le Responsable technique, les ressources humaines et le service juridique.

[3] Exemple : données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou qui comprennent des données génétiques, des données relatives à la santé ou à la vie sexuelle, ou des condamnations et infractions pénales ou des mesures de sécurité connexes.

[4] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 26 à 30.

[5] ICO, Guidance on data security breach management, 12.12.2012, p.3.; L'ICO (Information Commissioner's Office) est l'autorité de contrôle indépendante du Royaume-Uni, créée pour défendre les droits à l'information dans l'intérêt public, promouvoir l'ouverture des organismes publics et la protection des données personnelles.

[6] Par exemple, une organisation médicale traitera des catégories spéciales de données à caractère personnel, ce qui signifie qu'il y a un risque élevé.

Par conséquent, l'Equipe de Gestion des Violations de Données établira un **plan de récupération** avec l'aide de **l'Equipe de Gestion de Crise** d'Aedes, si nécessaire.

L'Equipe de Gestion des Violations de Données veillera à ce que tous les membres du personnel impliqués dans la réponse à l'incident de sécurité **suivent un protocole de communication** pendant l'enquête (par exemple en évitant les évaluations prématurées de la cause, de la faute et de la responsabilité).

Si la violation des données à caractère personnel doit être **divulguée aux employés d'Aedes**, l'Equipe de Gestion des Violations des Données doit gérer la sensibilisation et la communication de la violation et s'assurer que toutes les déclarations concernant l'incident de sécurité sont factuellement exactes et limitées de manière appropriée.

La communication interne doit également indiquer si les informations personnelles des employés sont affectées par l'incident de sécurité.

3.3.6 Notification à l'autorité de contrôle

Sur la base des informations consignées dans le "Formulaire de notification de violation de données à caractère personnel" (annexe 3), l'Equipe de Gestion des Violations de Données déterminera s'il est nécessaire de notifier la violation à l'autorité de contrôle compétente en matière de protection des données.

Par conséquent, l'Equipe de Gestion des Violations de Données envisagera les étapes suivantes :

A) Une notification est-elle requise ?

Les violations qui "ne sont pas susceptibles d'entraîner un risque pour les droits et libertés des personnes physiques" ne doivent pas être notifiées à l'autorité de contrôle.

Selon le CEPD, si des données à caractère personnel ont été rendues, pour l'essentiel, inintelligibles pour tout tiers non autorisé et s'il existe une copie ou une sauvegarde, une violation de la confidentialité portant sur des données à caractère personnel correctement cryptées peut ne pas devoir être notifiée à l'autorité de contrôle.

Toutefois, s'il y a une violation de données à caractère personnel cryptées ne faisant pas l'objet de sauvegarde, il y aura eu une violation de la disponibilité, ce qui pourrait présenter des risques pour les personnes concernées et donc nécessiter une notification[7].

Voir le point 3.3.4 pour de plus amples informations sur l'évaluation des risques ainsi que l'annexe 5 qui contient une liste non exhaustive d'exemples de violations de données à caractère personnel et une explication des cas dans lesquels la violation doit être notifiée.

[7] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 21.

B) Notification dans les 72 heures

L'Equipe de Gestion des Violations de Données notifie la violation de données à caractère personnel sans retard injustifié et, si possible, **au plus tard 72 heures après en avoir eu connaissance**[8].

Toutefois, l'Equipe de Gestion des Violations de Données ne disposera pas toujours de toutes les informations nécessaires concernant une violation dans les 72 heures après en avoir eu connaissance. L'article 33, paragraphe 4, du RGPD prévoit une **notification par étapes**, permettant au responsable du traitement de mener une enquête plus approfondie et d'assurer un suivi en fournissant des informations supplémentaires ultérieurement. Dans ce cas, le responsable du traitement doit fournir les raisons du retard.

C) Information à fournir

L'article 33, §3 du GDPR stipule que les informations suivantes, au minimum, doivent être incluses :

- **Description de la nature de la violation de données à caractère personnel**, y compris, si possible, les catégories et le nombre approximatif de personnes concernées et les catégories et le nombre approximatif de fichiers de données à caractère personnel concernés[9] ;
- **Le nom et les coordonnées du délégué à la protection des données** (ou d'un autre point de contact où l'on peut obtenir de plus amples informations) ;
- Les **conséquences probables** de la violation ;
- **Description des mesures prises** (ou proposées) par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures visant à atténuer les éventuels effets négatifs.

