Autorité de protection des données

Champs pour la notification d'une violation de données - PARTIE 2

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'article 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.

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

2.1. Avez-vous également notifié la violation de données auprès d'autres contrôleurs nationaux sur la base d'autres obligations de notification ? Ou avez-vous déposé plainte à la police et/ou au parquet ? Ou comptez-vous encore le faire et auprès de qui ?

Menu déroulant :
Oui (allez à la rubrique 2.1.1.)
non

2.1.1. Liste des contrôleurs

☐ Centre pour la Cybersécurité Belgium (CCB) – Cyber Emergency Response Team (CERT)

*Réf. CCB**

☐ Banque nationale de Belgique (BNB)

*Réf. BNB**

☐ SPF Économie

Réf. SPF Économie

☐ Institut belge des services postaux et des télécommunications (IBPT)

*Réf. IBPT**

☐ Police (locale ou fédérale) et/ou Parquet

*Numéro de PV**

□ Autre contrôleur

*Autre contrôleur**	*Référence autre Contrôleur**

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

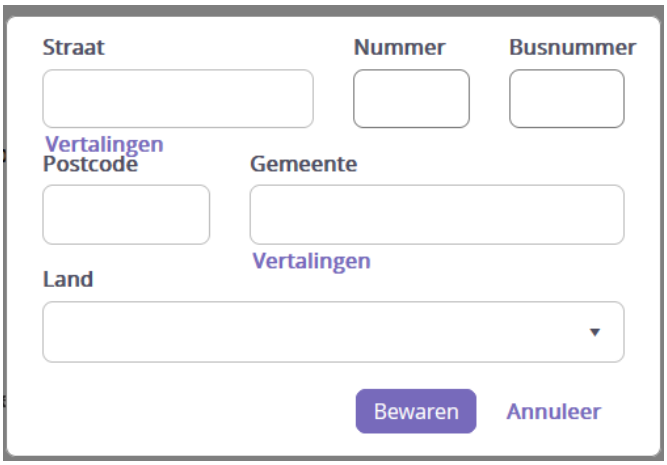
Santé humaine et activités d'action sociale
Entreprises d'utilité publique
Enseignement
Administration publique
Autres activités de services
Autre organisation – organisations philosophiques
Autre organisation – organisations politiques
Autre organisation – syndicats
Autres services aux entreprises – 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 tout à fait être saisies manuellement, 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 ?*

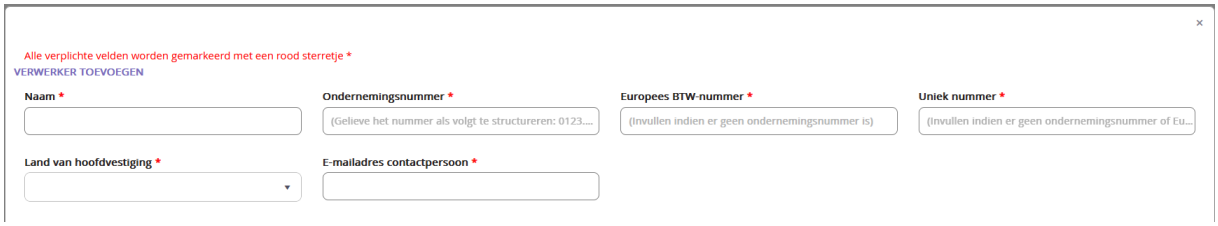
Menu déroulant :
oui
non

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

3.11. Le responsable du traitement dispose-t-il d'un DPO ?*

Menu déroulant :
Oui (allez à la rubrique 3.11.1.)
non

3.11.1. DPO-Case*

Sélectionnez

Si vous n'avez pas encore notifié votre DPO, commencez par le faire via le portail.

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*

4.1.3. L'établissement principal ou le seul établissement du responsable du traitement se trouve-t-il en Belgique ?*

Menu déroulant :
Oui
non

4.1.4. La notification est-elle effectuée sur la base du guichet unique ?*(?)

(?) Avez-vous besoin d'aide ? Guichet unique : Le guichet unique est le mécanisme par lequel une seule autorité de contrôle agit comme autorité de contrôle chef de file pour les responsables du traitement ayant plusieurs établissements dans l'Espace économique européen. Dans ce cas, l'autorité de contrôle chef de file est l'autorité de contrôle de l'État membre où se trouve l'établissement principal du responsable du traitement. Lors de la

notification de violations de données avec effets transfrontaliers, le responsable du traitement ayant plusieurs établissements dans l'EEE peut recourir au mécanisme de guichet unique en notifiant la violation de données (uniquement) à l'autorité de contrôle du pays dans lequel son établissement principal se trouve.

Menu déroulant :
Oui
non

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

4.2.2. La violation de données sera-t-elle encore notifiée à d'autres autorités de protection des données ?*

Menu déroulant :
Oui (allez à la rubrique 4.2.2.1.)
non

4.2.2.1. Veuillez indiquer dans quels pays vous allez encore notifier 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 5.4 si applicable)	*Champ d'heure : heure (allez à la rubrique 5.4 si applicable)*

5.3. Manière dont la violation de données a été découverte*

Menu déroulant :
Notification interne (allez à la rubrique 5.3.1.)
Notification externe (allez à la rubrique 5.3.2.)

5.3.1. Notification interne

Liste de choix : plusieurs réponses possibles

- ☐ Perte de matériel
- ☐ Procédure de gestion (par ex. système de notification d'incident ICT, sécurité de l'information, incident management, ...)
- ☐ Procédure cyber emergency team
- ☐ Système de contrôle afin de détecter des intrusions ou des violations et tout accès non autorisé
- ☐ Procédure de contrôle/règlement lanceurs d'alerte
- ☐ Service de traitement des plaintes
- ☐ Autres : *(champ de texte libre : Veuillez communiquer le nom et le moment*)*

5.3.2. Notification externe

Liste de choix : plusieurs réponses possibles

- ☐ Par un fournisseur ou un sous-traitant (allez à la rubrique 5.3.2.1.)
- ☐ Par un client (allez à la rubrique 5.3.2.1.)
- ☐ Par un tiers (allez à la rubrique 5.3.2.1.)
- ☐ Par un hackeur éthique
- ☐ Par une autorité (allez à la rubrique 5.3.2.1.)

