Violation de données à caractère personnel

Comment notifier l'incident à l'Autorité de protection des données ?

Union des Villes et Communes de Wallonie asbl

Wallonie

Webinaire – 5 avril 2023

Nos invitées

Fanny COTON
Avocate
LEXING

Aurélie WAETERINCKX
Conseillère Communication & porte-parole
APD

Menu de la séance

01 Violation de données à caractère personnel au regard du RGPD : définition et obligations

02 Notifier une violation de données à l'APD : quels conseils donner au notificateur ?

03 Echanges avec les participants

01 02 03

Violation de données à caractère personnel au regard du RGPD : définition et obligations

Fanny COTON

Lexing

LEXING
AVOCATS - ADVOCATEN - LAW FIRM

Rappel du cadre légal :

1. Violation de données, de quoi s'agit-il ?

2. En cas de violation de données, quelles obligations incombent aux responsables de traitement ?

LEXING
AVOCATS - ADVOCATEN - LAW FIRM

Violation de données, de quoi s'agit-il ?

Textes légaux pertinents

- **RGPD**
- **Loi du 30 juillet 2018 – pour les zones de police**
- **Directive NIS** (loi belge du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique) **: pour les opérateurs de services essentiels** (fournisseurs d'eau, transports…)

Définitions

RGPD	Loi 30 juillet 2018 (zones de police)	NIS (opérateurs de services essentiels)
« Violation de données » = 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.		« Incident » = tout événement ayant un **impact négatif réel sur la sécurité** des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels fournis.

À partir de quand y a-t-il un incident ?

RGPD	Loi 30 juillet 2018 (zones de police)	NIS (opérateurs de services essentiels)

Dès que perte de :

- **Confidentialité**
- **Intégrité**
- **Disponibilité**

Il n'est **pas nécessaire** :

- que les données « fuitent » réellement,
- qu'un dommage survienne,
- que la fuite soit connue du public,
- que la cause soit illicite (aussi cause accidentelle)…

Suite à une attaque :

- Installation de virus
- Phishing
- Ransomware
- Vol de données
- Hacking interne
- Paralysie des systèmes et indisponibilité des informations
- Attaque par déni de service

Mais aussi…

- Perte d'une clé USB non chiffrée contenant un fichier Excel avec les données de parents d'élèves
- Perte d'une mallette contenant les soumissions à un marché public
- Envoi d'un e-mail à tous les parents d'élèves d'une école en mettant les destinataires en CC
- Consultation de données médicales par une personne non autorisée au sein d'un hôpital…

Chaque fois, atteinte à :
Confidentialité / Disponibilité / Intégrité

LEXING
AVOCATS - ADVOCATEN - LAW FIRM

En cas de violation de données, quelles obligations incombent aux responsables de traitement ?

Obligations de notification

	RGPD	Loi 30 juillet 2018 (zones de police)	NIS (opérateurs de services essentiels)
À l'autorité compétente	À l'APD	À l'Organe de contrôle de l'information policière	- au CCB (centre belge pour la cybersécurité) - au NCCC (centre de crise national) - à l'autorité sectorielle → En 1 seule fois via la plateforme de notification NIS : **https://nis-incident.be/fr/**
Quand ?	**S'il y a un risque** pour les personnes concernées		Tous les incidents ayant un **impact**
Dans quel délai ?	**72 h**		**Sans retard**
Aux personnes concernées	S'il y a un risque **élevé** Dans les meilleurs délais		x

Comment déterminer le niveau de risque pour savoir s'il faut notifier ?

- Le contexte de la fuite (intentions de l'auteur)
- La nature, la sensibilité et la quantité des données
- La vulnérabilité des personnes concernées
- Les conséquences et préjudices possibles

Exemples tirés de la réalité :

Guidelines 01/2021 on Examples regarding Personal Data Breach Notification

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en

Que retenir de la jurisprudence de l'APD ?

- Pas d'exonération automatique de notification d'une violation de données qui concerne 1 seule personne
- Notifier une violation de données limitée, même si la victime indique porter plainte devant l'APD

Accountability :

- Disposer d'un **registre des incidents**
- Documenter les violations de données non notifiées
- Disposer d'une **procédure en cas de violation de données**
- Pouvoir démontrer la **conscientisation** du personnel

Merci pour votre attention !

