

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Contexte et définitions

La General Data Protection Regulation, « GDPR » (ou « RGPD », Règlement Général sur la Protection des Données) établit un certain nombre de règles concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Dans le cadre de la GDPR, on entend par données à caractère personnel, toute donnée ou information se rapportant à une personne physique identifiée ou identifiable.

Un traitement est 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 de données.

Le responsable du traitement est une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.

Le sous-traitant est une personne physique ou morale, une autorité publique, un service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, les mesures techniques et organisationnelles appropriées, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du Règlement Général sur la Protection des Données et de protéger les droits des personnes concernées.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient communiquées.

Objectifs du traitement

Cohezio asbl est un service externe agréé de prévention et de protection au travail. Les tâches et les missions des services externes sont définies au Livre II, titre 3 du code du bien-être au travail.

Dans le cadre de ses obligations découlant du code du bien-être au travail, l'employeur peut faire appel à un service externe de prévention et de protection au travail, **Cohezio asbl**. À cet effet, l'employeur conclut un contrat écrit avec **Cohezio** dans lequel sont fixées la nature, la portée et la durée minimale des prestations.



En tant que service externe de prévention et de protection au travail, **Cohezio** est chargé du traitement de données dans le cadre de ses missions légales relatives à la prévention et au bien-être des travailleurs au travail et est responsable du traitement des données à caractère personnel. En tant que responsable du traitement, **Cohezio** collecte et traite également les données confiées par les employeurs affiliés pour l'accomplissement de ses missions.

Traitement des données à caractère personnel

Toutes les données à caractère personnel devront être :

- traitées de manière licite, loyale et transparente ;
- collectées pour des finalités déterminées, explicites et légitimes ;
- adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- exactes et tenues à jour ;
- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- traitées de façon à garantir une sécurité appropriée des données à caractère personnel à l'aide de mesures techniques ou organisationnelles appropriées.

Le traitement des données à caractère personnel se déroule dans le cadre des dispositions légales relatives au bien-être au travail du travailleur, telles que prévues dans la loi du 4 août 1996 sur le bien-être au travail et le livre I^{er} à 10 du code du bien-être au travail.

Traitement des données à caractère personnel sensibles et particulières

Le traitement des données à caractère personnel particulières, comme les données concernant la santé (physique et mentale) d'une personne, s'effectue conformément à l'article 9, 2. du Règlement Général sur la Protection des Données.

Le traitement s'effectue dans le cadre :

- de l'enregistrement de données à caractère personnel et de données médicales dans le dossier médical : mention de l'aptitude ou de l'inaptitude à exercer une fonction et recommandations, mention des tests et examens complémentaires et de toute autre donnée médicale utile au médecin du travail (livre I^{er}, titre 4 – Mesures relatives à la surveillance de la santé des travailleurs, du code du bien-être au travail).
- enregistrement de données à caractère personnel dans le cadre de dossiers psychosociaux (loi sur le bien-être du 4 août 1996 et livre I^{er}, titre 3 – Prévention des risques psychosociaux au travail, du code du bien-être au travail).
- enregistrement de données à caractère personnel dans le cadre d'autres domaines du bien-être (missions légales du conseiller en prévention livre I^{er} à X du code du bien-être au travail).



Service Externe de Prévention et de Protection au Travail

Cohezio asbl • Siège social : Boulevard Bischoffsheim 1-8, 1000 Bruxelles

T. +32 (0)2 533 74 11 • F. +32 (0)2 538 79 32 • info@Cohezio.be • www.Cohezio.be

RPM Bruxelles • IBAN BE54 8777 94 38 02 97 • BIC BNAG BE BB • 0410.623.764

Quelles sont les données traitées ?

Toutes les données à caractère personnel sont traitées dans le cadre des missions légales de **Cohezio** ou des missions lui ayant été confiées.

Cohezio établit un dossier de santé du travailleur pour lequel une surveillance médicale a été organisée dans le cadre du livre I^{er}, titre 4 (mesures relatives à la surveillance de la santé des travailleurs) du code du bien-être au travail. Le dossier de santé constitue la mémoire des informations pertinentes concernant le travailleur, qui permet au conseiller en prévention-médecin du travail d'exercer la surveillance de la santé, et de mesurer l'efficacité des mesures de prévention et de protection appliquées dans l'entreprise. Le traitement de ces données s'effectue conformément aux dispositions du Règlement Général sur la Protection des Données.

Le traitement porte sur les données à caractère personnel suivantes :

Données d'identification personnelle : nom, adresse, numéro de téléphone, numéro de registre national.

Données relatives aux caractéristiques personnelles : âge, sexe, date et lieu de naissance, état civil, nationalité.

