|  |
| --- |
| **Formulaire de notification d’une violation de données à caractère personnel [[1]](#footnote-2)** |

**Formulaire à renvoyer dûment complété au** [Adresse électronique du DPO du pouvoir adjudicateur]

**Le déclarant agit en tant que :**

Sous-traitant[[2]](#footnote-3) du [Nom du pouvoir adjudicateur]

Responsable du traitement

|  |
| --- |
| **1 Informations relatives à la notification de la fuite de données** |
| **Coordonnées de l’organisation du déclarant** |
| Nom de l’organisation :  Numéro d’entreprise :  Numéro de TVA européen[[3]](#footnote-4) :  Adresse   Rue :  Numéro de rue :  Boite postale :  Code postale :  Commune/ville :   Pays :  Numéro de téléphone :  Adresse email : |
| **Personne qui notifie le Pouvoir adjudicateur de la fuite de données** |
| Nom/Prénom :  Fonction/Service/Entreprise : |
| **Nom du DPO ou à défaut d’un point de contact** |
| Nom :  Prénom :  **Coordonnées de contact :**  Adresse e-mail :  Numéro de téléphone : |
| **Date et heure de la notification de la fuite de données** |
| Date : XX/XX/XXXX  Heure : xxhxx |
| **2 Ligne du temps de la fuite de données** |
| **Date et heure de la découverte de la fuite de données** |
| Date : XX/XX/XXXX  Heure : xxhxx |
| **Date et heure de la survenance de la fuite de données** |
| Date et heure connues :  Date : XX/XX/XXXX  Heure : xxhxx  Date et heure non connues mais estimées au :  Date : XX/XX/XXXX  Heure : xxhxx  Date et heure non connues |
| **Date et heure de la remédiation de la fuite de données** |
| Date : XX/XX/XXXX  Heure : xxhxx  S’il n’y a pas encore eu de remédiation veuillez en expliquer les raisons : |
| **3 Traitement touché par la fuite de données** |
| **Finalité** |
| Finalité pour laquelle les données sont traitées : |
| **Nature des données qui ont été touchées par la fuite de données** |
| **Nature des données impactées :**  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, …)  Profils (par exemple prévision d'une certaine caractéristique ou attitude)  Caractéristiques personnelles (par exemple âge, sexe, état civil, …)  Données CMR (par exemple informations sur des clients)  Copies de passeport, eID 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  Produit et service (dépenses, consommation, entretien, etc.)  Études et formation  Profession et emploi, régime TVA  Photos ou enregistrements d'images ou de sons (par ex. cctv, caméra de surveillance, formation enregistrée, conversations téléphoniques enregistrées de call centers)  Données RH (relatives au salaire et à la présence du personnel, évaluations, KPI, plan de carrière)  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 au contrôle du personnel (par exemple journalisation, règlement relatif aux lanceurs d'alerte, ...)  Autre :  **Numéro d'identification unique**  Numéro national (par exemple le numéro de Registre national)  Numéro d'identification de la sécurité sociale  Numéro/code d’identification des agents  Autre  **Données à caractère personnel sensibles visées à l’article 9 du RGPD:**  Données révélant l’origine raciale ou ethnique.  Données révélant les opinions politiques.  Données révélant les convictions religieuses ou philosophiques  Données révélant l’appartenance syndicale  Données génétiques (par ex. ADN, groupe sanguin, ...)  Données biométriques (par exemple empreinte digitale)  Données concernant la santé  Données concernant la vie sexuelle ou l'orientation sexuelle  **Données à caractère personnel sensibles visées à l’article 10 du RGPD**:  Condamnations pénales  Infractions  Mesures de sécurité liées à des condamnations pénales ou à des infractions  Extrait du casier judiciaire  **Données à caractère personnel jugées sensibles au sens large car leur traitement implique un certain risque pour les droits et libertés des personnes concernées telles que :**  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, relevé de produits, salaire et revenu, etc.)  Code d'accès (mot de passe, code PIN, ...)  **Autres données:**  **Information non connue**  La nature des données touchées par la fuite de données n'est pas connue. |