Des questions ?

Fanny COTON
Spécialiste en droit de la vie privée

f.coton@lexing.be
T +32 2 381 11 91

01 02 03

Notifier une violation de données à l'APD : quels conseils donner au notificateur ?

Aurélie WAETERINCKX

APD

Notifier une violation de données

Procédure et conseils pratiques

05/04/2023

Autorité de protection des données
Gegevensbeschermingsautoriteit

Avant : prévention

Focus sur la prévention

- En amont : assurez-vous que l'on sache dans votre organisation ce qu'est une violation de données (« *CIA* ») et qui contacter en cas d'incident. Préparez un "*incident response plan*" pour pouvoir réagir au plus vite
  - Par ex. : assurez-vous que votre DPO sensibilise et forme votre personnel
  - Par ex. : veillez à ce que tout soit documenté et consigné (pour rappel, votre registre de traitement doit lister, dans la mesure du possible, les mesures de sécurité entourant vos traitements de données)

À l'aide, une fuite de données !

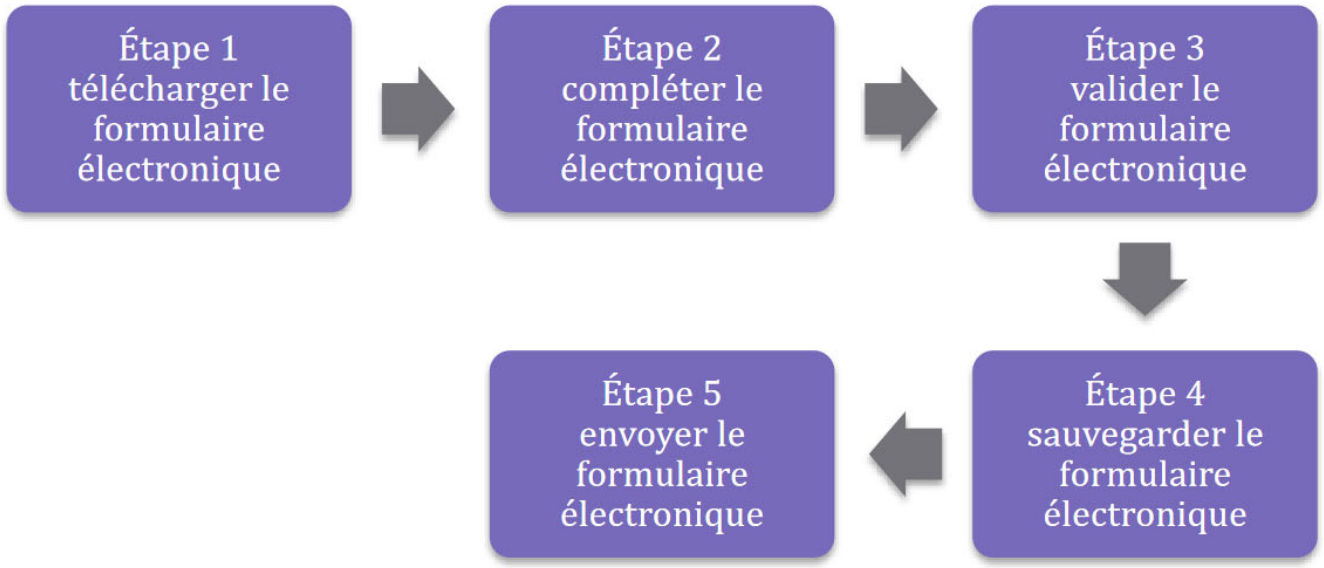
- Une fuite a eu lieu ? Pas de panique !
  - D'abord : évaluez la fuite pour comprendre ce qu'il s'est passé, éventuellement s'il est possible de colmater la fuite au plus vite et comment, et estimer si la violation de données est susceptible d'engendrer des risques pour les individus
  - Sur cette base : évaluez s'il est nécessaire de notifier l'APD, mais aussi les personnes concernées
  - Ces différentes étapes et processus permettront de répondre complétement aux questions du formulaire de notification de violation de données de l'APD
  - Consignez l'incident dans un registre des violations de données interne à votre organisation (contenant incidents passés, conséquences et mesures prises)

La violation de données pourrait engendrer des risques pour les individus concernés ?

