Politique relative au respect de la vie privée MENSURA SEPPT

Mensura Service Externe de Prévention et de Protection au Travail ASBL dont le siège social est sis Rue Gaucheret 88/90 1030 Bruxelles, avec le numéro d'entreprise 0410.664.742, inscrite au registre des personnes morales de Bruxelles, valablement représentée par Gretel Schrijvers en sa qualité de directrice générale

Ci-après dénommée « le responsable du traitement»; (conforme le conseil de COPREV, daté 26/01/2018)

Déclare ce qui suit :

Le responsable du traitement reconnaît l'importance du traitement sécurisé des données à caractère personnel de nos clients. À l'aide de cette politique relative au respect de la vie privée, le responsable du traitement désire donner une idée du traitement de vos données à caractère personnel.

Cette politique relative au respect de la vie privée a été établie, tout en respectant le Règlement européen relatif à la protection des données (soit le « RGPD ; Règlement Général sur la Protection des Données ») en date du 27 avril 2016. Cette Règlementation a été convertie en loi-cadre du 30 juillet 2018 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

*De même, la nouvelle directive européenne relative au respect de la vie privée électronique, en tant que lex specialis, a été prise en considération pour le traitement des données à caractère personnel dans le cadre du marketing direct et des cookies. (*lorsque cette Politique relative au respect de la vie privée a été rédigée, il s'agissait encore d'un projet)*

Si le contenu des textes de loi susmentionnés vient à changer, le responsable du traitement adaptera cette Politique relative au respect de la vie privée conformément à ces modifications. Nos clients seront informés en temps utile des modifications essentielles. Les modifications additionnelles ne seront pas informées à nos clients car notre Politique relative au respect de la vie privée peut être consulté à notre website publique.

Point 1. Champ d'application de la Politique relative au respect de la vie privée

Cette Politique relative au respect de la vie privée et ses annexes sont considérées comme des annexes du Contrat principal entre le responsable du traitement et le client. Cette Politique relative au respect de la vie privée est d'application pendant la durée du Contrat principal.

Si des dispositions contraires sur le traitement des données à caractère personnel sont reprises dans le Contrat principal, cette Politique relative au respect de la vie privée primera.

Toute dérogation à cette Politique relative au respect de la vie privée sera uniquement valable si les deux parties ont donné leur accord par écrit.

Point 2. Définitions

Pour l'application de cette politique relative au respect de la vie privée, les notions suivantes auront les significations suivantes conformément au texte du RGPD.

« Personne concernée » : *la personne physique identifiée ou identifiable.*

« Données à propos de la santé » : *les données à caractère personnel ayant un rapport avec la santé physique ou mentale d'une personne physique, parmi lesquelles les données à propos des services de santé dispensés avec lesquels sont fournies des informations à propos de sa santé.*

« Données personnelles sensibles » : *les données à caractère personnel desquelles ressortent la race ou l'origine ethnique, les idées politiques, les convictions religieuses ou philosophiques, ou l'adhésion à un syndicat, et le traitement des données génétiques, des données biométriques dans le but de l'identification unique d'une personne, et des données à propos de la santé, ou des données se rapportant au comportement sexuel ou à l'orientation sexuelle d'une personne.*

« Infraction en rapport avec les données à caractère personnel » : *une infraction au niveau de la protection qui donne lieu, par accident ou de manière illégitime, à la destruction, la perte, la modification ou la fourniture non autorisée de ou l'accès non autorisé à des données envoyées, sauvegardées ou autrement traitées.*

« Données à caractère personnel » : *toutes les informations à propos d'une personne physique identifiée ou identifiable (« la personne concernée ») ; par identifiable, nous considérons une personne physique qui peut être identifiée directement ou indirectement, notamment à l'aide d'un identifiant comme un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à l'aide d'un ou de plusieurs éléments caractéristiques pour l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.*

« Utilisation d'un pseudonyme » : *le traitement de données à caractère personnel d'une manière telle que les données à caractère personnel ne peuvent plus être associées à une personne concernée spécifique sans utiliser des données complémentaires, à condition que ces données complémentaires soient conservées séparément et que des mesures techniques et organisationnelles soient prises pour faire en sorte que les données à caractère personnel ne soient pas associées à une personne physique identifiée ou identifiable.*

