Politique relative au respect de la vie privée Certimed

Certimed, ASBL, ayant son siège social à Kempische Steenweg 309 bus 3.01, 3500 Hasselt, avec le numéro d'entreprise 0409.671.085, valablement représentée par Bart Teuwen en sa qualité de directeur général ;

Ci-après dénommée « le responsable du traitement » ;

Déclare ce qui suit :

Certimed asbl reconnaît l'importance du traitement sécurisé des Données à caractère personnel. À l'aide de la présente politique relative au respect de la vie privée, Certimed asbl souhaite vous informer au sujet du traitement de vos données à caractère personnel.
La présente Politique relative au respect de la vie privée a été établie dans le respect du 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.

Dans le cadre du RGPD, Certimed adopte la qualification de responsable du traitement du fait que les droits des Personnes concernées doivent être directement exercés auprès de Certimed asbl. Les Personnes concernées ne peuvent invoquer leurs droits relatifs au RGPD auprès de nos clients parce que ces clients ne peuvent avoir accès au dossier médical complet des Personnes concernées.

*De même, la directive européenne « vie privée et communications électroniques », 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. (*au moment où la présente Politique relative à la vie privée a été rédigée, la directive européenne « vie privée et communications électroniques » était encore à l'état de projet)*

Si le contenu des textes de loi susmentionnés vient à changer, Certimed asbl adaptera la présente Politique relative au respect de la vie privée conformément à ces modifications. Nos clients seront informés des modifications essentielles. Toute modification additionnelle ne sera pas communiquée au client. Notre Politique est librement consultable sur notre site web.

Point 1. Champ d'application de la Politique relative à la vie privée
La présente 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. La présente Politique relative au respect de la vie privée est d'application pendant la durée du Contrat principal.

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

Toute dérogation à la présente 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 la présente 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.*

« Tiers » : *une personne physique ou morale, une autorité publique, un service ou tout autre organisme à l'exception de la personne concernée, le responsable du traitement, le sous-traitant, les personnes qui sont autorisées à traiter les données à caractère personnel sous l'autorité directe du responsable du traitement ou du sous-traitant*

« 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 à caractère personnel 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*

« Sous-traitant ultérieur » : *le sous-traitant qui, sous l'autorité directe du sous-traitant, est autorisé à traiter les données à caractère personnel*

« 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 » : *toute personne physique, personne morale, autorité publique, ou tout service ou organisme qui traite des Données à caractère personnel pour le compte du 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 morale, l'autorité publique, le service ou tout autre organisme qui, seul ou avec d'autres, détermine à la fois l'objectif et les moyens du 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

Pour l'exécution des contrôles médicaux et la rédaction des rapports relatifs à l'absentéisme, l'on peut se baser sur les articles 6, 1, B et F du RGPD :

- Art. 6, 1, B) RGPD : *« le traitement est nécessaire à l'exécution d'un contrat auquel la Personne concernée est partie »*

- Art. 6, 1, F) RGPD : « *Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant* »

La fin légitime du client à l'art. 6, 1, F) RGPD est notamment l'intérêt de lutter préventivement contre l'absentéisme au sein de l'organisation.

Les Données à caractère personnel ci-dessous concernent notamment le nom, le(s) prénom(s), l'adresse, le code postal, la localité, l'adresse e-mail, la date de naissance, le sexe, l'état civil, des informations professionnelles (= identité d'un employeur, lieu de travail, titre éventuel de la fonction, date d'engagement, date de départ), etc. Un aperçu est disponible à l'annexe I de la présente 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 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.*

Le client a le droit de faire appel au responsable du traitement, en qualité de service de contrôle médical, dans le cadre de l'article 31 de la loi relative aux contrats de 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.*

Le client peut faire appel au responsable du traitement pour obtenir des analyses et des rapports relatifs à l'absentéisme dans son organisation. Ces services s'inscrivent dans le volet préventif de la médecine.

Les données sensibles traitées par le responsable du traitement portent sur les Données à propos de la santé ; entre autres des données physiques et psychiques, la durée de l'incapacité de travail, la nature de l'incapacité de travail, les données du médecin traitant, l'autorisation/interdiction de quitter le domicile, l'hospitalisation du travailleur, le premier

certificat/certificat de prolongation, etc. Un aperçu est disponible à l'annexe I de la présente Politique.

