Mpiris

Informing policy choices
through innovative social science research

GEGEVENSBESCHERMINGSBELEID

Laatst aangepast : 25-08-2023

Mpiris is een onderzoeksbureau dat overheden en organisaties helpt goede beslissingen te nemen. Daartoe verricht Mpiris sociaal-wetenschappelijk onderzoek dat opdrachtgevers de inzichten levert die hen toelaten hun beleid te bepalen of bij te sturen. Mpiris benut de traditionele onderzoeksmethodes uit de sociale wetenschappen zoals interviews, enquêtes en observaties, maar wil zich voornamelijk profileren door innovatieve technieken te benutten om data te verzamelen en te verwerken.

De beleidsmatige expertisevelden van Mpiris zijn onderwijs, arbeidsmarkt, competenties en sociaal beleid.

www.mpiris.be

Inhoud

Belang van informatieveiligheid en gegevensbescherming

Mpiris staat ervoor garant dat het verzamelen en verwerken van de gegevens van onze klanten en andere betrokkenen, medewerkers en derden gebeurt met de grootst mogelijke zorgvuldigheid, op een professionele manier, en met aandacht voor het beschermen van de persoonlijke levenssfeer van de betrokkenen. Mpiris streeft continu naar verbetering, met als doel een veilige informatieomgeving te creëren, en alle persoonsgegevens te beschermen conform de Europese Algemene Verordening voor Gegevensbescherming (AVG).

In het bijzonder wil Mpiris de gegevens beschermen tegen

- **Verlies**: de gegevens zijn niet meer beschikbaar.
- **Lekken**: gegevens komen in de verkeerde handen terecht.
- **Fouten**: gegevens zijn niet correct (bv. verouderd of onvolledig).
- **Niet toegankelijk zijn**: op het moment van de zorg zijn gegevens niet toegankelijk.
- **Onterecht inkijken**: ingekeken door personen die hiertoe niet gemachtigd zijn.
- **Ontbrekende verantwoording**: het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde.
- **Ongewenste verwerkingen:** verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen.

Mpiris wil beroep doen op iedereen die betrokken is bij het verwerken van persoonsgegevens om samen vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle dienstverlening aan te bieden, de verwerking van de persoonsgegevens van alle betrokkenen correct te laten verlopen.

Dit beleid dient als norm voor het verwerken van persoonsgegevens. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentie voor audit en controle. Het biedt elke klant, medewerker en derde een inzage in het veiligheidsbeleid en de manier waarop Mpiris omgaat met persoonsgegevens. Deze tekst draagt ook bij aan de bewustwording omtrent informatieveiligheid.

Het vormt het interne raamwerk dat dient gebruikt te worden bij het ontwerpen van procedures en richtlijnen omtrent gegevensbescherming in relatie tot medewerkers en externen. De relevante onderdelen worden verwerkt in overeenkomsten met personeel en leveranciers.

Het toepassingsgebied van het gegevensbeschermingsbeleid

Het beleid is van toepassing op de verwerking van persoonsgegevens. Mpiris verstaat hieronder niet alleen de persoonsgegevens van klanten, maar ook bijvoorbeeld van medewerkers, al dan niet in dienstverband, bezoekers, derden, … . De Algemene Verordening Gegevensbescherming is niet van toepassing op geanonimiseerde gegevens, dit zijn gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.

Het beleid strekt zich uit tot elke (semi)geautomatiseerde verwerking en tot handmatige verwerkingen indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Het beleid is van toepassing op alle verwerkingsdoeleinden.

Deze beleidstekst dient als norm voor iedereen die binnen Mpiris of in opdracht van Mpiris persoonsgegevens verwerkt. Deze tekst wordt via verschillende kanalen uitgedragen.

De organisatie van gegevensbescherming en informatieveiligheid

De doelstellingen en beleidsprincipes worden omgezet in de organisatiestructuur van Mpiris. Diverse partijen zijn betrokken bij het toepassen van alle relevante aspecten van gegevensbescherming. In dit hoofdstuk worden deze benoemd en wordt hun rol geschetst.

