Verwerkersovereenkomst Mediwet vzw

1. Inleiding

Deze verwerkersovereenkomst is opgemaakt in het kader van de Algemene Verordening Gegevensbescherming, afgekort AVG, hierna genoemd de GDPR van General Data Protection Regulation, zijnde de Verordening 2016/679 van 27 april 2016. Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens (art. 1, 2°GDPR)

Deze verwerkersovereenkomst, met zijn bijlagen, geldt als bijlage aan de Hoofdovereenkomst tussen Mediwet en de klant. Afwijkingen aan deze Privacy Policy zijn enkel en alleen geldig, indien beide partijen hun schriftelijk akkoord hieromtrent hebben verleend.

Onze klanten zullen van essentiële wijzigingen op de hoogte worden gesteld.

Door middel van deze overeenkomst wilt Mediwet inzicht bieden m.b.t. haar verwerking van Persoonsgegevens van haar klanten en diens werknemers.

In de relatie met de werknemers van de klant, dient Mediwet te worden beschouwd als verwerkingsverantwoordelijke conform het advies van COPREV van 26/01/2018. Dit betekent dat Mediwet zelf verantwoordelijk is voor het naleven van de verplichtingen van de GDPR (art. 5, 2° GDPR) in de relatie met de werknemers van haar klanten.

2. Rechtmatigheid, behoorlijkheid en transparantie.

De verwerking van persoonsgegevens door Mediwet is rechtmatig aangezien deze noodzakelijk is voor de vervulling van een taak van algemeen belang (art. 6, 1, e GDPR), minstens en alleszins om te voldoen aan een wettelijke verplichting die op de klant rust. (art. 6, 1, c GDPR). Meer specifiek is de verwerking noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, … (art. 9, h GDPR) of is de verwerking noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de klant op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht… (art. 9, b GDPR).

De persoonsgegevens die verwerkt worden, zijn de gebruikelijke identificatie en contactgegevens: naam, voornaam, leeftijd, geslacht, geboortedatum en –plaats, maar ook het rijksregisternummer en medische gegevens in de meest ruime zin waaronder: gewicht, lengte, BMI, arbeids(on)geschiktheid, letsels, …

3. Geen onverenigbare verdere verwerking

Mediwet verwerkt de gegevens van haar klanten en de werknemers van haar klanten enkel in het kader van de Welzijnswetgeving. Ook verdere verwerking zal enkel gebeuren in het kader van de Welzijnswetgeving, waaronder begrepen wetenschappelijk, historisch of statistisch onderzoek, in de mate van het mogelijke door pseudonimisering (art. 89 GDPR).

4. Minimale gegevensverwerking

Enkel die gegevens zullen verwerkt worden door Mediwet die toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is in het kader van de Welzijnswetgeving.

5. Juistheid

Mediwet streeft naar de correctheid van haar gegevens en actualisering. Betrokkene kunnen hiervoor steeds vragen om gegevens te rectificeren zoals ook bepaald is in onze Bijlage 2: NOTIFICATIE VERWERKING PERSOONSGEGEVENS.

6. Opslagbeperking

In het belang van de werknemers worden alle gegevens bewaard tot 30 jaar na het bereiken van de normale pensioengerechtigde leeftijd. Persoonsgegevens kunnen nog langer bewaard voor statistische doeleinden of in het kader van wetenschappelijk of historisch onderzoek, in welk geval de gegevens zo veel als mogelijk geanonimiseerd zullen worden.

7. Integriteit en vertrouwelijkheid

Mediwet zorgt ervoor dat de Persoonsgegevens voldoende beveiligd zijn. Om verlies en onrechtmatige verwerkingen te voorkomen, neemt Mediwet passende technische en organisatorische maatregelen. Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover werd opgenomen in Bijlage 3: Overzicht met beveiligingsmaatregelen.

Bovendien zullen groepsrapporteringen enkel anoniem gebeuren, d.w.z. pas vanaf datasets van 10.

De klant heeft het recht om te controleren of het verwerken van de persoonsgegevens aan de wet en de afspraken uit deze Verwerkingsovereenkomst voldoet, weliswaar enkel om na te kijken of de GDPR-conformiteit van de verwerking door Mediwet wordt gegarandeerd en uitsluitend met betrekking tot de gegevens die Mediwet voor de Klant verwerkt.

8. Exporteren Persoonsgegevens

Mediwet zal geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van de betrokkene.

