



# Privacyreglement

Versie : 4v0

Datum : 24 mei 2018

Max Ernst GGZ

Postbus 2051

6802 CB Arnhem

[www.max-ernst.nl](http://www.max-ernst.nl)

## Het doel

Max Ernst GGZ respecteert en beschermt de privacy en persoonsgegevens van haar cliënten. In haar dienstverlening houdt zij zich aan de wet en zoekt waar mogelijk de ruimte om de privacybelangen van zowel de cliënt als de doelstellingen van Max Ernst GGZ naar beste inzicht te behartigen. Belangrijk hierbij is dat de medewerkers van Max Ernst GGZ privacybewust zijn. Het doel van dit Privacyreglement is duidelijkheid te geven over hoe Max Ernst GGZ omgaat met persoonsgegevens. Met dit reglement beoogt de directie van Max Ernst GGZ de persoonlijke levenssfeer van iedere persoon waarvan persoonsgegevens zijn opgenomen te beschermen tegen misbruik en tegen opslag van onjuiste gegevens. Tevens heeft het reglement ten doel te voorkomen dat verstrekte gegevens voor een ander doel worden gebruikt dan het doel waarvoor deze verkregen zijn. De rechten van betrokkenen dienen gewaarborgd te zijn. Het Privacyreglement geeft hiermee een praktische uitwerking aan de bepalingen van de Algemene Verordening Gegevensbescherming.

## Artikel 1: Begripsbepaling

- 1. De organisatie**  
Max Ernst GGZ, gevestigd te Arnhem.
- 2. Persoonsgegevens**  
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- 3. Verwerking van persoonsgegevens**  
Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van persoonsgegevens. Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.
- 4. Verantwoordelijke**  
Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
- 5. Verwerker**  
De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
- 6. Betrokkene**  
De natuurlijke persoon op wie de persoonsgegevens betrekking hebben. Dit kan zowel een cliënt zijn, als een medewerker van de organisatie of een contactpersoon van de opdrachtgever.
- 7. AP**  
Autoriteit Persoonsgegevens, de toezichthoudende autoriteit voor de naleving van de geldende privacywetgeving.
- 8. AVG**  
Algemene Verordening Gegevensbescherming, voluit: Verordening (EU) 2016/679 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.

## Artikel 2: Reikwijdte

1. Dit privacyreglement is van toepassing op alle verwerkingen van persoonsgegevens die binnen de organisatie plaatsvinden. Het vormt een verdere uitwerking van de wettelijke regelgeving en een praktische handleiding voor de organisatie. Het geeft de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens. Op die manier kan hiermee een nog betere verwerking van persoonsgegevens plaatsvinden binnen de organisatie.
2. Daar waar in dit reglement een mannelijke persoonsaanduiding wordt gebruikt kan ook de vrouwelijke worden gelezen.

## Artikel 3: Verantwoordelijke voor de verwerking

De directie van Max Ernst GGZ is de verantwoordelijke voor de verwerkingen die door of namens Max Ernst GGZ worden uitgevoerd.

## Artikel 4: Doeleinden van de verwerking

1. Algemeen uitgangspunt is dat persoonsgegevens alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, duidelijk omschreven en gerechtvaardigd zijn. Ook moet steeds nagaan worden of het verwerken van persoonsgegevens noodzakelijk is voor het doel. De verwerkingsdoelen zijn het 'waarom' van het verwerken van persoonsgegevens. Doelen zijn van belang voor verschillende normen. Denk hierbij aan onder andere het bepalen wie verantwoordelijk is voor de verwerking van persoonsgegevens. Of de vraag of het delen van deze gegevens met andere organisaties is toegestaan. Ook zijn doelen van belang voor het vaststellen van bewaartermijnen en het informeren van de cliënt. Zo weet je hoe lang het nodig is om de persoonsgegevens te bewaren of waar je cliënten over moet informeren.
2. Een belangrijke eis is dat doelen vooraf specifiek geformuleerd moeten zijn. De doelen mogen dus niet te ruim en vaag omschreven zijn of achteraf bepaald worden. Verwerking voor een ander doel dan het oorspronkelijke doel is alleen onder strikte voorwaarden toegestaan. Zo zal er een directe relatie moeten zijn met het doel waarvoor de persoonsgegevens eerder zijn verzameld. Ook moet men rekening houden met de soort gegevens. Algemeen geldt: hoe gevoeliger het gegeven, hoe minder snel er sprake is van verenigbaar gebruik en de gegevens niet verder mogen worden verwerkt. Dus niet mogen worden gebruikt voor een ander doel dan waarvoor deze eerder zijn verzameld. Ook moet men rekening houden met de gevolgen van de beoogde verwerking voor de betrokkene. Denk hierbij aan het vooraf inlichten van de cliënt over het doel waarvoor de gegevens worden gebruikt als de cliënt zijn persoonsgegevens aan Max Ernst GGZ geeft.