Raad van Bestuur

De eindverantwoordelijkheid voor het naleven van de wettelijke verplichtingen m.b.t. gegevensbescherming als verwerkingsverantwoordelijke rust bij Mpiris, vertegenwoordigd door de Raad van Bestuur. In de uitvoering van het gegevensbeschermingsbeleid bekrachtigt de Raad van Bestuur de beleidsdoelen en kijkt hij toe op de naleving van de wettelijke verplichtingen.

De Raad van Bestuur is bevoegd om beslissingen te nemen die betrekking hebben op:

- De risicoanalyse en bijhorende methodiek;
- De effectieve risicobeoordeling;
- Het ontwikkelen van het informatieveiligheidsbeleid en de bijhorende richtlijnen;
- De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan);
- Het nakomen van alle wettelijke verplichtingen inzake gegevensbescherming.

Stuurgroep Gegevensbescherming (SG)

De Stuurgroep Gegevensbescherming voert het beleid uit en legt beslissingen voor aan de Raad van Bestuur. De SG adviseert de Raad van Bestuur. Momenteel zetelt enkel Johan Desseyn in deze stuurgroep.

De SG bereidt beslissingen van de Raad van Bestuur voor die betrekking hebben op gegevensbescherming, zoals in voorkomend geval:

- Het monitoren van de bedrijfsprocessen die in deze beleidstekst zijn beschreven met het oog op gegevensbescherming;
- Het formuleren van adviesvragen aan de functionaris voor gegevensbescherming;
- Het formuleren van advies aan het directiecomité;
- Het formuleren van voorstellen tot bijsturen van het beleid en toezien op uitvoering ervan op advies van de functionaris;
- Aanpak adviseren aan het directiecomité inzake de beslissingen, prioriteiten en uitvoering van de maatregelen naar aanleiding van de door de functionaris voor gegevensbescherming in kaart gebrachte risico's bij het verwerken van persoonsgegevens;
- De goedkeuring van de classificatieschema's die bijvoorbeeld bepalen wanneer een gegevensbeschermingseffectbeoordeling dient plaats te vinden, evenals de classificatieschema's voor het melden van inbreuken;
- Formuleren van een voorstel van beslissing over alle overwegingen uit hoofde van de Verordening Gegevensbescherming, waaronder verwerkingen gebaseerd op gerechtvaardigd belang, zoals deze die betrekking hebben op kinderen, alsook beslissingen inzake de verenigbaarheid van de doelen bij een latere verwerking van persoonsgegevens;
- Het aanleggen van de nodige documentatie bij alle voorstellen tot beslissingen;
- De rapportering van het beleid gegevensbescherming naar onder meer accreditatiecommissies;
- Het voorbereiden van het jaarlijks informatieveiligheidsplan;
- Jaarlijkse actualisatie van takenmatrix rond informatieveiligheid en gegevensbescherming.

De medewerker

Iedereen (intern of extern) die in opdracht van Mpiris persoonsgegevens verwerkt (bv. inkijkt, wijzigt, …), doet dit volgens de principes uit dit beleid. De medewerker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Stelt zich verantwoordelijk op ten aanzien van de gegevens van betrokkenen die hij/zij verwerkt
- Voert de veiligheidsrichtlijnen uit tijdens zijn/haar verwerkingsopdracht
- Verwerkt enkel die gegevens die horen bij de taak
- Draagt zorg voor de gegevens
- Meldt inbreuken
- Respecteert de discretieplicht

De ICT-leverancier

De ICT-leverancier is verantwoordelijk voor:

- De implementatie van de technische maatregelen en veiligheidsinstellingen in lijn met dit beleid
- Het melden van veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen
- Het fungeren als expert. Vanuit deze rol neemt hij/zij deel aan zowel de identificatie als de remediëring van de informatieveiligheidsrisico's
- Het nastreven van een transparant veiligheidsbeleid door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

Risicobeheer

Mpiris bracht de risico's inzake gegevensbescherming in kaart aan de hand van een risicoanalyse (nulmeting) die werd uitgevoerd in het eerste kwartaal van 2020. De risicoanalyse werd uitgevoerd op basis van volgende criteria (toetsingskader):

- De richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens, zoals deze werden gepubliceerd door de Gegevensbeschermingsautoriteit.
- De Algemene Verordening Gegevensbescherming.
- De ISO 27001 norm rond informatiebeveiliging.