De Klant geeft de toestemming aan Mediwet om een andere Verwerkingsverantwoordelijke en/of Verwerkers aan te stellen indien dit nodig is voor het verwerken van de persoonsgegevens. Wanneer Mediwet andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkingsovereenkomst.

De belangrijkste externe partijen die kunnen betrokken worden bij de verwerking van persoonsgegevens zijn: de overheid (de met het toezicht belaste ambtenaar, openbaar ministerie, Fedris, RSZ, Vaccinet, …), andere erkende externe diensten, waaronder Premed ook in de hoedanigheid van onze softwareleverancier, laboanalyses door erkende medische labo's, Monstarecon voor de verwerking van psychosociale vragenlijsten, behandelende artsen en de adviserend geneesheer van de mutualiteit in het kader van een re-integratiedossier (E-Health).

9. Geheimhouding

Mediwet zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is, en zal ervoor zorgen dat ook haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden.

10. Datalekken

Ingeval van een ontdekking van een mogelijk Datalek zal Mediwet de betrokkenen hierover informeren zonder onredelijke vertraging via elektronische weg en de informatie verstrekken die is aangegeven in Bijlage 4: Proces rondom het melden van Datalekken en de te verstrekken informatie.

Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

11. Data Protection Officer en register van verwerkingsactiviteiten

Mediwet heeft conform artikel 37 e.v. van de GDPR een Data Protection Officer (DPO) of Functionaris voor Gegevensbescherming aangesteld, welke te contacteren is via:

DPO Mediwet
Opvoedingstraat 143, 9000 Gent
Tel 09 221 06 07 – fax 09 221 78 67
e-mail: privacy@mediwet.be

Mediwet heeft ook een register van verwerkingsactiviteiten opgesteld conform artikel 30 e.v. GDPR. In dit register is per activiteit of proces omschreven wat de verwerkingsdoeleinden zijn, van welke categorieën van betrokkenen, wat de proces specifieke verwerkingsgrondslag is, hoe deze werden beveiligd, enz. Eventuele verduidelijkingen op basis van dit verwerkingsregister kan steeds bezorgd worden op eenvoudige vraag aan onze DPO.

12. Rechten van betrokkene

De GDPR garandeert aan alle betrokkene recht van inzage, verbetering, gegevenswissing, beperking en van bezwaar. Dit laatste recht zal meestal geen effect ressorteren aangezien Mediwet zich baseert op een wettelijke grondslag. Desalniettemin zal binnen de maand na ontvangst van het verzoek, de vraag beantwoord worden door Mediwet en dit conform artikel 12, 3° GDPR, waarbij in functie van de complexiteit deze termijn ook nog eens met twee maanden kan verlengd worden.

Voor inzage in het medisch dossier dient het verzoek gericht te worden tot de directeur afdeling medisch toezicht, Opvoedingstraat 143, 9000 Gent. Inzage in medische dossiers wordt niet rechtstreeks aan de werknemer gegeven, maar wel aan zijn/haar behandelende arts conform het advies van de Orde der Artsen van 7 september 1996.

Voor inzage in een psychosociaal dossier dient het verzoek te worden gericht aan de betrokken preventieadviseur-psychosociale aspecten.

13. Slotbepalingen

Deze Verwerkingsovereenkomst is onderdeel van de overeenkomst tussen Mediwet en de klant en geldt tot zolang deze overeenkomst duurt. Indien de overeenkomst eindigt, eindigt deze verwerkingsovereenkomst automatisch. De verwerkingsovereenkomst kan niet apart worden opgezegd.
Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkingsovereenkomst.

Na beëindiging van deze verwerkingsovereenkomst zullen de lopende verplichtingen, zoals het melden van datalekken, waarbij persoonsgegevens betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

Bij eventuele tegenstrijdigheden m.b.t. de bescherming van persoonsgegevens tussen de bepalingen in deze Verwerkingsovereenkomst en de Hoofovereenkomst, gelden de bepalingen uit deze Verwerkingsovereenkomst.

Op deze Verwerkingsovereenkomst is het Belgisch recht van toepassing. Over eventuele geschillen oordeelt de rechter bevoegd voor het arrondissement Gent.