L'autorité de contrôle peut demander des informations complémentaires dans le cadre de son enquête sur une violation.

Notez que le "Formulaire de notification de violation de données à caractère personnel" (annexe 3) comprend ces informations obligatoires.

D) Autorité de contrôle à notifier

L'Equipe de Gestion des Violations de Données doit identifier l'autorité de contrôle compétente. En ce qui concerne cette identification, il existe deux scénarios différents :

- Traitement de données local : en cas de violations concernant un traitement qui a lieu dans un seul État membre, l'autorité de contrôle de cet État membre doit être notifiée[10].

[8] Pour la notion de "en prendre conscience", voir l'étape 2.

[9] Selon le CEPD, les catégories de dossiers de données à caractère personnel peuvent se référer aux différents types de dossiers que le responsable du traitement peut traiter, tels que les données relatives à la santé, les dossiers scolaires, les informations relatives à l'aide sociale, les détails financiers, les numéros de compte bancaire, les numéros de passeport, etc.

[10] Article 33.1 RGPD en combinaison avec l'article 55 RGPD : Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève.

- Traitement de données transfrontalier[11]: chaque fois qu'une violation a lieu dans le cadre d'un traitement transfrontalier et qu'une notification est requise, Aedes devra notifier l'autorité de contrôle principale, qui est l'Autorité de la protection des données belge (Autorité de la protection des données, Rue de la Presse 35, 1000 Bruxelles, Belgique, Tél : +32 (0)2 274 48 00) car c'est l'autorité de contrôle du principal établissement du groupe Aedes[12]. Il est clair qu'en cas de violation impliquant un traitement transfrontalier, la notification doit être faite à l'autorité de contrôle principale, qui n'est pas nécessairement celle où se trouvent les personnes concernées, ni même celle où la violation a eu lieu. Lors de la notification à l'autorité de contrôle principale, l'Equipe de Gestion des Violations de Données doit indiquer, le cas échéant, si la violation concerne des établissements situés dans d'autres Etats membres, et dans quels Etats membres les personnes concernées sont susceptibles d'avoir été affectées par la violation[13].

E) Comment utiliser le « Formulaire de notification de violation de données à caractères personnel » (annexe 3) ?

Le "Formulaire de notification de violation de données à caractère personnel" figurant à l'annexe 3 n'est pas un document obligatoire, mais un modèle qui peut être utilisé pour notifier la violation à l'autorité de contrôle.

Avant d'utiliser le formulaire de notification de violations de données à caractère personnel à des fins de notification, l'Equipe de Gestion des Violations de Données doit **d'abord vérifier si, en vertu du droit national**, l'autorité de contrôle compétente a mis en place un formulaire de notification obligatoire et une procédure spécifique à suivre.

S'il existe un formulaire de notification obligatoire et une procédure nationale, le "Formulaire de notification de violation de données à caractère personnel" figurant à l'annexe 3 ne peut être utilisé qu'à des fins de communication interne et d'archivage.

S'il n'existe pas de formulaire et de procédure de notification obligatoire au niveau national, le "Formulaire de notification de violation de données à caractère personnel" (annexe 3) peut servir de modèle pour la notification à l'autorité de contrôle.

Les autorités de contrôle belge et luxembourgeoise ont publié un formulaire de notification obligatoire conforme au RGPD, vous les trouverez à l'annexe 6. Veuillez noter que l'utilisation de ce formulaire est obligatoire pour notifier une violation à ces autorités de contrôle.

[11] Article 4 (23) RGPD: : traitement transfrontalier signifie soit a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; soit b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres.

[12] Article 56 (1) GDPR

[13] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 19.

3.3.7 Communication aux personnes concernées

Sur la base des informations fournies dans le "Formulaire de notification de violation de données à caractère personnel" et de l'évaluation des risques (section 6.4), l'Equipe de Gestion des Violations de Données déterminera s'il est nécessaire de **communiquer la violation de données aux personnes concernées**.

À cet effet, l'Equipe de Gestion des Violations de Données envisagera les étapes suivantes :

A) Une communication est-elle requise ?

