Contrat de traitement de données Mediwet asbl

1. Préambule

Le présent contrat de traitement de données a été élaboré dans le cadre du Règlement général sur la protection des données, RGPD en abrégé, ci-après dénommé le RGPD ou le Règlement général sur la protection des données, soit le Règlement 2016/679 du 27 avril 2016. Ce règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel (art. 1, 2° RGPD).

Le présent contrat de traitement de données et ses annexes ont valeur d'annexe au contrat principal conclu entre Mediwet et le client. Les dérogations à la présente Politique de confidentialité sont uniquement valables si les deux parties ont donné leur accord écrit à ce sujet.

Nos clients seront informés de toute modification fondamentale.

Par le biais du présent contrat, Mediwet entend fournir des informations sur la manière dont elle traite les données à caractère personnel de ses clients et de leurs travailleurs.

Dans le cadre de la relation avec les travailleurs du client, Mediwet doit être considérée comme le responsable du traitement conformément à l'avis de Co-Prev du 26/01/2018. Cela signifie que Mediwet est elle-même responsable du respect des obligations du RGPD (art. 5, 2° RGPD) dans le cadre de la relation avec les travailleurs de ses clients.

2. Licéité, loyauté et transparence

Le traitement des données à caractère personnel par Mediwet est licite, étant donné qu'il est nécessaire à l'exécution d'une mission d'intérêt public (art. 6, 1, e RGPD), à tout le moins pour respecter une obligation légale à laquelle le client est soumis (art. 6, 1, c RGPD). Plus spécifiquement, le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux… (art. 9, h RGPD), ou le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au client en matière de droit du travail, de la sécurité sociale et de la protection sociale… (art. 9, b RGPD).

Les données à caractère personnel traitées sont des données d'identification et de contact courantes : nom, prénom, âge, sexe, date et lieu de naissance, mais aussi le numéro de registre national et les données médicales au sens le plus large du terme, dont : poids, taille, IMC, (in)capacité de travail, lésions…

3. Pas de traitement ultérieur incompatible

Mediwet traite les données de ses clients et des travailleurs de ses clients dans le cadre exclusif de la législation sur le bien-être. De même, un traitement ultérieur ne s'inscrira que dans le cadre de la législation sur le bien-être, y compris à des fins de recherche scientifique ou historique ou à des fins statistiques, dans la mesure du possible par pseudonymisation (art. 89 RGPD).

4. Traitement de données minimal

Mediwet traitera uniquement des données adéquates, pertinentes et limitées à ce qui est nécessaire dans le cadre de la législation sur le bien-être.

5. Exactitude

Mediwet vise l'exactitude et l'actualisation de ses données. À cette fin, les personnes concernées peuvent toujours demander la rectification de leurs données, tel que prévu à l'Annexe 2: NOTIFICATION DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL.

6. Limitation de la conservation

Dans l'intérêt des travailleurs, toutes les données sont conservées jusqu'à 30 ans après l'âge normal de la pension. Les données à caractère personnel peuvent être conservées plus longtemps à des fins statistiques ou dans le cadre de la recherche scientifique ou historique, auquel cas les données seront autant que possible anonymisées.

7. Intégrité et confidentialité

Mediwet veille à ce que les données à caractère personnel soient suffisamment sécurisées. Afin de prévenir les pertes et les traitements illicites, Mediwet met en œuvre des mesures techniques et organisationnelles appropriées. Ces mesures ont été adaptées au risque du traitement. Un aperçu de ces mesures et la politique à cet égard sont repris à l'Annexe 3: Aperçu des mesures de sécurité.

De plus, les rapports de groupe seront effectués de manière exclusivement anonyme, c.-à-d. seulement à partir de jeux de données de 10.

Le client a le droit de contrôler si le traitement des données à caractère personnel est conforme à la loi et aux conventions du présent Contrat de traitement de données, mais uniquement pour vérifier si la conformité au RGPD du traitement par Mediwet est garantie et exclusivement pour ce qui concerne les données que Mediwet traite pour le Client.

8. Exportation des données à caractère personnel

Mediwet ne fera pas traiter les données à caractère personnel par d'autres personnes ou organisations extérieures à l'Espace économique européen (EEE), sans avoir obtenu l'autorisation écrite préalable de la personne concernée.

Le Client autorise Mediwet à désigner un autre responsable du traitement et/ou d'autres sous-traitants si le traitement des données à caractère personnel le nécessite. Si Mediwet fait appel à d'autres organisations, elles devront au minimum satisfaire aux exigences reprises dans le présent Contrat de traitement de données.

