



Privacy beleid

Handboek Kwaliteit

Proceseigenaar : Cynthia Bekhuis
Functie : Kwaliteit, beleid en
regieverpleegkundige

Vastgesteld door : Directeur

Naam : Sevilay Luiken-Dalli
Handtekening :

A handwritten signature in black ink, appearing to read 'Sevilay Luiken-Dalli', is written over a horizontal line.

Datum : 10-04-2024

Datum : 10-04-2024

Inhoud

Privacy Beleid	3
1. Inleiding	3
2. Toepasselijkheid	3
3. Gegevensbescherming	3
3.1 Persoonsgegevens:.....	3
3.2 Verwerking:	3
3.3 Betrokken partijen:.....	4
4. Legitimiteit van de verwerking.....	4
4.1 Doelbinding en grondslagen.....	4
4.2 Rechtmatigheid, behoorlijk en transparantie	4
4.3 Minimale gegevensverwerking	4
4.4 Juistheid.....	5
4.5 Opslagbeperking.....	5
5. Rechten van betrokkenen	5
5.1 Recht op informatie.....	5
5.2 Recht op inzage en kopie.....	5
5.3 Recht op rectificatie en aanvulling	6
5.4 Recht op het wissen van gegevens.....	6
5.5 Recht op beperking van de verwerking.....	6
5.6 Recht op dataportabiliteit	6
5.7 Recht inzake geautomatiseerde besluitvorming.....	6
5.8 Recht op bezwaar	6
6. Datalekken.....	6
6.1 Datalekken.....	6
6.2 Voorkomen van een datalek	7
6.3 Meldplicht bij datalek.....	7
7. Register van verwerkingsactiviteiten en DPIA.....	8
8. Bewustwording.....	8
9. Technische en organisatorische beveiligingsmaatregelen.....	8

Privacy Beleid

1. Inleiding

IMEAN verwerkt dagelijks allerlei persoonsgegevens en hecht daarom veel belang aan een zorgvuldige omgang met deze veelal vertrouwelijke en gevoelige informatie. Met dit privacybeleid wil IMEAN uitvoering geven aan haar verantwoordelijkheid voor de bescherming van de haar toevertrouwde gegevens. In dit privacybeleid zal daarom tekst en toelichting worden gegeven over de manier waarop IMEAN met de bescherming van persoonsgegevens om wil gaan. Op die manier hoopt IMEAN binnen haar organisatie concrete handvatten te bieden en bewustzijn te creëren voor een vertrouwelijke en zorgvuldige omgang met persoonsgegevens. In het beleidsstuk zal voor nadere informatie of de grondslagen van bepaalde regels naar de Algemene Verordening Gegevensbescherming ("AVG") worden verwezen. Ten tijde van het opstellen van dit beleidsstuk is, CM. Bekhuis aangesteld als Functionaris Gegevensbescherming te bereiken op telefoonnummer 0619269757 en met mailadres cm.bekhuis@imean.nl

2. Toepasselijkheid

Het Privacy beleid is van toepassing op alle situaties waarin een medewerker van IMEAN, of dit nu een werknemer, stagiaire, opdrachtnemer of vrijwilliger is, met persoonsgegevens of andersoortige vertrouwelijke of privacygevoelige informatie te maken krijgt, ongeacht of deze informatie interne- dan wel externe aangelegenheden betreft. Het Privacy beleid is bijvoorbeeld van toepassing op de verwerking van de loonadministratie, waarbij allerlei 'interne' persoonsgegevens verwerkt worden. Het Privacy beleid is ook van toepassing bij het beheer van de sociale media, bij klachten, het te woord staan van derden of iedere andere gelegenheid waarbij vertrouwelijke informatie betrokken is.

Het privacybeleid geeft weer welke maatregelen er worden genomen om het beleid uit te voeren. Iedere medewerker van IMEAN heeft daarnaast van doen met wetgeving in het kader van de WMO en de beroepscode van het maatschappelijk werk waarin het beroepsgeheim verder is uitgewerkt.

IMEAN stuurt aan dat al haar medewerkers het Privacy beleid lezen en toepassen. Uiteraard kunnen voor specifieke situaties uitzonderingen of juist aanvullende afspraken gelden. Bij twijfel kan met de Functionaris Gegevensbescherming contact worden opgenomen. Zij helpt u graag verder! In sommige gevallen bent u zelfs verplicht contact op te nemen om IMEAN zo in staat te stellen bij een (dreigende) schending van de gegevensbescherming of andersoortig voorval adequaat actie te ondernemen. Daar leest u meer over in paragraaf 6.