Lorsque la violation des données à caractère personnel est **susceptible d'entraîner un *risque élevé* pour les droits et libertés des personnes physiques**, Aedes communique la violation à la personne concernée sans délai excessif[14].

La communication à la personne concernée n'est pas requise si l'une des conditions suivantes est remplie[15]:

- **Le responsable du traitement a mis en œuvre des mesures techniques et organisationnelles appropriées** pour protéger les données à caractère personnel avant la violation, en particulier les mesures qui rendent les données à caractère personnel inintelligibles pour toute personne qui n'est pas autorisée à y accéder. Par exemple, lorsque les données sont cryptées ;
- **Immédiatement après la violation, le responsable du traitement a pris des mesures** pour que le risque élevé pour les droits et libertés des personnes ne soit plus susceptible de se concrétiser. Par exemple, le responsable du traitement peut avoir immédiatement identifié et pris des mesures à l'encontre de la personne qui a accédé aux données à caractère personnel avant qu'elle n'ait pu faire quoi que ce soit avec ces données ;
- **Contacter les personnes concernées impliquerait des efforts disproportionnés**. Par exemple, lorsque les coordonnées de contact ont été perdues à la suite de la violation ou ne sont pas connues au départ. Toutefois, le responsable du traitement devrait plutôt prévoir une communication publique ou une mesure similaire permettant d'informer les personnes concernées de manière tout aussi efficace.

B) Notification sans retard injustifié

Contrairement à la notification à l'autorité de contrôle, qui doit être notifiée dans les 72 heures, il n'y a pas de délai spécifique pour la notification de la violation des données aux personnes concernées. Toutefois, la violation doit être communiquée à la personne concernée sans retard injustifié, c'est-à-dire **dès que possible**.

C) Informations à fournir

L'objectif principal de la notification aux personnes concernées est de fournir des informations spécifiques sur les mesures qu'ils doivent prendre pour se protéger[16].

[14] Article 34.1 RGPD.
[15] Article 34.3 RGPD.
[16] Considérant 86 RGPD

La communication à la personne concernée comprend au moins[17] :

- Une description de la nature de la violation des données à caractère personnel dans un langage clair et simple ;
- Le nom et les coordonnées du délégué à la protection des données (ou d'un autre point de contact où l'on peut obtenir de plus amples informations) ;
- Les conséquences probables de la violation ;
- Description des mesures prises (ou proposées) par le responsable du traitement pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures visant à atténuer les éventuels effets négatifs.

Le CEPD suggère que le responsable du traitement fournisse également des conseils spécifiques aux personnes concernées afin de les protéger contre les éventuelles conséquences négatives de la violation, comme la réinitialisation des mots de passe dans le cas où leurs droits d'accès ont été compromis[18].

D) Contacter la personne concernée

La communication de la violation aux personnes concernées doit être **claire et transparente**. Cela inclut les messages directs (par exemple, courrier électronique, SMS), les bannières ou notifications sur des sites web bien en vue, la communication postale[19].

Il faut veiller à ce que les personnes concernées soient en mesure de comprendre les informations qui leur sont fournies (par exemple, la langue utilisée dans le cadre des relations commerciales normales avec le destinataire sera généralement appropriée) [20].

3.3.8 Tenir un registre

La documentation de toutes les violations de données à caractère personnel doit être conservée, qu'une violation doive ou non être notifiée à l'autorité de contrôle.

Les aspects suivants doivent être documentés dans un registre[21] :

- les faits relatifs à la violation des données à caractère personnel,
- ses effets et
- les mesures correctives prises.

Le "Formulaire de notification de violation de données à caractère personnel" (annexe 3) fait référence à cette information obligatoire sous :

- Section 3 : À propos de la violation (concerne les faits) ;

[17] Article 34.2 RGPD.
[18] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 21.
[19] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 23 et 24.
[20] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 23 et 24.
[21] Article 33.5 RGPD.

- Section 7 : Conséquences (concerne les effets) ;
- Section 8 : Prendre des mesures (concerne les mesures correctives prises).

En outre, le CEPD recommande que le responsable du traitement documente **également les motifs de la décision prise** en réponse à une violation (par exemple, justification de l'absence de notification, raisons pour lesquelles la violation n'est pas susceptible d'entraîner un risque pour les droits et libertés des personnes) [22].