5.3.2.1. Si notification externe par un fournisseur, un sous-traitant, un client, un tiers ou une autorité*

Champ de texte libre : veuillez communiquer le nom et le moment

5.4. 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)

5.5. 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.)

5.5.1. La raison est la suivante :*

Champ de texte libre

5.5.2. 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 *(liste de choix : plusieurs réponses possibles)*

- ☐ 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 *(liste de choix : plusieurs réponses possibles)*

- ☐ Numéro national (par ex. 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) *(liste de choix : plusieurs réponses possibles)*

- ☐ 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

Données à caractère personnel relatives aux condamnations pénales et aux infractions (article 10 du RGPD) *(liste de choix : plusieurs réponses possibles)*

- ☐ 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 peut impliquer un certain risque pour les droits et libertés des personnes concernées comme *(liste de choix : plusieurs réponses possibles)*

- ☐ 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*

6.4. Groupes de personnes concernées touchées par la violation de données*

Plusieurs réponses possibles

- ☐ Citoyens
- ☐ Consommateurs
- ☐ Utilisateurs
- ☐ Détenus
- ☐ Fournisseurs
- ☐ Enfants
- ☐ Militaires ou membres de la police
- ☐ Personnes âgées
- ☐ Patients
- ☐ Élèves et/ou étudiants
- ☐ Réfugiés et demandeurs d'asile
- ☐ Travailleurs/collaborateurs (candidats)
- ☐ Autres *(champ de texte libre : Autres, à savoir :*)
- ☐ Non connu

6.5. Le degré et la possibilité d'identification des personnes concernées sur la base des données sous-jacentes* (?)

(?) Avez-vous besoin d'aide ? Degré d'identification de la (des) personne(s) concernée(s) : Données directement identifiables - Données révélant directement l'identité des personnes concernées à des tiers.

Données indirectement et facilement identifiables - Données ne révélant pas directement l'identité des personnes concernées, mais que des tiers peuvent assez facilement relier à des données d'identification accessibles (publiquement) des personnes concernées.

Données indirectement identifiables - Données ne permettant pas à tout tiers de retrouver directement l'identité de la personne concernée. Il existe toutefois des méthodes permettant de quand même retrouver l'identité civile de la personne concernée à l'aide de données complémentaires (non publiques).

Données reliables indirectement aux personnes concernées - Il existe des techniques et des méthodes permettant à des tiers de relier (une partie de) l'ensemble de données à des

individus spécifiques (le fait d'individualiser des personnes dans des ensembles de données ou "single out", en anglais).

Plusieurs réponses possibles

- ☐ Données directement identifiables
- ☐ Données identifiables indirectement et facilement
- ☐ Données indirectement identifiables
- ☐ Données pouvant être indirectement reliées à des personnes concernées

7. Causes

7.1. Quelle est la cause de la violation de données ?

La cause de la violation de données était*

Menu déroulant :
Interne (par exemple du fait du personnel)
Externe (par exemple du fait d'un hacker)

La violation de données a été causée par*

Menu déroulant :
Un acte technique lié au système
Une intervention humaine

L'intention derrière la violation de données était*

Menu déroulant :
Accidentelle
Action malveillante

7.2. Quelle est la nature de la violation de données ?

- ☐ Violation du caractère confidentiel des données à caractère personnel – violation de confidentialité (allez à la rubrique 7.2.1.)
- ☐ Violation de la disponibilité des données à caractère personnel – violation de disponibilité (allez à la rubrique 7.2.2.)
- ☐ Violation de l'intégrité des données à caractère personnel – violation d'intégrité (allez à la rubrique 7.2.3.)

7.2.1. Distribution - Ordre de grandeur des destinataires des données* (?)

(?) Avez-vous besoin d'aide ? Nombre de personnes :

- *Groupe limité : inférieur à 10 % du nombre de collaborateurs.*
- *Grand groupe : à partir de 10 % du nombre de collaborateurs.*

Booléen : une seule possibilité

- ○ Nombre de personnes inconnu
- ○ Nombre de personnes connu :
  - ○ Une seule personne ou organisation
  - ○ Un groupe limité
  - ○ Un grand groupe

7.2.2. Les données sont* (?)

(?) Avez-vous besoin d'aide ? Disponibilité des données :

- *Longue période : veuillez la déterminer vous-même selon la fonction et le contexte des activités de traitement.*
- *Courte période : veuillez la déterminer vous-même selon la fonction et le contexte des activités de traitement.*

Booléen : une seule possibilité

- Sont définitivement indisponibles
- Sont temporairement indisponibles :
  - Pendant une longue période
  - Pendant une courte période

7.2.3. Importance de l'impact*

- Les données sont peu fiables, incorrectes et ne peuvent plus être modifiées, récupérées ou restaurées.
- Les modifications aux données peuvent être retrouvées, récupérées ou restaurées sur la base de fichiers de journalisation et/ou de sauvegarde.

7.3. 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.

