Autorité de protection des données

Champs pour la notification d'une violation de données - PARTIE 1

Table des matières

1. Information

Information au sujet du traitement des données à caractère personnel

L'Autorité de protection des données traite vos données à caractère personnel car elle est légalement tenue d'enregistrer les violations de données à des fins de contrôle et de sanction du non-respect de la réglementation et, au besoin, afin de conseiller l'organisation au sujet de la violation de données Les données à caractère personnel sont conservées tant que cela est nécessaire dans le cadre de la formulation de conseils, du contrôle et de la sanction du non-respect de la réglementation, et ce jusqu'à 10 ans après la clôture du dossier (en cas d'action en justice, jusqu'à la fin de la procédure). Les données du présent formulaire peuvent être partagées avec d'autres autorités de protection des données européennes et/ou nationales, dans le cadre de la collaboration avec celles-ci.

Pour plus d'informations ou pour exercer vos droits en matière de protection des données, veuillez consulter notre déclaration de confidentialité.

Le présent formulaire de notification concerne une notification d'une violation de données à l'Autorité de protection des données conformément à l'article 33 du RGPD.

Lorsqu'il s'agit d'une violation de données qui relève également du champ d'application de la Loi sur les communications électroniques (LCE) et lorsque le responsable du traitement est un opérateur de services de communication électronique déclaré à l'IBPT, une copie de cette notification est transmise à l'IBPT, et ce conformément à l'article 107/3, § 2 de la LCE).

Le responsable du traitement informe l'Autorité de protection des données au plus tard 72 heures après la prise de connaissance de la violation de données.

Les champs de texte libre ont un maximum de 100 caractères (espaces compris), sauf mention contraire.

Pour introduire la violation de données efficacement, vous avez (éventuellement) besoin des informations suivantes lors du processus de notification.

- Si applicable : les coordonnées et les références du DPO-case actif de la notification de votre DPO
- La correspondance relative à la découverte de la violation de données
- Si applicable : le registre des activités de traitement (article 30 du RGPD)
- Le registre des violations de données (article 33.5 du RGPD)
- Les mesures qui étaient déjà en vigueur avant la violation de données
- Les mesures qui ont été prises pour mettre fin à la violation de données
- Les mesures qui ont été prises ou qui sont envisagées afin d'éviter la violation de données à l'avenir
- Si applicable : l'avis du DPO
- L'analyse d'impact relative à la protection des données (AIPD) (art. 35 du RGPD) (si applicable)

- Si applicable : la communication de la violation de données à la (aux) personne(s) concernée(s) (art. 34 du RGPD)

S'il a été question d'un piratage (au sens le plus large), d'un phishing ou de tout autre (cyber)incident et qu'une enquête (externe) a eu lieu :

- Le rapport d'enquête suite à la violation de données

Si vous collaborez avec un sous-traitant ou lorsque la violation de données a eu lieu chez une partie tierce :

- Le contrat de sous-traitance (art. 28 du RGPD)
- Les protocoles d'accord entre autorités (art. 20 de la loi-cadre)
- D'autres accords, comme un accord de coopération (art. 26 du RGPD)

Si vous êtes un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union :

- Le contrat de représentant (article 27 du RGPD).

Enquête en cas de piratage (au sens le plus large), de *phishing* ou de tout autre cyberincident impactant des données à caractère personnel

Lorsque vous notifiez à l'Autorité de protection des données une violation de données causée par le piratage (au sens le plus large), le phishing ou tout autre (cyber)incident impactant des données à caractère personnel, nous attendons de vous que vous réalisiez ou fassiez réaliser une enquête au plus vite sur l'ampleur de l'incident. Cette enquête est nécessaire pour :

- qu'il n'y ait pas de *backdoors* et que d'autres fichiers malveillants ne restent pas présents dans le système ;
- que l'on sache clairement si des données à caractère personnel ont été consultées, copiées, volées ou modifiées par des tiers.