## Artikel 5: Rechtmatige grondslag

1. Max Ernst GGZ verwerkt persoonsgegevens primair om uitvoering te geven aan de overeenkomst met betrokkene, dan wel om te kunnen voldoen aan een wettelijke verplichting.

Tevens verwerkt Max Ernst GGZ mogelijk persoonsgegevens, omdat er sprake is van een gerechtvaardigd belang, zoals:

- het op zo efficiënt mogelijke wijze kunnen verlenen van de dienstverlening
  - de bescherming van de financiële belangen
  - de verbetering van de dienstverlening
  - beveiliging en het beheer van de systemen.
2. Indien persoonsgegevens worden verwerkt op grond van toestemming, zal dat afzonderlijk aan betrokkene worden gevraagd.

## Artikel 6: Verwerking van persoonsgegevens

1. Max Ernst GGZ verkrijgt persoonsgegevens:
  - van de betrokkene zelf, bijvoorbeeld de gegevens die betrokkene verstrekt via de intake;
  - van een verwijzer, bijvoorbeeld de huisarts of zorgverzekeraar.
2. T.a.v. cliënten worden geen andere persoonsgegevens verwerkt dan:
  - naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, e-mailadres, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens;
  - een administratienummer dat geen andere informatie bevat dan hierboven bedoeld;
  - in geval van vertegenwoordiging: gegevens als hierboven bedoeld van de persoon of personen die optreden als vertegenwoordiger van betrokkene;
  - nationaliteit en geboorteplaats;
  - verzekeringsgegevens (alleen als het *verzekerde* dienstverlening betreft);
  - burgerservicenummer (alleen als hiervoor een *wettelijke verplichting* bestaat);
  - pasfoto (alleen als een *wettelijke rechtsgrond* uit artikel 9 lid 2 en 10 AVG of artikel 22-33 UAVG van toepassing is);
  - gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van betrokkene;
  - gegevens die van belang zijn voor het bieden van passende dienstverlening aan betrokkene;
  - gegevens betreffende de aard en het verloop van de dienstverlening, alsmede de behaalde resultaten;
  - gegevens met het oog op de organisatie van de dienstverlening;
  - gegevens met het oog op het berekenen, vastleggen en innen van facturen;
  - andere gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een van toepassing zijnde wet.
3. T.a.v. opdrachtgevers worden geen andere persoonsgegevens verwerkt dan:
  - naam, voornamen, voorletters, titulatuur, geslacht, (zakelijk) e-mailadres, (zakelijk) telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van contactpersonen;
  - een administratienummer dat geen andere informatie bevat dan hierboven bedoeld;
  - gegevens die van belang zijn voor het bieden van passende dienstverlening aan de opdrachtgever;
  - gegevens betreffende de aard en het verloop van de dienstverlening, alsmede de behaalde resultaten;

- gegevens met het oog op de organisatie van de dienstverlening;
  - gegevens met het oog op het berekenen, vastleggen en innen van facturen;
  - andere gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een van toepassing zijnde wet.
4. T.a.v. medewerkers worden geen andere persoonsgegevens verwerkt dan:
- naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, e-mailadres, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens;
  - een administratienummer dat geen andere informatie bevat dan hierboven bedoeld;
  - in geval van vertegenwoordiging: gegevens als hierboven bedoeld van de persoon of personen die optreden als vertegenwoordiger van betrokkene;
  - nationaliteit en geboorteplaats;
  - burgerservicenummer;
  - kopie identiteitsbewijs;
  - gegevens betreffende het dienstverband en arbeidsverleden;
  - CV;
  - functionele mogelijkheden en belastbaarheid;
  - ziekmeldingen;
  - gespreksverslagen;
  - inhoud van communicatie;
  - gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van betrokkene;
  - gegevens met het oog op het berekenen, vastleggen en uitkeren van salaris;
  - andere gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een van toepassing zijnde wet.