Plusieurs réponses possibles

- ☐ E-mail contenant des données à caractère personnel envoyé à de mauvais destinataires (allez à la rubrique 7.3.1.)
- ☐ E-mail contenant des données à caractère personnel envoyé avec des destinataires repris dans le champ "à" ou en cc, au lien de l'être en cci (allez à la rubrique 7.3.2.)
- ☐ Lettre ou colis contenant des données à caractère personnel envoyé ou déposé au mauvais destinataire (allez à la rubrique 7.3.3.)
- ☐ Autorisations de collaborateurs internes ou externes mal paramétrées (autorisations à l'égard d'un individu) (?) (allez aux rubriques 7.3.4. et 7.3.5.)
  (?) 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) (?) (allez aux rubriques 7.3.6 ; 7.3.7 et 7.3.8.)
  (?) 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 (?) (allez aux rubriques 7.3.6 ; 7.3.7 et 7.3.8.)
  (?) 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 (allez aux rubriques 7.3.9 ; 7.3.10 et 7.3.11)
- ☐ 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 (allez aux rubriques 7.3.9 ; 7.3.10 et 7.3.11)
- ☐ 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.)) (?) (allez aux rubriques 7.3.12 ; 7.3.13. et 7.3.14.)
  (?) 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 (allez aux rubriques 7.3.15 ; 7.3.16 et 7.3.17.)
- ☐ Données à caractère personnel non détruites (correctement) (par exemple des données à caractère personnel lisibles dans une corbeille à papier) (allez à la rubrique 7.3.18.)
- ☐ Données à caractère personnel détruites erronément (allez à la rubrique 7.3.18.)
- ☐ DNS spoofing/poisoning (usurpation/empoisonnement de DNS) (?) (allez aux rubriques 7.3.19 ; 7.3.20 ; 7.3.21 ; 7.3.22)
  (?) 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 (allez aux rubriques 7.3.23 ; 7.3.24 ; 7.3.25 ; 7.3.26 ; 7.3.27 ; 7.3.28 ; 7.3.29)
- ☐ Ransomware (allez aux rubriques 7.3.30 ; 7.3.31 ; 7.3.32 ; 7.3.33 et 7.3.34)
- ☐ Credential Stuffing (bourrage d'identifiant) (?) (allez aux rubriques 7.3.35 ; 7.3.36. et 7.3.37)
  (?) 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 (?) (allez aux rubriques 7.3.38 ; 7.3.39 ; 7.3.40 et 7.3.41.)
  (?) 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 (?) (allez aux rubriques 7.3.42 ; 7.3.43. et 7.3.44)
  (?) 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*

E-mail contenant des données à caractère personnel envoyé à de mauvais destinataires

7.3.1. Le mauvais destinataire a-t-il confirmé avoir supprimé l'e-mail et ne pas avoir utilisé (ultérieurement) les données à caractère personnel ?*

Menu déroulant :
Oui
Non

E-mail contenant des données à caractère personnel envoyé avec des destinataires repris dans le champ "à" ou en cc, au lien de l'être en cci

7.3.2. Avez-vous envoyé un (nouvel) e-mail aux destinataires (en les mettant cette fois en cci)

demandant de supprimer l'e-mail précédent et de ne pas utiliser (ultérieurement) les données à caractère personnel ?*

Menu déroulant :
Oui
Non

Lettre ou colis contenant des données à caractère personnel envoyé(e) ou déposé(e) au mauvais destinataire

7.3.3. Le mauvais destinataire a-t-il confirmé que les données à caractère personnel ont été détruites ou qu'elles ont été renvoyées ?

Menu déroulant :
Oui
Non

Autorisations de collaborateurs internes ou externes mal paramétrées (autorisations à l'égard d'un individu)

7.3.4. Avez-vous indiqué au collaborateur interne ou externe que les informations ne pouvaient pas être réutilisées à d'autres fins ?*

Menu déroulant :
Oui
Non

7.3.5. Le collaborateur interne ou externe a-t-il pris des copies de documents contenant des données à caractère personnel alors qu'il n'était pas autorisé à y accéder ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.5.1.)
Non
Non connu

7.3.5.1. Les copies ont-elles été récupérées ?

Menu déroulant :
Oui
Non

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) et cartes, applications ou localisation de réseau contenant des données à caractère personnel accessibles en dehors de l'organisation

7.3.6. Peut-on vérifier, sur la base des fichiers de journalisation ou de paramètres similaires, combien de personnes ont eu accès aux cartes, applications ou localisations de réseau ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.6.1.)
Non

7.3.6.1. Combien de personnes ont eu accès de manière illicite aux cartes, applications ou localisations de réseau ?*

Champ de chiffre

7.3.7. Peut-on vérifier, sur la base de fichiers de journalisation ou de paramètres similaires, à quel moment des personnes ont eu accès aux cartes, applications ou localisations de réseau ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.7.1.)
Non

7.3.7.1. À quel moment le premier accès illicite s'est-il produit ?*

Champ de date	*Champ d'heure*

7.3.8. Peut-on vérifier si l'on a effectué des téléchargements ou des copies similaires des

informations contenues dans les cartes, applications ou localisations de réseau ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.8.1.)
Non

7.3.8.1. Les téléchargements ou copies similaires ont-ils/elles été récupéré(e)s ?*

Menu déroulant :
Oui
Non

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 et 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

7.3.9. L'appareil ou le support de données était-il protégé par MFA ?*

Menu déroulant :
Oui
Non (allez à la rubrique 7.3.9.1.)

7.3.9.1. L'appareil ou le support de données était-il protégé par un mot de passe ?

Menu déroulant :
Oui
Non

7.3.10. Les données à caractère personnel sur l'appareil ou le support de données étaient-elles rendues illisibles par cryptage, des fonctions de hashing ou une technique similaire ?

Menu déroulant :
Oui (allez à la rubrique 7.3.10.1.)
Non

7.3.10.1. Quels protocole de cryptage, fonction de hashing ou technique similaire ont été utilisés concrètement ?*

Plusieurs réponses possibles

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Autres : *champ de texte libre**

Les données sur l'appareil ont-elles entre-temps été effacées à distance ?*

Menu déroulant :
Oui
Non

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.))

7.3.11. À quel endroit précis (lieu) les données à caractère personnel ont-elles été publiées ?*

Champ de texte libre

7.3.12. Les données à caractère personnel indûment publiées sont-elles encore accessibles ?*

Menu déroulant :
Oui

Non (allez à la rubrique 7.3.13.1.)