3. Gegevensbescherming

3.1 Persoonsgegevens:

Onder persoonsgegevens worden alle gegevens verstaan over een geïdentificeerde of identificeerbare natuurlijke persoon (*art. 4 lid 1 AVG*). Het gaat dus om alle gegevens die gekoppeld kunnen worden, direct dan wel indirect, aan een natuurlijk persoon. Denk daarbij aan voor de hand liggende gegevens zoals naam, (e-mail)adres of leeftijd. Het kan echter ook gaan om gegevens die slechts indirect aan een specifiek persoon te koppelen zijn, zoals een IP-adres, een telefoonnummer of zelfs extra gevoelige informatie zoals ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, medische gegevens etc. (*art. 9 AVG*).

3.2 Verwerking:

Onder verwerking van persoonsgegevens worden nagenoeg alle handelingen die ten aanzien van persoonsgegevens kunnen worden verricht begrepen (*art. 4 lid 2 AVG*). Denk daarbij aan het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, doorzenden, verspreiden en het vernietigen of wissen van persoonsgegevens. Voor al deze verwerkingen gelden de eisen van de gegevensbescherming zoals die in de AVG tot uitdrukking zijn gebracht.

3.3 Betrokken partijen:

In de gegevensbescherming zijn drie belangrijke partijen te onderscheiden. Allereerst de betrokkene. De betrokkene is de persoon wiens persoonsgegevens het betreft. Bij IMEAN zijn de betrokkenen cliënten, medewerkers en vrijwilligers. De betrokkene heeft diverse rechten in het kader van de gegevensbescherming, daar leest u in paragraaf 5 meer over.

Naast de betrokkene, is ook de verwerkingsverantwoordelijke een belangrijk figuur in de gegevensbescherming (*art. 4 lid 7 AVG*). Verwerkingsverantwoordelijke is degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. IMEAN is bijvoorbeeld verwerkingsverantwoordelijke ten aanzien van de verwerking van persoonsgegevens voor de cliëntenadministratie.

Tot slot is een belangrijke rol weggelegd voor de verwerker (*art. 4 lid 8 AVG*). De verwerker is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. Het gaat dus om een derde partij die door de verantwoordelijke wordt ingeschakeld en die in dat kader te maken krijgt met de verwerking van persoonsgegevens. Denk bijvoorbeeld aan de partij die voor IMEAN de cliëntendossiers beheert.

4. Legitimiteit van de verwerking

4.1 Doelbinding en grondslagen

De verwerking van persoonsgegevens binnen IMEAN moet voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden plaatsvinden. Verdere verwerking van persoonsgegevens op een wijze die onverenigbaar is met die oorspronkelijke doeleinden, is niet toegestaan. De verwerking van persoonsgegevens is in zoverre gebonden aan de doelen waarvoor deze persoonsgegevens in eerste instantie verzameld zijn.

IMEAN mag persoonsgegevens alleen verzamelen als daar een grondslag voor is. Er zijn een aantal grondslagen waarop IMEAN persoonsgegevens verwerkt.

- de gegevensverwerking is noodzakelijk voor de uitvoering van een wettelijke verplichting (bijvoorbeeld de gegevens die aan de Gemeente wordt verstrekt over de geleverde zorg).
- de gegevensverwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang (bijvoorbeeld als het voor een goede bedrijfsvoering noodzakelijk is), tenzij het belang van de betrokkene zwaarder weegt.
- degene wiens gegevens worden verwerkt heeft hiervoor toestemming gegeven.

IMEAN mag alleen persoonsgegevens verwerken als dat noodzakelijk is voor een bepaald doel. IMEAN mag de verzamelde gegevens niet zomaar voor een ander doel gebruiken. IMEAN waarborgt doelbinding doordat de verwerking in een verwerkingsregister zijn vastgesteld, welke periodiek geactualiseerd wordt.

4.2 Rechtmatigheid, behoorlijk en transparantie

IMEAN draagt verantwoordelijkheid om ervoor zorg te dragen dat de verwerking van persoonsgegevens op rechtmatige wijze plaats vindt. Door vastlegging in het register van verwerking onderzoekt en borgt IMEAN de rechtmatigheid van de verwerking.