L'Autorité de protection des données attend de vous que vous intégriez les questions suivantes dans votre enquête :

- Y a-t-il eu un accès aux données à caractère personnel, par exemple aux e-mails dans une boîte mail, à des demandes d'impression sur un serveur d'imprimantes, au contenu d'une base de données, à des fichiers sur un serveur de fichiers dans lequel des données à caractère personnel sont traitées, ...
- Ces données à caractère personnel ont-elles été copiées ou consultées par les pirates ou leur ont-elles été envoyées ? A-t-on détecté (via le pare-feu ou non) un flux d'information vers un environnement en dehors de l'entreprise ?
- Y a-t-il des données de connexion disponibles et si oui, est-il possible d'exclure, à l'aide de ces données de connexion, que des données à caractère personnel aient été copiées ou consultées ?

Obligation de documentation - registre des violations de données :

La notification à l'Autorité de protection des données d'une violation de données qui implique un risque potentiel pour les droits et libertés des personnes physiques fait partie des obligations en matière de violations de données. Les responsables du traitement sont également obligés de l'enregistrer en interne dans le registre des violations de données. Cette obligation de documentation vaut d'ailleurs pour toutes les violations de données, donc aussi pour celles qui n'impliquent pas de risque pour

les droits et libertés des personnes physiques. Conformément à l'art. 33.5 du RGPD, les informations suivantes doivent au moins être reprises :

- Les faits relatifs à la violation de données, comme la cause, ce qui s'est passé précisément, quelles mesures ont été prises exactement et à quel moment ainsi que les données à caractère personnel dont il s'agit ;
- Les conséquences de la violation de données ;
- Les mesures qui ont été prises pour mettre fin à la violation de données et pour éviter la récidive ;

Notification d'une violation de données impliquant différents niveaux de risque à l'égard de plusieurs personnes concernées

Si vous notifiez une violation de données impliquant différents niveaux de risque à l'égard de plusieurs personnes concernées avec comme origine un seul et même incident, vous devez reprendre dans votre notification les niveaux de risque les plus élevés.

Vérification : uniquement pour une introduction sans compte (uniquement pour les entreprises belges qui peuvent se connecter via le numéro BCE – FAS)

Numéro d'entreprise :

Déjà complété sur la base du processus de connexion

Pays :

Déjà complété : Belgique

2. Introduction

En vertu de quelle réglementation procédez-vous à la notification ?*

☐ Règlement général sur la protection des données (RGPD) - article 33 du RGPD
☐ Loi sur les communications électroniques (LCE) – art. 107/3, § 3 de la LCE
☐ Code de droit économique (CDE) – art. XII.27 du CDE

Si vous êtes soumis au NIS(II), vous devez également adresser une notification au CCB via le lien suivant : https://notif.safeonweb.be/fr

Si vous êtes un prestataire de services financiers, vous devez peut-être également procéder à une notification à la BNB en vertu du PSDII via le lien suivant :https://www.nbb.be/en/onegate

3. Organisation

3.1. Coordonnées du responsable du traitement

3.2. Nom de l'organisation*

champ de texte libre

3.3. Établissement principal*

- En Belgique (allez à la rubrique 3.3.1.)
- Dans un pays de l'UE/de l'EEE (allez aux rubriques 3.3.2 et 3.3.3.)
- En dehors d'un pays de l'UE/de l'EEE (allez aux rubriques 3.3.2 et 3.3.4.)

3.3.1. Numéro d'entreprise*

Déjà complété sur la base du processus de connexion ou du compte entreprise

3.3.2. Pays de l'établissement principal*

Menu déroulant : liste des pays - un seul choix possible

3.3.3. Numéro de TVA européen

Champ de texte structuré

3.3.4. Numéro national unique*

champ de texte libre

3.4. Dans quel secteur le responsable du traitement est-il actif ?

Menu déroulant secteur - plusieurs réponses possibles :
Activités de service administratif et de soutien
Autre (allez à la rubrique 3.4.1.)
(Agences pour l')emploi, agences d'intérim et gestion du personnel
Construction
Activités immobilières
Activités des organisations et organismes extraterritoriaux
Activités financières et d'assurance
Commerce de gros et de détail
Horeca
Industrie
Information et communication
Art, culture, divertissements et activités récréatives
Santé humaine et activités d'action sociale
Entreprises d'utilité publique
Enseignement
Administration publique
Autres activités de services
Autre organisation – organisations philosophiques

