**CONTRAT DE SOUS-TRAITANCE**

Ce Contrat de sous-traitance est une annexe au Contrat et aux annexes associées, telles que les conditions générales applicables.

**LES SOUSSIGNES :**

**Soussignés :**

1. Client, établi et dont le siège social se trouve à code postal, lieu, à l’adresse ci-après dénommé **“Client” ;** et

2. **XAFAX BELGIUM BVBA,** établie et dont le siège social se trouve à Ternat, à l'adresse (1740), Assesteenweg 25-29, représentée juridiquement par M. F. Duijzer, Directeur de la Société, ci-après dénommé **“Responsable du traitement des données” ;**

**CONSIDERANT QUE :**

a) Dans le cadre du règlement 2016/679, également connu sous le nom de Règlement Général sur la Protection des Données ("RGPD"), qui s'appliquera à partir du 25 mai 2018, les parties souhaitent conclure le présent contrat de traitement ("Contrat de sous-traitance") visé à l'article 28 du RGPD.

**DECLARENT AVOIR CONVENU CE QUI SUIT :**

**ARTICLE 1. DEFINITIONS**

Les termes suivants ont la signification suivante dans le Contrat de sous-traitance :

1.1 Autorité des Données personnelles (AD) : autorité de contrôle, telle que définie à l'article 4, alinéa 21 du RGPD.

1.2 RGPD : le Règlement Général sur la Protection des Données.

1.3 Responsable du traitement des données : partie qui, en tant que fournisseur de TIC dans le cadre de l'exécution du Contrat, traite les données personnelles pour le compte de son Client.

1.4 Personne concernée : une personne physique identifiée ou identifiable.

1.5 Client : partie pour qui le Responsable du traitement des données traite des données personnelles. Le Client peut être un responsable du traitement ("contrôleur") ou un autre sous-traitant.

1.6 Contrat : le contrat entre le Client et le Responsable du traitement des données, sur la base duquel le fournisseur de TIC fournit des services et/ou des produits au Client, dont le Contrat de sous-traitance fait partie.

1.7 Données personnelles : toutes les informations concernant une personne physique identifiée ou identifiable, telles que décrites à l'article 4, paragraphe 1 du RGPD, que le Responsable du traitement des données traite dans le cadre de l'exécution de ses obligations découlant du Contrat.

1.8 Contrat de sous-traitance : les présentes Clauses standard de traitement, formant ensemble le Contrat de sous-traitance visé à l'article 28, paragraphe 3 du RGPD.

**ARTICLE 2. GENERAL**

2.1 Les présentes Clauses standard de traitement s'appliquent à tous les traitements de Données personnelles effectués par le Responsable du traitement dans le cadre de la fourniture de ses produits et services et à tous les Contrats et offres. L'applicabilité des contrats de sous-traitance du Client est expressément rejetée.

2.2 Le Responsable du traitement des données traite les données personnelles au nom et sur instructions du Client conformément aux instructions écrites du Client convenues avec le Responsable du traitement des données.

2.3 Le Client, ou son client, est le responsable du traitement au sens du RGPD, a le contrôle du traitement des Données Personnelles et a déterminé la finalité et les moyens du traitement des Données Personnelles.

2.4 Le Responsable du traitement des données est un sous-traitant au sens du RGPD et n'a donc aucun contrôle sur la finalité et les moyens de traitement des Données personnelles et ne prend donc aucune décision concernant, entre autres, l'utilisation des Données Personnelles.

2.5 Le Responsable du traitement des données exécute le RGPD conformément aux présentes Clauses standard de traitement et au Contrat et agit conformément au RGPD. Sur la base de ces informations, il appartient au Client d'évaluer si le Responsable du traitement des données offre des garanties suffisantes en ce qui concerne l'application des mesures techniques et organisationnelles appropriées afin que le traitement réponde aux exigences du RGPD et que la protection des droits des Personnes concernées soit suffisamment garantie.

