

Privacyreglement, informatiebeveiliging en datalek protocol

Dit document voorziet in 3 reglementen betreffende persoonsgegevens.

Inhoudsopgave

Privacyreglement

1. Doel registratie en verwerking persoonsgegevens
2. Categorieën personen van wie gegevens worden verwerkt
3. Soorten geregistreerde gegevens
4. Verstrekken van gegevens aan derden
5. Verantwoordelijkheid, beheer en uitvoering
 - 5.1 Directiebeoordeling
6. Medische gegevens
7. Toegang tot persoonsgegevens
8. Geheimhouding
9. Inzage
10. Recht op verbetering, verwijdering, aanvulling of afscherming
11. Verzet
12. Bewaartermijn
13. Informatieverstrekking aan cliënt
14. Risicobeperking & doelstellingen
 - 14.1 check-up (interne audit)
 - 14.2 Externe audit

Informatiebeveiliging

1. Beveiliging
2. Controleorganen
 - intern
 - extern

Datalek

1. Registeren van het geconstateerde datalek
2. Besluit melden aan Autoriteit Persoonsgegevens
3. Besluit melden aan betrokkenen
4. Beoordeling noodzaak maatregelen
5. Vaststellen en doorvoeren maatregelen
6. Informeren en registeren van maatregelen
7. Evaluatie en herbeoordeling

1. Doel registratie en verwerking persoonsgegevens

De registratie van persoonsgegevens heeft uitsluitend tot doel relevante gegevens op te slaan en te leveren voor zover deze gegevens noodzakelijk zijn voor:

1. Het kunnen voorbereiden van zorgaanvragen ten behoeve van de persoon die hiertoe aan Haeck WorX een opdracht heeft verstrekt.
2. Het uitvoeren van administratieve procedures omtrent registratie, betaling, beschikkingen.
3. Het verstrekken van gegevens aan uitvoerende overheidsinstanties voor zover dit op grond van wettelijke regels verplicht, c.q. geoorloofd is en voor zover dit noodzakelijk is voor een doelmatige uitvoering van de dienstverlening van Haeck WorX.
4. Voor een juiste interne bedrijfsvoering van Haeck WorX.

2. Categorieën personen van wie gegevens worden verwerkt

Haeck WorX verwerkt uitsluitend gegevens over de volgende categorieën personen:

1. Clienten (en hun wettelijk vertegenwoordigers) die een hulpvraag indienen/waarover een beschikking is afgegeven.
2. Personeel
3. Contactpersonen van cliënten waarvoor de cliënt toestemming heeft gegeven.
4. Overige personen, voor zover noodzakelijk voor het uitvoeren van de diensten, en voor zover zij daarvoor toestemming hebben gegeven.

3. Soorten geregistreerde gegevens

1. Over cliënten worden de volgende persoonsgegevens verwerkt:
 - Voor- en achternaam, adres, geboortedatum, geslacht, bsn-nummer, bereikbaarheidsgegevens;
 - wensen van de zorgvrager met betrekking tot de zorgvraag, ook zijnde voorzieningen die niet via een wettelijk kader geregeld kunnen worden;
 - contactgegevens van zorgverleners (huisarts, specialist, maatschappelijk werk e.d.) voor zover relevant voor het verrichten van de diensten van Haeck WorX.
2. Over personeel word de volgende gegevens verwerkt:
 - naam, voorna(a)m(en), adres, woonplaats, geboortedatum, geslacht, bereikbaarheidsgegevens, gegevens identiteitsbewijs en zorgdisciplines waarvoor men kan worden ingezet;
 - wensen en eisen met betrekking tot de inzet bij (potentiële) cliënten van Haeck WorX.
3. Over instanties of andere zakelijke contacten worden de volgende gegevens verwerkt:
 - naam, adres(sen), vestigingsplaats(en), namen contactpersonen, nummer Kamer van Koophandel, BTW-nummer, bereikbaarheidsgegevens
4. Over de overige contactpersonen worden de volgende gegevens verwerkt:
 - Naam, contactgegevens

4. Verstrekken van gegevens aan derden

1. Wanneer derden gegevens opvragen zal de informatie alleen worden gegeven met toestemming van de betreffende persoon. Dit wordt geregistreerd via het tabblad 'contacten' in Zilliz. Accorderen geschiedt via het plan waarin de contactpersonen ook zijn toegevoegd.
2. Van het gestelde in lid 1 van dit artikel kan uitsluitend worden afgeweken, indien de inzage vragende partij het verzoek doet op basis van een wettelijke grondslag en het verzoek in overeenstemming is met de Wet of een uit de Wet voortvloeiende verplichting. In zulke gevallen wordt de cliënt altijd ingelicht.

