CERTIMED

Privacy Policy Certimed

Certimed vzw met maatschappelijke zetel te Kempische Steenweg 309 bus 3.01 te 3500 Hasselt, met ondernemingsnummer 0409.671.085, rechtsgeldig vertegenwoordigd door Bart Teuwen in de hoedanigheid van algemeen directeur;

Hierna genoemd "de verwerkingsverantwoordelijke";

Verklaart het volgende:

Certimed vzw erkent het belang betreffende de veilige verwerking van Persoonsgegevens. Door middel van deze Privacy Policy wil Certimed vzw 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.

In het kader van de GDPR neemt Certimed de kwalificatie aan van een verwerkingsverantwoordelijke. Dit omdat de rechten van de Betrokkenen rechtstreeks uitgeoefend dienen te worden bij Certimed vzw. De Betrokkenen kunnen hun rechten m.b.t. GDPR niet indienen bij onze klanten, omdat deze klanten geen toegang mogen krijgen in het volledig medische dossier van de Betrokkene(n).

*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 de Europese e-privacy richtlijn nog een draft tekst)*

Indien bovenstaande wetteksten inhoudelijk wijzigen, zal Certimed vzw 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 krijgen.
Afwijkingen aan deze Privacy Policy zijn enkel en alleen geldig, indien beide partijen hun schriftelijk akkoord hieromtrent hebben verleend.

CERTIMED

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*

"Derden": *een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken*

"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*

"Subverwerker": *de verwerker, die onder rechtstreeks gezag van de verwerker gemachtigd zijn om de persoonsgegevens te verwerken*

"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

Voor het uitvoeren van medische controles en het opstellen van rapporteringen m.b.t. verzuim kan men zich baseren op de artt. 6, 1, B en F van de GDPR:

- Art. 6, 1, B) GDPR: *"De verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de Betrokkene een partij is"*
- Art. 6, 1, F) GDPR: "*De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke (in casu: de klant) of van een derde, behalve wanneer de belangen of de grondrechten en de*

CERTIMED

> *fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is"*

Het gerechtvaardigde belang van de klant binnen art. 6, 1, F) GDPR is o.a. het belang om preventief het ziekteverzuim binnen de organisatie te bestrijden.

Bovenstaande Persoonsgegevens verwijzen naar o.a. naam, voorna(a)m(en), adres, postcode, woonplaats, e-mailadres, geboortedatum, geslacht, burgerlijke staat, informatie professionele betrekking (= identiteit werkgever, werkplaats, eventuele titel functie, datum aanwerving, datum vertrek), … 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 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 bied.*

De klant heeft het recht om beroep te doen op verwerkingsverantwoordelijke, als medische controledienst, in het kader van artikel 31 van de wet betreffende de arbeidsovereenkomsten.

- *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 klant kan beroep doen op verwerkingsverantwoordelijke, om analyses en rapporteringen te verkrijgen m.b.t. ziekteverzuim in zijn organisatie. Dergelijke dienstverlening kadert binnen het preventieve luik van geneeskunde.

De Gevoelige Gegevens die verwerkingsverantwoordelijke verwerkt, hebben betrekking op Gegevens over de gezondheid; nl. lichamelijke en psychische gegevens, duur van de arbeidsongeschiktheid, aard van de arbeidsongeschiktheid, gegevens behandelende arts, toegelaten/verboden woning te verlaten, hospitalisatie werknemer, eerste attest/verlengingsattest… Een overzicht kan worden teruggevonden in bijlage I van deze Policy.

Punt 5. Verwerking Persoonsgegevens en gevoelige Persoonsgegevens voor wetenschappelijke en statistische doeleinden

Verwerkingsverantwoordelijke verwerkt Persoonsgegevens voor wetenschappelijke en statistische doeleinden. Dit conform artikel 89 van de GDPR.

De bewaringstermijn van de Persoonsgegevens voor dit doeleinde gaat niet verder, dan de bewaringstermijn die verwerkingsverantwoordelijke hanteert in het kader van de andere doeleinden. Zie bijlage I van deze Policy voor meer verduidelijking.