Données relatives à la profession et à l'emploi : description de la fonction, date de recrutement, lieu de travail, modalités et conditions de travail.

Données médicales (médecine du travail – dossier de santé) : l'anamnèse professionnelle, les données particulières relevées par le conseiller en prévention-médecin du travail à l'occasion d'exams médicaux de prévention, les données d'exposition, la demande de surveillance de santé du travailleur, la date et le type d'examen médical préventif et les résultats, les résultats des examens dirigés ou des tests fonctionnels dirigés, les résultats de la surveillance biologique, les radiographies et les protocoles d'exams radiologiques, tous autres documents ou données relatifs aux examens dirigés subis par le travailleur et réalisés par des médecins ou des services extérieurs, le formulaire d'évaluation de santé, la date et la nature des vaccinations, les résultats des tests tuberculiniques, les fiches de vaccination, tous autres documents médicaux ou médico-sociaux, la déclaration de maladie professionnelle, une copie de la fiche d'accident du travail, le plan de réintégration et les rapports dans le cadre de la réintégration.

Le dossier individuel risques psychosociaux : le document qui atteste de l'entretien personnel informatif, le type d'intervention, les déclarations des personnes concernées, les avis.

Transmission des données à caractère personnel

Les données à caractère personnel ne peuvent être communiquées par **Cohezio** à des tiers, sauf dans le cadre de l'application de dispositions légales ou réglementaires (les fonctionnaires chargés de surveiller le respect du bien-être au travail) ou lorsque la communication est nécessaire à l'exécution de ses missions légales en tant que service externe de prévention et de protection au travail.

Les données médicales et les données relatives à un dossier individuel d'intervention psychosociale ou toute autre donnée à caractère personnel sensible ne peuvent être communiquées que moyennant le respect des dispositions générales relatives au secret professionnel.

Les données pourront être communiquées à la personne enregistrée.



Service Externe de Prévention et de Protection au Travail

Cohezio asbl • Siège social : Boulevard Bischoffsheim 1-8, 1000 Bruxelles

T. +32 (0)2 533 74 11 • F. +32 (0)2 538 79 32 • info@Cohezio.be • www.Cohezio.be

RPM Bruxelles • IBAN BE54 8777 94 38 02 97 • BIC BNAG BE BB • 0410.623.764

Délais de conservation des données

Les données à caractère personnel ne sont pas conservées au-delà du délai prévu par la législation.

Le dossier médical est conservé pendant quinze ans au moins à dater du départ du travailleur.
Le dossier individuel d'intervention psychosociale est conservé par le conseiller en prévention pour les aspects psychosociaux pendant vingt ans à partir de la date d'introduction de la demande d'intervention psychosociale.

Sécurisation

Les données à caractère personnel devront être traitées de manière à garantir une sécurisation et une confidentialité adéquates de ces données et à empêcher la possibilité d'accès non autorisé ou d'utilisation non autorisée des données à caractère personnel. À cette fin, le sous-traitant prend les mesures techniques et organisationnelles appropriées, telles que définies plus en détail ci-dessous.

Cohezio protégera plus particulièrement les données à caractère personnel contre l'accès non autorisé ou l'utilisation non autorisée des données transmises, stockées ou traitées, la modification, la perte ou la destruction de données, qu'elles soient accidentelles ou illégales.

Confidentialité des données

Toutes les données à caractère personnel communiquées à **Cohezio** devront être traitées de manière strictement confidentielle.

Toutes les parties s'engagent à préserver la confidentialité de toutes les données à caractère personnel et à ne pas les diffuser en interne ou en externe de quelque manière que ce soit, à moins que cela ne soit nécessaire pour se conformer à une obligation légale.

Traitement des données à caractère personnel en dehors d'un État membre de l'Union européenne

Les données à caractère personnel ne seront traitées qu'en Belgique et ne seront en aucun cas traitées en dehors d'un État membre de l'Union européenne.

Mesures de sécurité et de protection

Cohezio prendra les mesures techniques et organisationnelles appropriées pour garantir la confidentialité dans le traitement des données à caractère personnel et empêcher l'accès non autorisé ou l'utilisation non autorisée des données à caractère personnel.

1. Politique de sécurité de l'information

Cohezio dispose d'une politique de sécurité de l'information approuvée par la personne responsable de la gestion quotidienne. La politique impose un certain nombre de directives générales en matière de sécurité de l'information, telles que le respect des mesures de sécurité, la réalisation d'audits de conformité, la mise en œuvre de mesures, etc.

Les lignes directrices de cette politique sont communiquées à tous les membres du personnel de **Cohezio** et sont également respectées par tous les membres du personnel de **Cohezio**.



