Privacy Policy MENSURA EDPB

Mensura Externe Dienst voor Preventie en Bescherming op het Werk vzw met maatschappelijke zetel te Gaucheretstraat 88/90 1030 Brussel, met ondernemingsnummer 0410.664.742, ingeschreven in het rechtspersonenregister te Brussel, rechtsgeldig vertegenwoordigd door Gretel Schrijvers in de hoedanigheid van algemeen directeur

Hierna genoemd "de verwerkingsverantwoordelijke" (conform het advies van COPREV dd. 26/01/2018);

Verklaart het volgende;

De verwerkingsverantwoordelijke erkent het belang betreffende de veilige verwerking van Persoonsgegevens. Door middel van deze Privacy Policy wil de verwerkingsverantwoordelijke inzicht bieden m.b.t. de verwerking van uw Persoonsgegevens.

Deze Privacy Policy werd opgesteld, met inachtneming van de Europese Verordening betreffende Gegevensbescherming (ofwel de "GDPR; General Data Protection Regulation") dd. 27 april 2016. Deze Verordening werd omgezet in de Kaderwet dd. 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

*Eveneens werd de Europese e-privacy richtlijn, als lex specialis, in acht genomen voor de verwerking van Persoonsgegevens in het kader van direct marketing en cookies. (*op het moment dat deze Privacy Policy werd opgesteld, was dit nog een draft tekst)*

Indien bovenstaande wetteksten inhoudelijk wijzigen, zal de verwerkingsverantwoordelijke deze Privacy Policy conform deze wijzigingen aanpassen. Onze klanten zullen van essentiële wijzigingen op de hoogte worden gesteld. Additionele wijzigingen worden niet gemeld aan de klant. Onze Policy is publiek consulteerbaar op onze website.

Punt 1. Draagwijdte Privacy Policy

Deze Privacy Policy, met zijn bijlagen, geldt als bijlage t.a.v. de Hoofdovereenkomst tussen verwerkingsverantwoordelijke en de klant. Deze Privacy Policy is van toepassing gedurende de looptijd van de Hoofdovereenkomst.

Indien er in de Hoofdovereenkomst afwijkende bepalingen betreffende de verwerking van Persoonsgegevens staan, zal deze Privacy Policy voorrang verkrijgen.

Afwijkingen aan deze Privacy Policy zijn enkel en alleen geldig, indien beide partijen hun schriftelijk akkoord hieromtrent hebben verleend.

Punt 2. Definities

Voor de toepassing van deze Privacy Policy zullen de volgende begrippen de volgende betekenis hebben conform de tekst van de GDPR.

"Betrokkene": *de geïdentificeerde of identificeerbare natuurlijke persoon*

"Gegevens over gezondheid": *persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven*

"Gevoelige persoonsgegevens": *persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid*

"Inbreuk in verband met persoonsgegevens": *een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens*

"Persoonsgegevens": *alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon*

"Pseudonimisering": *het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld*

"Toestemming van de Betrokkene": *elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt*

"Verwerker": *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt*

"Verwerking": *een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens*

"Verwerkingsverantwoordelijke": *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*

Punt 3. De verwerking van de Persoonsgegevens

De verwerkingsverantwoordelijke garandeert dat uw Persoonsgegevens:

a) Verwerkt worden op een wijze die rechtmatig, behoorlijk en transparant is
b) Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld
c) Toereikend zijn, ter zake dienend zijn en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt
d) Juist zijn en zo nodig worden geactualiseerd

e) Worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de Persoonsgegevens worden verwerkt noodzakelijk is
f) Door het nemen van passende technische of organisatorische maatregelen; een passende beveiliging van de Persoonsgegevens wordt gewaarborgd, en dat de Persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging

De Persoonsgegevens worden rechtmatig verwerkt door de verwerkingsverantwoordelijke, aangezien de verwerking gebaseerd is op een wettelijke grondslag. Artikel 6, 1, C van de GDPR meldt dat de Persoonsgegevens rechtmatig worden verwerkt indien *"De verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die rust op de verwerkingsverantwoordelijke (in casu: de klant)".* In casu rust er op onze klanten de wettelijke verplichting om de nodige maatregelen te treffen in het kader van gezondheid en veiligheid op het werk. Deze wettelijke verplichtingen liggen vervat in de Codex Welzijn op het werk.