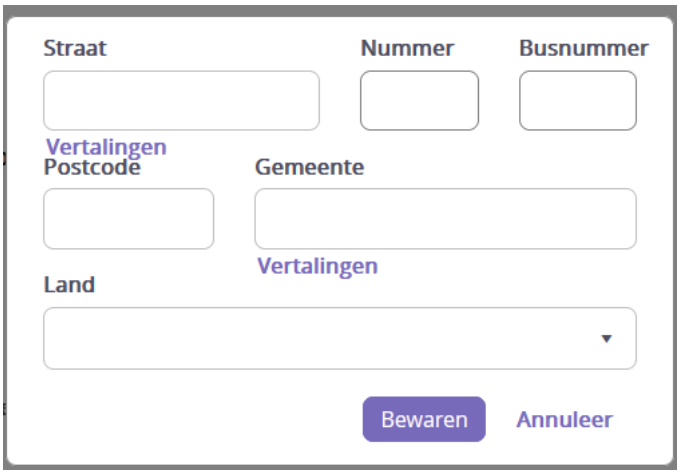
Autre organisation – organisations politiques
Autre organisation – syndicats
Autres services aux entreprises – comptabilité, conseil fiscal et administration
Autres services aux entreprises – recherche scientifique
Police et justice
Réseaux sociaux (entreprises)
Transport
Professions libérales et activités scientifiques et techniques

3.4.1. Autre secteur*

Champ de texte libre

3.5. Adresse et coordonnées du responsable du traitement* (?)

(?) Avez-vous besoin d'aide ? Information sur l'adresse : Seules les adresses belges sont automatiquement complétées. D'autres adresses peuvent être saisies manuellement sans problème, l'adresse suggérée pouvant être ignorée ou écrasée.



3.6. E-mail du Responsable du traitement* (?)

(?) Avez-vous besoin d'aide ? E-mail du Responsable du traitement : Veuillez compléter ici une adresse e-mail générale pour l'entreprise et non une adresse e-mail personnelle ou une adresse e-mail contenant des données à caractère personnel directement identifiables.

Champ de texte libre

3.7. Le responsable du traitement est-il un opérateur (de télécommunications) enregistré auprès de l'IBPT ?* (?)

(?) Avez-vous besoin d'aide ? IBPT : https://www.ibpt.be/operateurs/publication/liste-des-operateurs-de-telecommunications

Menu déroulant :
oui
non

3.8. Le responsable du traitement est-il une entreprise cotée en bourse ?*

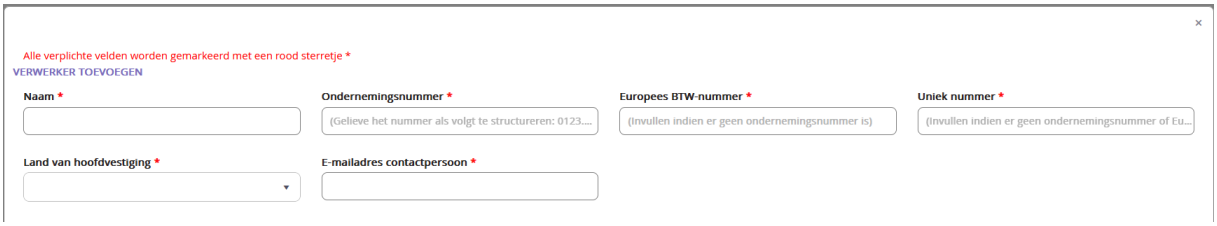
Menu déroulant :
oui
non

3.9. La violation de données a-t-elle eu lieu dans le cadre d'un traitement qui a été confié à un sous-traitant ?*

Menu déroulant :
Oui (allez à la rubrique 2.9.1.)
Non

3.9.1. De quel sous-traitant s'agit-il ?*

Ajouter : (plusieurs réponses possibles)



