Privacy & informatiebeveiligingsbeleid

1. Inleiding

Bij privacy gaat het wettelijk gezien om alle gegevens die te herleiden zijn tot een bepaald persoon. Alles wat met die persoonsgegevens wordt gedaan, wordt 'verwerken' genoemd. Denk hierbij aan: verzamelen, kopiëren, opslaan, publiceren, vernietigen en delen. Umah Hai vindt het belangrijk om zorgvuldig om te gaan met gegevens van betrokkenen zoals cliënten en medewerkers. Gegevens worden beschermd door enerzijds fysieke informatie in een afgesloten kast op te bergen en anderzijds door bijvoorbeeld elektronische gegevens af te schermen door middel van een toegangsbeveiliging.

Er zijn diverse wetten waarin bepalingen zijn opgenomen over privacy en informatiebeveiliging. Denk hierbij onder andere aan de Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg, Wet Maatschappelijke Ondersteuning, Wet Langdurige Zorg, de Jeugdwet en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (gebruik burgerservicenummer in de zorg).

Verwerking van persoonsgegevens

De verwerking van persoonsgegevens is geregeld in de Algemene Verordening Gegevensbescherming (AVG) die geldt voor de gehele Europese Unie (EU). De algemene verordening gegevensbescherming geeft burgers die hun persoonsgegevens verstrekken verschillende privacyrechten en draagt degenen die deze persoonsgegevens verwerken gelijktijdig enkele plichten op. Voor een aantal specifieke nationale aspecten is de Uitvoeringswet van de AVG in Nederland van kracht. Hierin zijn onder andere de bevoegdheden van de Autoriteit Persoonsgegevens geregeld.

De nieuwe Algemene Verordening Gegevensbescherming (AVG) kent de volgende uitgangspunten:

- Bewustwording
- Rechten van betrokkenen
- Overzicht van verwerkingen
- Gegevensbeschermingseffectbeoordeling
- Functionaris voor de gegevensbescherming (FG)
- Privacy by design & privacy by default
- Meldplicht datalekken
- Verwerkersovereenkomsten

- Toestemming

Informatiebeveiliging

Informatiebeveiliging omvat een samenhangend stelsel van maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en systemen te kunnen blijven realiseren.

Per 1 juli 2017 is de Wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg deels in werking getreden. Per 1 juli 2020 is de wet volledig in werking. Deze wet verplicht zorginstellingen om de informatiebeveiliging conform de NEN normen in te richten. De NEN normen zijn opgesteld door de Stichting Nederlands Normalisatie-instituut en specifiek gericht op de zorg:

- NEN 7510: norm voor het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg;
- NEN 7512: nadere invulling van NEN 7510 betreffende de veiligheid van gegevensuitwisseling tussen partijen in de zorg
- NEN 7513: nadere invulling van NEN 7510 betreffende het vastleggen van acties op elektronische cliëntendossiers

2. Visie, reikwijdte en uitgangspunten

Visie

Umah Hai vindt het vanzelfsprekend en van groot belang dat zorgvuldig en conform wet en regelgeving wordt omgegaan met (privacy)gevoelige gegevens. Daarbij vindt Umah Hai het belangrijk dat met de gegevens van een ander wordt omgegaan zoals iedereen zou willen dat er met de eigen (persoons)gegevens wordt omgegaan. Dit betekent bewust gedrag van iedere medewerker. Bij het maken van keuzes wordt rekening gehouden met onderstaande punten:

- Privacy en gegevensbescherming mag de zorg niet in de weg staan
- Er wordt gezocht naar een passend evenwicht tussen gebruikersgemak en gegevensbescherming
- Uitgangspunt is altijd het vertrouwen in de professionaliteit van de medewerker, er vindt tevens controle plaats (auditabilaty)
- Zorgvuldigheid staat voorop maar het helemaal uitsluiten van datalekken is niet mogelijk

Reikwijdte

Dit privacybeleid is van toepassing op alle processen: van uitvoering van zorg, uitbesteding, inkoop, deelname in een gemeenschappelijke regeling tot aan uitwisseling van gegevens met derden. Daarbij gaat het om zowel papieren als digitale informatie. Het omvat de gehele datacyclus: van genereren van gegevens, het dagelijkse gebruik daarvan, gegevensopslag tot en met vernietiging ervan.