« Autorisation de la personne concernée » : *toute volonté libre, spécifique, informée et explicite avec laquelle la personne concernée accepte le traitement des données à caractère personnel à l'aide d'une déclaration ou d'une action active explicite la concernant.*

« Sous-traitant » : *une personne physique ou une personne morale, un organisme public, un service ou un autre organe qui traite des données à caractère personnel pour le responsable du traitement*

« Traitement » : *une opération ou un ensemble d'opérations se rapportant aux données à caractère personnel ou à l'ensemble de données à caractère personnel, exécutées ou non par l'intermédiaire de procédés automatisés, comme la collecte, la détermination, le classement, la structuration, la sauvegarde, le traitement ou la modification, la demande, la consultation, l'utilisation, la fourniture au moyen d'un envoi, la diffusion ou d'une autre manière la mise à disposition, l'alignement ou la combinaison, la protection, l'effacement ou la destruction de données.*

« Responsable du traitement » : *une personne physique ou une personne morale, un organisme public, un service ou un autre organe qui constate, seul ou avec d'autres, l'objet de et les moyens pour le traitement des données à caractère personnel*

Point 3. Le traitement des données à caractère personnel

Le responsable du traitement garantit que vos données à caractère personnel :

a) Sont traitées d'une manière légitime, correcte et transparente
b) Sont collectées à des fins bien déterminées, expressément décrites et justifiées
c) Sont suffisantes, pertinentes et doivent se limiter à ce qui est nécessaire pour les objectifs pour lesquels elles sont traitées
d) Sont exactes et sont actualisées si nécessaire
e) Sont conservées sous une forme qui permet de ne plus identifier la personne concernée sauf lorsque c'est nécessaire pour les objectifs pour lesquels les données à caractère personnel sont traitées
f) En raison de la prise de mesures techniques ou organisationnelles appropriées ; une protection appropriée des données à caractère personnel est garantie, et que les données à caractère personnel sont entre autres protégées contre un traitement non autorisé ou injustifié et contre une perte, une destruction ou une détérioration involontaire

Les données à caractère personnel sont légitimement traitées par le responsable du traitement, étant donné que le traitement repose sur une base légale. L'article 6, 1, C du RGPD indique que les données à caractère personnel sont légitimement traitées si *« Le traitement est nécessaire pour satisfaire à l'obligation légale qui repose sur le responsable du traitement (ici : le client) »*. Dans ce cas, l'obligation légale de prendre les mesures nécessaires dans le cadre de la santé et de la sécurité sur le lieu de travail repose sur le client. Ces obligations légales sont reprises dans le Code relatif au bien-être sur le lieu de travail.

Les données à caractère personnel susmentionnées renvoient entre autres au nom, au prénom, à l'adresse, au téléphone, au sexe, à l'âge… Vous pouvez retrouver un aperçu à l'annexe I de cette politique.

Point 4. Le traitement des données à caractère personnel sensibles

Les données à caractère personnel sensibles (plus explicitement : « Les données à propos de la santé ») sont légitimement traitées par le responsable du traitement sur la base de l'article 9, b) et h) du RGPD ;

- *b) le traitement est nécessaire dans le but d'exécuter les obligations et l'exercice des droits spécifiques du responsable du traitement (ici : le client) ou de la personne concernée dans le domaine du droit du travail et du droit de la sécurité sociale et de la protection sociale, pour autant que cela soit autorisé par le droit de l'Union ou le droit d'un État membre ou dans le cadre d'une convention collective sur la base du droit d'un État membre qui offre des garanties appropriées pour les droits fondamentaux et les intérêts fondamentaux de la personne concernée.*

La prestation de services du responsable du traitement est principalement stipulée par la loi, à savoir dans le Code relatif au bien-être sur le lieu de travail. Le client est obligé – par la loi Belge – de s'affilier chez un service externe de prévention et protection au travail.