3.10. Personne de contact pour la violation de données

Nom de la personne*

Champ de texte libre

Prénom de la personne*

Champ de texte libre

Fonction de la personne de contact

Champ de texte libre

Numéro de téléphone de la personne de contact

Champ de texte structuré

E-mail de la personne de contact

Champ de texte structuré

4. Niveau international

4.1. Violation transfrontalière

4.1.1. La violation a-t-elle des conséquences pour des personnes concernées dans plusieurs pays ?*

Menu déroulant :
Oui (allez aux rubriques 4.1.2 et 4.2.1.)
Non

4.1.2. S'il est question d'un traitement transfrontalier, de quels pays s'agit-il (y compris la Belgique, si applicable) et quel est le nombre de personnes concernées dans ces pays (?)*

(?) Avez-vous besoin d'aide ? Veuillez indiquer ci-dessous les différents pays ainsi que le nombre de personnes dans ces pays pour lesquelles la violation de données transfrontalière a des conséquences. S'il n'est pas possible d'identifier le nombre exact de personnes, veuillez indiquer une estimation.

Ajouter : (plusieurs réponses possibles)

Pays	Personnes concernées
Liste de choix : pays	*Nombre de personnes concernées*

4.2. Contrôleurs compétents dans d'autres États membres de l'UE

4.2.1. Votre organisation a-t-elle notifié la violation à d'autres autorités de protection des données ?*

Menu déroulant :
Oui (allez à la rubrique 4.2.1.1.)
Non

4.2.1.1. Veuillez indiquer dans quels pays vous avez notifié la violation aux autorités de protection des données*

Ajouter : (plusieurs réponses possibles)

Liste de choix : pays

5. Ligne du temps

5.1. Date et heure auxquelles la violation de données s'est produite*

Quand la fuite de données s'est-elle produite ?*

Menu déroulant :
Non connu
La date et l'heure exactes auxquelles la violation de données a eu lieu sont connues, à savoir : (allez à la rubrique 5.1.1.)

La date et l'heure exactes auxquelles la violation de données a eu lieu ne sont pas connues, mais sont estimées à : (allez à la rubrique 5.1.1.)

5.1.1. Date et heure auxquelles la violation de données s'est produite*

Champ de date : calendrier	*Champ d'heure : heure*

5.2. Date et heure de la découverte de la violation de données *

Quand la violation de données a-t-elle été découverte ?*(?)
(?) Avez-vous besoin d'aide ? Violation de données - Date et heure de découverte de la violation de données : Le moment de la découverte d'une violation de données n'est pas celui auquel l'incident est notifié au DPO. Le DPO n'est pas responsable de l'obligation de notification à une Autorité de contrôle. L'Autorité de protection des données n'accepte donc pas le moment de la notification au DPO comme justification d'une notification tardive.

Champ de date : calendrier (allez à la rubrique 5.3 si applicable)	*Champ d'heure : heure (allez à la rubrique 5.3 si applicable)*

5.3. Justification de la notification tardive de la violation de données à l'Autorité de protection des données*

Si la présente notification n'est pas effectuée dans les 72 heures après la découverte de la violation de données, quelle en est la raison ? Champ de texte libre - (RGPD)
Si la présente notification n'est pas effectuée dans les 24 heures après la découverte de la violation de données, quelle en est la raison ? Champ de texte libre - (LCE/CDE)

5.4. Quand la violation de données a-t-elle été résolue ?*

Menu déroulant :
La violation de données n'a pas encore été résolue (allez à la rubrique 5.4.1.)
La violation de données a été résolue (allez à la rubrique 5.4.2.)