Uitgangspunten

We hanteren de volgende uitgangspunten:

- **Legitimiteit:** verwerking van gegevens vindt uitsluitend plaats voor zover dit wettelijk gerechtvaardigd is. Er moet een noodzaak zijn

- **Doelbinding:** gegevens worden alleen verwerkt om het vastgestelde doel te bereiken. De gegevens worden niet gebruikt voor doeleinden die onverenigbaar zijn met (of niet herleidbaar zijn tot) het oorspronkelijke doel waarvoor de gegevens nodig zijn

- **Subsidiariteit:** het vastgestelde doel kan niet met minder dan de verzamelde gegevens worden bereikt

- **Proportionaliteit:** de verzamelde gegevens staan in verhouding tot het vastgestelde doel. Er worden geen onnodige gegevens verzameld

- **Kwaliteit:** de verzamelde gegevens zijn juist, nauwkeurig en voldoende actueel

- **Informatieveiligheid:** de verzamelde gegevens staan op een veilige plek en er wordt gezorgd voor adequate toegangsbeveiliging.

- **Houdbaarheid:** gegevens die niet langer nodig zijn, worden onomkeerbaar vernietigd (tenzij dit wettelijk anders is bepaald) of geanonimiseerd. Betrokkene heeft het recht om vergeten te worden.

Gegevensbeschermingseffectbeoordeling

De nieuwe privacywet (AVG) verplicht organisaties om een gegevensbeschermingseffectbeoordeling uit te voeren. Een gegevensbeschermingseffectbeoordeling is een risico analyse op het gebied van privacy en informatiebeveiliging. Een instrument om voorafgaand de risico's van de verwerking van persoonsgegevens in kaart te brengen, zodat maatregelen genomen kunnen worden om deze risico's te beperken.

Een dergelijke beoordeling is een instrument dat ingezet wordt bij aanschaf van een applicatie of bij het opstarten van een project. Dit instrument geeft inzicht welke risico's er zijn met betrekking tot de verwerking van persoonsgegevens zodat er vooraf maatregelen genomen kunnen worden om

deze risico's te beperken. Umah Hai zal een gegevensbeschermingseffectbeoordeling inzetten in de volgende situaties:

- bij aanschaf van een systeem waarbij persoonsgegevens worden gebruikt
- bij grote update van een systeem
- bij projecten waarbij persoonsgegevens gedeeld worden met derden

Privacy by design & privacy by default

De begrippen Privacy by design & privacy by default zijn in de AVG belangrijke uitgangspunten. *Privacy by design* houdt in dat al bij het ontwerp van nieuwe producten wordt nagedacht over de verwerking van persoonsgegevens, onder andere hoe deze worden beschermd, opgeslagen en/of worden gedeeld. *Privacy by default* houdt in dat er technische maatregelen genomen worden die ervoor zorgen dat niet meer dan de noodzakelijke persoonsgegevens worden verwerkt en dat daarvoor op de juiste wijze toestemming wordt gevraagd.

3. Privacy framework

Het privacy framework is een overzicht van de aspecten van privacy waar Umah Hai mee bezig is. In dit framework wordt onderscheid gemaakt tussen beleid, awareness / risico inventarisatie en de tools die Umah Hai hiervoor inzet.

	Verantwoording	
Beleid	Awareness en risico inventarisatie	Hulpmiddelen
Privacy en informatiebeveiligingsbeleid	Awareness programma	Privacy administratie
Privacyverklaringen	Analyse datalekken	Website
Autorisatie en Authenticatiebeleid	Periodieke controle op autorisaties	
Gedragsregels en geheimhoudingsverklaringen	Risico inventarisatie vanuit NEN 7510	
	Onderzoeken	
	Periodieke beveiligings en penetratietesten	

3.1 Verantwoording

Privacy en informatiebeveiliging is een onderdeel van governance & compliance. Umah Hai heeft besloten om jaarlijks een verklaring van accountability te schrijven waarin aan alle stakeholders

uitgelegd wordt hoe Umah Hai met de bescherming van persoonsgegevens omgaat. Deze verklaring is bestemd voor cliënten, medewerkers, leveranciers, financiers en andere geïnteresseerden.

3.2 Beleid

In deze paragraaf zijn alle aspecten van het beleid rondom privacy en informatiebeveiliging beschreven.