Bijlage 1: DEFINITIES INZAKE GDPR

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD
van 27 april 2016
betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

Artikel 4
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

1) „**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 een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

2) „**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;

3) „**beperken van de verwerking**”: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;

4) „**profilering**”: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

5) „**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;

6) „**bestand**”: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

7) „**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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

8) „**verwerker**”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

9) „**ontvanger**”: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek

overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

10) „**derde**": 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;

11) „**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;

12) „**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;

13) „**genetische gegevens**": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

14) „**biometrische gegevens**": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

15) „**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;

16) „**hoofdvestiging**":

a. met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd;
b. met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

17) „**vertegenwoordiger**": een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

18) „**onderneming**": een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

19) „**concern**": een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

20) „**bindende bedrijfsvoorschriften**”: beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

21) „**toezichthoudende autoriteit**”: een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

22) „**betrokken toezichthoudende autoriteit**”: een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat:
a. de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd;
b. de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of
c. bij die toezichthoudende autoriteit een klacht is ingediend;

23) „**grensoverschrijdende verwerking**”:
a. verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of
b. verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;

24) „**relevant en gemotiveerd bezwaar**”: een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;

25) „**dienst van de informatiemaatschappij**”: een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad;

26) „**internationale organisatie**”: een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.

Mediwet

Bijlage 2: NOTIFICATIE VERWERKING PERSOONSGEGEVENS

MEDIWET
UW WERKWERELD, ONZE ZORG

GDPR
General Data Protection Regulation

Wat houdt het in?

Mediwet vzw, statutair gevestigd te Opvoedingstraat 143, 9000 Gent, met KBO-nummer: 0411.031.560, vertegenwoordigd door haar afgevaardigd bestuurder, de Heer Wim Schmitt, hecht veel belang aan een veilige, transparante en vertrouwelijke verzameling en verwerking van de persoonsgegevens.

Mediwet mag voor het uitvoeren van haar taken i.v.m. de Welzijnswetgeving uw persoonsgegevens verzamelen en verwerken tot 30 jaar na het bereiken van de normale pensioengerechtigde leeftijd, conform de GDPR wetgeving.

RECHT VAN INTREKKING VAN TOESTEMMING

U beschikt over het recht om voorafgaande toestemming i.v.m. de verwerking in te trekken.

RECHT OP INFORMATIE

We communiceren op een transpirante manier naar u waarom uw persoonsgegevens verzameld en verwerkt worden.

PROFILERING

We bevestigen dat u niet onderworpen bent aan automatische beslissingen of profilering o.b.v. de verwerkte persoonsgegevens.

RECHT OP TOEGANG EN INZAGE

U hebt toegang tot uw gegevens, en kan kosteloos nagaan waarvoor deze gebruikt worden.

RECHT VAN BEZWAAR

U mag bezwaar tekenen tegen de verwerking van uw persoonsgegevens wegens ernstige en legitieme motieven, zolang deze niet noodzakelijk zijn voor de uitvoering van onze wettelijke verplichtingen en zolang deze noodzakelijk zijn voor de doeleinden waarvoor deze werden verzameld.

RECHT OP RECTIFICATIE

U hebt het recht om incorrecte of onvolledige persoonsgegevens te verbeteren.

JUISTHEID

U bent verantwoordelijk voor alle gegevens die u ons verstrekt. Indien uw gegevens niet meer up-to-date zouden zijn, bent u verplicht om ons dit per kerende te melden.

RECHT OP OVERDRAAGBAARHEID

U hebt het recht om persoonsgegevens in een gestructureerde, leesbare vorm te krijgen en over te dragen aan een andere verantwoordelijke voor de verwerking.

RECHT OP VERWIJDERING OF BEPERKING

U mag ons verzoeken uw gegevens te wissen of de verwerking te beperken zolang wij deze niet noodzakelijk achten voor de uitvoering van onze wettelijke verplichtingen.

Data Protection Officer

Mediwet heeft een Data Protection Officer aangeduid die erop toeziet dat de verzameling en verwerking van persoonsgegevens correct verloopt.
We garanderen een gelijkaardig niveau van bescherming door contractuele verplichtingen tegenstelbaar te maken aan onze werknemers, medewerkers, aangestelden, die gelijkaardig zijn aan deze notificatie.

Bij vragen over GDPR kan u zich steeds wenden tot de DPO van Mediwet.