5.4.1. La raison est la suivante :*

Champ de texte libre

5.4.2. Quand la violation de données a-t-elle été résolue ?*

Champ de date : calendrier	*Champ d'heure : heure*

6. Traitement

6.1. Finalités pour lesquelles les données à caractère personnel sont traitées*

Champ de texte libre

6.2. Nature des données à caractère personnel qui ont été touchées par la violation de données*

Données à caractère personnel en général

- ☐ Données d'identification (par exemple nom, adresse, date de naissance, numéro de téléphone, plaque minéralogique, numéro de client, ...)
- ☐ Données d'identification électroniques (par exemple adresses e-mail, adresses IP, ...)
- ☐ Caractéristiques personnelles (par exemple âge, sexe, état civil, ...)
- ☐ Données physiques (par ex. taille, poids, apparence, ...)
- ☐ Composition du ménage
- ☐ Loisirs et intérêts
- ☐ Profil sur les médias sociaux
- ☐ Affiliations
- ☐ Données CRM (par ex. informations sur les clients, les contacts, la communication, la satisfaction, ...)
- ☐ Profils (clients) (par exemple prévision d'une certaine caractéristique ou attitude, ...)
- ☐ Habitudes en matière de vie, de clic, d'e-mail, de recherche, de navigation, de paiement et/ou de consommation
- ☐ Produits et services (dépenses, consommation, entretien, ...)
- ☐ Caractéristiques de l'habitation et de la voiture
- ☐ Photos ou enregistrements d'images (par ex. CCTV, caméra de surveillance, formation enregistrée, ...)
- ☐ Enregistrements de sons (par exemple conversations téléphoniques enregistrées d'un call center, d'un service client, ...)
- ☐ Études et formation
- ☐ Profession et emploi, régime TVA
- ☐ Données RH (relatives au salaire et à la présence du personnel, évaluations, KPI, plan de carrière)
- ☐ Données de sécurité physiques et/ou ICT des clients, du personnel et des visiteurs (par ex. autorisations et droits, utilisation d'un badge, accès à Internet, ...)
- ☐ Données relatives au contrôle des clients ou du personnel (par exemple connexion, règlement lanceurs d'alerte, traitement des plaintes, contrôle de qualité, ...)
- ☐ Autres : *(champ de texte libre)*

Numéro d'identification unique

- ☐ Numéro national (par exemple le numéro de Registre national)
- ☐ Numéro d'identification de la sécurité sociale
- ☐ Autres : *(champ de texte libre)*

Catégories particulières de données à caractère personnel (article 9.1 du RGPD)

- ☐ Origine raciale ou ethnique
- ☐ Opinions politiques
- ☐ Convictions religieuses ou philosophiques
- ☐ Appartenance syndicale
- ☐ Données génétiques (par ex. ADN, groupe sanguin, ...)
- ☐ Données biométriques (par ex. empreintes digitales, reconnaissance de l'iris, ...)
- ☐ Données concernant la santé
    - ☐ Données physiques
    - ☐ Données psychiques
    - ☐ Données relatives aux soins
    - ☐ Autres : *(champ de texte libre)*
- ☐ Données concernant la vie sexuelle ou l'orientation sexuelle

les données à caractère personnel relatives aux condamnations pénales et aux infractions (article 10 du RGPD)

- ☐ Condamnations pénales
- ☐ Infractions
- ☐ Mesures de sécurité liées à des condamnations pénales ou à des infractions
- ☐ Extrait du casier judiciaire

Données à caractère personnel en dehors des articles 9.1 et 10 du RGPD qui sont traitées en tant que données sensibles car leur traitement implique un certain risque pour les droits et libertés des personnes concernées comme :

- ☐ Contenu de données de communications électroniques
- ☐ Smart Grid (par exemple compteurs intelligents, ...)
- ☐ Données de localisation au sens large (par exemple traitées ou non par des opérateurs télécoms ou via un logiciel de navigation, un GPS, ...)
- ☐ Données financières (numéro de carte bancaire, numéro de compte, numéro de police d'assurance, salaire et revenus, ...)
- ☐ Code d'accès (mot de passe, code PIN, ...)
- ☐ Copies de passeport, eID ou d'autres titres de légitimation
- ☐ Autres : *(champ de texte libre)*

6.3. Nombre de personnes concernées dont des données à caractère personnel ont été affectées*

6.3.1. Le nombre exact de personnes concernées est-il connu ?*

Menu déroulant :
Oui (allez à la rubrique 6.3.1.1.)
Non (allez à la rubrique 6.3.1.2.)

6.3.1.1. Nombre de personnes/personnes concernées*

Nombre/chiffre

6.3.1.2. Nombre minimal/maximal de Personnes/Personnes concernées*

Quel est le nombre minimal de personnes dont des données à caractère personnel sont concernées par la violation de données (en tant que victimes) ?	Quel est le nombre maximal de personnes dont des données à caractère personnel sont concernées par la violation de données (en tant que victimes) ?
Nombre/chiffre	*Nombre/chiffre*

7. Causes

Quelle est la cause de la violation de données ?

