Notification d'une fuite de données, Loi du 30 juillet 2018[1]

Certaines fuites de données impliquent une obligation de notification auprès du Comité permanent R, autorité de protection des données (DPA), dès qu'il existe un risque pour les libertés et droits fondamentaux des personnes concernées (les personnes dont les données à caractère personnel ont été divulguées).

Le présent formulaire est destiné à servir de base à cette notification.

Veuillez noter que les notifications qui ne sont pas effectuées via le formulaire ne sont pas enregistrées par le Comité permanent R comme une notification d'une fuite de données mais tout au plus comme une question ou une réclamation. Les mentions dans des courriers électroniques, dans des entretiens téléphoniques ou dans des formulaires alternatifs concernant une fuite de données fournissent généralement trop peu d'informations pour permettre une enquête et ne peuvent a priori pas être considérées comme suffisantes pour répondre à l'obligation de notification. En outre, il n'y a aucune garantie que ces mentions alternatives seront enregistrées et examinées en tant que notification d'une fuite de données.

Le responsable du traitement concerné informe si possible le Comité permanent R au plus tard 72 heures après la prise de connaissance de la fuite de données.

Lorsque toutes les informations ne sont pas disponibles et que la fuite de données requiert un examen complémentaire, l'organisation peut procéder à une notification provisoire. Cette notification provisoire comprend un maximum de réponses aux questions reprises dans le formulaire.
En cas de notification provisoire l'organisation procède le plus rapidement possible à une notification complémentaire. Cette notification complémentaire comprend entre autres les informations reprises dans les autres champs du présent formulaire et éventuellement les informations mises à jour par rapport à la notification provisoire ou à la première notification. Enfin, une demande d'annulation peut également être introduite.

Le Comité permanent R attire votre attention sur le fait que le présent formulaire comprend des listes de catégories de données très larges, mais ne constitue aucunement une autorisation implicite de traitement de toutes ces catégories de données par les responsables de traitement visés au titre 3 de la Loi du 30 juillet 2018 précitée.

Information au sujet du traitement des données à caractère personnel

Le Comité permanent R traite vos données à caractère personnel car la loi l'y oblige en vue de l'enregistrement de fuites de données, à des fins de contrôle si nécessaire, afin de donner un avis à l'organisation à propos de la fuite de données. Les données à caractère personnel sont conservées tant que cela est nécessaire dans le cadre de la formulation d'avis et du contrôle, et ce jusqu'à 10 ans après la clôture du dossier (en cas d'action en justice, jusqu'à la fin de la procédure). Dans le cadre de la coopération avec d'autres autorités de protection des données en cas de fuites de données, des informations du présent formulaire peuvent être partagées avec ces autorités.

[1] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

La présente notification concerne :	□ une notification complète; □ une demande d'annulation de la notification précédente; □ une notification en plusieurs étapes; □ un complément ou une correction relatif à une notification précédente;

Veuillez compléter le questionnaire ci-dessous avec la plus grande précision. Utilisez s'il vous plaît un langage clair et simple et évitez (autant que possible) une terminologie trop technique ou juridique. Les réponses peuvent toujours être étayées par des documents complémentaires. Dans certains cas, ces documents sont réclamés explicitement.

1. Organisation

1.1 Qualité de l'organisation qui notifie la fuite de données

□ Responsable du traitement □ Sous-traitant pour le compte d'un responsable du traitement □ Responsable conjoint du traitement

1.2 Indiquez les coordonnées de l'organisation qui notifie la fuite de données

Nom de l'organisation	
Établissement principal	□ en Belgique □ dans un pays de l'UE or de l'EEE □ en dehors de l'UE ou de l'EEE
Numéro d'entreprise [0123.456.789]	
Numéro de TVA européen	