2.6 Le Client garantit au Responsable du traitement qu'il agit conformément au RGPD, qu'il protège ses systèmes et son infrastructure à tout moment et que le contenu, l'utilisation et/ou le traitement des Données Personnelles ne sont pas illégaux et ne portent atteinte à aucun droit d'un tiers.

2.7 Une pénalité administrative imposée par l’AD au Client ne peut être recouvrée auprès du Responsable du traitement des données, à moins qu'il n'y ait eu intention ou imprudence délibérée de la part de la direction du Responsable du traitement des données.

**ARTICLE 3. SECURITE**

3.1 Le Responsable du traitement des données prend les mesures de sécurité techniques et organisationnelles conformément au RGPD. En prenant les mesures de sécurité techniques et organisationnelles, le Responsable du traitement des données a tenu compte de l'état de la technique, des coûts de mise en œuvre des mesures de sécurité, de la nature, de la portée et du contexte du traitement, des finalités et de l'utilisation prévue de ses produits et services, des risques de traitement et des divers risques pour les droits et libertés des personnes concernées qu'il pourrait attendre compte tenu de l'utilisation prévue de ses produits et services.

3.2 Le produit ou le service du Responsable du traitement des données n'est pas conçu pour le traitement de catégories particulières de Données Personnelles ou de données relatives à des condamnations pénales ou à des infractions.

3.3 Le Responsable du traitement des données s'efforce de s'assurer que les mesures de sécurité à prendre sont appropriées à l'utilisation prévue du produit ou du service par le Responsable du traitement des données.

3.4 Les mesures de sécurité décrites doivent, de l'avis du Client et compte tenu des facteurs mentionnés à l'article 3.1, fournir un niveau de sécurité approprié au risque du traitement des Données Personnelles utilisées ou fournies par le Client.

3.5 Le Responsable du traitement des données peut modifier les mesures de sécurité en place s'il le juge nécessaire pour maintenir un niveau de sécurité approprié. Le Responsable du traitement des données enregistrera les changements importants et informera le Client de ces changements le cas échéant.

3.6 Le Client peut demander au Responsable du traitement des données de prendre d'autres mesures de sécurité. Le Responsable du traitement des données n'est pas tenu d'apporter des modifications à ses mesures de sécurité à cette demande. Le Responsable du traitement des données peut facturer au Client les coûts liés aux modifications apportées à la demande du Client. Le Responsable du traitement des données n'est tenu d'appliquer effectivement ces mesures de sécurité qu'après que les mesures de sécurité souhaitées par le Client aient été convenues par écrit et signées par les parties.

**ARTICLE 4. VIOLATIONS LIÉES AUX DONNÉES PERSONNELLES**

4.1 Le Responsable du traitement des données ne garantit pas l'efficacité des mesures de sécurité dans toutes les circonstances. Si le Responsable du traitement des données découvre une violation des données personnelles (au sens de l'article 4, alinéa 12 du RGPD), il en informe le Client sans délai déraisonnable.

4.2 Il appartient au Responsable du traitement (le Client ou son client) d'évaluer si l'atteinte à la protection des Données Personnelles dont le Responsable du traitement a été informé doit être signalée à l’AD ou à la Personne concernée. Le signalement des violations de Données Personnelles, qui doivent être signalées à la PA et/ou aux Personnes concernées conformément aux articles 33 et 34 du RGPD, reste à tout moment sous la responsabilité du Responsable du traitement (le Client ou son client). Le Responsable du traitement des données n'est pas tenu de signaler les atteintes à la protection des Données Personnelles à la PA et/ou à la Personne concernée.

4.3 Le Responsable du traitement des données fournira, si nécessaire, d'autres informations sur l'atteinte à la protection des Données Personnelles et coopérera en fournissant les informations nécessaires au Client aux fins d'une notification telle que visée aux articles 33 et 34 du RGPD.

4.4 Le Responsable du traitement des données peut facturer au Client les coûts raisonnables qu'il encourt à cet égard à ses tarifs alors en vigueur.