## Artikel 7: Wijze van verwerking

1. De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.
2. Persoonsgegevens moeten dus juist, ter zake dienend, up-to-date en niet bovenmatig veel zijn in het licht van het doel van de verwerking. Dit betekent dat alleen die persoonsgegevens mogen worden gebruikt die strikt noodzakelijk zijn voor het doel van de verwerking. Wanneer het bijvoorbeeld voldoende is om iemands contactgegevens te gebruiken, is het niet nodig om ook een pasfoto en BSN te vragen. Sowieso gelden voor het gebruik van het BSN strenge regels. Wanneer ook met anonieme gegevens volstaan kan worden, mogen geen herleidbare persoonsgegevens gebruikt worden.
3. Iedere persoon die toegang heeft tot de persoonsgegevens heeft een geheimhoudingsplicht ter zake van de gegevens waarvan hij op grond van die toegang heeft kennisgenomen. Ook

is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is. En hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Het is dus belangrijk dat de medewerkers van Max Ernst GGZ zich bewust zijn van de regels en gedragsnormen rondom privacy. Deze organisatorische maatregelen dragen ook bij aan een bewustwording binnen Max Ernst GGZ.

4. Daarnaast beveiligd Max Ernst GGZ alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Als uitgangspunt geldt dat naarmate de risico's van de verwerking hoger liggen er betere beveiligingsmaatregelen moeten worden getroffen. Max Ernst GGZ heeft hiervoor een specifiek beleid opgesteld in de vorm van het Informatiebeveiligings- en privacybeleid.

### **Artikel 8: Vertegenwoordiging**

1. De verplichtingen uit dit reglement worden nagekomen jegens de betrokkene of zijn vertegenwoordiger.
  - Indien de betrokkene jonger is dan twaalf jaar treden de ouders die de ouderlijke macht uitoefenen dan wel de voogd in de plaats van de betrokkene.
  - Hetzelfde geldt voor de betrokkene van twaalf tot zestien jaar die niet in staat is tot een redelijke waardering van zijn belangen ter zake.
  - Indien de betrokkene in de leeftijdscategorie van twaalf tot zestien jaar valt en tot redelijke waardering van zijn belangen in staat is, treedt naast de betrokkene de ouders die de ouderlijke macht uitoefenen of de voogd op.
  - Als de betrokkene zestien jaar of ouder is en niet in staat is zijn belangen op redelijke wijze te waarderen dan treden de volgende personen in zijn plaats op in volgorde: curator, mentor, schriftelijke gemachtigde, levensgezel, ouder, kind, broer of zus.
2. De persoon, die in de plaats treedt van de betrokkene, betracht de zorg van een goed vertegenwoordiger. Hij is gehouden de betrokkene zoveel mogelijk bij de vervulling van zijn taken te betrekken.
3. De verantwoordelijke komt zijn verplichtingen die voortvloeien uit wet en reglement na jegens de vertegenwoordiger van de betrokkene, tenzij die nakoming niet verenigbaar is met de zorg van een goed verantwoordelijke.

### **Artikel 9: Doorgifte aan derden**

1. In het kader van haar dienstverlening kan Max Ernst GGZ persoonsgegevens uitwisselen met derden, zoals de IT-leveranciers van website en systemen. Deze derden mogen de persoonsgegevens slechts verwerken voor de voornoemde doeleinden.
2. Persoonsgegevens kunnen verstrekt worden aan derden wanneer Max Ernst GGZ aan een wettelijke verplichting moet voldoen.
3. Max Ernst GGZ zal persoonsgegevens niet verstrekken aan derden voor commerciële of goede doelen.

## Artikel 10: Doorgifte buiten de EER

1. Onder doorgifte wordt hier o.a. verstaan: het opslaan (bijvoorbeeld in de Cloud) of het ter beschikking stellen aan een organisatie buiten de EER. Hieronder valt niet het via internet zichtbaar maken van persoonsgegevens aan personen buiten de EER.
2. Persoonsgegevens worden in principe niet buiten de EER verwerkt. De EER is de Europese Economische Ruimte, bestaande uit de landen van de Europese Unie, Liechtenstein, Noorwegen en IJsland. Binnen de EER is er een goede bescherming voor de persoonsgegevens, daarbuiten niet in alle gevallen.
3. Op grond van goedgekeurde afspraken door de Europese Commissie kan Max Ernst GGZ eventueel persoonsgegevens doorgeven aan een land buiten de Europese Economische Ruimte (EER) of aan een internationale organisatie.
4. Daarnaast kunnen persoonsgegevens door derden buiten de EER worden opgeslagen wanneer gebruik wordt gemaakt van partijen als Google Analytics, LinkedIn of Facebook in het contact met betrokkene. Deze partijen zijn "EU-VS Privacy Shield" gecertificeerd, zodat zij zich zullen houden aan de Europese privacyregelgeving.