- *h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, pour l'évaluation de l'aptitude au travail du travailleur, pour des diagnostics médicaux, la prestation de soins de santé ou de services sociaux ou de traitements ou la gestion des systèmes ou services de soins de santé ou des systèmes et services sociaux, sur la base du droit de l'Union ou du droit d'un État membre, ou en raison d'un contrat avec un prestataire de soins de santé et sous réserve des conditions et garanties stipulées à l'alinéa 3.*

Les données sensibles traitées par le responsable du traitement portent sur les données à propos de la santé ; entre autres le poids, l'IMC, l'aptitude (l'inaptitude) au travail stipulée sur le FES (Formulaire d'évaluation de la santé) ou le FER (Formulaire d'évaluation de la réintégration), les données médicales, les données psychologiques, les lésions après un grave accident du travail, le style de vie de la personne concernée… Vous pouvez retrouver un aperçu à l'annexe I de cette politique.

Point 5. Autorisation explicite de la personne concernée

Dans le cadre des prestations de services en vertu desquelles le responsable du traitement (Mensura) doit directement demander à la Personne concernée les Données à caractère personnel, le responsable du traitement (Mensura) informera la Personne préalablement concernée des éléments suivants aux termes de l'article 13 du RGPD :

- l'identité et les coordonnées de contact du responsable du traitement
- les coordonnées de contact du délégué à la protection des données
- l'objet et la base juridique du traitement
- les destinataires ou les catégories de destinataires des données à caractère personnel

- les modalités d'exercice des droits de la Personne concernée
- du fait que la Personne concernée peut encore retirer son autorisation explicite et les modalités pour ce faire
- du fait que la personne concernée a le droit d'introduire une plainte auprès de l'autorité de surveillance
- le délai de conservation des données à caractère personnel
- le cas échéant, l'existence d'une prise de décision automatisée

Lorsque le responsable du traitement fournit des services dans le cadre des points 3 et 4, le client doit communiquer les informations susmentionnées à la Personne concernée. Cette politique relative au respect de la vie privée peut être la base pour le client d'informer les Personnes concernées.

Point 6. Le traitement des données à caractère personnel à des fins de marketing

Concernant le traitement des données à caractère personnel à des fins de marketing, le responsable du traitement (ici : Mensura) peut s'appuyer sur une base légale (considération 47 du RGPD). On prévoit toujours une possibilité de refus pour la personne concernée (les personnes concernées).

Aucune donnée à caractère personnel d'employés du client n'est traitée par le Responsable du traitement à des fins de marketing. Les données à caractère personnel du client (coordonnées de contact) sont traitées uniquement pour permettre à Mensura de tenir le client informé des modifications apportées aux services obligatoires dans le cadre de la loi bien-être.

Point 7. Les rapports de groupe anonymes

Le responsable du traitement garantit que les rapports de groupe sont effectués de manière anonyme vu que les données à caractère personnel ne sont communiquées qu'à partir d'un ensemble de données de 10.

Les résultats de l'examen médical font par exemple partie de l'analyse de risque. Ces résultats sont communiqués sous la forme de résultats de groupe anonymes.

Point 8. Le registre des activités de traitement

Le responsable du traitement a établi un registre des activités de traitement, dans lequel les éléments suivants sont décrits de manière détaillée par prestation de services du responsable du traitement :

1° Quelles catégories de données à caractère personnel sont traitées ?

2° Qui peut recevoir ces données à caractère personnel (en interne/en externe) ?

3° Pendant combien de temps les données à caractère personnel sont conservées ?

4° De quelle manière les données à caractère personnel sont-elles protégées ?

5° Les données à caractère personnel sont-elles traitées hors de Belgique ?

6° Qui a accès aux données à caractère personnel (en interne/en externe) ?

7° Les fins de traitement

Si vous avez des questions ressortant de ce cadre et qui ne sont pas expliquées dans cette politique, nous vous demandons de contacter les personnes mentionnées au point 20.

Point 9. Les mesures techniques et organisationnelles

Tout en tenant compte de la situation de la technique, des frais d'exécution, ainsi que de la nature, de l'importance, du contexte et des objectifs de traitement et des risques variés concernant la probabilité et la gravité pour les droits et les libertés des personnes, le responsable du traitement prend des mesures techniques et organisationnelles appropriées afin que les données à caractère personnel soient traitées en toute sécurité. Vous pouvez trouver une liste de ces mesures à l'annexe II de cette politique.