**ARTICLE 5. CONFIDENTIALITE**

5.1 Le Responsable du traitement des données garantit que les personnes qui traitent les Données Personnelles sous sa responsabilité ont une obligation de confidentialité.

5.2 Le Responsable du traitement a le droit de fournir les Données Personnelles à des tiers, si et dans la mesure où la divulgation est nécessaire à la suite d'une décision judiciaire, d'une disposition légale ou sur la base d'un ordre donné par une autorité publique.

5.3 Tous les codes d'accès et/ou d'identification, les certificats, les informations relatives à la politique d'accès et/ou de mot de passe et toutes les informations fournies par le Responsable du traitement des données au Client pour mettre en œuvre les mesures de sécurité techniques et organisationnelles sont confidentiels et seront traités comme tels par le Client et ne seront divulgués qu'aux employés autorisés du Client. Le Client doit s'assurer que ses employés respectent les obligations découlant du présent article.

**ARTICLE 6. DUREE ET RESILIATION**

6.1 Le présent Contrat de sous-traitance fait partie intégrante du Contrat et tout accord nouveau ou ultérieur qui en découle entre en vigueur au moment de la conclusion du Contrat et est conclu pour une durée indéterminée.

6.2 Le présent Contrat de sous-traitance prend fin par effet de la loi à la résiliation du Contrat ou de tout accord nouveau ou ultérieur entre les parties.

6.3 En cas de résiliation du Contrat de sous-traitance, le Responsable du traitement des données doit supprimer toutes les Données Personnelles en sa possession et reçues du Client de telle sorte qu'elles ne puissent plus être utilisées et ne soient plus accessibles, ou, si convenu, retournées au Client dans un format lisible par machine.

6.4 Le Responsable du traitement des données peut facturer au Client les frais qu'il engage dans le cadre des dispositions de l'article 6.3.

6.5 Les dispositions de l'article 6.3 ne s'appliquent pas si une disposition légale empêche le Responsable du traitement des données de supprimer ou de renvoyer les Données Personnelles en tout ou en partie. Dans un tel cas, le Responsable du traitement ne continuera à traiter les Données Personnelles que dans la mesure nécessaire en vertu de ses obligations légales. Les dispositions de l'article 6.3 ne s'appliquent pas non plus si le Responsable du traitement des données est le responsable du traitement au sens du RGPD en ce qui concerne les Données Personnelles.

**ARTICLE 7. DROITS DES PERSONNES CONCERNEES, ANALYSE D’IMPACT SUR LA PROTECTION DES DONNEES (DPIA) ET DROITS D’AUDIT**

7.1 Dans la mesure du possible, le Responsable du traitement des données coopérera avec les demandes raisonnables du Client liées aux droits des Personnes concernées invoqués par le Client pour les Personnes concernées. Si le Responsable du traitement des données est approché directement par une Personne concernée, il en informera le Client dans la mesure du possible.

7.2 Si le Client est obligé de le faire, le Responsable du traitement des données coopère avec une analyse d'impact sur la protection des données (DPIA) ou une consultation préalable subséquente telle que visée aux articles 35 et 36 du RGPD, après qu'une demande raisonnable à cet effet ait été faite.

7.3 Le Responsable du traitement des données peut démontrer le respect des obligations qui lui incombent en vertu du Contrat de sous-traitance au moyen d'un certificat Data Pro valide ou d'un certificat ou d'un rapport d'audit au moins équivalent (Mémorandum de tiers) émanant d'un expert indépendant.