| **Nombre de personnes concernées** |
| Nombre minimal de personnes dont des données à caractère personnel sont concernées par la fuite de données (en tant que victimes) : |
| Nombre maximal de personnes dont des données à caractère personnel sont concernées par la fuite de données (en tant que victimes**) :** |
| **Traitement de données confié à un sous-traitant (ultérieur)** |
| la fuite de données n’a pas eu lieu dans le cadre d’un traitement confié à un sous-traitant(ultérieur)  la fuite de données a eu lieu dans le cadre d’un traitement confié à un sous-traitant(ultérieur). Dans ce cas, mentionner le nom du sous-traitant (ultérieur, son numéro d’entreprise (ou à défaut son numéro de TVA) et son adresse complète. |
| **4 Description de la fuite de données** |
| **Les causes de la fuite de données** |
| 1. cause interne (par exemple par le personnel) 2. cause externe (par exemple par un hacker) 3. cause encore inconnue 4. cause accidentelle 5. Mauvaise intention (par exemple vol, fraude, piratage et sabotage) 6. cause encore inconnue |
| **Description de la fuite de données** |
| En résumant le cas, donnez davantage d'informations sur :   * La cause * La manière dont la fuite de données a été détectée * Description du traitement * Les personnes touchées * Les données touchées * Les actions entreprises   **Description :** |
| **La nature de la fuite de données :  Indiquez quelle circonstance correspond à l’incident de sécurité.** |
| 1. Lecture seule (un tiers non autorisé a pu consulter des données (confidentielles). La confidentialité est en danger. |
| 1. Copie (un tiers non autorisé a pu copier des données). La confidentialité est en danger. |
| 1. Modification (un tiers non autorisé peut avoir modifié des données dans les systèmes). L’intégrité est menacée. |
| 1. Effacement ou destruction (un tiers non autorisé a effacé des données des systèmes ou détruit des données). La disponibilité est en danger. |
| 1. Vol – La disponibilité est menacée. |
| 1. Pas encore connu |
| **Nature de la fuite de données** |
| **Perte de confidentialité - Ordre de grandeur des destinataires des données**  Aucune donnée ne s'est retrouvée entre des mains non autorisées  une seule personne ou organisation  un groupe ou une organisation limité(e) / de petite taille (à déterminer selon le contexte de l'organisation)  un grand groupe (à déterminer selon le contexte de l'organisation)  Nombre de personnes inconnu  **Perte de disponibilité**  Les données n'ont jamais été indisponibles  Sont définitivement indisponibles  Sont temporairement indisponibles  Sont disponibles sur la base d'une sauvegarde/copie  Autre, à savoir :  **Perte d’intégrité.**  ll n'y a aucun problème d'intégrité  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.  Autre, à savoir : |
| **Mode de violation** |
| 1. Diffusion non souhaitée des données (suite à une perte, un vol, par   inadvertance, etc.)   1. Publication non souhaitée 2. Accès interne non autorisé 3. Accès externe non autorisé 4. Accès interne autorisé 5. Accès externe autorisé 6. Piratage 7. Malware 8. Phishing 9. Ransomware 10. Autre, à savoir: |
| **5 Prévention de gestion de la fuite de données** |
| 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  Non |
| Actions planifiées et/ou déjà entreprises : |
| Y a-t-il des fichiers de journalisation pertinents disponibles concernant l'incident de sécurité de l'information ?  Oui, à savoir :  Non, la raison en est : |
| **6 Évaluation des risques pour les droits et libertés des personnes**  **concernées** |