Les principales parties externes pouvant être impliquées dans le traitement des données à caractère personnel sont : les autorités publiques (le fonctionnaire chargé de la surveillance, le ministère public, Fedris, l'ONSS, Vaccinet…), d'autres services externes agréés, y compris Premed en tant que notre fournisseur de logiciel, des laboratoires médicaux agréés pour les analyses de laboratoire, Monstarecon pour le traitement des questionnaires psychosociaux, les médecins traitants et le médecin-conseil de la mutuelle dans le cadre d'un dossier de réintégration (E-Health).

9. Secret professionnel

Mediwet gardera le secret sur les données à caractère personnel fournies, sauf si cela s'avère impossible sur la base d'une obligation légale, et veillera à ce que son personnel et les préposés ou mandataires recrutés respectent également ce secret professionnel.

10. Fuites de données

En cas de découverte d'une possible fuite de données, Mediwet en informera les personnes concernées dans les meilleurs délais par voie électronique et fournira les informations indiquées à l'Annexe 4: Processus de notification de fuites de données et informations à fournir.

Les coûts éventuellement consentis pour résoudre la fuite de données et la prévenir dans le futur sont à la charge de celui qui les consent.

11. Data Protection Officer et registre des activités de traitement

Conformément à l'article 37 et suiv. du RGPD, Mediwet a désigné un Data Protection Officer (DPO) ou délégué à la protection des données, lequel peut être contacté via :

DPO Mediwet
Opvoedingstraat 143, 9000 Gand
Tél. 09 221 06 07 – Fax 09 221 78 67
e-mail: privacy@mediwet.be

Mediwet a également établi un registre des activités de traitement, conformément à l'article 30 et suiv. du RGPD. Ce registre décrit, par activité ou par processus, les finalités du traitement, les catégories de personnes concernées, le fondement de traitement spécifique au processus, les mesures de sécurité, etc. D'éventuels éclaircissements sur la base de ce registre de traitement peuvent toujours être fournis sur simple demande adressée à notre DPO.

12. Droits de la personne concernée

Le RGPD garantit à toutes les personnes concernées un droit d'accès, de rectification, d'effacement, de limitation et d'opposition. Ce dernier droit restera généralement sans effet car Mediwet se base sur un fondement légal. Néanmoins, Mediwet répondra à la demande dans un délai d'un mois à compter de sa réception, conformément à l'article 12, 3° du RGPD, lequel délai peut être prolongé de deux mois en fonction de la complexité de la demande.

Pour consulter un dossier médical, la demande doit être adressée au directeur du service de Surveillance de la santé, Opvoedingstraat 143, 9000 Gand. Le droit de consultation des dossiers médicaux n'est pas directement accordé au travailleur, mais à son médecin traitant conformément à l'avis de l'Ordre des médecins du 7 septembre 1996.

Pour consulter un dossier psychosocial, la demande doit être adressée au conseiller en prévention-aspects psychosociaux concerné.

13. Dispositions finales

Le présent Contrat de traitement de données fait partie du contrat conclu entre Mediwet et le client et reste en vigueur jusqu'au terme de ce contrat. Si le contrat prend fin, le présent Contrat de traitement de données prend automatiquement fin. Le Contrat de traitement de données ne peut être résilié séparément.
Par conséquent, tous les droits et obligations découlant du contrat s'appliquent également au Contrat de traitement de données.

Au terme du présent Contrat de traitement de données, les obligations en vigueur, telles que la notification de fuites de données impliquant des données à caractère personnel et l'obligation de secret professionnel, demeurent.

En cas d'éventuelles contradictions liées à la protection des données à caractère personnel entre les dispositions du présent Contrat de traitement de données et celles du Contrat principal, les dispositions du présent Contrat de traitement de données l'emportent.

Le présent Contrat de traitement de données est régi par le droit belge. Les éventuels litiges seront soumis au jugement des tribunaux de l'arrondissement de Gand.

Annexe 1: DEFINITIONS CONCERNANT GDPR

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL
du 27 avril 2016
relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
Article 4
Définitions

Aux fins du présent règlement, on entend par:
1) «**données à caractère personnel**», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2) «**traitement**», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

3) «**limitation du traitement**», le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur;

4) «**profilage**», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

5) «**pseudonymisation**», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

6) «**fichier**», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

7) «**responsable du traitement**», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

8) «**sous-traitant**», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

9) «**destinataire**», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre

ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

10) «**tiers**», une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

11) «**consentement**» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

12) «**violation de données à caractère personnel**», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

13) «**données génétiques**», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

14) «**données biométriques»,** les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

15) «**données concernant la santé**», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

16) «**établissement principal**»,
   a. en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal;
   b. en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement;

17) «**représentant**», une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement;

18) «**entreprise**», une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

19) «**groupe d'entreprises**», une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle;

20) «**règles d'entreprise contraignantes**», les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe;

21) «**autorité de contrôle**», une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51;