Le responsable du traitement garantit conformément à l'article 32 du RGPD prendre les mesures nécessaires, portant entre autres sur :

a) l'utilisation d'un pseudonyme et le cryptage des données à caractère personnel ;
b) la capacité à garantir sur une base permanente la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement et des services ;
c) la capacité de rétablir au moment opportun la disponibilité de et l'accès aux données à caractère personnel dans le cas d'un incident physique ou technique ;
d) une procédure pour tester, estimer et évaluer à intervalles réguliers l'efficacité des mesures techniques et organisationnelles visant à protéger le traitement.

Le responsable du traitement garantit que ses travailleurs, ayant accès aux données à caractère personnel, se limitent à ceux impliqués dans l'exercice de la prestation de services. De même, ces travailleurs sont contractuellement liés à une obligation de confidentialité.

Point 10. Tiers

Les tierces parties pouvant éventuellement avoir accès aux données à caractère personnel se limitent aussi à celles impliquées dans l'exercice de la prestation de services. Un aperçu des tiers peut être demander par nos clients.

Point 11. Sous-traitants

Si le responsable du traitement engage lui-même un sous-traitant pour effectuer des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations relatives à la protection des données sont imposées à ce sous-traitant que celles découlant de ce contrat, notamment, entre autres, l'obligation de prendre des mesures techniques et organisationnelles appropriées concernant le traitement des données à caractère personnel. À

cette fin, les sous-traitants ont signé un contrat de traitement conformément à l'article 28 point 3 RGPD. Un aperçu des sous-traitants peut être demander par nos clients.

Le responsable du traitement garantit que les sous-traitants traitent purement et simplement les données à caractère personnel ressortant de ses instructions écrites. Si les sous-traitants engagent eux-mêmes un sous-traitant ultérieur, les sous-traitants restent en principe responsables vis-à-vis le sous-traitant ultérieur.

Point 12. Traitement des données à caractère personnel en dehors d'un Etat membre de l'UE

Le responsable du traitement garantit que les données à caractère personnel ne sont pas traitées en dehors d'un État membre de l'Union européenne. Les données à caractère personnel sont uniquement traitées en Belgique.

Point 13. Traitement minimal des données à caractère personnel

La prestation de services du responsable du traitement est principalement stipulée par la loi, à savoir dans le Code relatif au bien-être sur le lieu de travail. Le responsable du traitement traitera uniquement les données à caractère personnel qui sont au minimum nécessaires dans le cadre de l'exécution de la prestation de services demandée. Vous pouvez retrouver un aperçu à l'annexe I de cette politique.

Le responsable du traitement garantit que les données à caractère personnel ne sont pas conservées plus longtemps que nécessaire, pour l'exécution de la prestation de services demandée. Le responsable du traitement est lié à des délais de conservation légaux. Vous pouvez retrouver un aperçu à l'annexe I de cette politique.

Point 14. Les droits de la personne concernée :

<u>14.1. Généralités</u>

Dans le cadre du RGPD, les personnes concernées ont les droits suivants vis-à-vis de leurs données à caractère personnel :

1° Droit de consultation

2° Droit de rectification des données à caractère personnel incorrectes

3° Droit de suppression des données (« Droit d'oubli »)

Dans la plupart des cas, le droit à la suppression des données ne sera pas exécuté par le responsable du traitement, étant donné que le traitement est basé sur une obligation de traitement légale.

4° Droit à la limitation du traitement

5° Droit au transfert des données

6° Droit d'objection

Dans la plupart des cas, le droit d'objection ne sera pas exécuté par le responsable du traitement, étant donné que le traitement est basé sur une obligation de traitement légale.

Le responsable du traitement garantit de répondre à la demande dans le mois, suivant la réception de la demande. Ceci, conformément aux obligations du responsable du traitement à l'article 12 point 3 du RGPD. En fonction de la complexité et du nombre de demandes, ce délai peut encore être prolongé de deux mois si nécessaire. Le responsable du traitement informe la personne concernée dans le mois suivant la réception de la demande d'une telle prolongation.