7.1. Type de violation de données* (?)

(?) Avez-vous besoin d'aide ? Type de violation de données : Pour plus d'informations quant aux différents types de violations de données dans ce formulaire, consultez notre manuel relatif aux violations de données sur le site Internet de l'Autorité de protection des données.

- ☐ E-mail contenant des données à caractère personnel envoyé à de mauvais destinataires
- ☐ E-mail contenant des données à caractère personnel envoyé avec des destinataires mentionnés dans le champ "à" ou en cc, au lien de l'être en cci
- ☐ Lettre ou colis contenant des données à caractère personnel envoyé(e) ou déposé(e) au mauvais destinataire
- ☐ Autorisations de collaborateurs internes ou externes mal paramétrées (autorisations à l'égard d'un individu) (?)
  (?) Avez-vous besoin d'aide ? La violation de données concerne une situation où les droits d'accès ou de lecture d'un utilisateur n'ont pas été adaptés ou l'ont été suite à une erreur intentionnelle ou de manière malveillante, permettant à un utilisateur de disposer de plus de possibilités dans le système que ce qu'il ne devrait. Par exemple : lors d'un changement de fonction, un rôle d'autorisation n'a pas été exécuté correctement ; droits d'accès paramétrés de manière trop large ; droits d'administrateur pour des personnes non autorisées ; etc.
- ☐ Cartes, applications ou localisation de réseau contenant des données à caractère personnel paramétrées avec un accès trop large au sein de l'organisation (autorisations à l'égard d'un fichier) (?)
  (?) Avez-vous besoin d'aide ? La violation de données concerne une situation où une carte, localisation ou application (partagée) au sein de l'organisation a été mal paramétrée et est consultable par des personnes internes non habilitées. Par exemple : une carte avec des données à caractère personnel réservée au département RH a été rendue accessible pour tous les collaborateurs.
- ☐ Cartes, applications ou localisation de réseau contenant des données à caractère personnel accessibles en dehors de l'organisation (?)
  (?) Avez-vous besoin d'aide ? La violation de données concerne une situation où un fichier, une localisation ou une application a une connexion avec Internet et est accessible à des personnes non autorisées via Internet. Par exemple l'extranet d'une organisation est accessible pour des personnes non autorisées, en dehors de l'organisation.
- ☐ Perte d'appareil (téléphone portable, tablette, etc.), de support de données (par exemple clé USB) et/ou de support papier contenant des données à caractère personnel
- ☐ Vol d'appareil (téléphone portable, tablette, etc.), de support de données (par exemple clé USB) et/ou de support papier contenant des données à caractère personnel
- ☐ Données à caractère personnel indûment publiées. (Par exemple indexation dans un moteur de recherche ; données publiées sur un site Internet, sur une plateforme d'un réseau social, sur un support papier (journal, magazine, etc.)) (?)
  (?) Avez-vous besoin d'aide ? La violation de données concerne une situation où (un fichier contenant) des données à caractère personnel ont (a) été publiées (publié) de manière accidentelle. Par exemple indexation d'un dossier dans des moteurs de recherche, publication de décisions non pseudonymisées, publication non souhaitée de données à caractère personnel sur des plateformes de réseaux sociaux, etc.
- ☐ Données à caractère personnel d'une autre personne affichées sur un portail personnel ou dans un environnement similaire
- ☐ Données à caractère personnel non détruites (correctement) (par exemple des données à caractère personnel lisibles dans une corbeille à papier)
- ☐ Données à caractère personnel indûment détruites
- ☐ DNS spoofing/poisoning (usurpation/empoisonnement de DNS) (?)
  (?) Avez-vous besoin d'aide ? Le DNS spoofing, appelé aussi empoisonnement du cache, est une violation de données où un navigateur est manipulé de sorte que les

visiteurs d'un site Internet sont détournés vers des sites Internet malveillants destinés à dérober des informations sensibles. Le DNS spoofing a lieu lorsque votre cache est infecté par ces détournements malveillants.