Bovenstaande Persoonsgegevens verwijzen naar o.a. naam, voornaam, adres, telefoon, geslacht, leeftijd, … Een overzicht kan worden teruggevonden in bijlage I van deze Policy.

Punt 4. De verwerking van de gevoelige persoonsgegevens

De gevoelige persoonsgegevens (meer expliciet: "Gegevens over gezondheid") worden door de verwerkingsverantwoordelijke rechtmatig verwerkt op basis van artikel 9, b) en h) van de GDPR;

- *b) de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke (in casu: de klant) of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt*

De dienstverlening van de verwerkingsverantwoordelijke is hoofdzakelijk wettelijk bepaald, nl. in de Codex Welzijn op het werk. De klant is wettelijk verplicht om zich aan te sluiten bij een externe dienst.

- *h) de verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen,*

het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten, op grond van Unierecht of lidstatelijk recht, of uit hoofde van een overeenkomst met een gezondheidswerker en behoudens de in lid 3 genoemde voorwaarden en waarborgen

De gevoelige persoonsgegevens die verwerkingsverantwoordelijke verwerkt, hebben betrekking op Gegevens over de gezondheid; m.a.w. het gewicht, het BMI, de arbeids(on)geschiktheid vermeld op het FGB (Formulier Gezondheidsbeoordeling) of het FRIB (Formulier Reintegratiebeoordeling), de medische gegevens, de psychologische gegevens, de letsels na een ernstig arbeidsongeval, de levensstijl van de betrokkene, ….

Een overzicht kan worden teruggevonden in bijlage I van deze Policy.

Punt 5. Expliciete toestemming van de Betrokkene(n)

In het kader van de dienstverleningen waar de Persoonsgegevens rechtstreeks bij de Betrokkene(n) worden opgevraagd, zal de verwerkingsverantwoordelijke (in casu: Mensura) hiertoe de Betrokkene(n) voorafgaand informeren over de volgende elementen –conform artikel 13 punt 1 GDPR:

- de identiteit en de contactgegevens van de verwerkingsverantwoordelijke
- de contactgegevens van de functionaris voor gegevensbescherming
- het doel en de rechtsgrond van de verwerking
- de ontvangers of de categorieën van ontvangers van de persoonsgegevens
- de wijze van uitoefening van de rechten van Betrokkene(n)
- het feit dat betrokkene zijn expliciete toestemming alsnog kan intrekken & de wijze waarop dit kan
- het feit dat betrokkene het recht heeft om een klacht in te dienen bij de toezichthoudende autoriteit
- de termijn van bewaring van de Persoonsgegevens
- indien van toepassing, het bestaan van geautomatiseerde besluitvorming

Daar waar verwerkingsverantwoordelijke diensten levert in het kader van punt 3 en 4, dient de klant bovenstaande informatie aan de Betrokkene(n) mee te delen. Hiervoor kan de klant deze Privacy Policy gebruiken.

Punt 6. De verwerking van Persoonsgegevens voor Marketingdoeleinden

Wat betreft de verwerking van Persoonsgegevens voor Marketingdoeleinden, kan verwerkingsverantwoordelijke (in casu: Mensura) terugvallen op een wettelijke grondslag (overweging 47 GDPR). Er wordt telkens een mogelijkheid tot opt-out voorzien.