Les procédures internes du responsable du traitement peuvent être trouvées aux points 14.2 et 14.3, de sorte que les personnes concernées du client peuvent correctement exécuter leurs droits auprès du responsable du traitement. Le client doit informer les personnes concernées de ces procédures internes du responsable du traitement, sous une forme succincte, transparente, compréhensible et facilement accessible et dans une langue claire et simple. Si les personnes concernées veulent exercer un droit ne ressortant pas des points 14.2. ou 14.3., la demande peut être envoyée à privacy@mensura.be. Les personnes concernées peuvent exercer leur droit aussi par lettre à l'attention du DPO sur l'adresse suivante : Kempische Steenweg 309 bus 0.01 – 3500 Hasselt.

14.2. Les droits de la personne concernée dans le cadre de la surveillance médicale

En ce qui concerne l'exercice de l'un des droits concernant son dossier médical, la personne concernée doit respecter la procédure interne suivante auprès du responsable du traitement:

- introduire la demande par courrier recommandé ; adressé au Dr. Marie-Noelle Schmickler, directrice du département de la surveillance médicale, Italiëlei 2 à 2000 Anvers.
- + une copie de la carte d'identité

Le droit de regard sur les dossiers médicaux n'est pas immédiatement accordé au travailleur, mais bien à son médecin traitant. Ceci, conformément à l'avis de l'Ordre des Médecins daté du 07-09-96.

14.3. Les droits de la personne concernée dans le cadre des dossiers psychosociaux

En ce qui concerne l'exercice de l'un des droits concernant son dossier psychosocial, la personne concernée doit respecter la procédure interne suivante auprès du responsable du traitement:

- introduire la demande par courrier recommandé ; adressé au conseiller en prévention aspects psychosociaux concerné

+ une copie de la carte d'identité

14.4. Le droit d'introduire une plainte auprès de l'autorité de surveillance belge (= « l'Autorité de protection des données »)

Conformément à l'article 77 du RGPD, la personne concernée a le droit d'introduire directement une plainte auprès l'Autorité de protection des données, si elle estime que ses données à caractère personnel ne sont pas protégées et/ou traitées conformément au RGPD par le responsable du traitement**.**

Point 15. La transmissibilité des données à caractère personnel si le client change de service externe

15.1. Transmission des données à caractère personnel du Département de la surveillance médicale :

La transmission des dossiers de santé est régie par le Code sur le Bien-être au travail, Livre I, Titre 4, Section 4.

Le dossier de santé est composé de quatre parties différentes :

a) les données socio-administratives relatives à l'identification du travailleur et du responsable du traitement

b) l'anamnèse professionnelle et les données à caractère personnel médicales objectives, qui sont déterminées à l'aide des opérations obligatoires réalisées pendant les examens médicaux préventifs. Ces données à caractère personnel ont un rapport avec le poste de travail ou l'activité du travailleur

c) les données spécifiques de nature personnelle déterminées par le médecin du travail lors des examens médicaux préventifs et qui sont réservées à ce médecin

D) les données d'exposition de chaque travailleur employé à un poste de travail ou à une activité dans le cadre de laquelle il est exposé à des agents biologiques, physiques ou chimiques.

Le dossier de santé ne contient pas d'informations à propos de la collaboration à des programmes concernant la santé publique n'ayant pas de rapport avec la profession.

La transmission des données médicales se fait sous la responsabilité du médecin dirigeant le département ou la division chargée de la surveillance médicale (directeur de la surveillance médicale).

Pour la transmission des dossiers médicaux, le directeur de la surveillance médicale du nouveau service externe doit adresser un courrier au directeur de la surveillance médicale de Mensura en demandant la transmission des données. C'est seulement après la réception de la demande que les dossiers demandés sont effectivement transmis.

15.2. Transmission des données à caractère personnel du département psycho

La transmission de ces données à caractère personnel est régie à l'article 34 du Code du bien-être au travail, livre I Titre 3 Prévention des risques psychosociaux au travail.