De analyse bracht operationele en tactische risico's in kaart. De bevindingen uit de nulmeting werden besproken en worden opgenomen in een actieplan om de gevonden risico's te behandelen. Hierin worden vier mogelijke risicobehandelingen onderkend:

- Accepteren: een risico wordt geaccepteerd, er worden geen aanvullende maatregelen genomen. Mpiris streeft ernaar zo min mogelijk risico's te accepteren.
- Overdragen: een risico wordt overgedragen waardoor de verantwoordelijkheid ten aanzien van het risico niet langer bij Mpiris rust.
- Beperken: Mpiris neemt de noodzakelijke maatregelen om een risico te beperken zodat het risico wordt teruggebracht tot een niveau waarop het te accepteren is.
- Uitsluiten: Mpiris neemt maatregelen om te voorkomen dat een risico zich überhaupt kan voordoen.

Het doel is dat de risicoanalyse jaarlijks wordt herzien.

Beleidsdoelstellingen voor gegevensbescherming

Algemene doelstellingen

Mpiris in zijn rol als verwerkingsverantwoordelijke:

1. Is transparant over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene als naar de toezichthouders toe. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer persoonsgegevens worden uitgewisseld.
2. Verwerkt enkel de gegevens die relevant zijn voor het uitvoeren van zijn taken. Elke taak waarbij persoonsgegevens worden verwerkt, is rechtmatig. Dit betekent onder meer dat de verwerking in overeenstemming is met de wettelijke en statutaire doelen van Mpiris. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel, waar nodig aan de hand van een gegevensbeschermingseffectbeoordeling.
3. Verwerkt enkel de persoonsgegevens die strikt noodzakelijk zijn voor de uitvoering van de activiteiten zoals benoemd in de gegevensbeschermingsbeleid. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
4. Kijkt toe op de integriteit van de persoonsgegevens tijdens de volledige verwerkingscyclus.
5. Bewaart gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en de rechten en vrijheden van de betrokkene.
6. Voorkomt inbreuken die voortvloeien uit het verwerken van persoonsgegevens. Informatieveiligheid, gegevensbescherming door ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover gerapporteerd in lijn met de regelgeving ter zake.
7. Is in staat om alle geldende rechten van een betrokkene, zoals het recht op inzage, afschrift en eventueel ook schrapping, uit te voeren. Mpiris waakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. Verwerkt gegevens in lijn met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. Mpiris leeft bijgevolg alle wettelijke en normerende kaders na (i.e. zowel Vlaamse, federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe zijn verantwoordelijkheid over de persoonsgegevens en die van anderen duidelijk in kaart gebracht. Mpiris monitort daarenboven ook de in de sector geldende gedragscodes (indien van toepassing) en past deze toe.
9. Kan aantonen dat het alle beleidsdoelstellingen naleeft, conform de wettelijke bepalingen. Deze verantwoordingsplicht wordt bewaakt door intern toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.
10. Stelt een lijst op van criteria die kunnen worden gebruikt om te identificeren of een voorgenomen verwerking een “verhoogd risico” inhoudt voor de betrokkene. Wanneer op basis van de criteria blijkt dat de voorgenomen verwerking een hoog risico inhoudt, wordt een gegevensbeschermingseffectbeoordeling (DPIA) uitgevoerd voorafgaand aan de verwerking. Op basis van de beoordeling worden de nodige maatregelen genomen om het risico op een inbreuk zo veel mogelijk te beperken. Indien de risico’s ondanks maatregelen niet voldoende kunnen worden ingeperkt, moet de verwerkingsverantwoordelijke de Gegevensbeschermingsautoriteit om raad vragen.
11. Beheert naast de lijst van criteria voor het uitvoeren van de gegevensbeschermingseffectbeoordeling (DPIA), ook het bedrijfsproces voor het initiëren, bewaken, bijwerken en uitvoeren ervan.