22) «**autorité de contrôle concernée**», une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que:

a. le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève;
b. des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être; ou
c. une réclamation a été introduite auprès de cette autorité de contrôle;

23) «**traitement transfrontalier**»,

a. un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou
b. un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres;

24) «**objection pertinente et motivée**», une objection à un projet de décision quant à savoir s'il y a ou non violation du présent règlement ou si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant respecte le présent règlement, qui démontre clairement l'importance des risques que présente le projet de décision pour les libertés et droits fondamentaux des personnes concernées et, le cas échéant, le libre flux des données à caractère personnel au sein de l'Union;

25) «**service de la société de l'information**», un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil;

26) «**organisation internationale**», une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

Mediwet

Annexe 2: NOTIFICATION DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

MEDIWET
AU SERVICE DE VOTRE BIEN-ÊTRE

RGPD

Règlement Général sur la Protection des Données

Qu'est-ce que ça veut dire?

Mediwet a.s.b.l., statutairement établie à Opvoedingstraat 143, 9000 Gand, enregistrée sous le numéro BCE : 0411.031.560, représentée par son administrateur délégué, M. Wim Schmitt, attache beaucoup d'importance à une collecte et à un traitement sûr, transparent et confidentiel des données à caractère personnel.
Mediwet peut collecter et traiter vos données à caractère personnel jusqu'à 30 ans après l'âge normal de la pension pour effectuer les activités dans le cadre de la législation sur le bien-être.

DROIT DE RETRAIT DU CONSENTEMENT

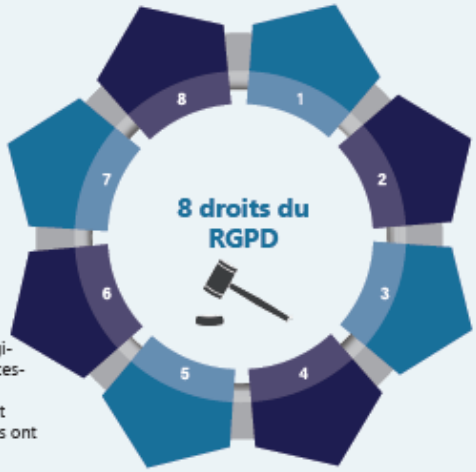
Vous avez le droit de retirer votre consentement préable concernant le traitement des données à caractère personnel.

DROIT D'INFORMATION

Nous communiquons avec vous d'une façon transparente pourquoi vos données à caractère personnel sont conservées et traitées.

PROFILAGE

Nous confirmons que le traitement des données à caractère personnel ne comprend pas de profilage et que vous n'êtes pas soumis à des décisions entièrement automatisées.



DROIT D'ACCÈS ET DE CONSULTATION

Vous avez accès à vos données et vous pouvez gratuitement vérifier à quelles fins elles sont utilisées.

DROIT D'OPPOSITION

Vous avez le droit de vous opposer au traitement de vos données à caractère personnel pour des motifs graves et légitimes, pourvu qu'elles ne soient pas nécessaires pour l'exécution d'une obligation légale et aussi longtemps qu'elles soient nécessaires aux fins pour lesquelles elles ont été collectées.

DROIT DE RECTIFICATION

Vous avez le droit de rectifier des données à caractère personnel qui sont inexacte et incomplètes.

EXACTITUDE

Vous êtes responsable pour toutes les données que vous nous transmettez. Si vos données devraient ne plus être à jour, vous êtes tenu de nous le signaler par retour de courrier.

DROIT À LA PORTABILITÉ

Vous avez le droit de recevoir les données à caractère personnel dans un format structuré et lisible et de les transmettre à un autre responsable du traitement.

DROIT À L'EFFACEMENT OU À LA LIMITATION

Vous pouvez nous demander d'effacer vos données à caractère personnel ou d'en limiter le traitement pourvu qu'elles ne soient pas nécessaires pour l'exécution d'une obligation légale.

Data Protection Officer

Mediwet a désigné un Data Protection Officer qui va surveiller si la collecte et le traitement de vos données à caractère personnel est correct.
Nous garantissons un niveau de protection comparable en opposant à ces travailleurs, collaborateurs et préposés des obligations contractuelles comparables à cette notification.

Si vous avez des questions sur le RGPD, vous pouvez les adresser au DPO de Mediwet.

09 221 06 07
privacy@mediwet.be
DPO Mediwet, Opvoedingstraat 143, 9000 Gand

Droit de consultation

D'un dossier médical
Vous pouvez adresser la demande au Directeur du service de la Surveillance de la santé, Opvoedingstraat 143, 9000 Gand. Le droit de consultation des dossiers médicaux n'est pas directement accordé au travailleur, mais à son médecin traitant.