7.4 Le Responsable du traitement des données doit, à la demande du Client, mettre à sa disposition toute autre information raisonnablement nécessaire pour démontrer la conformité aux ententes conclues dans le cadre du Contrat de sous-traitance. Si le Client a néanmoins des raisons de croire que le traitement des Données Personnelles n'a pas lieu conformément au Contrat de sous-traitance, il peut, au maximum une fois par an, faire réaliser un audit par un expert externe indépendant, certifié et ayant une expérience démontrable du type de traitement effectué sur la base du Contrat, aux frais du Client. L'audit se limite à la vérification du respect des accords relatifs au traitement des Données Personnelles tels que définis dans le présent Contrat de sous-traitance. L'expert a une obligation de confidentialité à l'égard de ce qu'il trouve et ne doit faire rapport au Client que si cela constitue une lacune dans l'exécution des obligations que le Responsable du traitement des données a en vertu du présent Contrat de sous-traitance. L'expert fournit une copie de son rapport au Responsable du traitement des données. Le Responsable du traitement des données peut refuser un audit ou une instruction de l'expert si, à son avis, cela est contraire au RGPD ou à toute autre législation ou constitue une violation inadmissible des mesures de sécurité qu'il a prises.

7.5 Les parties se consultent dès que possible sur les résultats du rapport. Les parties assureront le suivi des mesures d'amélioration proposées dans le rapport dans la mesure où cela peut raisonnablement être attendu d'elles. Le Responsable du traitement des données mettra en œuvre les mesures d'amélioration proposées dans la mesure où il estime qu'elles sont appropriées, compte tenu des risques de traitement associés à son produit ou service, de l'état de la technique, des coûts d'exécution, du marché sur lequel il opère et de l'utilisation prévue du produit ou du service.

7.6 Le Responsable du traitement des données est en droit de facturer au Client les coûts qu'il engage dans le cadre des dispositions du présent article.

**ARTICLE 8. SOUS-TRAITANTS**

8.1 Le Client autorise le Responsable du traitement des données à engager d'autres sous-traitants dans l'exécution de ses obligations découlant du Contrat.

8.2 Le Responsable du traitement des données doit informer le Client d'un changement chez les tiers engagés par le Responsable du traitement des données. Le Client a le droit de s'opposer à la modification susmentionnée par le Responsable du traitement des données. Le Responsable du traitement des données veille à ce que les tiers engagés par lui s'engagent au même niveau de sécurité en ce qui concerne la protection des Données Personnelles que le niveau de sécurité auquel le Responsable du traitement des données est tenu envers le Client.

**ARTICLE 9. AUTRES**

Les présentes Clauses standard font partie intégrante du présent Contrat. Tous les droits et obligations en vertu du Contrat, y compris les conditions générales applicables et/ou les limitations de responsabilité, s'appliquent donc également au Contrat de sous-traitance.

**Pour accord :**

Je suis d'accord avec ce document et déclare l'avoir reçu et lu.

Client : Xafax Belgium BVBA

Nom : (pouvoir de signature) Fokko Duijzer

Fonction : Directeur


Signature :

**Annexe 1 Données personnelles**

Informations générales

Nom du produit et / ou du service : Xafax NetPay

Lien vers la page du fournisseur et / ou du produit : [www.xafax.nl](http://www.xafax.nl)

Description du traitement

Traitement des transactions de chargement et des transactions effectuées sur des imprimantes multifonctions, des distributeurs automatiques et des caisses enregistreuses des personnes concernées.

Catégories et types de données personnelles

En fonction des services et des fonctionnalités que la personne concernée utilise, nous pouvons, entre autres, traiter les données personnelles suivantes de la personne concernée :

1. les données d'identification, telles que les nom, prénom, sexe et date de naissance ;
2. les informations de contact, telles que l'adresse (e-mail) et le numéro de téléphone (mobile) ;
3. les données de transaction, telles que les crédits et les débits ;
4. les données financières, telles que le numéro de compte bancaire (dans le cas où la personne concernée souhaite demander un remboursement) ;
5. des informations sur le comportement et les préférences en ligne, telles que l'adresse IP de l'appareil mobile ou de l'ordinateur et les pages que la personne concernée consulte sur le site Web ou dans les applications Xafax ;
6. les données que la personne concernée partage avec nos services de contact, la correspondance avec Xafax et les données de support (téléphone, conversations de chat et e-mail).