Point 5. Traitement des données à caractère personnel et des données à caractère personnel sensibles pour des fins de recherche scientifique ou à des fins statistiques

Le responsable de traitement traite les données à caractère personnel et les données à caractère personnel sensibles pour des fins de recherche scientifique ou à des fins statistiques. Ceci conforme l'article 89 du RGDP.

La durée de la conservation pour ces fins n'est pas plus longue, que la durée de la conservation pour les autres fins. En annexe 1 vous pouvez trouver plus d'informations concernant la durée de la conservation.

Point 6. Autorisation explicite de la personne concernée

Dans le cadre des prestations de services en vertu desquelles le responsable du traitement doit directement demander à la Personne concernée les Données à caractère personnel, le responsable du traitement informera préalablement la Personne concernée des éléments suivants aux termes de l'article 13 point 1 du RGPD :

- l'identité et les coordonnées de Certimed
- 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.

Point 7. 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 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 Certimed de tenir le client informé des modifications apportées aux services.

Point 8. 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 20.

Point 9. Le registre des opérations de traitement

Le responsable du traitement a établi un registre des opérations 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-elles 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-elles 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 objectifs de traitement

Si vous avez des questions ressortant de ce cadre et qui ne sont pas expliquées dans la présente politique, nous vous demandons de contacter les personnes mentionnées au point 21.

Point 10. 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 la présente 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 11. 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. Le client peut demander un aperçu des tiers au responsable du traitement.

Point 12. Sous-traitants
Si le responsable du traitement engage lui-même un sous-traitant pour effectuer des activités de traitement spécifiques pour le compte du client, les mêmes obligations relatives à la protection des données sont imposées à ce sous-traitant que celles découlant du présent 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 du RGPD. Le client peut demander un aperçu des sous-traitants au responsable.

Le responsable du traitement garantit que les sous-traitants désignés traitent uniquement les Données à caractère personnel sur la base des directives définies par le responsable du traitement. Lorsque le sous-traitant engagé désigne un sous-traitant ultérieur, le sous-traitant restera en principe responsable vis-à-vis de ce sous-traitant ultérieur.

Point 13. Traitement des données à caractère personnel en dehors d'un État membre de l'Union européenne
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 14. Traitement minimal des données à caractère personnel
Les services du responsable du traitement sont essentiellement fixés par la loi (article 31 de la loi relative aux contrats 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 la présente 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 la présente Politique.

Point 15. Les droits de la personne concernée :
15.1. Généralités
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 repose 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'opposition ne sera pas exécuté par le responsable du traitement, étant donné que le traitement repose sur une obligation de traitement légale.

Les droits susmentionnés seront exécutés dans le cadre de dossiers médicaux où le client ne peut pas et ne sait pas donner de suite juridique. C'est la raison pour laquelle les droits/demandes susmentionnés doivent immédiatement être introduits auprès du responsable du traitement. Le responsable du traitement garantit de répondre à la demande dans le mois suivant la réception de la demande. Ceci, conformément aux obligations à l'article 12 point 3 du RGPD. En fonction de la complexité et du nombre de demandes, ce délai peut 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.

La procédure interne du responsable du traitement peut être trouvée au point 15.2., de sorte que les personnes concernées du client peuvent correctement exécuter leurs droits relatifs au dossier médical individuel auprès du responsable du traitement. Le client doit informer les Personnes concernées de cette procédure interne du responsable du traitement, sous une forme succincte, transparente, compréhensible et facilement accessible et dans une langue claire et simple. Si la Personne concernée veut exercer un droit qui ne relève pas du point 15.2., la demande peut être adressée à privacy@certimed.be ou par lettre à l'attention du DPO (Kempische Steenweg 309 bus 3.01, 3500 Hasselt).