5. Verantwoordelijkheid, beheer en uitvoering

De bestuurder van Haeck WorX is verantwoordelijk voor een degelijke verwerking van persoonsgegevens zoals beschreven in dit reglement. Het beheer en uitvoering kan worden gedelegeerd aan anderen, intern of extern. Verantwoordelijkheid met betrekking tot georganiseerde uitvoering wordt gecommuniceerd d.m.v. interne training bij hiervoor bedoelde bijeenkomsten in de organisatie. De training is bedoeld om het belang van gezamenlijk de informatiebeveiliging te waarborgen en de eventuele gevolgen op zowel cliëntniveau als

Privacyreglement, informatiebeveiliging en datalek Protocol 4.2 organisatieniveau te voorzien. De verantwoordelijkheid van de communicatie naar personeel ligt bij het bestuur van Haeck Worx. De verantwoordelijkheid van uitvoering en kennisneming ligt bij het personeel.

5.1 Directiebeoordeling

I.s.m. de intern & extern geplande audits controleert de directie het systeem rond informatiebeveiliging. Directie neemt hierbij mee:

- bevindingen van interne en externe audits & huidige doelstellingen
- risicoprioriteiten
- aansturing bij doelstellingen
- Eventuele feedback vanuit belanghebbenden
- visie op continuïteit van waarborging en ontwikkeling

Daarnaast overziet de directie **de bevoegdheid van personeel** in omgang met informatiebeveiliging. Dit is gebaseerd op de competentie en bevoegde diploma(s)/ervaring. Deze bevoegdheid wordt opgeslagen in het personeelsdossier.

6. Medische gegevens

1. Haeck WorX legt geen medische gegevens vast.
2. In tegenstelling tot wat is bepaald in lid 1 van dit artikel, kan Haeck WorX de beschikking krijgen over medische gegevens, indien voldaan is aan de volgende voorwaarden:
 - o de medische gegevens zijn afkomstig van de betreffende cliënt of een wettelijk vertegenwoordiger (ouder, curator); een bewindvoerder wordt in dit kader niet gezien als een bevoegde wettelijk vertegenwoordiger;
 - o de medische gegevens dienen ter ondersteuning van een zorgaanvraag of bezwaarprocedure; Indien de medische informatie niet meer actueel of nodig is wordt het verwijderd uit het dossier.

7. Toegang tot de persoonsgegevens

1. De personen met toegang tot de persoonsgegevens:
 - De bestuurder van Haeck WorX voor zover noodzakelijk voor de uitoefening van toezicht;
 - Medewerkers van Haeck WorX voor zover noodzakelijk voor de uitoefening van hun taak.

8. Geheimhouding

De bestuurder en alle (ex-)medewerkers van Haeck WorX zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen.

9. Inzage

1. Degene, van wie gegevens zijn geregistreerd heeft recht op inzage van de hem of haar betreffende gegevens.
2. Haeck WorX deelt op diens verzoek uiterlijk binnen vier weken de opgevraagde informatie. Dit gebeurt door toegang in het eigen ECD via het portaal, of de documenten worden per email verstuurd.
3. Indien inzage niet kan worden verleend zonder dat daarbij inzage wordt gegeven in de gegevens van andere personen, dienen die andere personen eerst toestemming te verlenen.
4. Inzage wordt slechts geweigerd voor zover dit noodzakelijk is voor de bescherming van de cliënt of van de rechten en vrijheden van anderen. Verzoeker wordt geïnformeerd over de mogelijkheid hiertegen bezwaar te maken.