Si le client change de service externe pour la prévention et la protection au travail, la transmission du dossier individuel est réglée de la manière suivante :

1° Si la demande d'intervention psychosociale formelle est en cours de traitement au moment du changement :

a) le conseiller en prévention pour les aspects psychosociaux informe le plus rapidement possible le demandeur et l'autre personne directement concernée du fait que le service externe pour lequel il remplit ses missions ne sera plus compétent pour le traitement de la demande ;

b) le client communique au conseiller en prévention pour les aspects psychosociaux auprès duquel la demande a été introduite, à la demande de celui-ci, les coordonnées du nouveau service externe ;

c) le conseiller en prévention pour les aspects psychosociaux auprès duquel la demande a été introduite remet le dossier individuel au conseiller en prévention pour les aspects psychosociaux du nouveau service externe ;

d) le conseiller en prévention pour les aspects psychosociaux du nouveau service externe informe le demandeur et les autres personnes directement concernées du fait qu'il reprend le traitement de la demande.

2° Si le traitement de la demande d'intervention psychosociale formelle est clôturé au moment du changement de service externe pour la prévention et la protection au travail, le conseiller en prévention pour les aspects psychosociaux du nouveau service externe peut obtenir une copie du dossier individuel du conseiller en prévention pour les aspects psychosociaux auprès duquel la demande avait été introduite, si cela s'avère nécessaire pour l'exécution de ses missions.

La transmission du dossier individuel se fait en fonction des conditions qui garantissent le secret professionnel.

Point 16. Effacer les Données à caractère personnel à la fin du Contrat principal

Le responsable du traitement garantit que dans le mois à compter de la fin du Contrat principal, les données à caractère personnel traitées sont effacées ou cédées sur demande du client, à moins qu'une disposition légale autorise le responsable du traitement à conserver les données à caractère personnel pour une plus longue période.

Sur demande du client, le responsable du traitement en fournit les preuves nécessaires.

En outre, les sous-traitants et les tiers sont informés par le responsable du traitement de l'effacement des données à caractère personnel recueillies si le Contrat principal est terminé. Et ce, à moins qu'ils ne puissent se prévaloir d'une disposition légale permettant de conserver plus longtemps les données à caractère personnel.

Point 17. Demande de données à caractère personnel par des services publics

Le responsable du traitement informe le client dans les 3 jours ouvrables s'il :

(a) reçoit une demande d'informations, une citation ou une demande d'enquête ou de contrôle de la part d'une autorité publique en rapport avec le traitement des données à caractère personnel, sauf lorsque le responsable du traitement n'est pas légalement autorisé à effectuer une telle transmission

(b) a l'intention de fournir des données à caractère personnel à une autorité publique

(c) reçoit d'un tiers ou d'un travailleur, d'un client ou d'un fournisseur du client une demande de publication des données à caractère personnel du client ou d'informations se rapportant au traitement des données à caractère personnel du client

Le responsable du traitement donne au client 72 heures, à compter de la notification, pour faire part de ses réserves s'agissant de cette transmission des données à caractère personnel.

Point 18. Mesures si une infraction survient en rapport avec les données à caractère personnel

Le responsable du traitement a l'obligation de communiquer, dans les 72 heures, à l'autorité de surveillance belge les infractions relatives à la protection des données à caractère personnel. Ceci, sauf s'il n'est pas probable que l'infraction en rapport avec les données à caractère personnel implique un risque pour les droits et les libertés de la personne concernée (des personnes concernées).

Le responsable du traitement informe le client sans retard déraisonnable dès qu'il a pris connaissance d'une infraction en rapport avec les données à caractère personnel. Il est convenu que le responsable du traitement et le client se contactent dans les 48 heures suivant la prise de connaissance de l'infraction par le responsable du traitement et décident de manière conjointe si l'infraction est transmise à l'autorité de surveillance belge compétente.

Si l'infraction en rapport avec les données à caractère personnel implique probablement un risque élevé pour les droits et les libertés de personnes physiques, la personne concernée (les personnes concernées) doit être informée immédiatement de l'infraction en rapport avec les données à caractère personnel conformément à l'article 34 du RGPD.

Aussi bien le responsable du traitement que le client collaborent avec l'autorité de surveillance belge compétente pour fournir les informations nécessaires et pour limiter les conséquences de l'infraction.