- Il faut notifier l'Autorité de protection des données !
- La notification de la violation de données se fait toujours de manière électronique
  - via un ordinateur, et
  - via un formulaire réglementaire
- La notification se fait au plus tard dans les 72 heures après avoir pris connaissance de la violation de données
  - Vous n'avez pas encore pu enquêter sur tous les aspects de la fuite dans ce délai ? Pas de problème : vous pourrez effectuer une notification complémentaire plus tard avec des détails supplémentaires
  - Il vous est également possible d'annuler une notification précédente

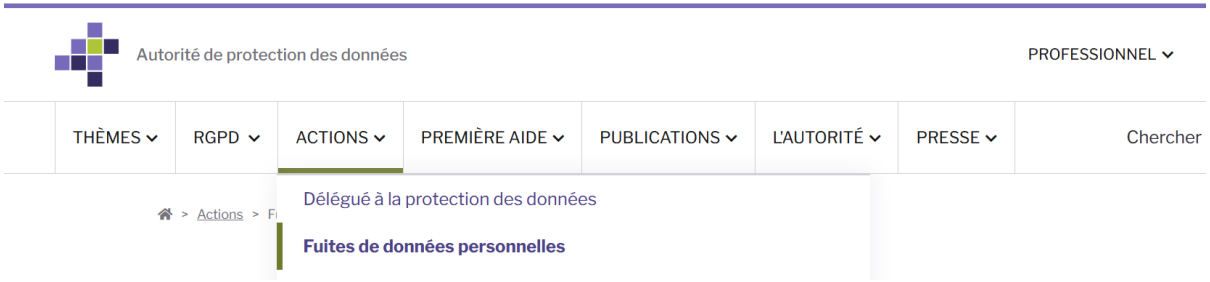
Pendant : gestion de l’incident et formulaire

Processus en 5 étapes



Etape 1 – Télécharger le formulaire (1)

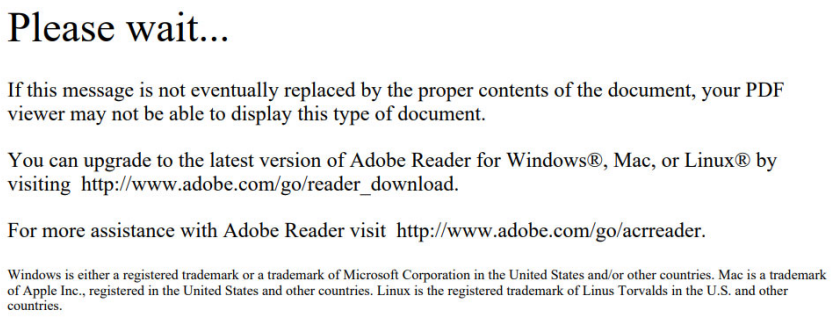
- Le formulaire de notification est disponible dans la partie “professionnels” du site de l’Autorité de protection des données



- Le formulaire existe en français, néerlandais et allemand (et doit être rempli dans l’une de ces langues nationales)
- La page comprend un mode d’emploi et des lignes directrices de l’EDPB avec des exemples pratiques de fuites de données et de comment les notifier

Etape 1 – Télécharger le formulaire (2)

- Téléchargez le formulaire à remplir à chaque nouvelle violation de données
  - Il est déconseillé d'utiliser un formulaire pré-enregistré sur votre ordinateur :
    - Le formulaire peut avoir été mis à jour entretemps
    - Le système ne reconnaîtra pas les champs d'une version dépassée du formulaire
- Après avoir cliqué sur "Téléchargez le formulaire", enregistrez le formulaire PDF sur votre machine
- Si vous ne l'enregistrez pas, vous serez confronté(e) au message suivant :



Please wait...

If this message is not eventually replaced by the proper contents of the document, your PDF viewer may not be able to display this type of document.