## Artikel 11: Functionaris voor de gegevensbescherming

1. Max Ernst GGZ heeft een functionaris voor de gegevensbescherming (FG) aangesteld, ook wel privacy officer genoemd. Door het aanstellen van een FG wordt een belangrijke stap gezet in de manier waarop Max Ernst GGZ aan haar cliënten, opdrachtgevers en medewerkers wil uitdragen dat zij serieus omgaat met de verwerking van persoonsgegevens. De FG is betrokken bij aangelegenheden die verband houden met de bescherming van persoonsgegevens.
2. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. De FG houdt vanuit een onafhankelijke positie intern toezicht op de manier waarop door Max Ernst GGZ wordt omgegaan met persoonsgegevens.
3. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens.
4. De FG is bereikbaar via [privacy@calderholding.nl](mailto:privacy@calderholding.nl).

## Artikel 12: Transparantie en communicatie

1. Betrokkenen moeten geïnformeerd worden over de verwerking van de eigen persoonsgegevens door Max Ernst GGZ. Het moment van informeren en de manier waarop is afhankelijk van de vraag hoe de persoonsgegevens worden verkregen:
  - Als de persoonsgegevens door de betrokkene zelf worden aangeleverd, dan moet de betrokkene vooraf over de verwerking van zijn gegevens worden geïnformeerd.
  - Als persoonsgegevens over de betrokkene via een andere organisatie of instantie zijn verkregen, dan moet de betrokkene geïnformeerd worden als die persoonsgegevens door Max Ernst GGZ worden vastgelegd.

2. Betrokkenen hebben recht op inzage in de eigen persoonsgegevens. De betrokkene hoeft geen reden op te geven voor zijn inzageverzoek, maar hij mag niet overdreven veel verzoeken in korte tijd indienen. Als een betrokkene vraagt om inzage, dan heeft hij recht op een volledig overzicht van de gegevens die worden gebruikt. Ook moet inzage worden gegeven in de herkomst van de gegevens, de ontvangers van de gegevens en de doelen van de verwerking van de persoonsgegevens. Max Ernst GGZ zorgt ervoor dat aan dit verzoek tijdig en volledig wordt voldaan.
3. Naast een recht op inzage heeft de betrokkene ook recht op correctie, aanvullen, verwijderen of afschermen van de eigen persoonsgegevens. Aan dit verzoek moet alleen gehoor worden gegeven als de gegevens onjuist zijn of onvolledig zijn voor het doel waarvoor de gegevens worden verzameld. Dit verzoek moet ook worden gerespecteerd als de gegevens niet relevant zijn of in strijd met de wet worden gebruikt. De betrokkene moet in zijn verzoek duidelijk aangeven welke gegevens om welke reden moeten worden aangepast. Het recht kan niet worden gebruikt om meningen of onderzoeksresultaten te wijzigen. Als positief wordt besloten op het verzoek, dan moeten de wijzigingen zo snel mogelijk worden doorgevoerd. De wijzigingen of verwijderingen van persoonsgegevens moeten ook worden doorgegeven aan andere organisaties aan wie Max Ernst GGZ de gegevens heeft verstrekt.
4. De AVG benoemt een aantal specifieke situaties waar de betrokkene het recht heeft om zich te verzetten tegen het gebruik van zijn persoonsgegevens, onder andere wanneer deze gebruikt worden voor direct marketing-doeleinden of liefdadigheidsdoelen.
5. Om gebruik te maken van zijn rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden bij de verantwoordelijke. Deze heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Als het verzoek niet wordt opgevolgd, heeft betrokkene de mogelijkheid om bezwaar te maken bij de functionaris voor de gegevensbescherming (FG) van Max Ernst GGZ.
6. Mocht betrokkene niet tevreden zijn over de wijze waarop zijn verzoek is afgehandeld, dan heeft betrokkene het recht om een klacht in te dienen bij de privacytoezichthouder, de Autoriteit Persoonsgegevens (AP).
7. Aan de hand van een verzoek kan Max Ernst GGZ aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

### **Artikel 13: Register van verwerkingsactiviteiten**

1. Max Ernst GGZ is verplicht om te documenteren welke persoonsgegevens worden verwerkt, wat het doel ervan is, van wie of waar deze gegevens afkomstig zijn en met wie deze gegevens worden gedeeld.
2. Daarnaast moet Max Ernst GGZ documenteren en verantwoorden op basis van welke wettelijke grondslag Max Ernst GGZ de persoonsgegevens verwerkt.

### **Artikel 14: Bewaartermijnen**

1. Max Ernst GGZ bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van de dienstverlening, en minimaal zolang als nodig is om te kunnen voldoen aan haar wettelijke verplichtingen.