Service Externe de Prévention et de Protection au Travail

Cohezio asbl • Siège social : Boulevard Bischoffsheim 1-8, 1000 Bruxelles

T. +32 (0)2 533 74 11 • F. +32 (0)2 538 79 32 • info@Cohezio.be • www.Cohezio.be

RPM Bruxelles • IBAN BE54 8777 94 38 02 97 • BIC BNAG BE BB • 0410.623.764

2. Évaluation des risques

Cohezio effectue, communique et entretient une évaluation des risques en matière de sécurité de l'information et de protection de la vie privée pour chaque processus et projet. Cette évaluation des risques tient compte des mesures et des garanties mises en place pour protéger les données à caractère personnel, limiter les risques et démontrer le respect des conditions du GDPR.

3. Organisation interne de la sécurité de l'information

Cohezio dispose d'une politique de sécurité de l'information dans laquelle sont définies toutes les responsabilités du collaborateur et de l'organisation en matière de sécurité de l'information et de respect de la vie privée. Tous les collaborateurs, les collaborateurs en sous-traitance ou les utilisateurs externes de **Cohezio** doivent, si besoin, signer la politique. Le sous-traitant veille à ce que les collaborateurs (internes et externes) reçoivent les informations nécessaires et une formation appropriée en matière de sécurité de l'information, dans la mesure où cela est nécessaire à l'exercice de leur fonction.

4. Gestion des accès

Cohezio a désigné un gestionnaire d'accès responsable de la gestion des droits d'accès aux systèmes informatiques. Le gestionnaire détermine les droits d'accès individuels de l'utilisateur sur la base d'une procédure validée par la direction. L'accès est limité aux applications nécessaires à l'exécution des tâches de l'utilisateur.

5. Gestion des fichiers d'historique

Le traitement des données à caractère personnel est enregistré dans des fichiers d'historique. Ceux-ci permettent à **Cohezio** de vérifier à tout moment qui a modifié, complété ou supprimé des données. Les fichiers d'historique font l'objet d'un contrôle périodique de l'utilisation ou de l'accès illicite aux données à caractère personnel.

6. Environnement physique sûr

Cohezio prend les mesures nécessaires pour limiter l'accès aux bâtiments et aux locaux où se trouvent des informations sensibles ou critiques aux personnes autorisées. **Cohezio** fixe également des modalités de réalisation des contrôles d'accès.

Cohezio prend des mesures pour éviter la perte, l'endommagement ou le vol des moyens d'exploitation.

7. Sécurisation des transferts de données

Le stockage, le traitement et l'envoi de données à caractère personnel, vers l'externe ou via l'Internet, sont toujours cryptés. La cryptographie est utilisée pour transférer des données qui ne peuvent pas être lisibles par d'autres parties. Seuls l'expéditeur et le destinataire disposent de la clé nécessaire pour rétablir les données dans leur forme originale. Ces données supplémentaires seront conservées séparément par **Cohezio** qui prendra à cette fin les mesures techniques et organisationnelles nécessaires.

8. Gestion de la continuité



Service Externe de Prévention et de Protection au Travail

Cohezio asbl • Siège social : Boulevard Bischoffsheim 1-8, 1000 Bruxelles

T. +32 (0)2 533 74 11 • F. +32 (0)2 538 79 32 • info@Cohezio.be • www.Cohezio.be

RPM Bruxelles • IBAN BE54 8777 94 38 02 97 • BIC BNAG BE BB • 0410.623.764

Les incidents physiques ou techniques tels que les pannes de matériel peuvent empêcher la disponibilité ou l'accès aux données à caractère personnel ou peuvent entraîner la perte de données à caractère personnel. **Cohezio** veille à ce que les mesures nécessaires soient prises pour que l'organisation puisse réagir de manière appropriée en cas d'incidents graves ou de catastrophes et récupérer les données à temps.

9. Gestion des incidents

Cohezio veille à l'établissement des procédures nécessaires à l'enregistrement et à la gestion des incidents de sécurité de l'information. Ces procédures sont connues de tous les collaborateurs de **Cohezio**.

Chaque collaborateur est tenu de signaler tout accès, utilisation, divulgation, perte ou destruction non autorisés d'informations personnelles. Les incidents doivent être signalés au conseiller en sécurité ou au délégué à la protection des données. Toutes les preuves relatives à l'incident seront collectées et stockées correctement.

Tout incident de sécurité de l'information sera évalué afin que les procédures puissent être adaptées et améliorées.