Privacy en informatiebeveiligingsbeleid

Het privacy en informatiebeveiligingsbeleid (verder te noemen privacybeleid) geeft richting aan de invulling van de privacyreglementen en de visie en uitgangspunten die Umah Hai hanteert met betrekking tot privacy en informatiebeveiliging vraagstukken. Het doel van het privacybeleid is om de kaders te stellen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens die voldoet aan de wettelijke eisen.

Privacyverklaringen

In privacyverklaringen geven we aan betrokkenen aan welke gegevens we van ze verwerken, de manier waarop we dat doen, of de gegevens aan anderen verstrekt worden of buiten Europa, hoe lang we persoonsgegevens bewaren en hoe we deze beveiligen. Daarnaast wordt in deze verklaringen aangegeven wat de rechten van betrokkenen zijn en waar ze terecht kunnen met vragen, verzoeken of klachten. De verklaringen zijn op de website van Umah Hai geplaatst. Er zijn twee privacyverklaringen:

- cliënten
- medewerkers, externen, stagiaires, vrijwilligers en sollicitanten

Van de privacyverklaring voor cliënten is ook een verkorte versie beschikbaar.

Autorisatie en authenticatie beleid

Het autorisatiebeleid geeft aan wie waarvoor toegang heeft in een bepaalde applicatie en welke periodieke controle daarop plaatsvindt. Authenticatie is het proces waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn.

De uitgangspunten voor de autorisatie van het inzien en verwerken van persoonsgegevens hebben betrekking op onze organisatie waarden:

- de cliënt staat centraal
- zoveel mogelijk samen met de cliënt of medewerker - open communiceren
- we werken vanuit vertrouwen
- bewust handelen door altijd de vraag te stellen of delen van gegevens wel noodzakelijk is
- professionaliteit vanuit herstelvisie - gelijkwaardigheid

Het uitwisselen van gegevens met de behandelaar is geregeld in de zorgovereenkomst zodat medewerkers niet steeds opnieuw toestemming hoeven te vragen om gegevens te kunnen uitwisselen met de behandelaar.

De toegang tot een medewerkersdossier is beperkt tot de directe leidinggevende en de salarisadministratie.

In het autorisatie en authenticatie beleid wordt vastgelegd wie waar toegang tot mag hebben.

Gedragsregels informatiebeveiliging en geheimhoudingsverklaring

In de gedragsregels voor informatiebeveiliging wordt beschreven hoe wij willen omgaan met privacy, maar ook clean desk policy en het gebruik van social media. Om ervoor te zorgen dat iedereen zich ook daadwerkelijk verbindt aan de gedragsregels tekenen externen een geheimhoudingsverklaring en krijgen medewerkers een aanvulling op de arbeidsovereenkomst.

3.3 Awareness en risico inventarisatie

Awareness programma

Umah Hai vindt het belangrijk dat haar medewerkers beschikken over voldoende kennis over privacy en informatiebeveiliging en in staat zijn om deze kennis toe te passen in de praktijk. Om in deze kennis en vaardigheden te voorzien zijn er regelmatig training sessies en wordt informatie gedeeld over nieuwe ontwikkelingen.

Analyse van datalekken

Datalekken wordt gemeld bij het bestuur en/of Odetta en onderzocht. Aan de hand van de analyse van de datalekken worden risico´s onderkent en maatregelen genomen.

Periodieke controle op autorisaties

De autorisatierechten in kernapplicaties worden twee keer per jaar gecontroleerd. Bij de overige applicaties worden de autorisaties jaarlijks gecontroleerd.

Risico inventarisatie vanuit de NEN 7510

Aan de hand van alle mogelijke bedreigingen heeft Umah Hai haar risico´s ten aanzien van informatiebeveiliging vastgesteld. Op basis van deze risico´s is gekeken welke maatregelen vanuit de NEN 7510 op Umah Hai van toepassing zijn en welke acties Umah Hai moet gaan nemen om hieraan te voldoen.

Onderzoeken

Aan de hand van signalen en incidenten worden onderzoeken gedaan naar het informatiebeveiliging aspect van processen en systemen. Eventuele verbeterpunten worden opgepakt.