7.3.12.1. Combien de temps les données à caractère personnel indûment publiées ont-elles été disponibles ?*

Du*		Au*	
Date	*Heure*	*Date*	*Heure*

7.3.13. Peut-on vérifier le nombre de personnes qui ont pris connaissance des données à caractère personnel indûment publiées ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.14.1.)
Non

7.3.13.1. Combien de personnes ont pris connaissance des données à caractère personnel indûment publiées ?*

Nombre de personnes : chiffre

Données à caractère personnel d'une autre personne affichées sur un portail personnel ou dans un environnement similaire

7.3.14. Quelle était la cause (mise à jour système, bug, mauvais paramétrage, homonyme, ...) qui a permis à une ou plusieurs personnes de voir des données à caractère personnel d'une autre personne concernée ?*

Champ de texte libre

7.3.15. Avez-vous signalé aux personnes qu'elles ne pouvaient pas réutiliser les données à caractère personnel des autres personnes concernées ?*

Menu déroulant :
Oui
Non

7.3.16. Les personnes concernées dont des données à caractère personnel ont été affichées chez d'autres personnes ont-elles été informées ?*

Menu déroulant :

Oui
Non

Données à caractère personnel non détruites (correctement) (par exemple des données à caractère personnel lisibles dans une corbeille à papier) et données à caractère personnel détruites erronément

7.3.17. Disposez-vous d'une politique//procédure pour la destruction de données à caractère personnel ?*

Menu déroulant :
Oui
Non

DNS spoofing/poisoning (usurpation/empoisonnement de DNS)

7.3.18. Disposez-vous de l'adresse web et/ou de l'adresse IP du clone ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.19.1.)
Non

7.3.18.1. Veuillez transmettre l'adresse web ou IP du clone

Champ de texte libre

7.3.19. Votre site Internet utilise-t-il le protocole Transport Layer Security (TLS) ?*(?)

(?) Avez-vous besoin d'aide ? Utilisation du protocole TLS : Le protocole TLS (Transport Layer Security) est un protocole cryptographique permettant une communication sûre dans un réseau, comme Internet. Il crypte les données et assure l'authentification et l'intégrité, de sorte que les informations telles que mots de passe, données de carte de crédit et e-mails restent protégées contre les interceptions ou la manipulation.

Menu déroulant :
Oui
Non

7.3.20. Votre site Internet dispose-t-il d'un certificat SSL opérationnel ?*(?)

(?) Avez-vous besoin d'aide ? Certificat SSL : Un certificat SSL (Secure Sockets Layer) est un certificat numérique permettant une communication sûre entre un site Internet et un utilisateur. Il crypte les données, telles que les mots de passe et les informations de cartes de crédit, et veille à ce que la connexion soit fiable. Les certificats SSL confirment également l'identité du site Internet.

Menu déroulant :
Oui
Non

7.3.21. Votre site Internet utilise-t-il le DNSSEC (Domain Name System Security Extensions) ?*(?)

(?) Avez-vous besoin d'aide ? DNSSEC : Le DNSSEC (Domain Name System Security Extensions) est une extension du système DNS qui garantit une sécurité supplémentaire en vérifiant les données qui sont extraites via DNS. Il prévient des attaques telles que l'empoisonnement du cache "cache poisoning" en contrôlant si les données DNS reçues sont véritables et si elles n'ont pas été manipulées.

Menu déroulant :
Oui
Non

Phishing

7.3.22. Par quel canal le phishing a-t-il été réalisé ?* (?)

(?) Avez-vous besoin d'aide ?

- *Vishing : (tentatives de) phishing réalisées par téléphone.*
- *Smishing : (tentatives de) phishing réalisées par sms*

Menu déroulant :
Échange d'e-mails
Vishing
Smishing et phishing via d'autres plateformes de messagerie (WhatsApp, Telegram, Signal,...)

7.3.23. De quel type de phishing s'agit-il ?* (?)

(?) Avez-vous besoin d'aide ?

Spearphishing : Le Spearphishing cible une personne ou une organisation spécifique, souvent avec un contenu adapté à la victime ou aux victimes. Avant l'attaque, un travail de reconnaissance est généralement nécessaire pour trouver les noms, les titres de fonction, les adresses e-mail, etc. Les pirates informatiques passent Internet au peigne fin pour relier ces informations à d'autres renseignements recherchés sur les collègues de la cible, ainsi qu'aux noms et relations professionnelles de collaborateurs importants au sein de son organisation. Le phisher construit ensuite un message de phishing crédible à l'aide de ces informations.

Whaling/fraude au PDG : phishing ciblant un décideur à un niveau élevé de l'organisation. La fraude au PDG (ou whaling) est une forme de cybercriminalité dans laquelle un fraudeur envoie un e-mail à partir de la boîte mail d'un collaborateur haut placé, comme un PDG ou un directeur financier, dans le but de faire réaliser un transfert d'argent sur le compte bancaire du fraudeur. La fraude au PDG est donc aussi une forme de fraude au paiement.

Clone-phishing : une attaque de phishing où l'assaillant crée une réplique d'un site Internet légitime ou d'un e-mail afin d'inciter les utilisateurs à introduire leurs données à caractère personnel. Dans cette attaque, les criminels créent une copie — ou clone — d'e-mails légitimes envoyés précédemment qui contiennent un lien ou une annexe. Le phisher remplace ensuite les liens ou les fichiers en annexe par des substituts malveillants qui ressemblent aux liens ou fichiers originaux.

Scareware : par exemple : un e-mail qui prétend que vous êtes un pédophile et que la police sait que vous avez visité tel site Internet ; un e-mail indiquant que vous devez confirmer votre compte bancaire, à défaut de quoi vous n'aurez plus accès à tel compte ; un e-mail réclamant une "action urgente" ;

Menu déroulant :
spearphishing
Whaling/fraude au PDG
Clonephishing
Scareware
Spoofing
Autre type de Phishing

7.3.24. La personne victime de phishing a-t-elle introduit ses données (nom d'utilisateur, mot de passe, ...) ?*

Menu déroulant :
Oui
Non

7.3.25. Le compte ciblé par le phishing était-il doté de la MFA au moment de la violation de données ?* (?)

(?) Avez-vous besoin d'aide ? Authentification à plusieurs facteurs : la MFA (Multi-Factor Authentication) est une méthode de sécurité qui recourt à plusieurs moyens pour confirmer votre identité, comme un mot de passe et un code envoyé sur votre téléphone.