Naast rechtmatigheid, moet IMEAN ook zorgdragen voor een behoorlijke en transparante verwerking van persoonsgegevens. IMEAN geeft invulling aan deze verplichting door, onder andere, op de website in haar privacy statement uit te leggen hoe zij met persoonsgegevens omgaat. Een geprint exemplaar van het privacy statement wordt binnen alle gemeenten waar IMEAN werkzaam is, op de hoofdvestiging, ter inzage gelegd. Als er vragen zijn over de wijze waarop IMEAN met persoonsgegevens omgaat, geven alle medewerkers de betrokkene een exemplaar van het privacy statement. Daarnaast worden betrokkene en medewerkers bij aanvang van de verwerking door IMEAN geïnformeerd over de verwerking en de beveiligingsmaatregelen.

4.3 Minimale gegevensverwerking

De verwerking van persoonsgegevens moet beperkt worden tot wat noodzakelijk en proportioneel is. IMEAN geeft hieraan invulling door in de werkprocessen niet meer dan de noodzakelijke persoonsgegevens voor de dienstverlening te verwerken. Daarnaast wordt vrijwel digitaal gewerkt.

4.4 Juistheid

IMEAN is ervoor verantwoordelijk dat de door haar verwerkte persoonsgegevens juist en actueel zijn. Voor zover persoonsgegevens niet (meer) juist zijn, zal IMEAN die persoonsgegevens corrigeren of wissen. IMEAN geeft hieraan invulling door met actuele persoonsgegevens te werken. Daarnaast is in werkprocessen vastgelegd dat wijzigingen binnen drie dagen verwerkt worden in het cliëntendossier. Zoals bijvoorbeeld bij een verhuizing of overlijden van een cliënt. Onder omstandigheden kan een betrokkene ook van IMEAN verlangen dat zij persoonsgegevens wist, bijvoorbeeld als deze redelijkerwijs niet langer nodig zijn. Daarover leest u meer in paragraaf 5.

4.5 Opslagbeperking

Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. IMEAN geeft hieraan invulling door bijvoorbeeld tijdens de intakegesprekken, methodisch te werken. Tijdens de intake wordt er gebruik gemaakt van de elf gezondheidspatronen van GORDON. Daarnaast worden er twee keer per jaar evaluatiegesprekken gevoerd en twee keer per jaar multidisciplinair overleg. Dit is wettelijk zo afgesproken. Bij elke wijziging van de zorgvraag wordt de evaluatiedatum bijgesteld. Denk bijvoorbeeld aan een hulpvraag voor zes maanden. Na zes maanden dient deze getoetst te worden zodat hiermee de PDCA-cyclus geborgd is. Cliëntdossiers zijn allemaal gedigitaliseerd en geborgd binnen E-care. Met betrekking tot de opslag van cliëntdossiers, deze worden digitaal verwerkt. Op drie manieren geeft IMEAN hier invulling aan:

- Bij een tijdelijke opname/ziekenhuis wordt de cliënt tijdelijk uit zorg gemeld. In praktijk blijft de cliënt zichtbaar in het systeem onder het kopje niet actief, de zorgverlener kan rapporteren maar kan geen zorgtijd registreren.
- Uit zorg betekent voor de zorgverlener ook écht uit zorg. Op het moment dat dezelfde cliënt weer in zorg komt, zal er een nieuw dossier aangemaakt moeten worden.

Nb. Echter werkt IMEAN als onderaannemer en dat betekent dat zorgaccent met behulp van het klantnummer achter de schermen het oude dossier indien nodig weer kan terughalen.

5. Rechten van betrokkenen

IMEAN neemt zoals gezegd de gegevensbescherming en dus de belangen van betrokkene uiterst serieus. IMEAN en daarmee alle medewerkers eerbiedigen de rechten en vrijheden van betrokkene.

IMEAN geeft hieraan invulling door een procedure te hanteren rondom de rechten van betrokkenen.

- Wanneer een medewerker van IMEAN wordt geconfronteerd met een verzoek van een betrokkene dient deze betrokkene te worden doorverwezen naar de Functionaris Gegevensbescherming.
- De Functionaris Gegevensbescherming zal het verzoek in behandeling nemen, de betrokkene vragen zich te identificeren en binnen de geldende termijnen reageren.
- Dat betekent dat in principe de betrokkene binnen één maand bericht ontvangt welk gevolg aan zijn verzoek zal worden gegeven, welke termijn met nog eens twee maanden verlengd kan worden indien nodig.
- Van die verlenging wordt dan uiterlijk binnen één maand na ontvangst van het verzoek melding gemaakt.
- IMEAN acht het van essentieel belang dat voor de behandeling van verzoeken van betrokkene één aanspreekpunt geldt. Het is dus uitdrukkelijk niet de bedoeling dat medewerkers op eigen initiatief of naar eigen goeddunken verzoeken van betrokkene in behandeling te nemen.