Periodieke beveiligings en penetratietesten

Umah Hai voert periodieke beveiligings en penetratietesten. Een penetratietest is een onderzoek naar kwetsbaarheden in computersystemen.

3.4 Hulpmiddelen

privacy administratie

In de privacy administratie van Umah Hai zijn alle verwerkingen van persoonsgegevens omschreven met de doelen waarvoor de geadministreerd zijn, de rechtmatigheid grondslag en de bewaartermijn. Daarnaast zijn alle partijen met wie Umah Hai persoonsgegevens uitwisselt in kaart gebracht, alle onderzoeken die gedaan zijn en de analyse van de datalekken.

website

De website van Umah Hai wordt gebruikt om informatie te delen met de betrokkenen van wie persoonsgegevens verwerkt worden.

4. Rollen en overlegstructuur

In dit hoofdstuk is per rol aangegeven wat de verantwoordelijkheden en bevoegdheden zijn van alle medewerkers van Umah Hai en de overlegstructuur rondom privacy en informatiebeveiliging.

4.1 Omschrijving van rollen

Raad van bestuur

De raad van bestuur is eindverantwoordelijk voor de naleving van de privacy en informatiebeveiliging wetgeving. Om aan deze verantwoordelijkheid te voldoen zijn de volgende keuzes gemaakt:

- de raad van bestuur stelt het privacy & informatiebeveiligingsbeleid vast, handhaaft en evalueert
- er wordt een privacy administratie ingericht voor het registreren van alle verwerkingen, onderzoeken, datalekken en beheersmaatregelen op het gebied van privacy vraagstukken en datalekken
- de raad van bestuur stelt een medewerker aan die de privacy administratie bijhoudt en datalekken onderzoekt, voor de borging van kennis wordt waar nodig voorzien in externe expertise
- er wordt extern advies ingehuurd om ervoor te zorgen dat de juiste expertise aanwezig is

De raad van bestuur moet samen met de medewerkers invulling geven aan de volgende verantwoordelijkheden:

- houden van toezicht op en toetsen dat er gehandeld wordt conform het privacybeleid en de gedragsregels middels audits door externe adviseur
- zorgen voor voldoende bewustzijn bij deelnemers en medewerkers omtrent privacy
- uitvoeren van gegevensbeschermingseffectbeoordelingen
- afhandeling van datalekken

- toezien op applicatie controls:
    - bijhouden van het applicatie logboek (alle wijzigingen met betrekking tot applicaties)
    - ervoor zorgen dat de back-up en recovery geregeld is

- het testen van nieuwe updates en vastleggen van testresultaten
- het up to date blijven en uitvoeren van nieuwe updates
- het regelen van rechten en toegang conform het autorisatiebeleid en de controle daarop.
- het regelen van ondersteuning bij de leverancier of een andere partij indien er calamiteiten zijn

Functionaris voor de gegevensbescherming (FG)

Zorginstelling moeten afhankelijk van de hoeveelheid medische gegevens een functionaris gegevensbescherming aanstellen. Umah Hai heeft onderzocht of deze verplichting ook voor haar geldt. Omdat het aantal betrokkenen waarvan Umah Hai gegevens verwerkt beperkt is en Umah Hai werkt in een beperkt geografisch gebied heeft de raad van bestuur besloten om geen functionaris gegevensbescherming aan te stellen. De exacte uitwerking van deze overweging en het wettelijk kader van deze beslissing is een apart document vastgelegd.

Extern adviseur

Om ervoor te zorgen dat er voldoende inhoudelijke kennis is op het gebied van privacy en informatiebeveiliging huurt Umah Hai een extern adviseur in. Deze adviseur stelt documenten op, zorgt dat externe ontwikkelingen op het gebied van privacy en informatiebeveiliging op de agenda komen en geeft awareness trainingen.

Coördinator activiteiten en facilitair

De coördinator activiteiten en facilitair is verantwoordelijk voor het applicatiebeheer, de administratieve inrichting van de organisatie en de contacten met ICT leveranciers.

Medewerker privacy en informatiebeveiliging

De medewerker privacy en informatiebeveiliging houdt de privacy administratie bij begeleid de afhandeling van datalekken.

Medewerkers
Medewerkers nemen kennis van en handelen conform de kaders van het privacybeleid en gedragscode. Dit geldt ook voor stagiaires, inhuur van extern bureaus, ZZP-ers, uitzendkrachten, vrijwilligers.