Point 19. Autres dispositions

En cas de nullité de l'une ou de plusieurs des dispositions de la présente Politique relative au respect de la vie privée, les autres dispositions demeurent pleinement en vigueur.

Le droit belge s'applique à cette Politique relative au respect de la vie privée. Les parties soumettront exclusivement leurs litiges afférents à cette Politique relative au respect de la vie privée aux tribunaux de Bruxelles.

Point 20. Besoin de plus amples informations ou d'une assistance ?

Le responsable du traitement garantit de proposer au client l'assistance et les informations nécessaires et complémentaires de sorte que le responsable du traitement puisse prouver le respect de ses obligations, en vertu du RGPD. Cette obligation d'information ne s'étend pas aux informations confidentielles ou qui pour des raisons légales ne peuvent pas être communiquées au client.

De même, le responsable du traitement fournira la collaboration nécessaire si un audit est réalisé auprès du responsable du traitement pour le compte du client, ou d'un contrôleur habilité par le client. Le client supporte les coûts du contrôleur désigné et de l'audit réalisé. L'audit se limitera toujours aux systèmes du responsable du traitement utilisés pour les traitements.

Le fonctionnaire pour la protection des données (ou le Data Protection Officer) et le Security Officer du responsable du traitement peuvent être contacté à l'adresse électronique suivante : privacy@mensura.be.

Annexe I : Les catégories des données à caractère personnel traitées et la durée de conservation

Les catégories des données à caractère personnel que le responsable du traitement peut traiter

- Données d'identification personnelles (par exemple : prénom, nom, adresse, numéro de téléphone, adresse électronique, type de permis de conduire, le cas échéant)
- Caractéristiques personnelles (par exemple : âge, sexe, date de naissance, lieu de naissance, état civil, nationalité)
- Données relatives à la santé (par exemple : santé physique et psychique)
- Profession et poste (par exemple : employeur, titre et description de la fonction, date d'engagement)
- Numéro de registre national
- Données raciales ou ethniques
- Photos
- Autre catégorie de données (par exemple : numéro de livre de marin, le cas échéant)

La durée de la conservation

Dossier médical = délais de conservation légaux (= 40 ans).

Dossiers psychosociaux = délai de conservation légal (= 20 ans).

Annexe II. Les mesures techniques et organisationnelles pour la protection

- La politique informatique interne approuvée par la direction (elle comprend la politique des mots de passe, l'utilisation acceptable des moyens de production, les politiques Clean Desk et Clear Screen, la politique des logiciels, la politique de l'Internet, la politique des courriers électroniques, la politique relative aux médias sociaux, la politique de confidentialité des données…)
- Les données sont uniquement stockées en Belgique.
- Nos systèmes sont redondants sur 2 centres de données avec une classification TIER III+. (DRP et BCP)
- L'hébergeur est certifié ISO27001.
- Des pare-feux sur plusieurs couches du réseau.
- Le Network Access Control, la séparation des réseaux, etc.
- Les données en transit sont uniquement autorisées de manière cryptée.
- L'accès à distance des utilisateurs uniquement par l'intermédiaire du VPN avec une authentification Multi Factor.
- Une sauvegarde vérifiée et des procédures de restauration.
- Les Data in rest (sauvegardes) seront cryptées
- « Role based access » en direction des applications
- Des formations User Awareness sont organisées.
- Antivirus/Antispam sur plusieurs couches. (Pare-feu, Endpoints, serveurs, systèmes de courrier électronique…)
- SIEM pour les security devices.
- Journaux et rapports.
- Tests réguliers de la sécurité.
- Gestion Mobile Device
- Capacity Management
- Mises à jour régulières de tous les systèmes et rapports à propos de celles-ci.
- Réunions de sécurité régulières avec notre hébergeur.
- Protection d'accès physique.
- Asset Management
- Contrôle du réseau et du système.
- Mesures DDOS et IPS.
- Implémentation Data Loss Prevention dans un avenir proche.
- Gestion du changement (Change Management)
- Environnements séparés pour le test, la validation et la production.
    - Évaluation régulière des fournisseurs