10. Recht op verbetering, verwijdering, aanvulling of afscherming van persoonsgegevens

1. De cliënt kan verzoeken de op hem/haar betrekking hebbende persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien de gegevens feitelijk onjuist zijn of niet ter zake doen, dan wel indien de gegevens in strijd met dit reglement zijn opgenomen.
2. Een verzoek als bedoeld in lid 1 van dit artikel wordt schriftelijk bij Haeck WorX ingediend. Het verzoek bevat de aan te brengen wijzigingen.
3. Indien Haeck WorX van mening is dat het verzoek gegrond is, draagt deze er zorg voor dat de noodzakelijke verbetering, aanvulling, verwijdering of afscherming binnen 4 weken nadat het verzoek is ontvangen, plaatsvindt, waarna hij cliënt dit schriftelijk meedeelt.
4. Indien Haeck WorX van mening is dat het verzoek niet of niet geheel gegrond is, wordt dit binnen vier weken en met redenen omkleed schriftelijk meegedeeld aan verzoeker, waarbij deze tevens geïnformeerd wordt over de mogelijkheid hiertegen bezwaar te maken.

11. Verzet

1. De cliënt kan op grond van bijzondere persoonlijke omstandigheden bij Haeck WorX verzet aantekenen tegen verwerking, of bepaalde verwerkingen, van zijn persoonsgegevens. Verzet is niet mogelijk tegen verwerkingen die plaatsvinden op grond van een wettelijke verplichting of op grond van toestemming van de cliënt.
2. Haeck WorX beoordeelt binnen vier weken na ontvangst van het verzet of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is, wordt de verwerking waartegen dit is gericht, beëindigd.
3. Indien Haeck WorX het verzet niet gerechtvaardigd acht, wordt dit schriftelijk aan de cliënt bericht, waarbij deze tevens geïnformeerd wordt over de mogelijkheid hiertegen bezwaar te maken.

12. Bewaartermijn

De geregistreerde gegevens worden verwerkt voor zover en zolang zij nodig zijn voor een goede vervulling van opdracht en taakstelling van Haeck WorX. De persoonsgegevens worden in ieder geval bewaard gedurende de looptijd van de overeenkomst met de cliënt en gedurende maximaal vijftien jaren na beëindiging van de overeenkomst voor WMO cliënten en 20 jaar voor WLZ cliënten. Daarna worden gegevens vernietigd.

13. Informatieverstrekking aan cliënt

De cliënt wordt bij aanvang van hulpverlening gewezen op informatie en de bron waar hij/zij deze opnieuw kan inzien. De informatie betreft o.a. dit reglement over privacy, het klachtenprotocol en dergelijke.

14. Risicobeperking & doelstellingen

Om de kwaliteit van informatiebeveiliging en daaraan verwante zaken te waarborgen heeft Haeck Worx, door zowel intern als externe partijen, momenten van reflectie en input. Extern verkrijgt HW feedback van betrokken zorgpartners & middels samenwerking met de HKZ. Intern verkrijgt Haeck Worx feedback door ICT-personeel & beleidsmedewerkers. D.m.v. een jaarplanning waarin protocol check-ups staan ingepland waarborgen we een continue verbetering van o.a. informatiebeveiliging. Door middel van deze geplande check-ups wordt er dus vast gemonitord, gemeten & geëvalueerd. Via het SMART formuleren van doelstellingen en de jaarplanning wordt er methodisch gehandeld in het bovenstaande.

14.1 check-up (interne audit)

Tijdens een check-up wordt er geëvalueerd op eventuele signalen (lees; externe & interne ontwikkelingen). Zodoende benut Haeck Worx eventuele kansen om het systeem effectiever toe te passen en risico's voor te zijn. Bij een check-up wordt er afgesloten met een nieuwe doelstelling voor aankomende periode die geprioriteerd wordt middels de mate waarin er risico op onveiligheid mogelijk is. N.a.v. de mate van prioriteit wordt er SMART een PvA geformuleerd en gedelegeerd.

De check-up wordt uitgevoerd door aangestelde auditoren. Zij documenteren de bevindingen van het bovenstaande en houden de monitoring en uit te voeren doelstellingen meetbaar.