Verplichtingen van de verwerkingsverantwoordelijke

Los van de algemene verplichtingen zijn er ook een aantal specifieke verplichtingen die de AVG oplegt:

- **Het afsluiten van gepaste verwerkersovereenkomsten**
  Mpiris draagt zorg voor de gepaste verwerkersovereenkomsten met alle verwerkers en ziet toe op de naleving van de voorwaarden die hierin zijn opgenomen.
- **Het bijhouden van een register van verwerkingsactiviteiten**
  Mpiris beheert een register van alle activiteiten waarbij persoonsgegevens worden verwerkt.
- **Maatregelen ter beveiliging van de verwerking**
  Persoonsgegevens mogen slechts verwerkt worden indien er passende technische en organisatorische maatregelen zijn genomen voor het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte persoonsgegevens.
- **Melden van inbreuken in verband met verwerking van persoonsgegevens**
  Uit de AVG volgt een plicht voor Mpiris om een incidentmeldingssysteem voor de interne registratie van inbreuken te hebben die betrekking heeft op het verwerken van persoonsgegevens.
- **Het uitvoeren van een gegevensbeschermingseffectbeoordeling**
  Indien er een verwerkingsactiviteit plaatsvindt die een groot risico vormt voor de rechten en vrijheden van de betrokkene, zal Mpiris een gegevensbeschermingseffectbeoordeling uitvoeren om de risico's te remediëren.
- **Aanstellen van een functionaris voor de gegevensbescherming (DPO)**
  Mpiris moet volgende de huidige wetgeving geen Data Protection Officer aanstellen.
- **Naleving van de rechten van de betrokkene**
  Mpiris dient gedocumenteerde bedrijfsprocessen op te stellen die voorzien in het naleven van de rechten van de betrokkene (het recht op inzage, afschrift, gegevenswissing, rectificatie, beperking van de verwerking, kennisgeving, overdraagbaarheid).

Verplichtingen van Mpiris als verwerker

In geval van verwerkingen waarbij Mpiris verwerker (en geen verwerkingsverantwoordelijke) is, is het verplicht bijstand te verlenen aan de verwerkingsverantwoordelijke.

Zo dient de verwerker de verwerkingsverantwoordelijke zonder onredelijke vertraging te informeren zodra hij kennis heeft genomen van een inbreuk in verband met de persoonsgegevens. Tevens dient de verwerker er zich in een verwerkersovereenkomst toe te verbinden om de verwerkingsverantwoordelijke waar nodig bij te staan bij de verdere afhandeling van de meldingsprocedure (door bv. informatie te verstrekken over de feiten omtrent het incident) en moet hij de nodige maatregelen nemen op niveau van gegevensbeveiliging om het incident te verhelpen.

Daarnaast staat Mpiris de verwerkingsverantwoordelijke bij in het naleven van de rechten van de betrokkene en bij vragen van de verwerkingsverantwoordelijke met het oog op het uitvoeren van een gegevensbeschermingseffectbeoordeling.

Ingeval Mpiris optreedt als verwerker, zal het de noodzakelijke bijdrage leveren aan de beveiliging van de verwerking en zal het een register van verwerkingsactiviteiten aanleggen vanuit de rol van verwerker.

Gegevensbescherming en informatieveiligheid

Onderscheid gegevensbescherming en informatieveiligheid

Informatieveiligheid is een belangrijk onderdeel binnen gegevensbescherming, beide zijn echter wel degelijk verschillend.

Informatieveiligheid betreft de beveiliging van alle soorten informatie binnen een organisatie, waaronder persoonsgegevens. Gegevensbescherming omvat dan weer alle aspecten rond de omgang met persoonsgegevens, waaronder de beveiliging.

Doelstellingen voor informatieveiligheid

Beheer bedrijfsmiddelen

Mpiris beheert een overzicht van alle in gebruik zijnde bedrijfsmiddelen en wie deze in gebruik heeft, het betreft voornamelijk laptops.

Logische toegangscontrole

Dit betreft iedere vorm van toegangscontrole op het niveau van software en systemen waardoor gebruikers van die systemen of software geïdentificeerd en geauthentiseerd worden.