5.1 Recht op informatie

De betrokkene heeft recht op informatie met betrekking tot de verwerking van zijn persoonsgegevens (*art. 12 AVG*). IMEAN informeert betrokkene op een beknopte en begrijpelijke wijze in gemakkelijk toegankelijke vorm over haar eigen rol als verantwoordelijke, over de persoonsgegevens die verwerkt worden, de doelen en rechtvaardiging voor die verwerking, de geldende bewaartermijnen, de noodzaak van verstrekking van persoonsgegevens en de gevolgen als een betrokkene dat weigert en de contactgegevens van de Functionaris Gegevensbescherming. Daarnaast wijst IMEAN de betrokkene op zijn/haar rechten, waaronder het recht op inzage, kopie, data-portabiliteit, vergetelheid etc.

IMEAN geeft invulling aan haar verplichting om betrokkene informatie te verstrekken door middel van haar privacy statement. Zoals onder 4.1 aangegeven zal een geprint exemplaar van het privacy statement, binnen alle gemeenten waar IMEAN werkzaam is, op de hoofdvestiging, ter inzage worden gelegd. Medewerkers stellen deze aan betrokkene op eerste verzoek ter beschikking. Daarnaast wordt de betrokkene op de hoogte gebracht van zijn/haar rechten bij het tekenen van de zorgovereenkomst.

5.2 Recht op inzage en kopie

De betrokkene heeft het recht op inzage in zijn persoonsgegevens die IMEAN verwerkt (*art. 15 AVG*). Daarbij dient IMEAN de betreffende betrokkene te informeren over bijvoorbeeld de doelen waarvoor zijn persoonsgegevens worden verwerkt, de partijen waar die persoonsgegevens eventueel aan verstrekt worden, de rechten van de betrokkene op rectificatie of het

wissen van persoonsgegevens, het recht om een klacht bij de Autoriteit Persoonsgegevens in te dienen, het recht om bij IMEAN bezwaar te maken tegen een verwerking etc. Daarnaast heeft een betrokkene ook recht op een kopie van zijn persoonsgegevens die door IMEAN verwerkt worden (*art. 15 lid 3 AVG*). IMEAN geeft hieraan invulling door te onderzoeken welke persoonsgegevens verwerkt worden en of hiervan een kopie verstrekt kan worden.

5.3 Recht op rectificatie en aanvulling

Zoals onder 4.4 uiteengezet is de juistheid van de door IMEAN verwerkte persoonsgegevens van groot belang. De betrokkene die constateert dat onjuiste gegevens aangaande zijn persoon worden verwerkt, heeft het recht op rectificatie daarvan (*art. 16 AVG*). Naast het recht op rectificatie, heeft een betrokkene ook recht op aanvulling van onvolledige persoonsgegevens. Die aanvulling kan plaatsvinden door bijvoorbeeld in het betrokken informatiesysteem een aanvullende verklaring van de betrokkene op te nemen.

5.4 Recht op het wissen van gegevens

De betrokkene heeft het recht om van IMEAN te verlangen dat zijn persoonsgegevens gewist worden (*art. 17 AVG*). IMEAN geeft hieraan invulling door te onderzoeken of persoonsgegevens gewist kunnen worden. Aan een verzoek tot verwijdering kan voldaan worden indien er geen wettelijke bewaarplicht geldt of de persoonsgegevens niet langer nodig zijn voor het doel waarvoor zij verzameld zijn.

5.5 Recht op beperking van de verwerking

Onder omstandigheden kan een betrokkene IMEAN verzoeken om de verwerking van zijn persoonsgegevens te beperken (*art. 18 AVG*). De situaties waarin beperking van de verwerking mogelijk is zijn de volgende: de juistheid van de persoonsgegevens wordt betwist; de verwerking is onrechtmatig; de client heeft de persoonsgegevens nodig voor een rechtsvordering; de client heeft bezwaar gemaakt tegen de verwerking en verzoekt in afwachting van het besluit hieromtrent om beperking van de verwerking. IMEAN geeft hieraan invulling door het verzoek te analyseren en binnen een maand een besluit hierover te nemen.