Toutes les données traitées par Xafax sont de nature non spéciale.

Catégories de personnes concernées

* Étudiants / élèves
* Parents / tuteur
* Collaborateurs
* Participants

Finalités du traitement

Nous utilisons les données personnelles de la personne concernée aux fins suivantes :

* Pour lui donner accès à son compte, lui offrir la possibilité d'acheter du crédit, traiter sa commande et utiliser nos fonctionnalités et services ;
* La vérification du compte de la personne concernée, de son jeton / pass ou de toute autre information ajoutée ;
* Le traitement des transactions de paiement, la remise de jetons / passes, la sécurisation de la plateforme et des comptes, l'identification et la fourniture de services ;
* Maintenir les conditions d'utilisation de (my) NetPay ;
* Se conformer aux lois et règlements ;
* Aider des tiers pour la fourniture des produits / services que la personne concernée demande à des tiers ;
* Régler les litiges et les opérations de paiement contestées ;
* Reconnaître, prévenir, limiter et combattre les abus et la fraude ;
* Pour rester en contact avec la personne concernée, lui fournir des informations et répondre à ses questions, demandes ou plaintes ;
* Obtenir des informations sur l'utilisation de nos produits et services en effectuant des analyses de données pour les améliorer.

Durée de conservation des données à caractère personnel

Les données personnelles seront conservées aussi longtemps que nécessaire aux fins énoncées ci-dessus ou aussi longtemps que la loi l'exige. Le règlement général sur la protection des données ne stipule aucune période de conservation spécifique pour les données à caractère personnel. D'autres lois peuvent contenir des périodes de conservation minimales. Dans ce cas, il faut conserver ces données aussi longtemps.

## Catégories Employés

|  |  |  |  |
| --- | --- | --- | --- |
| **Catégories d'employés (rôles / groupes d'emplois) des sous-traitants qui traitent des données personnelles** | **(catégorie) Données personnelles traitées par les employés** | **Type de traitement** | **Pays de traitement** |
| Gestion technique et des applications | 1, 2, 3, 6 | 1, 2, 3, 6 | NL |
| Service d’assistance | 1, 2, 6 | 1, 2, 6 | NL |
| Finances | 1, 2, 3, 4, 6 | 1, 2, 3, 4, 6 | NL |
| R&D | 5 | 5 | NL |

## Sous-traitants ultérieurs

Ne s'applique pas

## Transfert

Ne s'applique pas

## Coordonnées

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Coordonnées générales**  | **Nom** | **Fonction** | **Adresse e-mail** | **Numéro de téléphone** |
| Sous-traitant | Pauline Terkoolt | Délégué à la protection des données | privacy@xafax.nl | 072-5667400 |
|  |
|  | **Nom** | **Fonction** | **Adresse e-mail** | **Numéro de téléphone** |
| **Coordonnées de l'infraction en relation avec des données personnelles** |  |  |  |  |
| Sous-traitant | Julian van Wickeren | Chef d'équipe de la gestion technique et des applications | jvwickeren@xafax.nl | 072-5667400 |

Annexe 2 : mesures de sécurité

**Généralités**

Le sous-traitant a une politique appropriée pour sécuriser le traitement des données à caractère personnel, l'efficacité des mesures techniques et organisationnelles étant évaluée de façon périodique et, si nécessaire, ajustée.

Une politique de sécurité de l'information a été élaborée et des accords ont été conclus avec les employés concernant la conformité. Des procédures ont été établies pour l’évaluation et le traitement des risques, la gestion des changements et la gestion des incidents.

Le sous-traitant utilise un document de politique qui décrit explicitement les mesures prises par le sous-traitant pour sécuriser le traitement des données et garantir la confidentialité. Ce document de politique est basé sur les normes de sécurité généralement utilisées telles que ISO 27002: 2013.

**Accès autorisé aux données à caractère personnel**

Des mesures de sécurité sont incluses dans tous les systèmes d’application, y compris un contrôle d’accès adéquat.