10. Fuites de données

Toutes les fuites de données, c'est-à-dire toute violation de la sécurité entraînant accidentellement ou illégalement la destruction, la perte, la modification, la divulgation non autorisée ou l'accès non autorisé aux données transmises, stockées ou traitées, devront être signalées à l'Autorité de protection des données dans les 72 heures suivant la découverte de la fuite de données.

Cohezio a mis au point les procédures nécessaires lui permettant de détecter toutes les fuites de données le plus tôt possible. **Cohezio** tient également un registre de tous les faits relatifs aux fuites de données, à leurs conséquences et à toute mesure corrective prise.

Droits des personnes dont les données à caractère personnel sont traitées

1. Droit d'accès et de correction

La personne concernée a le droit, à tout moment et gratuitement, de prendre connaissance de toutes ses données à caractère personnel et de les corriger.

La personne concernée peut corriger ou compléter ses données moyennant l'envoi d'un courrier avec une copie de sa carte d'identité, à l'attention de la directrice générale de **Cohezio**, Mme Evelyne Kerger, Boulevard Bischoffsheim 1-8, 1000 Bruxelles.

2. Droit à l'effacement des données (droit à l'oubli)

Les données à caractère personnel nécessaires à l'exécution des missions légales de **Cohezio** ne peuvent pas être supprimées.

Les dossiers médicaux ne peuvent être supprimés, sauf si la suppression est conforme aux dispositions légales du code du bien-être au travail.

3. Droit à la limitation du traitement



Service Externe de Prévention et de Protection au Travail

Cohezio asbl • Siège social : Boulevard Bischoffsheim 1-8, 1000 Bruxelles

T. +32 (0)2 533 74 11 • F. +32 (0)2 538 79 32 • info@Cohezio.be • www.Cohezio.be

RPM Bruxelles • IBAN BE54 8777 94 38 02 97 • BIC BNAG BE BB • 0410.623.764

Cohezio traite les données à caractère personnel dans la mesure où cela est nécessaire à l'exécution de ses missions légales découlant de la loi sur le bien-être au travail et du code du bien-être au travail.

4. Droit à la portabilité des données

Le droit à la portabilité signifie que la personne concernée a le droit de recevoir ses données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine et le droit de les transmettre, directement ou indirectement, à un autre responsable du traitement (ou employeur).

Le dossier de santé de la personne concernée constitue la mémoire des informations pertinentes concernant le travailleur, qui permet au conseiller en prévention-médecin du travail d'exercer la surveillance de la santé. La transmission du dossier de santé s'effectue sous la responsabilité du médecin dirigeant le département chargé de la surveillance médicale.

En cas de changement de service externe, la transmission d'un dossier individuel d'intervention psychosociale est régie de la manière suivante : le conseiller en prévention aspects psychosociaux avertit le demandeur et l'autre personne directement impliquée dans le dossier du fait que **Cohezio** ne sera plus compétent pour le traitement de la demande. Le conseiller en prévention aspects psychosociaux auprès de qui la demande avait été introduite remet le dossier individuel au conseiller en prévention aspects psychosociaux du nouveau service externe. Le conseiller en prévention aspects psychosociaux du nouveau service externe informe le demandeur du fait qu'il reprend le traitement de la demande.

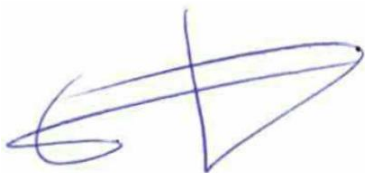
Lorsque le traitement de la demande d'intervention psychosociale formelle est clôturé au moment du changement de service externe de prévention et de protection au travail, le conseiller en prévention aspects psychosociaux du nouveau service externe peut, lorsque cela est nécessaire à l'exécution de ses missions, obtenir une copie du dossier individuel tenu par le conseiller en prévention aspects psychosociaux auprès de qui la demande avait été introduite.

Plaintes

Toute personne concernée qui pense être victime d'une violation de ses droits dans le cadre du Règlement Général sur la Protection des Données a le droit d'introduire une plainte auprès de l'Autorité de protection des données.

Besoin de plus amples informations

Vous pouvez contacter le délégué à la protection des données si vous avez besoin de plus d'informations : Johan Van Middel (infosecurity@cohezio.be).



Olivier LEGRAND
Administrateur-délégué

V3 01/01/2020



Service Externe de Prévention et de Protection au Travail

Cohezio asbl • Siège social : Boulevard Bischoffsheim 1-8, 1000 Bruxelles

T. +32 (0)2 533 74 11 • F. +32 (0)2 538 79 32 • info@Cohezio.be • www.Cohezio.be

RPM Bruxelles • IBAN BE54 8777 94 38 02 97 • BIC BNAG BE BB • 0410.623.764