5.6 Recht op dataportabiliteit

Het recht op dataportabiliteit houdt concreet in dat een betrokkene onder omstandigheden het recht heeft om zijn persoonsgegevens in een bruikbare vorm terug te krijgen, of deze aan een andere verantwoordelijke over te dragen (*art. 20 AVG*). Het moet dan wel gaan om geautomatiseerde verwerkingen die berusten op toestemming of de uitvoering van een overeenkomst. Het idee achter het recht op dataportabiliteit is om de betrokkene in staat te stellen om (een verzameling) persoonsgegevens die op geautomatiseerde wijze worden verwerkt bij een andere verantwoordelijke onder te brengen. IMEAN geeft hieraan invulling door het verzoek te analyseren en binnen een maand een besluit hierover te nemen.

5.7 Recht inzake geautomatiseerde besluitvorming

Een betrokkene heeft het recht niet te worden onderworpen aan een geheel op een geautomatiseerde verwerking gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of welk besluit anderszins aanzienlijke gevolgen heeft (*art. 22 AVG*). IMEAN maakt geen gebruik van geautomatiseerde besluitvorming.

5.8 Recht op bezwaar

De betrokkene heeft het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens door IMEAN (*art. 21 AVG*). IMEAN geeft hieraan invulling door een gerezen bezwaar toe te wijzen tenzij er dwingende gerechtvaardigde gronden zijn voor de verwerking die zwaarder wegen dan het door de betrokkene aangevoerde bezwaar.

6. Datalekken

Alhoewel IMEAN zich tot het uiterste inspant om datalekken te voorkomen, kan het desondanks gebeuren dat per ongeluk of op onrechtmatige wijze persoonsgegevens verstrekt of verloren worden. IMEAN neemt datalekken uiterst serieus. IMEAN geeft hieraan invulling door het trainen van medewerkers in het herkennen van datalekken en door bewustwording te bevorderen.

6.1 Datalekken

Er zijn 3 soorten datalekken:

- Inbreuk op de vertrouwelijkheid: persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
- Inbreuk op de integriteit: persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.
- Inbreuk op de beschikbaarheid: de organisatie waar het datalek is (geweest) kan niet meer bij de persoonsgegevens komen. Of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

Afhankelijk van de omstandigheden kan een datalek in meer dan een van deze categorieën vallen.

6.2 Voorkomen van een datalek

IMEAN heeft diverse technische maatregelen getroffen om datalekken te voorkomen, zoals tweefactor-authenticatie. Met deze technische maatregelen is het risico op een datalek in belangrijke mate verkleind. Door organisatorische maatregelen kan het risico op een datalek verder verkleind worden. IMEAN geeft hieraan invulling door medewerkers aan te sturen in de volgende gedragsregels:

- Geen mobiele gegevensdragers onbeheerd achterlaten;
- Nooit persoonsgegevens naar de eigen privémail of per Whatsapp etc. sturen;
- Tijdig updates aan de werkplek (laten) uitvoeren;
- Persoonsgegevens niet bespreken in openbare ruimtes of waar onbevoegde derden kunnen meeluisteren;
- Alleen persoonsgegevens verwerken via de door IMEAN ter beschikking gestelde informatiesystemen (Sharepoint en-/ of TEAMS);
- Clean desk policy;
- Geen e-mails van onbekende afzenders openen;
- Werkplek bij ieder vertrek, hoe kort ook, versleutelen;
- Nooit 'zo maar' persoonsgegevens aan collega's of andere derden verstrekken.

6.3 Meldplicht bij datalek

IMEAN bevordert bewustwording bij haar medewerkers waardoor zij waakzaam zijn voor mogelijke datalekken en daarbij proactief handelen, zowel in het constateren als het melden. Alleen dan kan IMEAN in het onverhoopte geval van een datalek aan haar verplichtingen in dat kader voldoen. Onder die verplichtingen valt onder meer de tijdige melding van het datalek aan de Autoriteit Persoonsgegevens en onder omstandigheden de betrokkene zelf (*art. 33 en 34 AVG*).

Aan de hand van een procedure maken medewerkers onmiddellijk melding bij de functionaris gegevensbescherming als zij constateren of vermoeden dat sprake is van een datalek. De medewerker geeft aan wat de aard is van het datalek, de getroffen (categorieën) persoonsgegevens en (bij benadering) het aantal getroffen personen. In het geval van een datalek neemt de organisatie passende maatregelen om het voortduren of zelfs verergeren van dat lek te voorkomen. De Functionaris Gegevensbescherming zal vervolgens de verdere afhandeling van het datalek, waaronder de melding aan de Autoriteit Persoonsgegevens en eventueel de betrokkene, regelen.