Par conséquent, afin de documenter de manière appropriée toute mesure de suivi prise, de sorte que l'enquête et l'évaluation de la réponse puissent être effectuées à une date ultérieure, l'Equipe de Gestion des Violations de Données doit remplir le modèle de "Formulaire de mesure prise" (annexe 4).

Le dossier doit **permettre à l'autorité de contrôle de vérifier le respect** de l'article 33 du RGPD[23]. Le fait de ne pas documenter correctement une violation peut conduire l'autorité de contrôle à imposer une amende administrative.

3.3.9 Evaluer les actions prises

Il est important **d'évaluer l'efficacité de la réponse à la violation**.

L'objectif de cet examen est de s'assurer que les mesures prises lors de l'incident de sécurité étaient appropriées et d'identifier les domaines dans lesquels des améliorations peuvent être apportées. Par conséquent, le modèle de "Formulaire de mesures prises" (annexe 4) peut aider à effectuer cette évaluation.

Les points suivants devraient **aider l'Equipe de Gestion des Violations de Données**[24] :

- Savoir quelles sont les données personnelles détenues, où et comment elles sont stockées ;
- Déterminer où se situent les risques les plus importants ;
- Identifier les points faibles des mesures de sécurité existantes ;
- Surveiller la sensibilisation du personnel aux questions de sécurité et chercher à combler les lacunes éventuelles par des formations ou des conseils personnalisés ;
- Déterminer s'il est nécessaire de créer un groupe de personnel technique et non technique qui discutera des scénarios possibles ;

[22] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 30 et 31.
[23] Article 33.5 RGPD.
[24] ICO, Guidance on data security breach management, 12.12.2012, p.7.

4. Quel est votre point de contact ?

4.1 Aide et conseils supplémentaires

Pour tout complément d'information sur les politiques, lignes directrices et lois relatives à la protection des données personnelles, veuillez consulter privacy@aedesgroup.be.

5. Annexes

5.1 Annexe 1 – Signaler un incident de sécurité réel ou présumé

À remplir par la personne qui signale l'incident de sécurité ou le membre du personnel qui reçoit un rapport verbal par téléphone.

Notice confidentielle

Les informations sur les incidents de sécurité réels et présumés sont confidentielles et doivent être partagées uniquement avec les membres du personnel ayant des responsabilités désignées pour la gestion de ces incidents de sécurité.

Formulaire de rapport d'incident de sécurité	
Date de l'incident de sécurité :	Lieu de l'incident de sécurité :
Nom de la personne rapportant l'incident de sécurité : Coordonnées : courriel, téléphone/adresse	
L'incident de sécurité a-t-il un impact sur des données à caractère personnel[25]? ☐ Oui ☐ Non	
Pour le DPO uniquement	
Commentaires du DPO	
Nom de la personne physique impactée (si nécessaire/si possible) Coordonnées : courriel, téléphone/adresse	
Brève description ou détails de l'incident de sécurité (impact, niveau de criticité estimé, emplacement, système ou application touché...)	
Quelles sont les conséquences probables de l'incident de sécurité ?	
Brève description de toute mesure prise au moment de la découverte (qui, quoi, quand...)	
Pour le Responsable de la sécurité uniquement	
Numéro de référence de l'incident de sécurité	
Reçu par	*Sur*
Transmis pour action à	*Sur*

[25] Une donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») » (art. 4.1 RGPD).

5.2 Annexe 2 - Ligne directrice pour la classification des incidents de sécurité

Le tableau ci-dessous est indicatif et ne doit être utilisé qu'à titre indicatif. En cas de doute, veuillez contacter le Responsable de la sécurité informatique à privacy@aedesgroup.be.