Menu déroulant :
Oui
Non

7.3.26. Le compte ciblé par le phishing disposait-il d'un système d'avertissement ou d'un système de notification similaire au moment de la violation de données, générant un signalement en cas de (tentative de) connexion au départ d'un lieu suspect/non connu ?*

Menu déroulant :
Oui
Non

7.3.27. De nouveaux messages/e-mails de phishing ont-ils été envoyés à partir du compte ciblé par le phishing ?*

Menu déroulant :
Oui (allez aux rubriques 7.3.28.1 et 7.3.28.2)
Non
Non connu (allez à la rubrique 7.3.28.2)

7.3.27.1. Combien de messages/e-mails de phishing ont été envoyés à partir du compte ciblé par le phishing ?*

Menu déroulant :
Le nombre exact d'e-mails de phishing envoyés est connu : *nombre*
Le nombre exact d'e-mails de phishing envoyés n'est pas connu, mais est estimé à : *nombre*

7.3.27.2. Avez-vous envoyé un message d'avertissement aux destinataires des messages/e-mails de phishing à partir du compte ciblé par le phishing si vous disposez de la liste des destinataires. Si vous n'en disposez pas, avez-vous envoyé un message d'avertissement à toutes les personnes de contact ?*

Menu déroulant :
Oui
Non

7.3.28. Avez-vous (ou un acteur externe) enquêté sur la cause et/ou l'ampleur de la violation de données, pour savoir par exemple à quels documents, e-mails et autres un accès a pu être établi à l'aide du compte

compromis, incluant les données à caractère personnel qu'il contient ?*

Menu déroulant :
Oui
Non
Enquête pas encore clôturée (allez à la rubrique 7.3.29.1.)

7.3.28.1. Date à laquelle les résultats de l'enquête relative à la violation de données seront probablement disponibles*

Champ de date

Ransomware

7.3.29. Le groupe ou le hacker de ransomware a-t-il laissé une note de rançon ?*

Menu déroulant
Oui
Non

7.3.30. L'organisation dispose-t-elle d'une sauvegarde non compromise après l'attaque de ransomware ?*

Menu déroulant :
Oui
Non
Ne peut pas être déterminé avec certitude (pour le moment)

7.3.31. Y a-t-il eu un accès illicite aux données à caractère personnel ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.32.1.)
Non
Ne peut pas être déterminé avec certitude (pour le moment) (allez à la rubrique 7.3.32.1.)

7.3.31.1. Les données à caractère personnel auxquelles un accès a (potentiellement) été obtenu étaient-elles cryptées/hachées ou rendues illisibles autrement avant que l'accès ne se produise ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.32.1.1)
Non

7.3.31.1.1. Quel protocole de cryptage, fonction de hashing ou technique similaire a concrètement été utilisé(e) ?*

Plusieurs réponses possibles

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Autres *: champ de texte libre**

7.3.32. Y a-t-il eu exfiltration de données à caractère personnel ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.33.1.)
Non
Ne peut pas être déterminé avec certitude (pour le moment) (allez à la rubrique 7.3.33.1.)

7.3.32.1. Les données à caractère personnel qui ont (potentiellement) été exfiltrées étaient-elles cryptées/hachées ou rendues illisibles autrement avant que l'extraction ne se produise ?*

Menu déroulant :
Oui (allez à la rubrique 7.3.33.1.1.)
Non

7.3.32.1.1. Quel protocole de cryptage, fonction de hashing ou technique similaire a concrètement été utilisé(e) ?*

Plusieurs réponses possibles

- ☐ 3DES
- ☐ AES
- ☐ RAS
- ☐ Twofish
- ☐ RC4
- ☐ ECDSA
- ☐ MD5
- ☐ SHA-1
- ☐ SHA-2
- ☐ SHA-3
- ☐ Autres *: champ de texte libre**

7.3.33. Avez-vous (ou un acteur externe) enquêté sur la cause et/ou l'ampleur de la violation de données, pour

savoir par exemple à quels documents, e-mails et autres un accès (potentiellement) illicite a été obtenu et/ou quelles données à caractère personnel ont (potentiellement) été exfiltrées ?

Menu déroulant :
Oui
Non
Enquête pas encore clôturée (allez à la rubrique 7.3.34.1.)

7.3.33.1. Date à laquelle les résultats de l'enquête relative à la violation de données seront probablement disponibles*

Champ de date

Credential Stuffing (bourrage d'identifiant)

7.3.34. Les comptes auxquels un accès a été obtenu suite à l'attaque de credential stuffing disposaient-ils de la MFA ?*(?)

(?) Avez-vous besoin d'aide ? Authentification à plusieurs facteurs : la MFA (Multi-Factor Authentication) est une méthode de sécurité qui recourt à plusieurs moyens pour confirmer votre identité, comme un mot de passe et un code envoyé sur votre téléphone.

Menu déroulant :
Oui
Non (allez aux rubriques 7.3.35.1. ; 7.3.35.2 ; 7.3.35.3 et 7.3.35.4)

7.3.34.1. Utilise-t-on un CAPTCHA ou un puzzle similaire lors de la connexion aux comptes ?*

Menu déroulant
Oui
Non

7.3.34.2. Votre organisation procède-t-elle au blocage d'IP, comme le geo-blocking ou la mise sur liste noire de certaines adresses IP ?*

Menu déroulant
Oui
Non

7.3.34.3. Votre organisation prévoit-elle un nombre maximal de tentatives de connexion à un compte dans un laps de temps donné au départ d'une adresse IP déterminée ou une limitation similaire ?*

Menu déroulant
Oui
Non

7.3.34.4. Votre organisation prévoit-elle d'autres mesures de prévention pour lutter contre le credential stuffing ?*

Champ de texte libre

7.3.35. Avez-vous informé les personnes concernées des comptes compromis du fait qu'il y a eu un accès illicite (ou une tentative d'accès illicite) à leurs comptes, et que si elles utilisent les mêmes informations de connexion ailleurs, celles-ci sont également potentiellement compromises ?*

Menu déroulant
Oui
Non

7.3.36. Avez-vous (ou un acteur externe) enquêté sur la cause et/ou l'ampleur de la violation de données ?*

Menu déroulant :
Oui
Non
Enquête pas encore clôturée (allez à la rubrique 7.3.37.1.)