CLASSIFICATION PAR L'AUTEUR SI NECESSAIRE

Numéro unique attribué dans le pays d'enregistrement - précisez aussi de quel numéro il s'agit	
Rue	
Numéro	
Boîte postale	
Code postal	
Commune/Ville	
Numéro de téléphone [Débutez toujours votre numéro de téléphone par l'indicatif international, pour la Belgique par exemple il s'agit de +32]	
L'activité de traitement concerne-t-elle une activité de traitement transfrontalière (internationale) ?	□ oui □ non
L'activité de traitement a-t-elle un impact sur des personnes concernées en Belgique ?	□ oui □ non
L'activité de traitement a-t-elle un impact sur des personnes concernées d'un autre ou de plusieurs autres États membres que la Belgique ?	□ oui □ non
Cette notification fait-elle partie d'une notification globale à d'autres contrôleurs en vertu d'autres obligations légales (par exemple à la BNB, la BCE, la CERT, la FSMA, etc.) ? Si oui, lesquels ?	
Le responsable du traitement est-il déclaré auprès de l'IBPT en tant qu'opérateur ?	□ oui □ non
Le responsable du traitement est-il une entreprise cotée en bourse ?	□ oui □ non

1.3 Personne de contact pour la fuite de données

Qualité de la personne de contact	
Nom de la personne de contact	
Numéro de téléphone de la personne de contact [Débutez toujours votre numéro de téléphone par l'indicatif international, pour la Belgique par exemple il s'agit de +32]	
E-mail de la personne de contact	

La personne de contact est-elle un délégué à la protection des données (ci-après "DPO") ?

□ Oui;
□ Non, car l'organisation n'a pas désigné de DPO;
□ Non, mais l'organisation dispose d'un DPO, qui a déjà été déclaré
□ Non, mais l'organisation dispose d'un DPO, qui n'a pas encore été déclaré. Dans ce cas, veuillez communiquer les coordonnées complètes de ce dernier :

2. Traitement touché par la fuite de données

Finalité pour laquelle les données sont traitées	
Nature des données qui ont été touchées par la fuite de données *(Cochez une ou plusieurs cases)*	□ Données d'identification (par exemple nom, adresse, date de naissance, numéro de téléphone, numéro de carte d'identité, numéro de permis de conduire, plaque minéralogique, numéro de client, numéro de travailleur, ...) □ Données d'identification électroniques (par exemple adresses électroniques, adresses IP, adresse Mac, identifiants réseaux sociaux, identifiant Skype, ...) □ Profils (évaluation de la personne concernée avec intégration dans une classe ou prédiction d'une certaine caractéristique ou d'un certain comportement) □ Caractéristiques personnelles (par ex. âge, sexe, état civil, ...) □ CRM data (par ex. informations sur les clients, leurs besoins, les contacts, la communication, la satisfaction, etc.)

	□ Copies de passeport, elD ou d'autres titres de légitimation □ Données physiques (par ex. taille, poids, apparence, ...) □ Habitudes de vie, de clic, de recherche, de navigation, de paiement □ Données psychiques (par ex. personnalité, caractère, ...) □ Composition du ménage □ Loisirs et intérêts □ Profil sur les médias sociaux □ Affiliations □ Habitudes de consommation □ Produits et services (par ex. numéro de carte bancaire, numéro de compte, numéro de police d'assurance, relevé de produits, salaire et revenu, dépenses, consommation, entretien, etc.) □ Caractéristiques de l'habitation et de la voiture □ Études et formation □ Profession et emploi, régime TVA □ Photos ou enregistrements d'images (par ex. cctv, caméra de surveillance, formation enregistrée, etc.) □ Enregistrements de sons (par exemple conversations téléphoniques enregistrées d'un call center, formation, etc.) □ Données RH relatives au salaire et à la présence du personnel □ Données RH relatives aux évaluations, aux fonctions et missions, aux KPI, au plan de carrière □ Données de sécurité physique des clients, du personnel et des visiteurs (par ex. autorisations et droits) □ Données de sécurité ICT des clients, du personnel et des visiteurs (par exemple autorisations et droits, utilisation d'un badge, accès à Internet) □ Données relatives aux habilitations, attestations et avis de sécurité (Loi du 11 décembre 1998) □ Données relatives au contrôle des clients □ Données relatives au contrôle du personnel (par ex. journalisation, règlement relatif aux lanceurs d'alerte, mandats, prévention du délit d'initié, gestion des plaintes et contrôle de la qualité, etc.) □ Données liées aux méthodes de recueil des données et/ou aux mesures d'appui et de soutien (Loi du 30 novembre 1998) □ Numéro national (par exemple le numéro de Registre national) □ Numéro d'identification de la sécurité sociale □ Origine raciale ou ethnique □ Opinions politiques □ Convictions religieuses ou philosophiques □ Appartenance syndicale □ Données génétiques (par ex. ADN, groupe sanguin, ...) □ Données biométriques □ Données concernant la santé □ Données relatives aux soins □ Données concernant la vie sexuelle ou l'orientation sexuelle