Er worden geen persoonsgegevens verwerkt, voor Marketingdoeleinden, van de werknemers van de klant van Verwerkingsverantwoordelijke. Enkel de persoonsgegevens van de klant (contactgegevens) worden hiervoor verwerkt, zodat Mensura de klant op de hoogte kan houden van wijzigingen t.a.v. diensten in het kader van de Welzijnswetgeving.

Punt 7. De anonieme groepsrapporteringen

Verwerkingsverantwoordelijke garandeert dat groepsrapporteringen anoniem gebeuren aangezien persoonsgegevens pas worden meegedeeld vanaf een dataset van 10.

De resultaten van het medisch onderzoek maken bijvoorbeeld deel uit van de risicoanalyse. Deze resultaten worden in de vorm van anonieme groepsresultaten gerapporteerd.

Punt 8. Het register van verwerkingsactiviteiten

De verwerkingsverantwoordelijke heeft een register van verwerkingsactiviteiten opgesteld, waar de volgende elementen gedetailleerd in worden omschreven per dienstverlening:

1° Welke categorieën van Persoonsgegevens worden verwerkt?

2° Wie kan deze Persoonsgegevens ontvangen (intern/extern)?

3° Hoe lang worden de Persoonsgegevens bewaard?

4° Hoe worden de Persoonsgegevens beveiligd?

5° Worden de Persoonsgegevens buiten België verwerkt?

6° Wie heeft toegang tot de Persoonsgegevens (intern/extern)?

7° De verwerkingsdoeleinden

Heeft u vragen die binnen dit kader vallen en niet verduidelijkt worden in deze Policy, vragen wij u contact op te nemen met de personen in punt 20 vermeld.

Punt 9. De passende technische en organisatorische maatregelen

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, neemt de

verwerkingsverantwoordelijke passende technische en organisatorische maatregelen opdat de Persoonsgegevens veilig verwerkt worden. In bijlage II van deze Policy kan u een oplijsting van deze maatregelen vinden.

De verwerkingsverantwoordelijke garandeert conform artikel 32 van de GDPR de nodige maatregelen te nemen, die onder andere betrekking hebben op:

a) de pseudonimisering en versleuteling van persoonsgegevens;

b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

De verwerkingsverantwoordelijke garandeert dat zijn werknemers, die toegang hebben tot de Persoonsgegevens, beperkt worden tot diegenen die betrokken zijn met de uitoefening van de dienstverlening. Tevens zijn deze werknemers contractueel gebonden aan een confidentialiteitsverplichting.

Punt 10. Derden

Derden die eventueel toegang kunnen hebben tot de Persoonsgegevens, worden eveneens beperkt tot diegenen die betrokken zijn met de uitoefening van de dienstverlening. Een lijst van derden kan door de klant opgevraagd worden.

Punt 11. Verwerkers

Wanneer de verwerkingsverantwoordelijke een verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze verwerkers dezelfde verplichtingen betreffende gegevensbescherming opgelegd als die welke uit deze overeenkomst voortvloeien, in het bijzonder o.a. de verplichting om passende technische en organisatorische maatregelen te nemen t.a.v. de verwerking van de Persoonsgegevens. Hiertoe hebben de verwerkers een verwerkingsovereenkomst conform artikel 28 punt 3 GDPR ondertekend. Een lijst van verwerkers kan door de klant opgevraagd worden.

De verwerkingsverantwoordelijke garandeert dat de aangeduide verwerkers louter en alleen de Persoonsgegevens verwerken op basis van uitgeschreven richtlijnen door de verwerkingsverantwoordelijke. Wanneer de aangestelde verwerker een subverwerker aanduidt, zal de verwerker in beginsel aansprakelijk blijven t.a.v. deze subverwerker.

Punt 12. Gegevensverwerking buiten een lidstaat van de EU

De verwerkingsverantwoordelijke garandeert dat de Persoonsgegevens niet buiten een lidstaat van de EU worden verwerkt. De Persoonsgegevens worden enkel en alleen in België verwerkt.