Le sous-traitant utilise un système d'autorisation où seuls les employés autorisés peuvent accéder au traitement des données personnelles. Le sous-traitant a établi des procédures d'identification, d'autorisation et d'authentification des employés, ainsi que d'enregistrement, d'inscription et de désenregistrement des employés.

Le sous-traitant dispose de procédures pour accorder l'accès aux données personnelles (y compris une procédure d'enregistrement et de désenregistrement pour l'attribution de droits d'accès), ainsi que pour la journalisation des événements liés aux activités des utilisateurs, aux exceptions et aux événements de sécurité des informations.

**Sécurité physique**

Les installations et équipements informatiques sont physiquement protégés contre les accès non autorisés et contre les dommages et les perturbations.

**Confidentialité**

Les employés du sous-traitant qui sont impliqués dans le traitement des données personnelles sont liés par une obligation de confidentialité / un code d'intégrité.

**Formation / éducation**

Tous les employés de l'organisation et, le cas échéant, le personnel recruté et les utilisateurs externes suivent une formation appropriée et une formation continue régulière sur les politiques et procédures de sécurité de l'information de l'organisation, en fonction de leur poste. Dans le cadre de la formation et de la formation continue, une attention particulière est accordée au traitement de données à caractère personnel (catégories spéciales, ou autrement sensibles).

**Politique pour le mot de passe**

Il existe une politique d’authentification et de mot de passe qui impose l’utilisation obligatoire de mots de passe forts et / ou 2FA pour permettre aux utilisateurs autorisés d’accéder aux systèmes et services d’information dont ils ont besoin pour effectuer leurs tâches et pour empêcher tout accès non autorisé aux systèmes d’information.

**Incidents de sécurité**

Il y a une procédure permettant de traiter rapidement et efficacement les incidents de sécurité des informations et les vulnérabilités de sécurité dès qu'ils sont signalés.

**Sauvegarde**

Une procédure adéquate de sauvegarde et de récupération est prévue afin de pouvoir restaurer une corruption ou une perte indésirable de données (personnelles).

Un plan de continuité des opérations a été élaboré pour garantir la continuité des services en cas de défaillance du système.

**Surveillance**

Le réseau et les systèmes d’information sont activement surveillés et gérés pour détecter les activités de traitement de l’information non autorisées. Une procédure a été mise en place pour traiter les fuites de données. Une partie de cette procédure consiste à informer le responsable du traitement.

Le sous-traitant installe des solutions opportunes publiées par les fournisseurs pour les fuites de sécurité. Tout cela uniquement si et dans la mesure où le logiciel en question a été / sera fourni par le sous-traitant, utilisé ou mis à jour pour le responsable du traitement.

Une procédure a été mise en place pour maintenir les applications à jour.

**Test de vulnérabilité**

Le sous-traitant a pris des mesures pour identifier les faiblesses concernant le traitement des données à caractère personnel dans les systèmes. Par exemple, les vulnérabilités techniques du réseau et des systèmes environnants sont régulièrement testées.

Si possible, un logiciel antivirus et anti-malware est installé et actif.

**Données à caractère personnel**

Le sous-traitant a classifié les données à caractère personnel traitées en termes de disponibilité, d'intégrité et de confidentialité et a pris des mesures de sécurité sur la base de cette classification afin de limiter les risques liés au traitement des données à caractère personnel.

Un cryptage adéquat est toujours appliqué au transport et au stockage d'informations confidentielles sur des réseaux explicitement désignés comme tels par le responsable de traitement.

A security incident (hereinafter: data leak) is a breach, intentional or accidental, in relation to personal data. A data leak exists in the event of a security breach resulting in:

* (final) destruction of personal data (e.g. due to fire or erasure); or
* loss of personal data (e.g. due to a USB or laptop being lost); or
* unintentional modification of personal data; or
* unauthorised disclosure of personal data (e.g. email/files sent to wrong addressee);or
* unauthorised access to transmitted/stored/otherwise processed personal data (e.g. by a hacker or an unauthorised staff member).