7.3.36.1. Date à laquelle les résultats de l'enquête relative à la violation de données seront probablement disponibles*

Champ de date

Injection SQL

7.3.37. Utilisez-vous des instructions préparées/requêtes paramétrées (prepared statements/parametrized queries) ?*

Menu déroulant
Oui
Non

7.3.38. Était-il possible de se connecter à l'application de l'extérieur en tant que root user ?*

Menu déroulant
Oui
Non

7.3.39. Utilisez-vous des "sanitization libraries" ou d'autres mécanismes de nettoyage pour "nettoyer" les données dans la base de données ?*

Menu déroulant
Oui
Non

7.3.40. Avez-vous (ou un acteur externe) enquêté sur la cause et/ou l'ampleur de la violation de données ?*

Menu déroulant :
Oui
Non
Enquête pas encore clôturée (allez à la rubrique 7.3.41.1.)

7.3.40.1. Date à laquelle les résultats de l'enquête relative à la violation de données seront probablement disponibles*

Champ de date

Attaque (D)DOS

7.3.41. Les utilisateurs légitimes avaient-ils toujours la possibilité, pendant l'attaque DDOS, de se connecter au serveur impacté ?*

Menu déroulant
Oui
Non (allez à la rubrique 7.3.42.1.)

7.3.41.1. Le serveur impacté a-t-il été indisponible plus de 24 heures ?*

Menu déroulant			
Oui			
Non			
Début de la période d'indisponibilité*		Fin de la période d'indisponibilité*	
Champ de date	*Champ d'heure*	*Champ de date*	*Champ d'heure*

7.3.42. Disposez-vous d'applications de Security Information and Event Management (SIEM), d'Endpoint Detection and Response (EDR) et/ou d'Extended Detection and Response (XDR) afin de surveiller les flux de données et d'intervenir à cet égard ?*

Menu déroulant
Oui (allez à la rubrique 7.3.43.1.)
Non

7.3.42.1. Veuillez indiquer les applications SIEM, EDR et/ou XDR dont votre organisation dispose*

Champ de texte libre

7.3.43. Avez-vous (ou un acteur externe) enquêté sur la cause et/ou l'ampleur de la violation de données ?*

Menu déroulant :
Oui
Non
Enquête pas encore clôturée (allez à la rubrique 7.3.44.1.)

7.3.43.1. Date à laquelle les résultats de l'enquête relative à la violation de données seront probablement disponibles*

Champ de date

7.4. 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

7.5. Le DPO a-t-il émis un avis sur la notification de la violation de données, l'éventuelle communication à l'égard des personnes concernées et/ou les mesures à prendre ?

Menu déroulant :
Oui
Non

Enquête pas encore clôturée (allez à la rubrique 7.5.1.)

7.5.1. Veuillez communiquer l'avis du DPO*

Champ de texte libre : maximum 500 caractères

8. Gestion

8.1. Quelles mesures (techniques et organisationnelles) spécifiques étaient en vigueur afin de protéger les données à caractère personnel affectées / de prévenir ce type de violation de données ? (?)

(?) Avez-vous besoin d'aide ? Quelles mesures (techniques et organisationnelles) spécifiques étaient en vigueur afin de protéger les données à caractère personnel affectées / de prévenir ce type de violation de données ?

Veuillez décrire uniquement les mesures qui sont directement pertinentes pour prévenir la violation de données plutôt que de donner un relevé général de toutes les mesures.

Par exemple : pseudonimisation, agrégation, hashing, audit logs, authentification à plusieurs facteurs, cloisonnement/séparation des données, système d'identification et d'autorisation, effacement à distance, cryptage, firewall, mots de passe, ...)

Mesure technique en vigueur*	Mesure organisationnelle en vigueur*
Ajouter	Ajouter
Mesure	*Mesure*
+	+

8.2. Quelles mesures (techniques et organisationnelles) nouvelles/complémentaires ont été prises spécifiquement suite à la violation de données ? (?)

(?) Avez-vous besoin d'aide ? Quelles mesures (techniques et organisationnelles) nouvelles/complémentaires ont été prises spécifiquement suite à la violation de données ?

Veuillez décrire uniquement les mesures qui ont été prises suite à la violation de données qui a eu lieu concrètement et ne pas donner une liste de toutes les mesures.

Par exemple : détermination de l'ampleur de la violation des données, suspension de l'ensemble ou d'une partie du traitement de données à caractère personnel, modification des droits d'accès, modification des mots de passe par défaut des administrateurs et/ou des utilisateurs, modification de l'administrateur et/ou des moyens d'authentification des utilisateurs, appel à une assistance technique (veuillez identifier la partie concernée), notification de la violation de données au responsable informatique d'une application liée, interruption/sécurisation de la connexion avec d'autres applications, réindexation ou désindexation des données compromises, effacement avec confirmation de l'appareil et notification de confirmation de l'action réussie par l'appareil, modification du système de cryptage, signalement aux autorités de contrôle compétentes (veuillez les identifier), mise à jour (patch) réussie des systèmes, ... *Indiquez également la date d'implémentation.*

Mesures techniques*		Mesures organisationnelles*	
Ajouter		Ajouter	
Mesure	*Date*	*Mesure*	*Date*
+	+	+	+

8.3. Quelles mesures (techniques et organisationnelles) nouvelles/complémentaires seront spécifiquement prises à l'avenir (suite à la violation de données) ? (?)

(?) Avez-vous besoin d'aide ? Quelles mesures (techniques et organisationnelles) nouvelles/complémentaires seront spécifiquement prises à l'avenir (suite à la violation de données) ?

Veuillez décrire les futures mesures qui seront prises suite à la violation de données qui a eu lieu concrètement.

Par exemple : déploiement de la MFA pour tous les utilisateurs, modification de la structure Active Directory, segmentation du système informatique, installation d'une nouvelle application de sauvegarde, installation d'une (nouvelle) application EDR/XDR, ... Indiquez également la date d'implémentation prévue.