Punt 13. Minimale verwerking van Persoonsgegevens

De dienstverlening van de verwerkingsverantwoordelijke is hoofdzakelijk wettelijk bepaald, nl. in de Codex Welzijn op het werk. De verwerkingsverantwoordelijke zal enkel die Persoonsgegevens verwerken, die minimaal noodzakelijk zijn in het kader van de uitvoering van de aangevraagde dienstverlening. Een overzicht kan worden teruggevonden in bijlage I van deze Policy.

De verwerkingsverantwoordelijke garandeert dat de Persoonsgegevens niet langer dan noodzakelijk worden bewaard, voor de uitvoering van de aangevraagde dienstverlening. De verwerkingsverantwoordelijke is gebonden aan wettelijke bewaartermijnen. Een overzicht kan worden teruggevonden in bijlage I van deze Policy.

Punt 14. De rechten van de betrokkenen:

<u>14.1. Algemeen</u>

In het kader van de GDPR hebben de betrokkenen de volgende rechten t.a.v. hun Persoonsgegevens:

1° Recht van inzage

2° Recht op rectificatie van onjuiste Persoonsgegevens

3° Recht op gegevenswissing ("Recht op vergetelheid")

Het recht op gegevenswissing zal in de meeste gevallen niet uitgevoerd worden, aangezien de verwerkingsverantwoordelijke zijn verwerking baseert op een wettelijke grondslag.

4° Recht op beperking van de verwerking

5° Recht op overdraagbaarheid van gegevens

6° Recht van bezwaar

Het recht van bezwaar zal in de meeste gevallen niet uitgevoerd worden, aangezien verwerkingsverantwoordelijke zijn verwerking baseert op een wettelijke grondslag.

De verwerkingsverantwoordelijke garandeert binnen 1 maand, na ontvangst van het verzoek, de aanvraag te beantwoorden. Dit conform de verplichtingen in artikel 12 punt 3 van de GDPR. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging.

In punt 14.2. en 14.3. kunnen de interne procedures van verwerkingsverantwoordelijke gevonden worden, opdat de betrokkenen hun rechten correct kunnen uitoefenen. De klant dient de Betrokkenen van deze interne procedures van verwerkingsverantwoordelijke –in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal- te informeren. Indien de Betrokkenen een recht willen uitoefenen dat niet valt onder punt 14.2. of 14.3. kan het verzoek verstuurd worden naar privacy@mensura.be. De Betrokkenen kunnen ook per post hun verzoek sturen ter attentie van de DPO (Kempische Steenweg 309 bus 0.01 – 3500 Hasselt).

<u>14.2. De rechten van betrokkene in het kader van het medisch toezicht</u>

Wat betreft het uitoefenen van één van de rechten t.a.v. zijn/haar medisch dossier dient de betrokkene de volgende interne procedure bij de verwerkingsverantwoordelijke te respecteren:

- per aangetekend schrijven het verzoek indienen; gericht aan Dr. Marie-Noelle Schmickler, directeur afdeling medisch toezicht, Italiëlei 2 te 2000 Antwerpen.
- + een kopij van de identiteitskaart

Inzage in de medische dossiers wordt niet rechtstreeks aan de werknemer gegeven, maar wel aan zijn/haar behandelende arts. Dit conform het advies van de Orde der Artsen dd. 07/09/1996.

<u>14.3. De rechten van betrokkene in het kader van psychosociale dossiers</u>

Wat betreft het uitoefenen van één van de rechten t.a.v. zijn/haar psychosociale dossier dient de betrokkene de volgende interne procedure bij de verwerkingsverantwoordelijke te respecteren:

- per aangetekend schrijven het verzoek indienen; gericht aan de betrokken preventieadviseur-psychosociale aspecten

- + een kopij van de identiteitskaart

14.4. Klacht indienen bij de Belgische toezichthoudende Privacy-autoriteit (= "de Gegevensbeschermingsautoriteit")

De betrokkene heeft conform artikel 77 van de GDPR het recht om rechtstreeks een klacht in te dienen bij de Gegevensbeschermingsautoriteit, indien hij/zij meent dat hun Persoonsgegevens niet conform de GDPR beveiligd en/of verwerkt worden door de verwerkingsverantwoordelijke.