Punt 6. Expliciete toestemming van de Betrokkene(n)

In het kader van de dienstverleningen waar verwerkingsverantwoordelijke de Persoonsgegevens rechtstreeks bij de Betrokkene(n) dient op te vragen, zal verwerkingsverantwoordelijke hiertoe de Betrokkene(n) voorafgaand informeren over de volgende elementen –conform artikel 13 punt 1 GDPR:

- de identiteit en de contactgegevens van Certimed
- 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.

Punt 7. De verwerking van Persoonsgegevens voor Marketingdoeleinden

Wat betreft de verwerking van Persoonsgegevens voor Marketingdoeleinden, kan verwerkingsverantwoordelijke 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 Certimed de klant op de hoogte kan houden van wijzigingen t.a.v. de dienstverlening.

Punt 8. De anonieme groepsrapporteringen

Verwerkingsverantwoordelijke garandeert dat groepsrapporteringen anoniem gebeuren aangezien persoonsgegevens pas worden meegedeeld vanaf een dataset van 20.

Punt 9. Het register van verwerkingsactiviteiten

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

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 21 vermeld.

Punt 10. 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 11. Derden
Derden die eventueel toegang kunnen hebben tot de Persoonsgegevens, worden eveneens beperkt tot diegenen die betrokken zijn met de uitoefening van de dienstverlening. De klant kan een lijst van derden opvragen bij de verwerkingsverantwoordelijke.

Punt 12. Verwerkers
Wanneer de verwerkingsverantwoordelijke een verwerker in dienst neemt om voor rekening van de klant specifieke verwerkingsactiviteiten te verrichten, worden aan deze verwerker dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke uit deze overeenkomst voortvloeien, met name 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. De klant kan een lijst van verwerkers opvragen bij de verwerkingsverantwoordelijke.

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 13. Gegevensverwerking buiten een lidstaat van de Europese Unie
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 14. Minimale verwerking van Persoonsgegevens
De dienstverlening van de verwerkingsverantwoordelijke is hoofdzakelijk wettelijk bepaald (artikel 31 van de wet betreffende de arbeidsovereenkomsten). 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 15. De rechten van de betrokkenen:
<u>15.1. 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 door verwerkingsverantwoordelijke, aangezien de verwerking gebaseerd wordt op een wettelijke verwerkingsverplichting.
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 door verwerkingsverantwoordelijke, aangezien de verwerking gebaseerd wordt op een wettelijke verwerkingsverplichting.

Bovenstaande rechten zullen uitgeoefend worden ten aanzien van medische dossiers waar de klant juridisch geen gevolg aan mag en kan geven. Vandaar dat bovenstaande rechten/verzoeken rechtstreeks ingediend dienen te worden bij de verwerkingsverantwoordelijke. 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 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 15.2. kan de interne procedure van verwerkingsverantwoordelijke gevonden worden, opdat de betrokkenen van de klant hun rechten t.a.v. het individueel medisch dossier correct kunnen uitoefenen bij de verwerkingsverantwoordelijke. De klant dient de Betrokkenen van deze interne procedure van verwerkingsverantwoordelijke -in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal- te informeren. Indien de Betrokkene een recht wil uitoefenen dat niet valt onder punt 15.2. kan het verzoek verstuurd worden naar privacy@certimed.be ofwel per post ter attentie van de DPO (Kempische Steenweg 309 bus 3.01 – 3500 Hasselt).

<u>15.2. Recht op inzage / recht op kopij m.b.t. het individueel medisch dossier</u>
Wat betreft het uitoefenen van het recht op inzage of het recht op kopij t.a.v. zijn/haar medisch dossier dient de betrokkene de volgende interne procedure bij verwerkingsverantwoordelijke te respecteren:

- per aangetekend schrijven (ondertekend en gedagtekend) het verzoek richten aan Certimed vzw, t.a.v. de hoofdgeneesheer, Kempische Steenweg 309 bus 3.01 te 3500 Hasselt
- + een kopij van zijn/haar identiteitskaart toe te voegen

<u>15.3. Klacht indienen bij de Belgische toezichthoudende Privacy-autoriteit (= "de Gegevensbeschermingsautoriteit")</u>
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.