Authenticatiegegevens voor informatieverwerkende systemen (bv. gebruikersnaam en wachtwoord) zijn persoonlijk en dienen niet doorgegeven te worden.

Gebruikers hebben de verantwoordelijkheid om op een veilige manier om te gaan met authenticatiegegevens zoals wachtwoorden en zijn hiervan op de hoogte gebracht door Mpiris.

Het toekennen van authenticatiegegevens gebeurt op een veilige manier waarbij, voor systemen die dit ondersteunen, gebruikers zelf hun wachtwoord kunnen wijzigen. Deze wijziging wordt niet afgedwongen doch wel aangeraden.

De toegang van medewerkers tot projecten en data afkomstig van opdrachtgevers wordt steeds beperkt tot het strikt noodzakelijke.

Cryptografie

Mpiris heeft zijn website beveiligd met een https-verbinding, en heeft alle mobiele informatieverwerkende systemen (laptops) voorzien van full disk encryption.

Fysieke veiligheid en bescherming van de omgeving

Fysieke toegangscontrole betreft het beveiligen van de fysieke omgeving waar data worden bewaard of opgeslagen. Organisatorische toegang betreft de manier waarop de organisatie toegang tot informatie (via rechten, rollen, procedures, organen, …) mogelijk maakt.

Het kantoor is enkel toegankelijk met een badge. Er is een alarm voorzien bij de ingang van het bedrijvencentrum. Er is een automatische schermvergrendeling actief op de werkstations van de medewerkers. Medewerkers worden geacht geen onnodige gegevens (op papier dan wel digitaal) op hun werkplek achter te laten. Er wordt ook gevraagd geen bestanden lokaal te bewaren, alle gegevens zijn beschikbaar via clouddiensten.

Operationele veiligheid

Operationele veiligheid richt zich op de dagdagelijkse processen rond IT en onderhoud die plaatsvinden (bescherming tegen malware en virussen, voorzien van back-ups, logging en monitoring op toepassingen en applicaties, het beheer van gebruikte software en het toepassen van updates).

Back-ups zijn voorzien door de externe dienstverlener. Updates & patching worden uitgevoerd door de medewerkers.

Halfjaarlijks wordt er een fysieke back-up genomen, deze back-up wordt fysiek achter slot bewaard door de Algemeen Directeur.

Communicatieveiligheid

Met veiligheid van communicatie wordt het gebruik van netwerken voor het verzenden van informatie, zowel binnen als buiten de organisatie, bedoeld.

Netwerk is aangelegd en onderhouden door de externe dienstverlener en voorzien van een firewall inclusief spamfilter. Er is een afgescheiden wifi-netwerk aanwezig dat enkel geraadpleegd kan worden door de medewerkers van Mpiris. Voor bezoekers is er het algemeen gastennetwerk dat is afgescheiden van het primaire netwerk van Mpiris.

Voor e-mail beschikt het kantoor over een eigen Exchange server die in onderhoud is bij de externe dienstverlener.

Ontwikkeling en onderhoud van systemen

Mpiris ontwikkelt zelf geen software en maakt gebruik van de software van de externe dienstverlener die in het kader van de verwerkersovereenkomst gehouden is aan het voldoende beveiligen van de gebruikte software.

Leveranciersrelaties

Toegang van leveranciers tot Mpiris-informatie of informatieverwerkende systemen zal beperkt zijn tot hetgeen de leverancier nodig heeft voor de invulling van het contract of de gemaakte afspraken. De gemaakte afspraken bevatten gepaste organisatorische en technische maatregelen ter beveiliging, waar nodig vastgelegd in een verwerkersovereenkomst.

Beheer van informatieveiligheidsincidenten

Een inbreuk in verband met persoonsgegevens is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of verwerkte gegevens.

Ook andere incidenten op vlak van security of informatieveiligheid (ook al is er geen datalek) moeten geregistreerd worden (incidentenbeheer). De wijze waarop men hiermee omgaat, is minstens even belangrijk als het registeren van de incidenten.