D'un dossier psychosocial
La demande doit être adressée au conseiller en prévention-aspects psychosociaux concerné.

Certaines données à caractère personnel qui sont collectées par nos soins seront transmises et éventuellement traitées par des prestataires de services tiers, tels que les autorités publiques, des laboratoires, notre fournisseur informatique... Ces données peuvent être transférer à des pays tiers offrant un niveau de protection adéquat. Mediwet a.s.b.l ne peut en aucun cas être tenue responsable de tout préjudice direct ou indirect découlant d'une utilisation fautive ou illicite des données à caractère personnel par un tiers. Si vos droits sont bafoués, vous pouvez déposer une plainte aupres de la Commission de la protection de la vie privée, Rue de la Presse 35, 1000 Bruxelles. Tél. 02 274 48 00

Annexe 3: Aperçu des mesures de sécurité

Mesures de sécurité techniques

- ☐ Système d'exploitation à jour
- ☐ Scan antivirus à jour
- ☐ Pare-feu à jour
- ☐ Mots de passe complexes, régulièrement modifiés
- ☐ Système de journalisation et modifications
- ☐ Identifiant distinct pour logiciel EOM

Mesures de sécurité organisationnelles

- ☐ Politique de confidentialité avec les collaborateurs
- ☐ Toujours verrouiller l'écran du PC quand l'utilisateur quitte temporairement son poste de travail et l'éteindre totalement à la fin de la journée de travail
- ☐ Ne jamais laisser un ordinateur portable sans surveillance dans la voiture
- ☐ Sécurisation des postes de travail
- ☐ Destruction sécurisée des documents anciens
- ☐ Utilisation rigoureuse et limitée des données mobiles
- ☐ Informations Extranet uniquement accessibles par la personne de contact générale et les personnes désignées par elle
- ☐ Attention particulière pour la protection des données à caractère personnel lors de l'évaluation de nos processus et l'élaboration de nouvelles instructions internes.

Annexe 4: Processus de notification de fuites de données et informations à fournir

Une fuite de données est un incident de sécurité, dans le cadre duquel des données à caractère personnel ont potentiellement été perdues ou rendues involontairement accessibles à des tiers. Il s'agit de données associées à ces personnes, telles que, mais sans s'y limiter, les noms, adresses, numéros de téléphone, adresses e-mail, données de connexion, cookies, adresses IP ou données d'identification d'ordinateurs ou de téléphones.

Vous trouverez ci-dessous une série d'exemples d'incidents de sécurité à signaler à l'Autorité de contrôle en matière de données à caractère personnel.

- Le site Internet et ses données de connexion ont été piratés ou rendus accessibles à des tiers.
- Perte involontaire ou vol d'un ordinateur portable, tablette, téléphone (smartphone) ou clé USB contenant des données à caractère personnel.
- Des courriers ou e-mails ont été envoyés à une mauvaise adresse.
- Attaque d'un pirate sur le système TIC.

S'il est constaté en interne qu'un incident de sécurité s'est produit, il est signalé à la direction et au DPO immédiatement après sa constatation.

Les éléments suivants seront signalés :

1. Résumer la fuite de sécurité / l'incident de sécurité / la fuite de données : que s'est-il passé ? Indiquer également le nom du système et/ou du fournisseur concerné.
2. Fournir un relevé des types de données à caractère personnel faisant l'objet de l'incident de sécurité (par exemple nom, adresse, adresse e-mail, adresse IP, numéro de registre national, photo d'identité et toute autre donnée permettant d'identifier une personne).
3. Combien de personnes sont concernées par l'incident de sécurité ?
4. Description du groupe de personnes concernées par les données. S'agit-il de données de collaborateurs, de données d'utilisateurs Internet ? Accorder une attention particulière aux données de groupes vulnérables, comme les enfants.
5. Les coordonnées des personnes concernées sont-elles connues ? Il se peut que les personnes concernées doivent être informées de la fuite de données. Ces personnes doivent alors pouvoir être jointes via le responsable du traitement.
6. Quelle est la cause fondamentale (root cause) de l'incident de sécurité ? Comment l'incident de sécurité a-t-il pu se produire ?
7. À quelle date ou durant quelle période l'incident de sécurité a-t-il pu se produire ?

Il est possible que toutes ces données ne soient pas connues au moment de la constatation de la fuite de données. Ceci ne peut justifier le non-signalement de la fuite de données. Celle-ci doit quoi qu'il en soit être signalée, de préférence en expliquant pourquoi il manque (encore) des réponses à certaines questions.

Après le signalement, la direction décide, en concertation avec le Data Protection Officer, des suites adéquates à donner à la fuite de données, pouvant aboutir au signalement de la fuite de données à l'autorité de protection des données et, le cas échéant, aux personnes concernées.