Mesures techniques*		Mesures organisationnelles*	
Ajouter		Ajouter	
Mesure	*Date*	*Mesure*	*Date*
+	+	+	+

9. Risque

9.1. L'organisation dispose-t-elle d'une méthode (générale) de recensement et d'évaluation (sur la base de la gravité et de la probabilité) des risques pour les droits et libertés des personnes physiques en cas de violation de données à caractère personnel ?*

Menu déroulant
Oui (allez à la rubrique 9.1.1.)
Non

9.1.1. Quelle méthode utilisez-vous à cet égard (ENISA, méthode développée en interne, autre, ...)*

Menu déroulant
ENISA
Méthode développée en interne
Autre, comme CRAMM, OWASP, FAIR privacy, NIST Privacy Risk Assessment Matrix (PRAM)

9.2. Résultat de l'analyse à l'égard du (des) risque(s) pour les droits et libertés des personnes concernées*

Menu déroulant
Risque élevé probable
Risque probable
Probablement aucun risque

9.3. Impact/conséquences pour les personnes concernées*

- ☐ Perte de contrôle des données à caractère personnel
- ☐ Il y a une perte de confidentialité de données à caractère personnel protégées par le secret professionnel (conformément à l'article 458 du Code pénal)
- ☐ Violation de l'intégrité physique
- ☐ Violation de l'intégrité psychique
- ☐ Violation de la vie privée intime (orientation sexuelle, photos dénudées, ...)
- ☐ Abus de faiblesse (par exemple mineurs, personnes âgées, moins valides, ...)
- ☐ Dommages matériels
- ☐ Dommages immatériels
- ☐ Empêchement temporaire de l'accès au service
- ☐ Empêchement permanent de l'accès au service
- ☐ Discrimination
- ☐ Vol d'identité ou fraude à l'identité
- ☐ Pertes financières
- ☐ Annulation non autorisée de la pseudonymisation
- ☐ Atteinte à la réputation
- ☐ Limitation de la liberté de mouvement (par exemple un refus de passer la frontière)
- ☐ Tout autre dommage économique ou social important (allez à la rubrique 9.3.1.)
- ☐ Limitation d'autres libertés (allez à la rubrique 9.3.2.)
- ☐ Limitation d'autres droits (allez à la rubrique 9.3.3.)
- ☐ Autre impact (allez à la rubrique 9.3.4.)

9.3.1. Veuillez détailler tout autre dommage économique ou social important*

Champ de texte libre

9.3.2. Veuillez détailler la limitation d'autres libertés*

Champ de texte libre

9.3.3. Veuillez détailler la limitation d'autres droits*

Champ de texte libre

9.3.4. Veuillez détailler tout autre impact*

Champ de texte libre

10. 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)*
- *de 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*

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

Menu déroulant :
Oui (allez à la rubrique 10.1.1.)

Non (allez aux rubriques 10.2. et 10.3.)

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

Menu déroulant :
Oui (allez aux rubriques 10.1.1.1 ; 10.1.1.2. ; 10.1.1.3.)
Non (allez aux rubriques 10.1.1.4. ; 10.1.1.5 et 10.3.)

10.1.1.1. 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)*

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

nombre

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

Champ de date : calendrier

10.1.1.4. 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)*

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

Champ de date : calendrier

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

Menu déroulant :
Oui (allez aux rubriques 10.2.1. ; 10.2.2.)
Non (allez à la rubrique 10.3.)
Pas encore connu (allez à la rubrique 10.3.)

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

Champ de date : Calendrier

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

Menu déroulant :

Oui (allez aux rubriques 10.2.2.1 ; 10.2.2.2.)
Non (allez aux rubriques 10.2.2.3. ; 10.2.2.4 et 10.3.)

10.2.2.1. 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)*

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

Chiffre/nombre

10.2.2.3. 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)*

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

Chiffre/nombre

10.3. Veuillez indiquer la raison pour laquelle on renonce à la communication (individuelle) à l'égard des personnes concernées dont les données à caractère personnel ont été affectées par la violation de données*

Plusieurs réponses possibles

- ☐ Parce que nous estimons qu'il n'y a probablement aucun risque pour les droits et libertés des personnes physiques
- ☐ Informer chaque personne concernée individuellement exigerait des efforts disproportionnés (allez à la rubrique 10.3.1.)
- ☐ Des mesures techniques et organisationnelles appropriées étaient en place pour protéger les données à caractère personnel avant que la violation de données ne se produise (allez à la rubrique 10.3.2.)
- ☐ Des mesures ont été prises après la violation de sorte qu'un risque élevé n'est plus probable (allez à la rubrique 10.3.3.)
- ☐ En raison de directives émanant d'autres autorités pertinentes, comme des autorités de contrôle (allez aux rubriques 10.3.4. et 10.3.5.)

10.3.1. Disposez-vous des coordonnées (électroniques) individuelles des personnes concernées?*

Menu déroulant
Oui *texte : L'APD part du principe que lorsque vous disposez des coordonnées individuelles des personnes concernées, vous devez les utiliser pour adresser une communication individuelle. On ne peut alors pas appliquer l'exception concernant les efforts disproportionnés.*
Non

10.3.2. Quelles mesures avez-vous prises préalablement, rendant inutile d'informer les personnes concernées ?*

Champ de texte libre

10.3.3. Quelles mesures avez-vous prises suite à la violation de données, rendant inutile d'informer les personnes concernées ?*

Champ de texte libre

10.3.4. Quelle autorité a transmis des directives, rendant inutile/inopportun d'informer les personnes concernées ?*

Champ de texte libre

10.3.5. Veuillez résumer le contenu des directives*

Champ de texte libre

11. Éléments complémentaires

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.

12. Annexes

Copie datée de la communication aux personnes concernées

Selon les réponses que vous avez données, il s'agit d'une communication individuelle ou collective (voir l'onglet 10). Selon le type et la nature de la violation de données, les éléments suivants doivent aussi éventuellement être repris dans la communication aux personnes concernées :

- Pour les données à caractère personnel de la mauvaise personne affichées sur le portail personnel ou un environnement similaire : le fait que les données à caractère personnel des personnes concernées ont été affichées pour d'autres personnes physiques (voir l'onglet 7) ;
- Pour le *credential stuffing* : le fait qu'il y a eu (une tentative d') accès illicite au compte des personnes concernées et l'avertissement à ces personnes concernées que si elles utilisent les mêmes informations de connexion ailleurs, ces comptes sont potentiellement compromis aussi (voir l'onglet 7) ;
- Pour le *phishing* : il convient de distinguer trois groupes de personnes concernées susceptibles de devoir recevoir une communication :
    - les personnes concernées de la boîte mail ou d'un environnement similaire proprement dit (voir l'onglet 7) ;
    - les personnes concernées auxquelles de nouveaux messages de phishing ont pu être envoyés (voir l'onglet 7) ;

- les personnes concernées dont les données à caractère personnel se trouvaient dans la boîte mail ou dans un environnement similaire (voir l'onglet 7).