2. In een aantal wetten zijn specifieke bewaartermijnen opgenomen voor bepaalde persoonsgegevens. In de AVG worden geen bewaartermijnen genoemd. Als geen bewaartermijn aanwezig is, dan moet goed kunnen worden onderbouwd waarom persoonsgegevens voor een bepaalde termijn worden bewaard.
3. Na afloop van de bewaartermijnen moeten de persoonsgegevens worden vernietigd of geanonimiseerd. Dit geldt niet alleen voor de gegevens zelf, maar ook voor kopieën en back-ups. Voor alle persoonsgegevens geldt dat de vernietiging onomkeerbaar moet zijn.

### **Artikel 15: Meldplicht datalekken**

1. Een datalek is een inbreuk op de beveiliging, die flinke nadelige gevolgen heeft voor de cliënt of voor de bescherming van de persoonsgegevens. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak op het netwerk (hack).
2. Via haar Informatiebeveiligings- en privacybeleid neemt Max Ernst GGZ alle mogelijke maatregelen om te voorkomen dat datalekken zich voor zullen doen.
3. Indien zich onverhoopt toch een datalek voordoet, treedt het protocol datalekken in werking. Daarin is beschreven op welke wijze bij de AP datalekken moeten worden gemeld. Op het niet (tijdig) melden van datalekken staat een boete. Onder tijdig wordt verstaan: onverwijld, zonder onnodige vertraging en zo mogelijk binnen 72 uur na ontdekking, tenzij gebleken is dat het incident niet onder de meldplicht valt.
4. Als de privacy van betrokkenen is geschaad, moeten ook zij worden geïnformeerd over het datalek. Daarnaast moet de betrokkene worden geïnformeerd over welke maatregelen Max Ernst GGZ neemt om de risico's en schade te beperken.
5. Naast het melden moet Max Ernst GGZ ook alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of Max Ernst GGZ aan de meldplicht heeft voldaan.

### **Artikel 16: Verwerkersovereenkomst**

1. Verwerkersovereenkomsten moeten worden afgesloten wanneer derden – ook wel verwerkers genoemd – in opdracht van Max Ernst GGZ persoonsgegevens verwerken. Hierin moeten duidelijke afspraken worden gemaakt over hoe de derde partij moet omgaan met de gegevens die zij van Max Ernst GGZ krijgt.
2. Max Ernst GGZ heeft een standaard verwerkersovereenkomst beschikbaar die in deze gevallen kan worden gebruikt.

### **Artikel 17: Privacy Impact Assessment (PIA)**

1. Met een PIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. Max Ernst GGZ voert een PIA uit wanneer:
  - er een (geautomatiseerde) verwerking plaatsvindt met een hoog risico;
  - er een (geautomatiseerde) verwerking plaatsvindt waarvan de Autoriteit Persoonsgegevens heeft aangegeven dat daarvoor een PIA verplicht is;

- een grootschalige verwerking plaatsvindt;
- er een grootschalige monitoring van openbare ruimten plaatsvindt.

### **Artikel 18: Privacy by Design en privacy by default**

1. Bij de aanschaf of ontwikkeling van producten, systemen of processen moet altijd rekening worden gehouden met de bescherming van persoonsgegevens. We noemen dit Privacy by Design en privacy by default. Voor alle producten, systemen of processen moeten de technische en organisatorische maatregelen ervoor zorgen dat standaard alleen die gegevens worden gebruikt die nodig zijn voor het doel.

### **Artikel 19: Gouden regels van privacy & informatiebeveiliging**

1. Behandel persoonsgegevens vertrouwelijk en integer.
2. Verwerk niet meer persoonsgegevens dan nodig.
3. Motiveer en leg vast wat je doet.
4. Leg uit waarom we persoonsgegevens verwerken en wees transparant.
5. Weet wanneer je persoonsgegevens mag delen met anderen.
6. Ga zorgvuldig met persoonsgegevens om.
7. Ga verantwoord om met wachtwoorden.
8. Ken de risico's van e-mail, internet en sociale media.
9. Ga verantwoord om met mobiele faciliteiten.
10. Maak melding van beveiligingsincidenten.

### **Artikel 20: Wijziging van het reglement**

1. Wijzigingen in dit reglement worden aangebracht door de verantwoordelijke. De wijzigingen in het reglement zijn van kracht vier weken nadat ze bekend zijn gemaakt aan belanghebbenden.
2. Door wet- en regelgeving opgelegde wijzigingen zijn per direct van kracht.

### **Artikel 21: Inwerkingtreding**

1. Versie 4v0 van dit reglement treedt per 24 mei 2018 in werking.