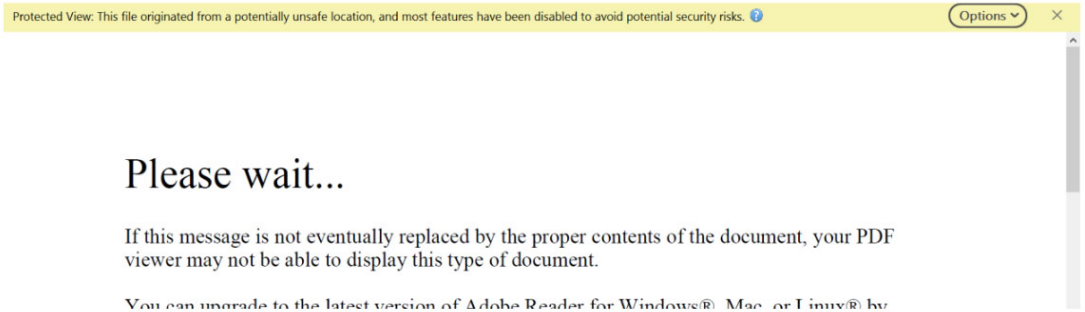
You can upgrade to the latest version of Adobe Reader for Windows®, Mac, or Linux® by visiting http://www.adobe.com/go/reader_download.

For more assistance with Adobe Reader visit http://www.adobe.com/go/acrreader.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. Mac is a trademark of Apple Inc., registered in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Etape 1 – Télécharger le formulaire (3)

- Questions fréquentes :
  - J'ai téléchargé le PDF sur mon appareil, mais je vois toujours apparaître le message d'erreur "*Please wait*"



  - Il vous faudra cliquer sur "*enable all features*" ou "*trust host*" pour accéder au formulaire et toutes ses fonctionnalités
  - Nous conseillons l'utilisation d'*Adobe Acrobat reader* pour compléter le PDF (compatibilité assurée)

Etape 2 – Compléter le formulaire

- Le formulaire peut être utilisé à titre de :
  - Nouvelle notification
  - Notification complémentaire
  - Demande d'annulation d'une notification précédente

- Il convient de remplir un maximum de champs avec le plus de détails possible (soit dans l'immédiat, soit par notification complémentaire au terme de l'enquête sur l'incident)
  - Certains champs sont obligatoires pour valider et envoyer le document

- Remplir le formulaire n'est pas qu'une formalité administrative. S'il permet à l'APD d'évaluer l'incident, il constitue aussi un « exercice de conformité ». Il permet au responsable du traitement d'identifier des vulnérabilités dans ses systèmes et processus, et de prendre des mesures pour éviter des problèmes à l'avenir.

Etape 2 – Compléter le formulaire

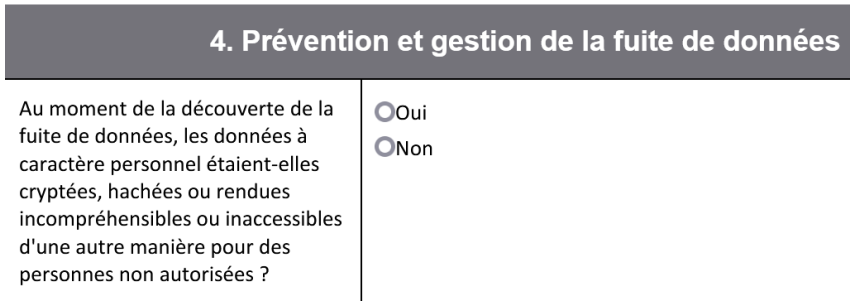
- Eléments importants :
  - La nature des données concernées par la violation
  - Le public touché (nombre, type particulier de public)
  - « CIA » (*Confidentiality*, *Integrity*, & *Availability*)
    - La fuite a-t-elle porté atteinte à la confidentialité, à la disponibilité ou à l'intégrité (fiabilité) des données ?
  - La ligne du temps et le processus
    - Comment la violation a-t-elle été découverte ? Quelle est son origine ? Quelles actions ont été mises en place ?
- Tous ces éléments sont nécessaires car ils permettent :
  - d'estimer les risques potentiellement encourus par les personnes concernées
  - d'identifier les mesures correctrices à prendre pour diminuer ou éviter ces risques
  - de mettre en place de nouveaux processus ou dispositifs de sécurité pour l'avenir