Niveau	Exemples	Sécurité			Effort de récupération	Impact	Etendue	Urgence	Autres considérations
		Disponibilité	Confidentialité	Intégrité					
Bas	Infection d'un PC par un virus	Aucun effet sur la capacité de l'organisation à fournir des services aux clients ;	Aucun	Corruption de données non actives (archives, sauvegardes)	Le temps de récupération est prévisible avec les ressources existantes.	Aucun risque financier, de réputation, juridique ou réglementaire	Cas individuels ou isolés	Plus de 24h	A compléter par le Responsable de la sécurité informatique
Moyen	Accès FTP compromis	Effet minime ; l'organisation peut toujours fournir des services essentiels	Divulgation d'informations confidentielles	Intégrité compromise ou corruption de données au sein du/des service(s) interne(s)	Le délai de rétablissement est prévisible grâce à des ressources supplémentaires et une coordination centrale est nécessaire.	Impact financier, juridique, de réputation ou réglementaire potentiel	Plusieurs systèmes sur un même site	Dans les 24 h	Tout incident de sécurité ayant un impact potentiel sur le **plan juridique, financier ou de la réputation** est immédiatement au moins de niveau moyen
Elevé	Vulnérabilité centrale	Impact sur les services essentiels	Divulgation de données strictement confidentielles	Intégrité compromise ou corruption de données au sein du ou des principaux services commerciaux	Le temps de rétablissement est imprévisible ; des ressources supplémentaires et une aide spécialisée sont nécessaires. Une coordination centrale	Forte probabilité d'impact financier, juridique, de réputation ou réglementaire	Plusieurs systèmes sur plusieurs sites	Dans les 4h	* Visible de l'extérieur * Exploitable à distance

Niveau	Exemples	Sécurité			Effort de récupération	Impact	Etendue	Urgence	Autres considérations
		Disponibilité	**Confidentialité**	**Intégrité**					
					au niveau de la direction est nécessaire.				
Critique	Dégradation d'un site web ; compromission d'un réseau d'entreprise par l'exfiltration de données	Un impact sérieux sur les services essentiels	Divulgation de secrets commerciaux ou d'informations stratégiques	Intégrité compromise ou corruption étendue des données au sein d'un ou de plusieurs services essentiels	Récupération de l'incident de sécurité à un coût élevé ou impossible (par exemple, données sensibles exfiltrées et affichées publiquement) ; enquête et communication externe nécessaires.	Incident de sécurité publiquement visible ou en violation d'un contrat, d'une loi ou d'un règlement ; Perte financière.	Plus de 33 % des systèmes concernés	Immédiat	* Visible de l'extérieur * Exploitable à distance * Impact commercial élevé (processus critiques affectés)

5.3 Annexe 3 – Formulaire de notification de violation de données à caractère personnel

Veuillez remplir le formulaire de notification de violation de données à caractère personnel ci-joint :

Annexe 3 Formulaire notification violation .

5.4 Annexe 4 - Formulaire des mesures prises

Formulaire des mesures prises	**A remplir par l'Equipe de Gestion des Violations de Données**
Numéro de l'incident de sécurité :	Ex. année/001
Rapport reçu par :	
Heure de l'incident de sécurité :	
Lieu de l'incident de sécurité :	
Mesures prises par l'Equipe de Gestion des Violations de Données : - Chronologie de l'action - Qui a participé à la réponse à l'incident de sécurité	
Quelles modifications ont été apportées aux systèmes concernés à des fins d'assainissement ?	
Notification à l'autorité de contrôle	☐ Oui, le …./…../…….. ☐ Non, pourquoi ?
Notification aux personnes concernées	☐ Oui, le …./…../…….. ☐ Non, pourquoi ?
Notifications à d'autres personnes	☐ Oui, le …./…../…….. Détails: ☐ Non, pourquoi ?
Réponse à l'autorité de contrôle	☐ Oui, le …./…../…….. Détails: ☐ Non, pourquoi ?

A remplir par l'Equipe de Gestion des Violations de Données :	
Nom:	
Date:	

5.5 Annexe 5 – CEPD : Exemples de violations de données à caractère personnel

Le CEPD fournit les exemples suivants, non exhaustifs, de violations de données à caractère personnel[26] :