Annexe 3 : Procédure de fuite de données

Un incident de sécurité (ci-après une fuite de données) est une violation, intentionnelle ou accidentelle, liée à des données personnelles. Il y a fuite de données si une violation de la sécurité entraîne :

* la destruction (définitive) de données personnelles (par exemple, suite à un incendie ou à une suppression) ; ou
* la perte de données personnelles (par exemple une clé USB ou un ordinateur portable qui se perd) ; ou
* le changement de données personnelles (sans que cela soit l'intention) ; ou
* la divulgation non autorisée de données personnelles (par exemple, des courriers électroniques / fichiers envoyés à un mauvais destinataire) ; ou
* l'accès non autorisé à des données à caractère personnel transmises / stockées / autrement traitées (par exemple par un pirate informatique ou un membre du personnel non autorisé).

Les accords suivants ont été conclus entre les parties en ce qui concerne l'obligation de signaler les fuites de données :

Étape 1 : Xafax détermine si fuite de données il y a ;

Étape 2 : L'équipe de confidentialité de Xafax discute de la fuite de données et des mesures à prendre. L’équipe de protection de la confidentialité de Xafax comprend : un membre de la direction, un chef d’équipe de gestion technique et des applications et le responsable de la protection des données ;

Étape 3: Xafax prend des mesures en fonction du questionnaire pour arrêter la fuite (active) ou en limiter les conséquences ;

Étape 4 : Xafax étudie et collecte autant de données que possible sur la fuite de données ;

Étape 5 : Xafax informe le responsable du traitement dans les meilleurs délais et communique les informations pertinentes sur l'incident à l'aide du questionnaire ci-dessous ;

Étape 6 : Xafax prend des mesures pour empêcher un type similaire de fuite de données à l'avenir ;

Étape 7 : Le responsable du traitement évaluera si un rapport doit être effectué au point d'accès. Le responsable du traitement consultera Xafax ;

Étape 8 : Avant que le responsable du traitement ne transmette le rapport à l'AP, le responsable discutera du contenu du rapport avec Xafax ;

Étape 9 : Si le responsable du traitement estime que les personnes concernées doivent également être informées de la fuite des données, il discutera du contenu de ces informations avec Xafax.

**Questionnaire sur la fuite de données - avec procédure de déclaration des fuites de données**

1. **Coordonnées**

Responsable du traitement :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Fonction | Téléphone | E-mail |
| Nom du 1er contact |  |  |  |  |
| Nom 2ème contact |  |  |  |  |

Xafax (sous-traitant) :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Fonction | Téléphone | E-mail |
| Nom du 1er contact | Julian van Wickeren | Chef d'équipe de la gestion technique et des applications | 072-5667400 | privacy@xafax.nl |
| Nom 2ème contact | Pauline Terkoolt | Délégué à la protection des données | 072-5667400 | privacy@xafax.nl |

1. **De quel genre de fuite de données s'agit-il :**

.... (à remplir par Xafax)

Choisissez 1 :

* Appareil, support de données (p. ex Clé USB) et / ou papier avec des données personnelles perdu(e) ou volé(e) ;
* Lettre ou colis postal contenant les données personnelles perdu(e) ou renvoyé(e) ouvert(e) ;
* Accès non autorisé à des données personnelles transmises / stockées / autrement traitées (par exemple, pirate informatique, logiciels malveillants, phishing ou personnel non autorisé).
* Données personnelles modifiées ou supprimées définitivement de manière accidentelle ;
* Destruction de données personnelles (par exemple, incendie ou suppression) ;
* Les données personnelles toujours présentes sur un périphérique mis au rebut ou un support de données mis au rebut (par ex. Clé USB) ;
* Données personnelles publiées par accident ;
* Données personnelles du mauvais client affichées dans le portail client ;
* Données personnelles envoyées ou transmises au mauvais destinataire ;
1. **Faites un résumé de la fuite de données :**