15.2. Droits (= droit de l'accès et droit de copie) relatifs au dossier médical individuel
En ce qui concerne l'exercice du droit de l'accès ou de droit de copie concernant son dossier médical, la personne concernée doit respecter la procédure interne suivante auprès du responsable du traitement :

- adresser la demande par courrier recommandé à Certimed asbl, (daté et signé) à l'attention du médecin principal, Kempische Steenweg 309 bus 3.01 à 3500 Hasselt
- + ajouter une copie de sa carte d'identité

15.3. Déposer plainte auprès de l'autorité belge de surveillance de la vie privée (= « 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 de 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.

Point 16. La transmissibilité des données à caractère personnel si le client change de service de contrôle médical
Le responsable du traitement et le client conviendront de commun accord comment les Données à caractère personnel seront transmises.

Point 17. 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 à la demande du client, à moins qu'une disposition légale n'autorise le responsable du traitement à conserver les Données à caractère personnel pour une plus longue période (voir annexe I).

À la 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 18. 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 19. Mesures si une infraction survient en rapport avec les données à caractère personnel
Les responsables du traitement ont l'obligation de communiquer, dans les 72 heures, à l'autorité de surveillance belge compétente les infractions relatives à la protection des Données à caractère personnel, 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) sera 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 20. 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 la présente Politique relative au respect de la vie privée. Les parties soumettront exclusivement leurs litiges afférents à la présente Politique relative au respect de la vie privée aux tribunaux de Bruxelles.

Point 21. 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 Délégué à la protection des données (ou Data Protection Officer) et le Security Officer du responsable du traitement peuvent être contacté à l'adresse électronique suivante : Privacy@certimed.be.

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

Les catégories de Données à caractère personnel que le responsable du traitement peut traiter

Nom, prénom(s), adresse, code postal, localité, adresse e-mail, date de naissance, sexe, état civil, données relatives à la santé (données physiques et psychiques), adresse de résidence, langue, nom conjoint, informations professionnelles (= identité de l'employeur, lieu de travail, éventuel titre de la fonction, date d'engagement, date de départ, statut, niveau de fonction, barème, réseau, direction, code population, code de nomination, échelle, compétence, colonne, rang, subdivision, service provincial, code medex, méthode de gestion des maladies, référence organigramme, gestionnaire, catégorie ONSS), blocage du contrôle, durée de l'incapacité de travail, nature de l'incapacité de travail, coordonnées du médecin traitant, autorisation/interdiction de quitter le domicile, hospitalisation du travailleur, premier certificat/certificat de prolongation et date d'oblitération.

La durée de la conservation

Conformément à l'article 15 de la loi relative aux contrats de travail, les données à caractère personnel sont conservées : *« jusqu'à 5 ans après le fait qui a donné naissance à l'action »*. Ce délai de conservation est appliqué en ce qui concerne les rapports de groupe et les analyses et pour les contrôles médicaux.

Un même délai de conservation est d'application pour la finalité de traiter des données à caractère personnel pour des fins de recherche scientifique ou à des fins statistiques.

Annexe II. Les mesures techniques et organisationnelles pour la protection

- Les flux de communication sont examinés
- Le Registre des données a été créé.
- Les utilisateurs sont informés à propos du RGPD.
- La politique en matière de délais de conservation est réexaminée.
- Une nouvelle déclaration relative à la vie privée a été rédigée.
- Un DPO est désigné.
- Une analyse de l'impact de la protection des données est effectuée.
- La conclusion de contrats de traitement avec des fournisseurs/sous-traitants dans le cadre du RGPD.
- le responsable du traitement élabore une nouvelle procédure de réponse aux incidents afin de gérer correctement les infractions à la sécurité des informations.
- Politique IT 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, etc.).
- Les données sont uniquement stockées en Belgique.
- Les systèmes sont redondants dans 2 centres de données avec une classification TIER III+ (DRP et BCP).
- L'hébergeur est certifié ISO27001.
- Des pare-feu sur plusieurs couches du réseau.
- Network Access Control, séparation des réseaux, etc.
- Les données en transit sont uniquement autorisées de manière cryptée.
- Une sauvegarde vérifiée et des procédures de restauration.
- Les Data in rest (sauvegardes) seront cryptées dans un avenir proche.
- « 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
- Gestion de la capacité.
- 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.