- ☐ Phishing
- ☐ Ransomware
- ☐ *Credential Stuffing* (bourrage d'identifiant) (?)
  (?) Avez-vous besoin d'aide ? Le credential stuffing est la saisie automatique de noms d'utilisateurs et de mots de passe volés ("données de connexion") dans des formulaires de connexion de sites Internet afin d'accéder frauduleusement à des comptes d'utilisateurs.
- ☐ Injection SQL (?)
  (?) Avez-vous besoin d'aide ? L'injection SQL (SQLi) est une vulnérabilité dans la sécurité web où un assaillant peut perturber les requêtes qu'une application envoie à sa base de données. L'assaillant peut ainsi consulter les données auxquelles il n'a normalement pas accès. Il peut s'agir de données appartenant à d'autres utilisateurs ou d'autres données auxquelles l'application a accès. Très souvent, l'assaillant peut modifier ou supprimer ces données, modifiant ainsi constamment le contenu et le comportement de l'application.
- ☐ Attaque (D)DOS (?)
  (?) Avez-vous besoin d'aide ? Une attaque "distributed denial-of-service" (DDoS) est une tentative malveillante de perturber le flux normal d'un serveur, d'un service ou d'un réseau consistant à submerger la cible ou l'infrastructure environnante d'un torrent de trafic Internet.
- ☐ Modèles d'IA (leakage/regurgitation, ...) (?)
  (?) Avez-vous besoin d'aide ? La régurgitation est un phénomène dans lequel un modèle d'IA génère des réactions proches des données d'entraînement, révélant ainsi potentiellement des informations sensibles.
- ☐ Coordinated Vulnerability Disclosure Policy/Bug-bounty (?)
  (?) Avez-vous besoin d'aide ? Une politique de révélation coordonnée de vulnérabilités (en anglais : "Coordinated Vulnerability Disclosure Policy" - CVDP) est un ensemble de règles prédéterminées par une organisation responsable de systèmes informatiques permettant à des participants (ou "hackers éthiques") bien intentionnés de détecter d'éventuelles vulnérabilités dans ses systèmes ou de lui transmettre toutes les informations pertinentes à ce sujet.
  Un programme de récompense pour la détection de vulnérabilités (en anglais : "bug bounty") désigne l'ensemble des règles définies par une organisation responsable afin d'attribuer des récompenses aux participants qui identifient des vulnérabilités dans les technologies qu'elle utilise. Il s'agit d'une forme de politique de révélation coordonnée des vulnérabilités qui prévoit l'octroi d'une récompense au participant en fonction de la quantité, de l'importance ou de la qualité des informations fournies.
- ☐ Autre *: champ de texte libre*

7.2. Résumé de la violation de données* (?)

(?) Avez-vous besoin d'aide ? Résumé de la violation de données : Dans le résumé de la violation de données, donnez davantage d'informations sur :

- *La cause, la nature, le type et les circonstances de la violation de données*
- *Le moment de la violation de données et sa découverte*
- *La description du traitement (affecté) et les données à caractère personnel affectées*
- *Les actions et décisions prises (ligne du temps) jusqu'à présent*

Champ de texte libre - maximum 2500 caractères

8. Communication (?)

(?) Avez-vous besoin d'aide ? Communication d'informations : Notification des personnes concernées en cas de violation de données :

L'APD recommande d'informer les personnes concernées en cas de violations de données qui concernent :

- *des catégories particulières de données à caractère personnel (art. 9.1 du RGPD).*
- *des données pénales (art. 10 du RGPD).*
- *des copies de titres d'identité/de passeports ou des numéros de Registre national*
- *des données de groupes vulnérables (par exemple des mineurs)*
- *des grandes quantités de données ou un nombre important de personnes concernées*

Et qui peuvent donner lieu à :

- *la discrimination, la fraude à l'identité, des pertes financières ou une atteinte à la réputation ;*
- *la violation de la vie privée, du secret professionnel ou un impact important sur les droits et libertés.*

Recommandations APD (art. 34 du RGPD) :