	□ Condamnations pénales □ Infractions □ Mesures de sécurité liées à des condamnations pénales ou à des infractions □ Extrait du casier judiciaire □ Contenu de données de communications électroniques □ Données relatives au trafic des communications électroniques ou téléphoniques □ Données de localisation au sens large (par ex. traitées ou non par des opérateurs télécoms ou via un logiciel de navigation, un GPS, ...) □ Données financières □ Code d'accès (mot de passe, code PIN, ...) □ Autre: □ La nature des données touchées par la fuite de données n'est pas connue
Quel est le nombre minimal de personnes dont des données à caractère personnel sont concernées par la fuite de données (en tant que victimes) ? Quel est le nombre **maximal** de personnes dont des données à caractère personnel sont concernées par la fuite de données (en tant que victimes) ? Décrivez le(s) groupe(s) de personnes dont des données à caractère personnel sont concernées par la fuite de données	Nombre de personnes (personnes concernées): □ Description :
La fuite de données a-t-elle eu lieu dans le cadre d'un traitement qui a été confié en sous-traitance à une autre organisation ?	□ Oui □ Non

3. Description de la fuite de données

3.1 Quelle est le fait à l'origine de la fuite de données ?

Le fait de la fuite de données est plutôt :	□ Interne (par exemple par le personnel) □ Externe (par exemple par un hacker)
La fuite de données a été le résultat :	□ d'une opération technique du système (non humaine) □ d'une intervention humaine □ d'un accident. Précisez: □ d'une mauvaise intention (par exemple vol, fraude, piratage et sabotage) □ d'une autre cause:

3.2 Quelle est la nature de la fuite de données ?

□ Violation du caractère confidentiel des données à caractère personnel
□ Perte de disponibilité des données à caractère personnel
□ Violation de l'intégrité des données à caractère personnel
□ Autre violation de données à caractère personnel :

3.3. Faites un résumé de la fuite de données

En résumant le cas, donnez davantage d'informations sur :

- le moment de la fuite de données et la découverte de la fuite de données,
- les actions et décisions prises (ligne du temps) jusqu'à présent,
- la structure technique de l'activité de traitement, le type d'environnement du traitement, le type de traitement (End user computing, gestion du site Internet, gestion opérationnelle, analyse big data, data warehouse, etc.) et le mode de traitement,
- la motivation de la décision d'informer le Comité R par rapport à d'autres autorités (belges ou étrangères).