Punt 15. De overdraagbaarheid van de Persoonsgegevens indien de klant van Externe dienst wijzigt

15.1. Overdracht Persoonsgegevens Afdeling Medisch Toezicht

De overdracht van de gezondheidsdossiers is geregeld in de Codex Welzijn op het Werk, Boek I, Titel 4, Afdeling 4.

Het gezondheidsdossier bestaat uit vier verschillende delen:

a) de sociaal-administratieve gegevens betreffende de identificatie van de werknemer en zijn werkgever

b) de beroepsanamnese en de objectieve medische persoonsgegevens, die zijn vastgesteld aan de hand van de verplichte handelingen verricht tijdens de preventieve medische onderzoeken. Deze persoonsgegevens houden verband met de werkpost of de activiteit van de werknemer

c) de specifieke gegevens van persoonlijke aard vastgesteld door de arbeidsarts tijdens de preventieve medische onderzoeken en die aan laatstgenoemde arts zijn voorbehouden

d) de blootstellinggegevens van elke werknemer die is tewerkgesteld op een werkpost of aan een activiteit waarbij hij blootstaat aan biologische, fysische of chemische agentia.

Het gezondheidsdossier bevat geen informatie over de medewerking aan programma's inzake volksgezondheid die geen verband houden met het beroep.

De overdracht van de medische gegevens gebeurt onder de verantwoordelijkheid van de arts die de leiding heeft over het departement of de afdeling belast met het medisch toezicht (directeur medisch toezicht).

Voor overdracht van de medische dossiers dient de directeur medisch toezicht van de nieuwe externe dienst een schrijven te richten aan de directeur medisch toezicht van de verwerkingsverantwoordelijke, met de vraag voor gegevensoverdracht. Pas na ontvangst van de aanvraag worden de opgevraagde dossiers effectief overgedragen.

15.2. Overdracht Persoonsgegevens Afdeling Psycho

De overdracht van deze persoonsgegevens wordt geregeld in artikel 34 van de Codex Welzijn op het werk, boek I Titel 3 Preventie van psychosociale risico's op het werk.

Wanneer de klant verandert van externe dienst voor preventie en bescherming op het werk, wordt de overdracht van het individueel dossier als volgt geregeld:

1° Wanneer het verzoek tot formele psychosociale interventie in behandeling is op het moment van de verandering:

a) de preventieadviseur psychosociale aspecten brengt de verzoeker en de andere rechtstreeks betrokken persoon zo snel mogelijk op de hoogte van het feit dat de externe dienst waarvoor hij zijn opdrachten vervult niet meer bevoegd zal zijn voor de behandeling van het verzoek;

b) de klant deelt aan de preventieadviseur psychosociale aspecten bij wie het verzoek werd ingediend, op zijn verzoek, de coördinaten mee van de nieuwe externe dienst;

c) de preventieadviseur psychosociale aspecten bij wie het verzoek werd ingediend, bezorgt het individueel dossier aan de preventieadviseur psychosociale aspecten van de nieuwe externe dienst;

d) de preventieadviseur psychosociale aspecten van de nieuwe externe dienst brengt de verzoeker en de andere rechtstreeks betrokken persoon op de hoogte van het feit dat hij de behandeling van het verzoek overneemt.

2° Wanneer de behandeling van het verzoek tot formele psychosociale interventie afgesloten is op het moment van de verandering van externe dienst voor preventie en bescherming op het werk, kan de preventieadviseur psychosociale aspecten van de nieuwe externe dienst, wanneer dit noodzakelijk is voor het uitvoeren van zijn opdrachten, een kopie bekomen van het

individueel dossier van de preventieadviseur psychosociale aspecten bij wie het verzoek werd ingediend.