4.2 Overlegstructuur

Door de beperkte omvang van de organisatie is de overlegstructuur op het gebied van privacy en informatiebeveiliging compact. De stuurgroep privacy en informatiebeveiliging bestaat uit de raad van bestuur, de coördinator activiteiten en facilitair, de medewerker privacy en informatiebeveiliging, een vertegenwoordiging van cliënten en de extern adviseur.

De stuurgroep richt zich op het opstellen van het beleid en de naleving ervan. Verbeterpunten en risico´s worden besproken en beheersmaatregelen worden geformuleerd

5. Rechten van betrokkene

Betrokkenen hebben rechten en kunnen klachten en verzoeken indienen, ook als het gaat om privacy. Binnen Umah Hai streven we ernaar om zoveel mogelijk de klacht in goed overleg af te handelen. Daarnaast kunnen betrokkenen gebruikmaken van de klachtencommissie. Een betrokken mag ook altijd direct een klacht indienen bij de Autoriteit persoonsgegevens.

Betrokkene hebben de volgende rechten:

- het recht op informatie over het doel van een betreffende informatieverwerking
- het recht op inzage in de eigen gegevens
- het recht op het laten verbeteren of verwijderen van de eigen gegevens
- het recht om vergeten te worden. Betrokkene kunnen te allen tijde een verzoek doen te worden geschrapt uit een registratie of administratie. Hier dient altijd gehoor aan te worden gegevens tenzij door wetgeving anders wordt bepaald
- het recht om tegen het gebruik van hun gegevens verzet aan te tekenen. Umah Hai dient dan een afweging te maken en te communiceren
- het recht op dataportabiliteit of gegevensoverdraagbaarheid, de mogelijkheid om persoonsgegeven van het ene platform probleemloos naar een ander platform over te brengen. Met dit recht kan een betrokkene bijvoorbeeld zijn begeleidingsdossier overdragen van de ene naar de andere zorgverlener.
- recht op beperking van de verwerking
- recht om niet te worden onderworpen aan profiling, een proces waarbij persoonsgegevens worden verwerkt om een verband aan te tonen tussen kenmerken van individuen en hun gedrag, met als doel voorspellingen te maken van toekomstig gedrag

6. Gegevens verwerken

Alle medewerkers van Umah Hai verwerken persoonsgegevens uitsluitend voor zover dit valt binnen hun functie binnen vooraf duidelijke, omschreven en gerechtvaardigde doelen. Persoonsgegevens mogen alleen worden verwerkt op basis van de volgende grondslagen (AVG):

- nakoming van wettelijke plichten
- ter bestrijding van een ernstig gevaar voor de gezondheid van de betrokkene(n)
- totstandkoming of uitvoering van een overeenkomst
- behartiging van een gerechtvaardigd belang van Umah Hai of een derde aan wie gegevens worden verstrekt
- ondubbelzinnige toestemming van de betrokkene

Zonder een grondslag is de verwerking van persoonsgegevens dus niet toegestaan.

Umah Hai verwerkt onder andere gegevens van cliënten, medewerkers, stagiaires, inhuurkrachten en vrijwilligers. Binnen Umah Hai is een autorisatieprotocol van kracht. Hierin is vastgelegd wie toegang heeft tot welke gegevens. Bijvoorbeeld op basis van functiegroep of werklocatie of een combinatie hiervan.

Twee hoofdcategorieën van verwerkingen zijn hieronder omschreven. Naast deze verwerkingen zijn er nog diverse andere verwerkingen die verder uitgewerkt zijn in de privacy administratie.

Cliëntgegevens administreren

Om goede zorg te kunnen verlenen, werken we met cliëntendossiers. Hierin staat alle belangrijke informatie over een cliënt vanuit het oogpunt van de begeleiding. Het dossier zorgt ervoor dat informatie voor begeleiders volledig, toegankelijk en overdraagbaar is.