| Le risque existe que :  Les données soient diffusées plus largement que nécessaire ou que la  personne concernée risque de perdre son contrôle sur ces données  (par exemple large diffusion à un tiers, publication non souhaitée sur  Internet, perte du contrôle de l'information sur les médias sociaux)  Des liens puissent être établis avec d'autres informations de la (des)  personne(s) concernée(s) (comparaison de fichiers sur la base d'une  caractéristique ou d'un code unique, utilisation de profils,  corrélations, algorithmes, ... data mining, couplage avec la  géolocalisation, ...)  Les données puissent être utilisées pour d'autres finalités ou d'une  manière déloyale, inattendue ou inacceptable pour la personne  concernée (par exemple fins commerciales, usurpation d'identité,  utilisation à l'encontre des personnes concernées)  Il y ait une perte de confidentialité de données à caractère personnel  protégées par le secret professionnel (conformément à l'art. 458 du  Code pénal) |
| Des lacunes surviennent au niveau des données ou des traitements,  empêchant la poursuite de la fourniture du service attendu (par  exemple ralentissement ou blocage de processus administratifs ou  commerciaux, impossibilité de continuer à dispenser des soins du fait  de la disparition de dossiers médicaux, impossibilité pour des  concernées d'exercer leurs droits, ...) |
| Les données puissent être modifiées en des données invalides,  empêchant toute utilisation correcte, le traitement pouvant  engendrer des erreurs, des dysfonctionnements ou l'interruption de  l'offre du service attendu.  Les données puissent être modifiées en d'autres données valides, de  telle sorte que les traitements soient détournés (par exemple  exploitation pour usurper des identités en changeant la relation  entre l'identité des personnes et les données biométriques d'autres  personnes, ...)  Dommages corporels, matériels ou immatériels à des personnes physiques  Perte de contrôle de leurs données à caractère personnel  Limitation de leurs droits  Limitation de la liberté de mouvement (par exemple un refus de passer la frontière)  Discrimination  Exclusion ou modification des conditions du service, de la vie sociale, etc.  Vol d'identité ou fraude à l'identité  Pertes financières  Annulation non autorisée de la pseudonymisation  Atteinte à la réputation  Tout autre préjudice économique ou social important pour la  personne physique en question comme une humiliation grave ou une atteinte à la réputation  Des dommages ou une atteinte aux droits et libertés de personnes physiques, comme lorsque les personnes concernées ne peuvent plus exercer leurs droits et libertés ou sont empêchées d'exercer le contrôle sur leurs données à caractère personnel.  **Autre impact (donnez une description) :** |
| **7 Notification officielle de la fuite des données** |
| Obligation de déclaration de la fuite de données à l’autorité de contrôle |
| Le déclarant a notifié la fuite de données[[4]](#footnote-5)  Date de notification :  Numéro de dossier :  Le déclarant n’a pas notifié la fuite de données.    Motivation:  L’incident ne présente pas de risque pour les personnes concernées  En tant que sous-traitant, le déclarant ne doit pas notifier la fuite de données. C’est la responsabilité du responsable du traitement en fonction de son évaluation du risque.  Autre motif : |
| Obligation de déclaration de la fuite de données aux personnes concernées |
| Le déclarant a notifié la fuite de données[[5]](#footnote-6)  Date de notification :  Mode de communication :  Le déclarant n’a pas notifié la fuite de données.    Motivation:  L’incident ne présente pas de risque élevé pour les personnes concernées  En tant que sous-traitant, le déclarant ne doit pas notifier la fuite de données. C’est la responsabilité du responsable du traitement en fonction de son évaluation du risque.  Autre motif : |

1. Au sens de l’article 4.12 du RGPD, ci-après dénommée « fuite de données » [↑](#footnote-ref-2)
2. Sous-traitant au sens de l’article 4.8 du RGPD [↑](#footnote-ref-3)
3. A compléter s’il n’y a pas de numéro d’entreprise [↑](#footnote-ref-4)
4. Le DPO du pouvoir adjudicateur doit en être informé au préalable [↑](#footnote-ref-5)
5. Le DPO du pouvoir adjudicateur doit en être informé au préalable [↑](#footnote-ref-6)