7. Register van verwerkingsactiviteiten en DPIA

IMEAN houdt een register van verwerkingen bij art. 30 AVG. In het verwerkingsregister vermeldt IMEAN haar eigen contactgegevens alsook de contactgegevens van de Functionaris Gegevensbescherming. Daarnaast worden in het register van verwerkingsactiviteiten de verschillende verwerkingen van persoonsgegevens die binnen IMEAN plaatsvinden bijgehouden. Het register vermeldt tenminste: de categorieën personen en persoonsgegevens die verwerkt worden; de verwerkingsdoeleinden; eventuele derden waaraan de persoonsgegevens verstrekt worden en indien mogelijk de verschillende bewaringstermijnen. De Autoriteit persoonsgegevens kan te allen tijde inzage in het register van verwerkingsactiviteiten verlangen.

Wanneer een verwerking van persoonsgegevens, gelet op de aard, de omvang, de context en de doelen daarvan waarschijnlijk een hoog risico in houdt voor de rechten en vrijheden van natuurlijke personen, voert IMEAN voorafgaand aan de verwerkingen een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. De gegevensbeschermingseffectbeoordeling zal worden uitgevoerd door de Functionaris Gegevensbescherming, die zich in dat kader kan laten adviseren en bijstaan door de “kerngebruiker” van het betrokken proces en/of gegevensverwerkingsstelsel. Pas na goedkeuring van de Functionaris Gegevensbescherming zal de voorgenomen verwerking kunnen worden uitgevoerd.

8. Bewustwording

Vanaf het moment dat medewerkers onboarden bij IMEAN worden zij geïnformeerd en voorzien van onze informatie op gebied van gegevensbescherming. Voorbeelden hiervan zijn uitleg over ons privacybeleid, wie de aangewezen functionarissen zijn op het moment zich onverhoopt een datalek voordoet en ook de tools die ingezet worden. Bestaande medewerkers worden van (wettige) veranderingen tijdig op de hoogte gebracht door terugkoppeling tijdens teamvergaderingen. Dit verloopt dan via de coach. Daarnaast hangt op alle locaties een template waarop staat hoe de organisatie bewust omgaat met gegevens bescherming en wat de rol van de medewerker hierin is. Voor begeleiding bij het cliëntdossier heeft de organisatie een begeleider aangesteld, in de rol van digicoach.

9. Technische en organisatorische beveiligingsmaatregelen

IMEAN treft technische en organisatorische maatregelen om persoonsgegevens te beschermen en te beveiligen. IMEAN geeft hier als volgt invulling aan:

Om de technische processen op orde te houden wordt er intern samengewerkt met de support coördinator. Naast de tweefactorauthenticatie wordt dit systeem ook elk jaar getoetst op de standaard ISO-normeringen. SharePoint / Office wordt beschermd door Gebruikersnaam/ Wachtwoord en 2FA middels sms of Authenticator. Nieuwe medewerkers krijgen bij de eerste inlog de vraag om 2FA in te stellen via de gebruikelijke MS Authenticator app of sms. Bestaande gebruikers werken hier inmiddels al mee. Het systeem Puur wordt gehost in Azure. Hier zijn ook beveiligingsmaatregelen genomen zoals Firewalls. Daarnaast worden de volgende maatregelen genomen:

- MFA;
- Verwerkersovereenkomsten;
- Digitaal cliëntensysteem met autorisatiematrix;
- Geheimhoudingsovereenkomsten;
- Archiefvernietiging;
- Clean desk/clean screen beleid.
- VOG-verklaringen

Binnen de werkprocessen van IMEAN wordt er gewerkt volgens de normen van de NTA7516. Dit betekent dat het beleid erop ingericht is dat mailen beveiligd gebeurt via ZIVVER. Cliëntgegevens in Ecare worden opgevraagd via een unieke code, middels een token en de computer opstarten met behulp van het account gebeurt met behulp van tweefactorauthenticatie.

Alle medewerkers werkzaam binnen IMEAN zijn opgeleid in het omgaan met integriteitskwesaties. Daarvoor legt men een eed af voordat men gediplomeerd wordt. Daarnaast heeft de kwaliteits- en beleidsverpleegkundige per kwartaal een afstemmingsoverleg met de ICT-beheerder om de processen te herzien en waar nodig door te ontwikkelen om zo cybercriminaliteit te voorkomen.

Wanneer wetswijzigingen aangeven dat het informatiebeveiligingssysteem aangepast moet worden, dan wordt dit proactief aangepast waarbij er tijdig wordt geschakeld met de support coördinator.