3.4 Ligne du temps de la fuite de données

Quand la fuite de données a-t-elle été découverte ?	Date :
[HH:MM]	Heure :
Quand la fuite de données s'est-elle produite ? [HH:MM]	□ La date et l'heure exactes auxquelles la fuite de données a eu lieu sont connues, à savoir : ... □ La date et l'heure exactes de la fuite de données ne sont pas connues mais sont estimées au : □ Inconnu Date : Heure :
Quand les premières mesures de sécurité supplémentaires ont-elles été prises ?	□ Aucune mesure de sécurité complémentaire n'a (encore) été prise □ Les premières mesures de sécurité supplémentaires ont été prises et sont:
Quand a-t-il été remédié à la fuite de données ?	□ Il n'a pas encore été remédié à la fuite de données. □ Il a été remédié à la fuite de données le Par le biais des mesures techniques ou organisationnelles suivantes :
Si la présente notification n'est pas effectuée dans les 72 heures après la découverte de la fuite de données, quelle en est la raison ?	

3.5 Détection de la fuite de données

Circonstances dans lesquelles la fuite de données a été constatée	□ Notification interne de la perte d'un équipement (hardware) ou de documents □ Procédure de gestion d'incident interne (par ex. système de notification d'incident ICT, sécurité de l'information incident management, ...) □ Procédure interne cyber emergency team □ Système de contrôle interne afin de détecter des intrusions ou des fuites et de repérer un accès non autorisé

	□ Procédure de contrôle interne / règlement relatif aux lanceurs d'alerte □ Service interne de traitement des réclamations □ Notification externe par un fournisseur ou un sous-traitant □ Notification externe par un client □ Notification externe par un tiers □ Notification externe par une autorité □ Autre, à savoir :
Quelles données ont été divulguées ?	□ Toutes les données traitées (voir le point 2) □ Pas encore déterminées □ Les données à caractère personnel suivantes :

4. Prévention et gestion de la fuite de données

Quelles mesures préventives ont été spécifiquement prises pour protéger les données divulguées? (décrivez uniquement les mesures qui sont directement pertinentes pour prévenir la violation plutôt que de donner un relevé général de toutes les mesures) *(par exemple : pseudonimisation, agrégation, hashing, audit logs, authentification à facteurs multiples, cloisonnement/ séparation des données, système d'identification et d'autorisation, wipe à distance, cryptage, firewall, mots de passe, ...) Indiquez si la mesure a été introduite dès le début du traitement.*	Mesures techniques : Mesures organisationnelles :
Le degré et la possibilité d'identification d'une personne concernée sur la base des données sous-jacentes.	Les données comportent : Des données directement identifiables

[Voir notre mode d'emploi pour des exemples concrets pour les différentes possibilités de réponse.]	□ *Des données révélant directement l'identité des personnes concernées à des tiers.* Des données identifiables indirectement et facilement □ *Des données ne révélant pas directement l'identité des personnes concernées, mais que des tiers peuvent assez facilement relier à des données d'identification des personnes concernées accessibles (publiquement).* Des données indirectement identifiables □ *Des données ne permettant pas à tout un chacun de retrouver directement l'identité de la personne concernée. Il existe toutefois des méthodes permettant de quand même retrouver l'identité de la personne concernée à l'aide de données complémentaires (non publiques).* □ Des données pouvant être indirectement reliées à des personnes *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).* Des données anonymes □ *Des données ne révélant ni directement ni indirectement l'identité des personnes concernées, par exemple parce qu'il s'agit de données suffisamment agrégées. La collecte de données ne comporte pas de données individuelles ou du moins comporte des données suffisamment agrégées.*
Au moment de la découverte de la fuite de données, les données à caractère personnel étaient-elles cryptées, hachées ou rendues incompréhensibles ou inaccessibles d'une autre manière pour des personnes non autorisées ?	□ Oui par la méthode suivante : □ Non □ Partiellement, à savoir :
Actions prévues et/ou déjà prises *(Cochez une ou plusieurs cases)*	□ Arrêt de tout ou partie du traitement de données à caractère personnel □ Modification des droits d'accès □ Modification des mots de passe administrateur et/ou utilisateurs □ Modification de l'administrateur et/ou des authentifiants des utilisateurs □ Recours à une assistance technique, si oui veuillez l'identifier : □ Notification de la fuite de données au responsable de l'information d'une application liée □ Interruption/sécurisation du couplage avec d'autres applications □ Réindexation ou désindexation des données divulguées (moteurs de recherche)