Punt 16. De overdraagbaarheid van de Persoonsgegevens indien de klant van medische controledienst wijzigt
In onderling overleg zullen verwerkingsverantwoordelijke en de klant afspreken hoe de Persoonsgegevens overgedragen worden.

Punt 17. Wissen van de Persoonsgegevens bij einde van de Hoofdovereenkomst
De 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 (zie bijlage I).
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 18. Opvragen persoonsgegevens door openbare overheidsdiensten
De 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
De 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 19. Maatregelen indien er zich een inbreuk voordoet i.v.m. de Persoonsgegevens
De verwerkingsverantwoordelijken hebben 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 betrokkene(n) de inbreuk in verband met de persoonsgegevens onverwijld meegedeeld conform artikel 34 van de GDPR.

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

Punt 20. 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 21. 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@certimed.be.

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

<u>De categorieën van Persoonsgegevens die verwerkingsverantwoordelijke kan verwerken</u>
Naam, voorna(a)m(en), adres, postcode, woonplaats, e-mailadres, geboortedatum, geslacht, burgerlijke staat, gegevens betreffende de gezondheid (lichamelijke en psychische gegevens), verblijfsadres, taal, naam echtgenoot, informatie professionele betrekking (= identiteit werkgever, werkplaats, eventuele titel functie, datum aanwerving, datum vertrek, statuut, functieniveau, barema, netwerk, directie, code populatie, benoemingscode, schaal, competentie, zuil, rang, subdivisie, provinciale dienst, code medex, wijze beheer ziekte, referentie organigram, beheerder, categorie rsz), blokkeren voor controle, duur van de arbeidsongeschiktheid, aard van de arbeidsongeschiktheid, gegevens behandelende arts, toegelaten/verboden woning te verlaten, hospitalisatie werknemer, eerste attest/verlengingsattest en datum obliteratie.

<u>De duurtijd van bewaring</u>
De persoonsgegevens worden conform artikel 15 van de wet betreffende de arbeidsovereenkomsten bewaard: *"tot 5 jaar na het feit waaruit de vordering kan ontstaan"*.
Deze bewaartermijn geldt ten aanzien van de verwerking van persoonsgegevens in het kader van uitvoering medische controles en t.a.v. de groepsrapporteringen en analyses.
Voor wat betreft de verwerking van persoonsgegevens omwille van wetenschappelijke of statistische doeleinden, wordt eveneens een bewaringstermijn van 5 jaar gehanteerd.

Certimed V.Z.W.
Maatschappelijke zetel:
Corda Campus (gebouw Corda 2)
Kempische Steenweg 309/3.01
3500 Hasselt
T +32 11 30 12 52
F +32 11 30 12 62
E info@certimed.be
www.certimed.be
IBAN: BE84 3350 0249 4259
BIC: BBRU BE BB
KBO: 0409.671.085

Bijlage II. De technische en organisatorische maatregelen ter beveiliging

- Communicatie stromen worden bekeken
- Data Register werd aangelegd.
- Gebruikers worden ingelicht over GDPR.
- Het beleid rond bewaartermijnen wordt herbekeken.
- Een nieuwe Privacy verklaring werd geschreven.
- Er is een DPO aangesteld.
- Een gegevensbeschermingsimpactanalyse wordt uitgevoerd.
- Het afsluiten van verwerkersovereenkomsten met leveranciers/onderaannemers in het kader van GDPR.
- verwerkingsverantwoordelijke werkt een nieuwe incident response procedure uit om op een correcte manier om te gaan met inbreuken tegen de informatieveiligheid.
- 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.
- 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.
- Geverifieerde backup en restore procedures.
- Data in rest (backups) worden geëncrypteerd indien dit technisch mogelijk is
- “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