Exemple	Notifier la violation à l'autorité de contrôle ?	Notifier la violation aux personnes concernées ?	Notes / Recommandations
i. Un responsable du traitement a stocké une sauvegarde d'une archive de données à caractère personnel cryptées sur une clé USB. La clé est volée lors d'un cambriolage.	Non	Non	Tant que les données sont cryptées à l'aide d'un algorithme de pointe, que des sauvegardes des données existent, que la clé unique n'est pas compromise et que les données peuvent être restaurées en temps utile, cette violation peut ne pas devoir être notifiée. Si les données sont en revanche ultérieurement compromises, la notification est nécessaire.
ii. Un responsable du traitement assure un service en ligne. À la suite d'une cyberattaque sur ce service, des données à caractère personnel de personnes physiques en sont soutirées. Le responsable du traitement n'a de clients que dans un seul État membre.	Oui, avertir l'autorité de contrôle en cas de conséquences probables pour les personnes concernées.	Oui, avertir les personnes concernées en fonction de la nature des données à caractère personnel concernées et si la gravité des conséquences probables pour celles-ci est élevée.	
iii. Une courte panne de courant de quelques minutes dans le centre d'appel d'un responsable du traitement empêche les clients d'appeler ce dernier et d'accéder à leurs dossiers.	Non	Non	Pas d'obligation de notifier la violation, mais l'incident doit être documenté en vertu de l'article 33, paragraphe 5. Des registres appropriés devraient être tenus par le responsable du traitement.

[26] CEPD, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 35 à 38.

Exemple	Notifier la violation à l'autorité de contrôle ?	Notifier la violation aux personnes concernées ?	Notes / Recommandations
iv. Un responsable du traitement est victime d'une cyberattaque au moyen d'un rançongiciel qui crypte toutes ses données. Aucune sauvegarde n'est disponible et les données ne peuvent pas être restaurées. L'enquête révèle que la seule fonctionnalité du rançongiciel était de crypter les données et qu'aucun autre programme malveillant n'est présent dans le système.	Oui, avertir l'autorité de contrôle en cas de conséquences probables pour les personnes concernées, dès lors qu'il s'agit d'une perte de disponibilité.	Oui, avertir les personnes concernées en fonction de la nature des données à caractère personnel concernées et des conséquences potentielles de la perte de disponibilité des données, ainsi que des autres conséquences probables.	Si une sauvegarde avait été disponible et si les données avaient pu être restaurées en temps utile, il n'aurait pas été nécessaire de notifier la violation à l'autorité de contrôle ou aux personnes concernées dès lors qu'il n'y aurait pas eu de perte permanente de la disponibilité ou de la confidentialité. Toutefois, si l'autorité de contrôle prenait connaissance de l'incident par d'autres moyens, elle pourrait envisager de procéder à une enquête afin d'évaluer le respect des exigences de sécurité plus générales de l'article 32.
v. Une personne appelle le centre d'appel d'une banque pour signaler une violation de données. La personne en question a reçu le relevé mensuel d'une autre personne. Le responsable du traitement procède à une courte enquête (c.-à-d. terminée sous 24 heures), établit, avec un degré de certitude raisonnable, qu'une violation de données à caractère personnel s'est produite et signale l'existence potentielle d'un défaut systémique impliquant que d'autres personnes sont ou pourraient être affectées.	Oui	Seules les personnes concernées sont informées en cas de risque élevé et s'il est évident qu'aucune autre personne n'a été affectée.	Si, après une enquête complémentaire, on s'aperçoit que davantage de personnes sont concernées, il convient de notifier cette évolution à l'autorité de contrôle et de prendre des mesures complémentaires afin d'informer les autres personnes concernées en cas de risque élevé pour celles-ci.

Exemple	Notifier la violation à l'autorité de contrôle ?	Notifier la violation aux personnes concernées ?	Notes / Recommandations
vi. Un responsable du traitement gère un marché en ligne et a des clients dans plusieurs États membres. Le marché en question est victime d'une cyberattaque et les noms d'utilisateur, les mots de passe et les historiques d'achat sont publiés en ligne par le pirate.	Oui, informer l'autorité de contrôle chef de file si l'attaque concerne un traitement transfrontalier.	Oui, dès lors que l'attaque pourrait engendrer un risque élevé.	Le responsable devrait prendre des mesures, p. ex. en forçant la réinitialisation des mots de passe des comptes touchés, ainsi que d'autres mesures pour limiter le risque. Le responsable du traitement devrait également tenir compte d'autres obligations de notification, p. ex. en vertu de la directive SRI en tant que fournisseur de service numérique.
vii. Une entreprise d'hébergement de sites internet agissant en tant que sous-traitant détecte une erreur dans le code qui contrôle l'autorisation utilisateur. En raison de ce défaut, n'importe quel utilisateur peut accéder aux informations de compte de n'importe quel autre utilisateur.	En tant que sous-traitant, l'entreprise d'hébergement de sites internet doit avertir les clients concernés (les responsables du traitement) dans les meilleurs délais. En partant du principe que l'entreprise d'hébergement de sites internet a mené sa propre enquête, les responsables du traitement concernés devraient être relativement certains de l'occurrence éventuelle d'une violation, et ils seront probablement considérés comme ayant «pris connaissance» une fois que l'entreprise d'hébergement (le sous-traitant) les en aura informés. Le responsable du traitement doit alors informer l'autorité de contrôle.	Si la violation est peu susceptible d'entraîner un risque élevé pour les personnes concernées, il ne sera pas nécessaire de la leur notifier.	L'entreprise d'hébergement de sites internet (sous-traitant) doit également tenir compte d'autres obligations de notification (p. ex. en vertu de la directive SRI en tant que fournisseur de service numérique). S'il n'existe aucune preuve que cette vulnérabilité a été exploitée chez l'un des responsables du traitement de l'entreprise, il se pourrait que l'incident ne soit pas soumis à l'obligation de notification, mais il est probable qu'il doive être documenté ou qu'il soit le signe d'une non-conformité à l'article 32.