Het dossier geeft informatie over de gezondheid van de cliënt. Informatie over de gezondheid is een onderwerp dat in de AVG aangemerkt staat als ‘bijzondere gegevens’. Bijzondere gegevens worden door deze wet extra beschermd. Indien de gegevens toch gedeeld worden, is er extra risico op

nadelige gevolgen voor de persoon waarover het gaat. Bij Umah Hai worden de cliëntgegevens verwerkt in het elektronisch cliëntendossier. Het verwerken van persoonsgegevens met betrekking tot de gezondheid mag alleen gebeuren door personen, die direct bij de behandeling of begeleiding van de cliënt betrokken zijn.

Medewerkergegevens administreren

Elke medewerker heeft een medewerkersdossier waar onder andere de volgende items zijn opgenomen: salarisgegevens, arbeidsovereenkomst, secundaire voorwaarden, ziekteverzuim en reïntegratie, functioneringsgesprekken, opleiding en sollicitatie. Wanneer het gaat om het verwerken van gegevens over de gezondheid van een medewerker wordt dit alleen bijgehouden door de ARBO dienst. Met Umah Hai worden gegevens gedeeld die nodig zijn voor de reïntegratie.

Anonimiseren van gegevens

In rapportages of verslagen kunnen ook mede-cliënten, medewerkers of naasten worden genoemd. Omdat het dossier alleen voor hulpverleners of de cliënt zelf is in te zien, hoeven deze gegevens niet te worden geanonimiseerd.

Gegevens van derden die niet noodzakelijk zijn voor een goede overdracht of heldere rapportage, worden niet opgenomen in de rapportage.

In e-mailberichten worden geen namen genoemd in de onderwerpregel. Hierbij is ook de regel om in de tekst zoveel mogelijk afkortingen van persoonsnamen te gebruiken: voorletter en achternaam. Als er geen andere NAW gegevens genoemd worden is de persoon moeilijk te herleiden voor een derde waarvoor het e-mailbericht niet bestemd is.

7. Gegevensuitwisseling met derden

Als Umah Hai persoonsgegevens uitwisselt met derden moet hiervoor altijd een wettelijke grondslag zijn. Naast deze wettelijke grondslag moet Umah Hai in het geval van een relatie tussen een verwerkingsverantwoordelijke en een verwerker een verwerkingsovereenkomst afsluiten. De grond hiervoor is terug te vinden in artikel 28 van de AVG. In deze (verwerkers)overeenkomst moet het volgende opgenomen zijn: het onderwerp, de duur van de verwerking, de aard en het doel, het soort persoonsgegevens en de categorieën van de betrokkene, de rechten en verplichtingen van de verwerkingsverantwoordelijke.

In het geval van een relatie tussen twee verwerkingsverantwoordelijken wordt er een gegevensuitwisselingsovereenkomst afgesloten. Dit laatste is geen wettelijke verplichting maar wel wenselijk.

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.

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

8. Melden van datalekken

Het is wettelijk verplicht om datalekken te melden. Voorbeelden van datalekken zijn: inbraak in het systeem, het kwijtraken van een telefoon, diefstal of het delen van persoonsgegevens zonder toestemming. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Een datalek moet worden gemeld door het bestuur. Ernstige datalekken moeten gemeld worden aan betrokkenen en de Autoriteit Persoonsgegevens. De melding aan de Autoriteit moet binnen 72 uur na het constateren gedaan zijn.

Wanneer een beveiligingsincident wordt geconstateerd, dient er direct een melding te worden gemaakt in ons meldsysteem. Het bestuur en/of Odetta onderzoekt het beveiligingsincident en stelt vast of er werkelijk een datalek is. Ook wordt gekeken welke maatregelen er genomen moeten worden, welke informatie naar betrokkene verstrekt dient te worden en of het verplicht is om een melding te doen bij de AP. Niet elk datalek hoeft gemeld te worden bij de AP. De wet bepaalt dat het verplicht is alleen de 'ernstige' datalekken te melden. Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig).

De deelnemersraad wordt op casusniveau (zonder persoonsgegevens van het datalek te delen) meegenomen in de afhandeling van het datalek als het gegevens van een cliënt betreft.

Odetta adviseert de raad van bestuur, eventueel met extern advies, welke stappen genomen dienen te worden rondom een datalek. De raad van bestuur besluit uiteindelijk of er melding bij de Autoriteit Persoonsgegevens wordt gedaan en welke maatregelen ingezet dienen te worden.

In het datalek protocol van Umah Hai is verder uitgewerkt hoe een datalek afgehandeld moet worden.