Conseils

- The devil is in the details
  - Soyez le plus détaillé possible. Par ex. :
    - Finalité du traitement : soyez précis, ne dites pas “RH” mais “RH: recrutement”, “RH : paiement des salaires”, etc. Le registre de traitement est un bon outil pour identifier les finalités précises
    - Les personnes concernées se situent dans différents pays ? Indiquez-nous lesquels et combien de personnes sont concernées par pays
    - Résumé de la fuite : donnez une ligne du temps précise et reprenez de manière structurée tous les éléments listés dans le formulaire. Pas assez de place ? Vous pouvez ajouter des documents supplémentaires en pièces jointes
    - Personnes concernées notifiées ? Fournissez une copie datée de votre communication
  - Détails pas encore connus ? Si vous cochez “pas encore connu” dans le formulaire, l’APD attend votre notification complémentaire
    - Fournissez une date à laquelle votre enquête interne sera clôturée : la date doit être réaliste et raisonnable

Erreurs courantes

- **Timing :** si votre notification a lieu en dehors des 72 heures prévues, fournissez une justification pour ce délai supplémentaire
  - Notification systématiquement faite en dehors de l'intervalle de 72 heures ? Indice d'un problème interne lié aux mesures organisationnelles
- **Chiffrement des données :** l'APD dans son formulaire demande si les données ont été chiffrées préalablement à la fuite. Dans le scénario où, suite à une attaque par ransomware, vos données ont été chiffrées par des pirates et rendues illisibles, cochez "non"



Erreurs courantes

- Restez structurés :
  - Rendez le formulaire lisible, répondez aux questions (par ex. : ne répétez pas des informations déjà données dans des champs non prévus à cet effet)
- Evaluation des risques :
  - Ne prenez pas seulement en compte les risques immédiats pour les personnes concernées, mais aussi les éventuels risques futurs
    - Par ex. : croisements de données
  - Inspirez-vous des ressources à votre disposition comme :
    - Le RGPD (considérant 75)
    - Les lignes directrices de l'EDPB applicables (01/2021 et 9/2022)
    - European Union agency for Cybersecurity (ENISA) : outils de self assessment
- Données sensibles : ! attention interprétation large
  - Une donnée permettant d'inférer une donnée sensible est aussi sensible (CJUE C-184/20)

Étapes 3 et 4 – Valider et sauvegarder

- Le formulaire rempli **doit être validé**. L'étape de validation permet de vérifier si aucune donnée n'est manquante ou erronée
  - ! Un formulaire non validé ne sera pas pris en compte par le système
  - !! La validation ne suffit pas pour nous faire parvenir le formulaire, celui-ci doit encore être envoyé sur un portail spécifique (« *e-forms* »)
- Une fois validé, le formulaire doit être sauvegardé à l'aide du bouton "sauvegarder"
- Tips
  - Le formulaire peut être sauvegardé localement en tant que brouillon
  - Gardez l'enregistrement de votre formulaire
    - pour votre documentation interne
    - au cas où vous devriez le réutiliser (par exemple si vous introduisez une notification complémentaire)
  - Les cadres rouges indiquent les champs obligatoires et/ou incorrectement remplis

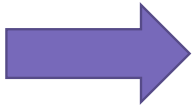
Étape 5 – Envoyez le formulaire électronique

ENVOYEZ LE FORMULAIRE

Envoyez le formulaire complété via notre

portail Internet e-forms

Si l'envoi a bien fonctionné, vous recevrez un e-mail avec un code unique.
Seule la réception de cet e-mail confirme la bonne réception de la notification.