Copie datée de l'analyse de risque réalisée

Si vous avez réalisé une analyse de risque concernant la violation de données (voir l'onglet 9).

Copie datée du rapport d'enquête

Si une enquête a été réalisée par vous-même ou par un tiers au sujet de la cause et/ou de l'ampleur de la violation de données. Il peut s'agir de tous les types de violations de données (voir l'onglet 8). L'Autorité de protection des données estime nécessaire que pour les types suivants de violations de données, une enquête soit menée et que le rapport y afférent soit fourni : DNS-spoofing/poisoning, Phishing, Ransomware, Credential Stuffing, SQL-injection, (D)DoS-attack, AI-models, Coordinated Vulnerability Disclosure Policy (voir l'onglet 7).

Copie datée de la note de rançon

S'il s'agit d'une violation de données de type ransomware et si une note de rançon a été laissée (voir l'onglet 7).

Copie datée du message de phishing

S'il s'agit d'une violation de données de type phishing et si vous disposez encore du message initial (capture d'écran) par lequel le phishing a été réalisé (voir l'onglet 7).

Copie datée de la notification de tentative de connexion suspecte

S'il s'agit d'une violation de données de type phishing et si vous disposez encore de la notification générée par le système d'avertissement pour la (tentative de) connexion suspecte (voir l'onglet 7).

Copie datée de la politique de destruction de données à caractère personnel

Si vous disposez d'une politique de destruction des données à caractère personnel et qu'il s'agit des types suivants de violations de données :

- Données à caractère personnel non détruites (correctement) (voir l'onglet 7) ;
- Données à caractère personnel détruites indûment (voir l'onglet 7).

Copie datée de la communication avec les mauvais destinataires

En fonction du type de violation de données, il peut s'agir des communications suivantes :

- e-mail, lettre ou colis contenant des données à caractère personnel envoyé(e) au mauvais destinataire : communication demandant de supprimer ou de renvoyer l'e-mail, la lettre ou le colis et de ne pas utiliser (ultérieurement) les données à caractère personnel (voir l'onglet 7) ;
- e-mail contenant des données à caractère personnel envoyé à des destinataires mentionnés dans le champ "à" ou en cc, au lieu de l'être en cci : communication demandant de supprimer l'e-mail et de ne pas utiliser (ultérieurement) les données à caractère personnel (voir l'onglet 7) ;
- autorisations à l'égard de collaborateurs internes ou externes mal paramétrées : communication au collaborateur interne ou externe demandant de supprimer d'éventuelles copies et de ne pas utiliser (ultérieurement) les données à caractère personnel (voir l'onglet 7) ;

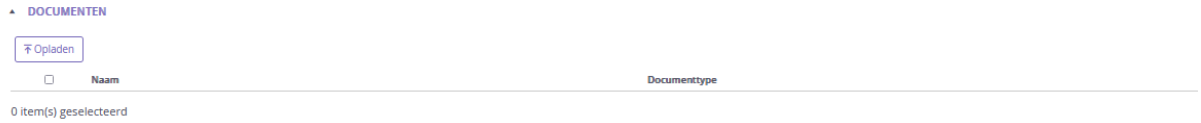
- cartes, applications ou localisations de réseau paramétrées de manière trop large au sein ou en dehors de l'organisation : communication au collaborateur interne ou externe ou à la personne en dehors de l'organisation demandant de supprimer d'éventuelles copies et de ne pas utiliser (ultérieurement) les données à caractère personnel (voir l'onglet 7) ;
- données à caractère personnel d'une mauvaise personne affichées sur un portail personnel ou un environnement similaire : communication à la personne qui a pu voir indûment des données à caractère personnel de personnes concernées demandant de supprimer d'éventuelles copies et de ne pas utiliser (ultérieurement) les données à caractère personnel (voir l'onglet 7).

Copie datée de la notification externe de la violation de données

Si la découverte de la violation de données s'est faite sur la base d'un signalement externe (voir l'onglet 5).

Indiquez quelle annexe vous téléversez lors de l'introduction de la notification

☐ Copie datée de la communication aux personnes concernées
☐ Copie datée de l'analyse de risque réalisée
☐ Copie datée du rapport d'enquête
☐ Copie datée de la note de rançon
☐ Copie datée du message de phishing
☐ Copie datée de la notification de tentative de connexion suspecte
☐ Copie datée de la politique de destruction de données à caractère personnel
☐ Copie datée de la communication avec les mauvais destinataires
☐ Copie datée de la notification externe de la violation de données



13. Disposition finale

○ Oui, je déclare par la présente que la partie 2 est complète.
○ Non, je souhaite conserver mes modifications pour l'instant et continuer à compléter le formulaire ultérieurement avec des données supplémentaires (allez à la rubrique 13.1 si vous cliquez sur conserver les modifications)

13.1. Attention - Opgelet - Achtung

Si vous ne faites pas d'autres ajouts à cette notification temporaire, les valeurs que vous avez saisies seront considérées comme définitives dans un délai de 21 jours à compter de l'envoi de la partie 1.

Indien u geen aanvullingen meer doet op deze tijdelijke bewaaropdracht, zullen de waardes die u hebt ingegeven binnen 21 dagen na het indienen van deel 1 als definitief worden beschouwd.

Wenn Sie keine weiteren Ergänzungen zu dieser vorläufigen Sorgerechtsverfügung

vornehmen, werden die von Ihnen eingegebenen Werte innerhalb von 21 Tagen nach Einreichung von Teil 1 als endgültig betrachtet.