Wanneer er zich een inbreuk heeft voorgedaan, zal Mpiris hierop adequaat reageren (al dan niet melden aan de toezichthoudende autoriteit en betrokkenen, de nodige maatregelen nemen). Hiervoor werden een procedure en incidentenregister aangelegd.

Informatieveiligheidsaspecten van bedrijfscontinuïteitsbeheer

Continuïteitsbeheer richt zich hoofdzakelijk op de capaciteiten van een organisatie om in het geval van problemen of calamiteit de noodzakelijke dienstverlening te blijven garanderen.

Alle cloudtoepassingen en servers zijn steeds voorzien van een back-up.

Naleving

Mpiris heeft verantwoordelijkheden toebedeeld om ervoor te zorgen dat alle wettelijke, contractuele, en regelgevende kaders bekend zijn en dat Mpiris hieraan voldoet. Mpiris draagt er zorg voor dat enkel legale software gebruikt wordt en dat deze enkel wordt aangeschaft bij erkende verkopers. Waar nodig zijn voldoende licenties beschikbaar voor het aantal gebruikers van gegeven software.

Mpiris beheert een fysieke opslagruimte voor het bewaren van de noodzakelijke registraties, bijvoorbeeld in verband met de boekhouding, contracten of uitzendkrachten.

Annex: Begrippenkader

Doorheen deze beleidstekst worden verschillende begrippen gebruikt uit het wetgevend kader voor gegevensbescherming en informatieveiligheid. Zij worden hierna kort toegelicht.

Verordening Gegevensbescherming (AVG): de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG. Deze Verordening treedt op 25 mei 2018 in werking. Deze Verordening wordt vaak ook GDPR genoemd (*General Data Protection Regulation*). Recent wordt ook gebruik gemaakt van de term AVG (*Algemene Verordening Gegevensbescherming*).

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (en dus geen rechtspersoon). Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Ook gepseudonimiseerde gegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, zijn dus persoonsgegevens. Anonieme gegevens, die op geen enkele wijze nog kunnen worden gelinkt aan een persoon, vallen niet onder de Verordening Gegevensbescherming.

Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon van wie gegevens worden verwerkt.

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.

Gezamenlijke verwerkingsverantwoordelijken: wanneer een natuurlijke of rechtspersoon samen met een andere natuurlijke of rechtspersoon optreedt als verwerkingsverantwoordelijke. Het is daarbij niet vereist dat de invloed van beide verantwoordelijken evenwaardig is of dat elk van hen in staat is om op zichzelf te voldoen aan de verplichtingen van de Algemene Verordening Gegevensbescherming. Determinerend is dat ze beiden een beslissingsbevoegdheid hebben, ook al is dit niet in dezelfde mate en hebben ze niet dezelfde toegang tot de persoonsgegevens op zich.

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

Medewerkers binnen het Gerechtsdeurwaarderkantoor worden niet als verwerkers beschouwd.

Informatieveiligheid: Informatieveiligheid omvat het geheel van technische en organisatorische maatregelen die ervoor zorgen dat een door het veiligheidsbeleid vooropgesteld veiligheidsniveau wordt nagestreefd. Hierbij staat de integriteit, de beschikbaarheid en de vertrouwelijkheid van de gegevens centraal. Onder de term "**beheersmaatregel**" dienen alle maatregelen verstaan te worden

met betrekking tot het beleid, procedures, richtlijnen, werkwijzen en organisatiestructuren. Deze maatregelen kunnen zowel administratief, technisch, beheersmatig als juridisch van aard zijn.

Gegevensbescherming: Gegevensbescherming bepaalt en streeft de naleving na van de regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens, zoals deze worden bepaald in de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 en de andere regelgevingen die criteria vastleggen die betrekking hebben op de verwerking van deze persoonsgegevens.

Functionaris voor Gegevensbescherming of *Data Protection Officer (DPO)*: een expert die toeziet op de naleving van de Verordening Gegevensbescherming binnen de instelling en die de verwerkingsverantwoordelijke hierin adviseert en bijstaat.

Gegevensbeschermingsautoriteit: De Gegevensbeschermingsautoriteit is verantwoordelijk voor het toezicht op de naleving van de grondbeginselen van de bescherming van de persoonsgegevens.