Étape 5 – Envoyez le formulaire électronique

- Vous devrez envoyer votre formulaire via notre portail "*e-forms*", disponible via la page "Notifier une fuite de données"
- Seuls les formulaires électroniques validés seront acceptés par le système
- Vous pouvez ajouter des annexes à votre envoi (attention : pas plus de 2 MB par fichier annexe)
- Après envoi, vous recevrez un accusé de réception et un code d'enregistrement unique: faites-nous donc parvenir une adresse email correcte
  - Seule la réception du code unique confirme l'envoi du formulaire (contactez-nous si vous ne l'avez pas reçu dans les 30 minutes)
  - Si le formulaire envoyé n'est pas validé, vous recevrez un message d'erreur. Les formulaires non validés ne sont ni reçus ni traités par l'APD. Répétez l'opération en envoyant un formulaire validé

Après ? Lessons learned

Une gestion qui va plus loin qu’un simple formulaire

Une gestion qui va plus loin qu'un simple formulaire

- Le processus de notification n'est pas un simple processus administratif : il permet de tirer des leçons et d'éviter des fuites à l'avenir
- La violation de données est susceptible d'engendrer des risques élevés pour les individus ? N'oubliez pas de notifier la fuite également aux personnes concernées
  - L'APD vérifiera que cette étape a eu lieu via son formulaire (et si elle n'a pas eu lieu : pourquoi ?)
- L'APD porte une grande attention aux **mesures de sécurité et organisationnelles** qui étaient mises en place **avant une fuite** (et qui ont pu contribuer à l'atténuer), qui sont mises en place **pendant la fuite** (pour la colmater), et qui sont planifiées **après la fuite**
- Nettoyez régulièrement les données que vous possédez et détruisez efficacement les supports de données (cf. Recommandation 03/2020 de l'APD)
- Restez au fait de l'actualité, suivez le Cert, le Center for Cybersecurity Belgium, d'autres autorités, et inscrivez-vous à notre newsletter

Retour d'expérience : "mieux vaut prévenir que guérir"

- Gardez votre registre de traitement des données à jour (quelles données sont traitées dans quels systèmes ?)
  - Le saviez-vous ? L'APD propose des templates de registre dans sa toolbox
- Mettez en place et maintenez à jour un plan de gestion des incidents
  - Assurez-vous que vos travailleurs sachent vers qui se tourner dès qu'une violation est soupçonnée ou détectée
  - Ayez un back-up sécurisé de vos données (séparé de votre système principal)
  - Ransomware ? Un plan de reprise d'activité après sinistre (*Disaster Recovery plan*) est rarement disponible dans les organisations
  - Faites des campagnes de sensibilisation en interne (culture de sécurité des données = approche fructueuse pour éviter les risques)

Retour d’expérience : conseils pratiques

- Certaines fuites de données peuvent être évitées en conservant une base de données actualisée des programmes logiciels et de leurs versions
  - Tenez cette base de données des logiciels et de leurs éventuelles vulnérabilités à jour grâce aux canaux (officiels) appropriés (tels que le CERT). Les vulnérabilités connues doivent être corrigées le plus rapidement possible afin que les acteurs malveillants ne puissent pas les exploiter
- Prenez des mesures techniques ad hoc supplémentaires (ex. : 2FA, chiffrement, etc.)
- Une grande partie des violations de données continuent de se produire par le biais d'e-mails, entre autres lors de l'envoi et de la réception d'e-mails et en raison de comptes de messagerie électronique insuffisamment sécurisés
  - Mettre en place l’authentification multi-facteurs (MFA)
  - Mots de passe forts changés régulièrement
  - Attention aux champs “cc” et “bcc”
  - Former les collaborateurs contre le phishing

Contact

Aurélie Waeterinckx

communication@apd-gba.be

Rue de la presse 35, 1000 Bruxelles
Drukpersstraat 35, 1000 Brussel

T +32 (0)2 274 48 00
contact@apd-gba.be

Autorité de protection des données
Gegevensbeschermingsautoriteit

Pour aller plus loin…

Nos webinaires en replay : nouvelles technologies
https://www.uvcw.be/formations/webinaires

Nos formations « Management de la donnée»
https://www.uvcw.be/formations/list/data

Prochain événement pour les DPO actifs au sein des pouvoirs locaux wallons :
Matinée de rencontre des DPO (juin 2023 à Namur). Un sondage va vous être envoyé pour identifier la thématique de cette matinée

Votre espace eCampus
Procédure de connexion :
https://vimeo.com/518713611/f3c95176c9

Merci pour votre participation !

À bientôt !