14.2 Externe audit

Een onafhankelijke partij bewerkstelligd een audit met als grond de eisen van ISO 27001:2022. Zij geven d.m.v. een samengestelde rapportage advies aan Haeck Worx, rekening houdend met de bedrijfsvoering, voorgaande audits & hun eigen objectiviteit. Deze rapportage wordt overgedragen aan het relevante management (zie; H5). Eerdere aanbevelingen en daaruit volgende feedback (lees; maatregelen door geformuleerde doelstellingen), worden geanalyseerd meegenomen in het rapport bij zowel het behalen als het verbeteren ervan. Zodoende blijft de continue kwaliteitsverbetering gewaarborgd.

Informatiebeveiliging van de persoonsgegevens

Doel

Het bewaren van gegevens die nodig zijn om goede zorg te bieden.

Organisatie

Clientgebonden documenten kunnen door elke functie in het ECD worden geplaatst. Wanneer het op extern gezet wordt, zijn de gegevens ook in te zien door de client via het extranet.

Organisatiegebonden documenten kunnen door overheadfuncties op sharepoint worden geplaatst.

Mogelijkheid autorisatie is lezen, bewerken of volledige toegang volgens het principe Least Privilege.

Documenten worden op categorie geplaatst en volgens het reglement Documentbeheer.

Ontheffingen (uitzonderingen)

Medische gegevens rapporteren wij niet. Alleen als de client zelf medische gegevens verstrekt en deze nodig zijn voor het leveren van de juiste zorg worden deze opgeslagen.

Rapporteren en overtredingen

Er wordt gerapporteerd volgens het Beleid Clientdossier. Bij overtredingen wordt de werknemer aangesproken en maatregelen afgesproken.

Het managementsysteem voor informatiebeveiliging

Het managementsysteem voor informatiebeveiliging is opgezet in 'het sturingsdocument'. Dit document is het onderdeel van het kwaliteitsmanagementsysteem van Haeck WorX.

Het borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Omdat het management voor informatiebeveiliging aan dezelfde eisen dient te voldoen als alle andere vlakken die onderdeel zijn van ons brede kwaliteitsmanagementsysteem, hebben we de informatiebeveiliging hierin meegenomen. De contextanalyse, SWOT analyse, doelen en KPI's, registreren van incidenten en signalen en de opvolging daarvan (verbetermaatregelen) zijn allemaal te vinden in het sturingsdocument. Ook de evaluatie geschiedt regelmatig en wordt meegenomen in de directiebeoordeling. Zo verbeteren we, voortdurend.

Een groot aantal punten vanuit de HKZ norm zijn al meegenomen in het privacy reglement.

Informatie die niet al eerder aan bod is gekomen of nog eens bedrukt wordt staat hieronder vermeld:

Om te voorkomen dat privacygevoelige informatie bij onbevoegden terecht komt, hebben we de volgende beveiliging:

- Onze digitale systemen zijn beveiligd met tweestaps verificatie waarbij wachtwoorden met regelmaat worden gewijzigd.
- Er wordt niet gewerkt met papieren dossiers of losse notities.
- In contact met gemeentes maken we gebruik van de beveiligde omgeving van de gemeente met een persoonlijk tijdelijk wachtwoord die de gemeente verzorgd.
- We werken met het principe Least Privilege. Iedereen krijgt alleen toegang tot wat nodig is.

Om te voorkomen dat privacygevoelige informatie bij onbevoegden terecht komt, en om te leren en verbeteren hebben wij de volgende controle organen:

Intern

- Er is een interne privacy functionaris aangesteld aandacht heeft voor privacy in het bedrijf. Deze toetst door middel van steekproeven of er voldoen wordt aan het reglement. Ook houdt deze functionaris de dagelijkse gang van zaken in de gaten en koppelt signalen terug. Dit registreert de functionaris in het sturingsdocument.
- Elke functie is verantwoordelijk voor het registreren van signalen, klachten en incidenten rondom privacy in ons kwaliteitssysteem. De beleidsmedewerker analyseert elk kwartaal, en zo is er inzichtelijk of

de opvolging naar wens en protocol verlopen is. Tevens kan er een tendens worden herkend. In dit geval is er een verplichting tot het nemen van maatregelen en opnemen in het jaarplan.