Exemple	Notifier la violation à l'autorité de contrôle ?	Notifier la violation aux personnes concernées ?	Notes / Recommandations
viii. Une cyberattaque rend indisponibles les dossiers médicaux d'un hôpital pendant 30 heures.	Oui, l'hôpital est tenu de le signaler à l'autorité de contrôle dès lors qu'un risque élevé pour le bien-être des patients et leur vie privée pourrait en résulter.	Oui, informer les personnes concernées.	
ix. Des données à caractère personnel d'un grand nombre d'étudiants sont envoyées par erreur à une mauvaise liste d'adresses contenant plus de 1.000 destinataires.	Oui, avertir l'autorité de contrôle.	Oui, avertir les personnes concernées en fonction de la portée et du type de données à caractère personnel concernées ainsi que de la gravité des conséquences potentielles.	
x. Un courrier électronique de marketing direct est envoyé aux destinataires dans les champs «à:» ou «cc:», permettant ainsi à chaque destinataire de voir l'adresse électronique des autres destinataires.	Oui, il pourrait être obligatoire de le notifier à l'autorité de contrôle si un grand nombre de personnes sont touchées, si des données sensibles sont révélées (p. ex. une liste d'adresses de patients d'un psychothérapeute) ou si d'autres facteurs présentent des risques élevés (p. ex. le courrier électronique contient les mots de passe initiaux).	Oui, avertir les personnes concernées en fonction de la portée et du type de données à caractère personnel concernées ainsi que de la gravité des conséquences potentielles.	La notification pourrait ne pas être nécessaire si aucune donnée sensible n'est révélée et si seul un nombre limité d'adresses électroniques a été divulgué.

5.6 Annexe 6 - Formulaire de notification nationale obligatoire

Autorité de contrôle belge :

Si vous devez en informer l'autorité de contrôle belge, veuillez remplir ce formulaire :

Veuillez noter que le formulaire doit être rempli dans l'une des trois langues nationales. Les annexes techniques du formulaire de demande peuvent également être rédigées en anglais, en plus des trois langues nationales (les autres langues ne sont pas autorisées). Si cette condition linguistique n'est pas remplie, la demande sera considérée comme irrecevable.

- Version française du formulaire:

formulaire-pour-une-notification-de-fuite-d

- Version néerlandaise du formulaire:

formulier-voor-de-melding-van-een-gegev

- Version allemande du formulaire:

formular-meldung-eines-datenschutzverstc

Un manuel d'instructions a été rédigé par l'autorité de contrôle pour vous aider à remplir le formulaire :

Mode_demploi_eforms_20190207.pdf

Une fois le formulaire rempli, vous devez l'envoyer via le portail e-forms de l'autorité de contrôle belge : https://eforms.autoriteprotectiondonnees.be/privacy-commission/home/public/upload?language=fr

Autorité de contrôle luxembourgeois :

Si vous devez notifier l'autorité de contrôle luxembourgeoise, veuillez remplir ce formulaire :

- Version française du formulaire:

formulaire-cnpd-data-breach-notification-F

- Version anglaise du formulaire:

formulaire-cnpd-data-breach-notification-E

Veuillez renvoyer ce formulaire dans sa version docx à l'adresse électronique suivante : databreach@cnpd.lu