	□ Exécution d'un wipe avec confirmation de l'appareil et signal de confirmation de l'action réussie par l'appareil. □ Modification du système de cryptage □ Notification aux instances de contrôle appropriées, si oui veuillez les identifier : □ Mise à jour (exécution des patches) réussie des systèmes ou équipements □ Autre:
Y a-t-il des fichiers de journalisation pertinents disponibles concernant l'incident de sécurité de l'information ? Ceux-ci sont-ils protégés contre les modifications non autorisées ou les suppressions?	□ Oui, à savoir : □ Non, la raison est la suivante : Si des fichiers de journalisation sont disponibles, ceux-ci doivent être mis à disposition à la demande de le Comité permanent R et être préservés de modifications pendant l'enquête. □ Oui, via les moyens techniques suivants: □ Non
Date à laquelle les résultats de l'enquête sur la fuite de données seront probablement disponibles [HH:MM]	Date : Heure :

5. Méthode pour évaluer les risques pour les droits et libertés des personnes concernées

L'organisation a-t-elle une	
méthode générale pour dresser l'inventaire et évaluer les risques pour les droits et libertés des personnes concernées en cas de projet où des données à caractère personnel sont traitées ou pour traiter un incident avec des données à caractère personnel ?	□ Oui □ Non
Dans ce cadre, le risque et l'impact de l'événement potentiellement	□ Oui □ Non

dommageable pour les personnes concernées sont-ils examinés ?	
Quel est le degré ou le niveau de gravité de cette fuite de données lors de l'analyse des risques pour les droits et libertés des personnes concernées ?	□ Critique □ Élevé □ Moyen □ Faible □ Négligeable
Décrivez succinctement la (les) méthode(s) d'évaluation des risques pour les droits et libertés des personnes concernées d'un incident et les différentes catégories (gradations des risques ?) en fonction de la méthode utilisée ou motivez les raisons pour lesquelles vous n'utilisez pas (encore) cette méthode	

Quel impact la fuite de données peut-elle avoir pour les droits et libertés des personnes concernées (que le risque soit élevé ou faible) ?

Choisissez une ou plusieurs options, le risque existe

En cas d'atteinte à la confidentialité, que:	Décrivez le risque :
En cas de perte de disponibilité, que :	Décrivez le risque :
En cas d'atteinte à l'intégrité, que:	Décrivez le risque :
La violation a un autre impact sur les droits et libertés des personnes concernées, à savoir qu'elle peut engendrer:	Décrivez le risque :

Probabilité. Comment la possibilité qu'un impact susmentionné survienne est-elle évaluée (par risque) ? L'organisation possède une méthode pour calculer la possibilité	Décrivez la méthode utilisée :
Vu la possibilité et l'impact pour les droits et libertés des personnes concernées, quelles mesures techniques et organisationnelles complémentaires sont/seront prises en sus des actions prévues afin de limiter ou de prévenir le risque (inhérent) pour les droits et libertés, à moins qu'il ait déjà été suffisamment remédié au risque ?	Mesures techniques complémentaires : Mesures organisationnelles complémentaires :
Mesures/actions conseillées aux personnes concernées *(par ex. modification de mots de passe)*	

6. Information

Combien d'institutions ou de personnes concernées avez-vous informées ou allez-vous informer ?	

7. Considérations complémentaires

Indiquez ici toute information susceptible de favoriser une meilleure compréhension de la notification	

8. Indiquez ici quels documents vous joignez au présent formulaire

□ Un exemple (du contenu) de la communication aux personnes concernées (le cas échéant)
□ AIPD concernant le traitement (le cas échéant)
□ Autre :

9. Déclaration

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

Data Protection Officer Responsable de traitement