- De ICT-medewerker controleert elk kwartaal de toegang tot de systemen. Hierbij is aandacht voor de bevoegdheden per personeelslid.
- De ICT-medewerker deelt jaarlijks kennis rondom veiligheid en kan testen door middel van fake-links of personeel voldoende kundig is.
- Een extern adviesbureau, Buro KliX, neemt jaarlijks een interne audit af. Er volgt binnen een maand een rapport met de uitkomsten van het onderzoek. Indien er maatregelen vereist zijn, is hier een hersteltermijn van 3 maanden voor.
- Het documentenplatform biedt audit logs zodat er inzichtelijk is wie op welk moment een document heeft geopend, gewijzigd of verwijderd.

Extern

- Het Keurmerk Instituut neemt jaarlijks een audit af. Er volgt binnen een maand een rapport met de uitkomsten van het onderzoek. Indien er maatregelen vereist zijn, is hier een hersteltermijn van 3 maanden voor. Met positieve afronding blijft het HKZ certificaat geldig.
- Haeck WorX heeft jaarlijks één of meerdere quickscans of uitgebreide audits door de VGGM in opdracht van een gemeente. Hieruit voortvloeiend volgt een verslag waarbij indien nodig een hersteltermijn van 3 maanden is voor verbetermaatregelen.

Data lek

1. Registreren van het geconstateerde datalek

Het datalek wordt als incident geregistreerd middels een incidentmelding en wordt direct doorgegeven aan de directie en kwaliteitsmedewerker. De directie beoordeelt het gerapporteerde beveiligingsincident in samenspraak kwaliteitsmedewerker.

2. De directie besluit of het datalek gemeld moet worden aan de Autoriteit Persoonsgegevens.

Een datalek hoeft alleen gemeld te worden als dit leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens of als een aanzienlijke kans bestaat dat dit gebeurt.

Bij een meldingsplicht dient het datalek te worden gemeld middels het formulier '[Meldloket datalekken](#)' dat te vinden is op de website van de Autoriteit Persoonsgegevens.

3. De directie besluit of het datalek gemeld moet worden aan de betrokkenen (werknemer/cliënt)

De betrokkenen hoeven alleen geïnformeerd te worden als een datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer. De melding aan de betrokkenen mag eventueel achterwege gelaten worden als er passende technische beschermingsmaatregelen zijn getroffen, waardoor de gelekte persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor onbevoegden door bijvoorbeeld goede encryptie.

4. Het beoordelen van de noodzaak om maatregelen te treffen wordt uitgevoerd door directie in samenwerking met de kwaliteitsmedewerker.

Als de oorzaak bekend is, wordt bekeken of het noodzakelijk is om corrigerende maatregelen te treffen. De beslissing om te komen tot corrigerende maatregelen dient beoordeeld te worden tijdens de vaste overleggen of tussentijds in overleg met de directie.

5. Het vaststellen en doorvoeren van de benodigde maatregelen wordt vastgelegd in notities, e-mails/brieven, verslagen, procedures of rapporten.

Alle betrokkenen worden geïnformeerd en verzocht te handelen zoals de maatregel aangeeft.

6. Afhankelijk van de uitslag van de beoordeling wordt vastgesteld of een herbeoordeling noodzakelijk is, of er wederom maatregelen genomen moeten worden, of dat de maatregel voldoende is geweest.

Verificatie van de doeltreffendheid van maatregelen wordt gedaan bij het vaststellen van de doeltreffendheid van de afgehandelde actiepunten.

Sanctiebeleid

Sancties zoals bepaald in de arbeidsovereenkomst als onderdeel van de geheimhoudingsverklaring voor met name bewuste acties die de organisatie schaadt zijn o.a. ontslag op staande voet en/of het verhalen van de gevolgschade op de betrokken personeelsleden. Sancties m.b.t. slecht omgaan met bedrijfsmiddelen zijn gericht op het verhalen van de reparatiekosten aan de bewuste persoon/personen.

Indien werkzaamheden worden uitbesteed aan derden dan wordt er met deze leveranciers / freelancers een verwerkingsovereenkomst afgesloten.