De overdracht van het individueel dossier gebeurt onder voorwaarden die het beroepsgeheim waarborgen.

Punt 16. Wissen van de Persoonsgegevens bij einde van de Hoofdovereenkomst

Verwerkingsverantwoordelijke garandeert dat binnen de maand na het einde van de Hoofdovereenkomst de verwerkte Persoonsgegevens worden gewist of overgedragen op vraag van de klant, tenzij een wettelijke bepaling de verwerkingsverantwoordelijke toelaat om de Persoonsgegevens voor een langere termijn te bewaren.

Op vraag van de klant levert de verwerkingsverantwoordelijke hiervan de nodige bewijsmiddelen.

Tevens worden de verwerkers en derden ingelicht door de verwerkingsverantwoordelijke over het wissen van de verkregen Persoonsgegevens, indien de Hoofdovereenkomst beëindigd is. Dit tenzij ook zij zich kunnen beroepen op een wettelijke bepaling waardoor de Persoonsgegevens langer bewaard mogen worden.

Punt 17. Opvragen persoonsgegevens door openbare overheidsdiensten

Verwerkingsverantwoordelijke brengt de klant binnen de 3 werkdagen op de hoogte ingeval hij:

(a) met betrekking tot de verwerking van Persoonsgegevens van een overheidsinstantie een verzoek om informatie, een dagvaarding of een onderzoeks- of controleverzoek ontvangt, behalve wanneer verwerkingsverantwoordelijke anderszins rechtens niet bevoegd is tot een dergelijke verstrekking

(b) voornemens is om Persoonsgegevens te verstrekken aan een overheidsinstantie

(c) van een derde of een werknemer, klant of opdrachtnemer van de klant een verzoek ontvangt tot openbaarmaking van Persoonsgegevens van de klant of informatie met betrekking tot de verwerking van Persoonsgegevens van de klant

Verwerkingsverantwoordelijke geeft de klant 72 uren, vanaf de melding, de tijd om zijn bezwaren te uiten m.b.t. een dergelijke overdracht van Persoonsgegevens.

Punt 18. Maatregelen indien er zich een inbreuk voordoet i.v.m. de Persoonsgegevens

De verwerkingsverantwoordelijke heeft de verplichting om inbreuken m.b.t. de beveiliging van de Persoonsgegevens, binnen de 72 uren, te melden aan de bevoegde Belgische toezichthoudende autoriteit. Dit tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van de betrokkene(n).

De verwerkingsverantwoordelijke informeert de klant zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens. Er wordt overeengekomen dat de verwerkingsverantwoordelijke en de klant onderling binnen de 48 uren, na kennisname van de inbreuk bij de verwerkingsverantwoordelijke, elkaar contacteren en onderling afstemmen of de inbreuk wordt doorgegeven aan de bevoegde Belgische toezichthoudende autoriteit.

Indien de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, wordt de inbreuk in verband met de persoonsgegevens onverwijld meegedeeld aan de betrokkene(n) conform artikel 34 van de GDPR.

Zowel de klant als de verwerkingsverantwoordelijke werken samen met de bevoegde Belgische toezichthoudende autoriteit om de nodige informatie te verschaffen en de gevolgen van de inbreuk te beperken.

Punt 19. Overige bepalingen

In geval van nietigheid van één of meer van de bepalingen uit deze Privacy Policy, blijven de overige bepalingen onverkort van kracht.

Op deze Privacy Policy is het Belgische recht van toepassing. Partijen zullen hun geschillen verband houdende met deze Privacy Policy uitsluitend voorleggen aan de rechtbanken te Brussel.

Punt 20. Meer informatie of ondersteuning nodig?