.... (à remplir par Xafax)

1. **Si la fuite de données s'est produite chez un sous-traitant ultérieur :**

… (nom du sous-traitant ultérieur)

1. **Les données personnelles de combien de personnes sont concernées par la fuite de données ?**

Minimum .... (à remplir par Xafax)

Maximum .... (à compléter par Xafax)

1. **Décrivez le groupe de personnes dont les données personnelles sont concernées par la fuite de données :**

… (à remplir par Xafax) (par exemple, élèves, parents, employés, invités)

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

Le (date) .... (à remplir par Xafax)

Entre (date de début) et (date de fin)

Pas encore connu

1. **Quand la fuite de données a-t-elle été découverte ?**

.... (à remplir par Xafax)

1. **Quelle est la nature de la fuite de données ? Encerclez les réponses et complétez si nécessaire**
* Une personne non autorisée peut-elle lire les données : oui / non
* Les données peuvent-elles être copiées/sont-elles copiées

par une personne non autorisée : oui / non

* Les données (source) peuvent-elles être modifiées/sont-elles

modifiées (par exemple par un pirate dans le système) : oui/non

* Les données (source) peuvent-elles être supprimées

ou détruites/sont-elles supprimées ou détruites ?

(ex. ransom ware ou incendie du centre de données) : oui / non

* Les données ont-elles été volées : oui / non
1. **De quel type de données s'agit-il ? Encerclez les réponses et complétez si nécessaire :**
* Données d'identification, telles que nom, nom de famille,

sexe et date de naissance : oui / non

* Informations de contact, telles que l'adresse (e-mail)

et le numéro de téléphone (mobile) : oui / non

* Données de transaction, telles que crédits et débits : oui / non
* Données financières, telles que le numéro de compte bancaire

(dans le cas où la personne concernée réclame un remboursement) : oui / non

* Données sur le comportement et les préférences en ligne,

telles que l'adresse IP de l'appareil mobile ou de l'ordinateur

et les pages consultées par la personne concernée sur le site ou

dans les applications Xafax : oui / non

* Données que la personne concernée partage avec nos services de

contact, correspondance avec Xafax et données de support \(téléphone, conversations de chat et e-mail) : oui / non

1. **Quelles conséquences la fuite de données peut-elle avoir pour les personnes concernées ? Encerclez les réponses et complétez si nécessaire :**
* Stigmatisation ou exclusion : oui / non
* Dommage pour la santé : oui / non
* Risque de fraude d'identité : oui / non
* Risque de dommages financiers (par exemple, fraude avec

coordonnées de carte de crédit) : oui / non

* Exposition au spam ou au phishing : oui / non
* Autres conséquences, à savoir :
1. **Décrivez quelles mesures techniques et organisationnelles ont été prises pour remédier à la fuite de données, en limiter les effets négatifs et prévenir de nouvelles violations et, dans la mesure du possible et le cas échéant, appliquer à l'avenir les mesures proposées avec ces objectifs ?**

.... (à remplir par Xafax)

1. **Les données personnelles qui ont fui sont-elles sécurisées ? Encerclez les réponses et complétez si nécessaire :**

Les données sont-elles cryptées :

Si oui quel cryptage :…. (à compléter par Xafax)

Ce cryptage s'applique-t-il à toutes les données personnelles ou à une partie de celles-ci ? S'il ne concerne qu'une partie, la citer :…. (à compléter par Xafax)

Les données ont-elles été piratées :

Si oui comment :…. (à compléter par Xafax)

Les données peuvent-elles être supprimées à distance :

Si oui est-ce que c'est arrivé et quand :… (à compléter par Xafax)

Les données ont-elles été rendues incompréhensibles ou inaccessibles d'une autre manière :

Si oui de quelle manière :…. (à compléter par Xafax)

1. **Les données personnelles de personnes dans d'autres pays de l'UE ont-elles été affectées par la fuite de données ? Si oui, lesquelles et dans quels pays :**

.... (à remplir par Xafax)