09 221 06 07
privacy@mediwet.be
DPO Mediwet, Opvoedingstraat 143, 9000 Gent

Inzagerecht

In het medisch dossier
U kan uw verzoek richten aan de Directeur afdeling Medisch Toezicht, Opvoedingstraat 143, 9000 Gent.
Inzage in medische dossiers wordt niet rechtstreeks aan de werknemers gegeven, maar wel aan zijn/haar behandelende arts.

In een psychosociaal dossier
U kan uw verzoek richten aan de betrokken preventieadviseur-psychosociaal welzijn.

Bepaalde persoonsgegevens die door ons worden verzameld, zullen worden doorgegeven aan en mogelijk verwerkt worden door derde dienstverleners, zoals de overheid, laboratoria, onze IT-leverancier, e.d. Deze gegevens kunnen evenwel doorgestuurd worden naar derde landen met een passend beschermingsniveau. In geen geval kan Mediwet vzw aansprakelijk worden geacht voor enige directe of indirecte schade die voortvloeit uit een foutief of onrechtmatig gebruik door een derde van de persoonsgegevens. Bij een inbreuk op uw rechten kan u een klacht neerleggen bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Drukpersstraat 35, 1000 Brussel. Tel. 02 274 48 00

Bijlage 3: Overzicht met beveiligingsmaatregelen

Technische beveiligingsmaatregelen

- ☐ Up to date besturingssysteem
- ☐ Up to date virusscan
- ☐ Up to date firewall
- ☐ Complexe wachtwoorden die regelmatig worden aangepast
- ☐ Logging systeem en wijzigingen
- ☐ Afzonderlijke login voor EOM software

Organisatorische beveiligingsmaatregelen

- ☐ Privacy policy met de medewerkers
- ☐ PC's altijd op lock screen indien de gebruiker tijdelijk de werkplaats vergaat en volledige shut down bij einde werkdag
- ☐ Laptop nooit onbewaakt achterlaten in de auto
- ☐ Beveiliging werkplaatsen
- ☐ Beveiligde vernietiging van oude documenten
- ☐ Zorgvuldig en beperkt gebruik van mobiele data
- ☐ Informatie Extranet enkel toegankelijk door algemene contactpersoon en de personen die door deze aangeduid zijn.
- ☐ Bijzondere aandacht voor bescherming van persoonsgegevens bij de evaluatie van onze processen en het opmaken van nieuwe interne instructies.

Bijlage 4: Proces rondom het melden van Datalekken en de te verstrekken informatie.

Een datalek is een beveiligingsincident waarbij persoonsgegevens mogelijk verloren zijn gegaan of onbedoeld toegankelijk worden gesteld voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Gegevensbeschermingsautoriteit.

- De website met logingegevens is gehackt of is toegankelijk voor derden.
- Verlies onvrijwillig of door diefstal van een laptop, tablet, telefoon (smartphone) of USB-stick met persoonsgegevens.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT systeem.

Indien er intern vastgesteld wordt dat er zich een beveiligingsincident voordeed, dan wordt dit onmiddellijk na de vaststelling ervan, gemeld aan de directie en de DPO.

Hierbij worden volgende zaken gemeld :

1. Er wordt een samenvatting gegeven van het beveiligingslek / beveiligingsincident / datalek: wat is er gebeurd? De naam van het betrokken systeem en/of leverancier wordt ook opgegeven.
2. Een overzicht van de typen persoonsgegevens die voorwerp zijn van het beveiligingsincident, wordt opgegeven (bijvoorbeeld naam, adres, e-mailadres, IP-nummer, rijksregisternummer, pasfoto en ieder ander tot een persoon te herleiden gegeven)
3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident?
4. Omschrijving groep personen om wiens gegevens het gaat. Gaat het om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend? Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek. Deze personen moeten in dat geval bereikt kunnen worden via de Verwerkingsverantwoordelijke.
6. Wat is de oorzaak (root cause) van het beveiligingsincident? Hoe is het beveiligingsincident kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?

Het is mogelijk dat niet al deze gegevens gekend zijn op het moment van het vaststellen van het datalek. Dit mag geen reden zijn om het datalek niet te melden. De melding dient sowieso te gebeuren, bij voorkeur met toelichting waarom bepaalde vragen (nog) niet kunnen beantwoord worden.

Na de melding beslist de directie in samenspraak met de data protection officer over het gepaste gevolg dat moet gegeven worden aan het datalek, waarbij mogelijk een melding van het datalek wordt gedaan aan de Gegevensbeschermingsautoriteit en in voorkomend geval aan de betrokkenen.