De verwerkingsverantwoordelijke garandeert de klant om de nodige, bijkomende ondersteuning en informatie aan te bieden zodat de verwerkingsverantwoordelijke de nakoming van haar verplichtingen, onder de GDPR, kan aantonen. Deze informatieverplichting strekt zich niet uit tot informatie die confidentieel is of omwille van wettelijke redenen niet meegedeeld kan worden aan de klant.

Tevens zal de verwerkingsverantwoordelijke de nodige samenwerking verlenen indien een audit in opdracht van de klant, of een door de klant gemachtigde controleur, wordt uitgevoerd bij de verwerkingsverantwoordelijke. De klant draagt de kosten van de aangestelde controleur en uitgevoerde audit. De audit zal zich altijd beperken tot de systemen van de verwerkingsverantwoordelijke die voor de verwerkingen worden gebruikt.

De Functionaris voor gegevensbescherming (ofwel de Data Protection Officer) en de Security Officer van de verwerkingsverantwoordelijke kunnen gecontacteerd worden op het volgende mailadres: Privacy@mensura.be.

Bijlage I. De categorieën van verwerkte Persoonsgegevens en de duurtijd van bewaring

De categorieën van Persoonsgegevens die verwerkingsverantwoordelijke kan verwerken

- Persoonlijke identificatiegegevens (zoals o.a. voornaam, familienaam, adres, telefoonnummer, e-mailadres, type rijbewijs indien van toepassing)
- Persoonlijke kenmerken (zoals o.a. leeftijd, geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit)
- Gegevens betreffende de gezondheid (zoals lichamelijke gezondheid en psychische gezondheid)
- Beroep en betrekking (zoals o.a. werkgever, titel en beschrijving van de functie, datum van aanwerving)
- Rijksregisternummer
- Raciale of etnische gegevens
- Beeldopnamen (foto)
- Andere categorie van gegevens (zoals bv. zeemansboeknummer indien van toepassing)

De duurtijd van bewaring

Medisch dossier = wettelijke bewaartermijnen (= 40 jaar)

Psychosociale dossiers = wettelijke bewaartermijn (= 20 jaar)

Bijlage II. De technische en organisatorische maatregelen ter beveiliging

- Interne IT Policy goedgekeurd door directie (omvat wachtwoordbeleid, aanvaardbaar gebruik van bedrijfsmiddelen, Clean Desk en Clear Screen beleid, Softwarebeleid, internetbeleid, e-mail beleid, sociale media beleid, beleid van vertrouwelijkheid van gegevens, …)
- Data wordt enkel in België opgeslagen
- Onze systemen zijn redundant over 2 datacenters met TIER III+ classificatie. (DRP en BCP)
- Hosting provider is ISO27001 gecertifieerd.
- Firewalls op meerdere netwerklagen.
- Network Access Control, scheiding van netwerken enz…
- Data in transit wordt enkel geëncrypteerd toegestaan.
- Remote toegang van gebruikers enkel via VPN met Multi Factor authenticatie.
- Geverifieerde backup en restore procedures.
- Data in rest (backups) worden geëncrypteerd
- “Role based access” naar toepassingen.
- User Awareness trainingen worden georganiseerd.
- Antivirus/Antispam op meerdere lagen. (Firewall, Endpoints, Servers, mailsystemen…)
- SIEM voor security devices.
- Logging en rapportering.
- Regelmatige security testing.
- Mobile Device management
- Capacity Management
- Regelmatige updates van alle systemen en rapportering daarvan.
- Regelmatige Security meetings met onze hosting provider.
- Fysieke toegangsbeveiliging.
- Asset Management
- Netwerk en systeem monitoring.
- DDOS en IPS maatregelen.
- Data Loss Prevention implementatie in de nabije toekomst.
- Wijzigingsbeheer (Change Management)
- Gescheiden Test, Validatie en Productie-omgevingen.
- Regelmatige beoordeling van leveranciers