- *Si les coordonnées individuelles des personnes concernées sont disponibles, une notification individuelle doit en principe être envoyée, quel que soit le nombre de personnes concernées.*
- *Une communication publique, comme une bannière sur le site web, doit être aussi efficace qu'une communication individuelle.*
- *Les mesures visant à prévenir de futures infractions ne suffisent pas ; seules les mesures qui limitent les risques liés à l'infraction actuelle permettent de se prévaloir de l'exception prévue à l'article 34 du RGPD.*

Contenu de la notification : Il est préférable que la communication contienne:

- *les catégories spécifiques de données affectées afin d'informer les personnes à propos des risques ;*
- *Contenir des suggestions de mesures que les personnes concernées peuvent prendre elles-mêmes.*

Incidents de phishing : En cas de phishing, il peut être nécessaire d'informer trois groupes :

- *Les personnes ayant reçu des e-mails de phishing et le propriétaire de la boîte mail piratée.*
- *Les personnes dont les données figurent dans les e-mails ou les pièces jointes de la boîte mail piratée.*

8.1. Avez-vous déjà notifié la violation aux personnes concernées ?*

Menu déroulant :
Oui (allez à la rubrique 8.1.1.)
Non (allez à la rubrique 8.2.)

8.1.1. Avez-vous informé les personnes concernées individuellement ?*

Menu déroulant :
Oui (allez aux rubriques 8.1.1.1 ; 8.1.1.2. ; 8.1.1.3.)
Non (allez aux rubriques 8.1.1.4 ; 8.1.1.5.)

8.1.1.1. Quel moyen ou canal de communication avez-vous utilisé pour informer individuellement les personnes concernées ?*

☐ Par téléphone : ☐ Par courrier ☐ Par e-mail : ☐ Autre canal : *(champ de texte libre)*

8.1.1.2. À combien de personnes concernées avez-vous notifié individuellement la violation de données ?*

Nombre

8.1.1.3. Quand avez-vous notifié individuellement la violation de données aux personnes concernées ?*

Champ de date : calendrier

8.1.1.4. Quel moyen ou canal de communication avez-vous utilisé pour informer collectivement les personnes concernées ?*

☐ Via une communication sur le site internet ☐ Via les réseaux sociaux ☐ Via une publication dans le journal ☐ Autre canal : *(champ de texte libre)*

8.1.1.5. Quand avez-vous notifié collectivement la violation de données aux personnes concernées ?*

Champ de date : calendrier

8.2. Allez-vous encore notifier la violation aux personnes concernées ?*

Menu déroulant :
Oui (allez aux rubriques 8.2.1. ; 8.2.2.)
Non
Encore inconnu

8.2.1. Quand allez-vous (envisagez-vous de) notifier la violation aux personnes concernées ?*

Champ de date : Calendrier

8.2.2. Allez-vous informer les personnes concernées individuellement ?*

Menu déroulant :
Oui (allez aux rubriques 8.2.2.1 ; 8.2.2.2.)
Non (allez aux rubriques 8.2.2.3 ; 8.2.2.4.)

8.2.2.1. Quel moyen ou canal de communication utiliserez-vous pour informer individuellement les personnes concernées ?*

☐ Par téléphone ☐ Par courrier ☐ Par e-mail ☐ Autre canal : *(champ de texte libre)*

8.2.2.2. À combien de personnes concernées allez-vous notifier la violation de données ?*

Chiffre/nombre

8.2.2.3. Quel moyen ou canal de communication avez-vous utilisé pour informer collectivement les personnes concernées ?*

☐ Via une communication sur le site Internet ☐ Via les réseaux sociaux ☐ Via une publication dans le journal ☐ Autre canal : *(champ de texte libre)*

8.2.2.4. À combien de personnes concernées allez-vous notifier la violation de données ?*

Chiffre/nombre

9. Informations supplémentaires

Indiquez ici toute information susceptible de favoriser une meilleure compréhension de la notification (Maximum 2000 caractères)

Explication

☐ En cochant cette case, vous déclarez être habilité à effectuer la présente notification et que les informations qui y sont fournies sont exactes.

Prouvez que vous n'êtes pas un robot et résolvez l'addition suivante : uniquement pour une introduction sans compte (uniquement pour les entreprises belges qui peuvent se connecter via le numéro BCE – FAS)