Data Privacy

beleid

*<Dienst>*

**Verantwoordelijkheden**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Naam** | **Functie** | **Handtekening en datum** |
| Geschreven door |  |  |  |
| Herzien door |  |  |  |
| Goedgekeurd door |  |  |  |

**Aanpassingen historiek**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Reden voor de aanpassing** | **Auteur** | **Versie** |
|  | Initiële aanzet |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Contact informatie**

|  |  |  |  |
| --- | --- | --- | --- |
| **Contact informatie *<Dienst>*** | | | |
| **Naam** | **Functie** | **Telefoon** | **Email** |
|  |  |  |  |
|  |  |  |  |

#### Inhoudsopgave

1. Toepasbaarheid 4

1.1. Voorwoord 4

1.2. Kadrering 4

1.3. Toepassingsgebied 5

1.4. Doelpubliek 6

1.5. Eigenaarschap, goedkeuring, publicatie en herziening van het strategisch informatie veiligheidsbeleid 6

2. beleidsprincipes 7

2.1. Uitganspunt en principes 7

2.2. Wat doet *<Dienst>*? 7

3. Data Privacy beleid 8

3.1. Rollen en verantwoordelijkheden 8

3.2. Bewustwording en training 8

3.3. beleidslijnen 9

4. Naleving en controle 13

5. Verklarende woordenlijst 14

# Toepasbaarheid

## Voorwoord

Opslag en verwerking van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van de diensten voor gezinszorg en aanvullende thuiszorg, de diensten voor logistieke hulp en voor oppashulp. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan cliënten, medewerkers en andere betrokkenen bij deze diensten. *<Dienst>* hecht dan ook veel waarde aan het beschermen van de persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van persoonsgegevens is de verantwoordelijkheid van het bestuur van *<Dienst>*.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt *<Dienst>* haar

verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

## Kadrering

Dit document kadert in de structurele opbouw van een ISMS (Information Security Management System). Inhoudelijk werd elk ISMS gedefinieerd als bestaande uit volgende elementen die continu onderhouden zullen worden door *<Dienst>*:

* Strategisch informatie veiligheidsbeleid;
* (tactische) beleidslijnen;
* operationeel veiligheidsbeleid, actuele situatie;
* operationeel veiligheidsbeleid, streefdoel;
* Operationeel veiligheidsplan;
* Standaarden, procedures, richtlijnen.

Dit document is een tactische beleidslijn in het gelaagde model gebruikt voor de ISMS:



## Toepassingsgebied

Het Data Privacy beleid is van toepassing op alle informatie en informatiesystemen die persoonsgegevens verwerken binnen *<Dienst>* ongeacht:

* de gebruikte technologie;
* de hoedanigheid van de gebruiker;
* de fysieke locatie.

Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen *<Dienst>* waaronder in ieder geval alle medewerkers, cliënten, bezoekers en externe relaties, alsook op andere betrokkenen waarvan *<Dienst>* persoonsgegevens verwerkt.

In het beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van *<Dienst>* alsook op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het beleid bij *<Dienst>* heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij *<Dienst>*.

## Doelpubliek

Het doelpubliek van dit document is:

* alle medewerkers van *<Dienst>*;
* contractanten, leveranciers en overige derden die toegang hebben tot de informatie of informatiesystemen van *<Dienst>* waar persoonsgegevens verwerkt worden (verder in het document gelijkgesteld met medewerkers).

## Eigenaarschap, goedkeuring, publicatie en herziening van het strategisch informatie veiligheidsbeleid

De functionaris gegevensbescherming is de eigenaar van het Data Privacy beleid. Het beleid moet voorgelegd worden aan de Directie voor formele goedkeuring en publicatie.

Dit beleid moet om de 5 jaar, evenals bij belangrijke organisatorische wijzigingen, verhoogde risicosituaties of aanzienlijke veiligheidsincidenten herzien worden.

# beleidsprincipes

## Uitganspunt en principes

Algemeen beleidsuitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden gezocht tussen het belang van *<Dienst>* om persoonsgegevens te verwerken en het belang van de betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

Om aan bovenstaand uitgangspunt te voldoen, gelden de volgende principes:

* Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 6 van de Algemene Verordening Gegevensbescherming[[1]](#footnote-1).
* Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
* Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake en niet bovenmatig te zijn.
* Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
* Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.
* Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
* Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
* Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, rekening houdende met de toepasbare wet- en regelgeving. Hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen.
* Iedere betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de hem betreffende persoonsgegevens conform artikel 15, 16, 17 en 18 van de Algemene Verordening Gegevensbescherming, en heeft het recht van verzet, zoals geformuleerd in hoofdstuk 3.3.6 van dit beleid.
* Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige Opt-in procedure worden aangeboden.

## Wat doet *<Dienst>*?

*<Dienst>* is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. Zij wordt aangemerkt als de verantwoordelijkein de zin van de Algemene Verordening Gegevensbescherming. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van *<Dienst>* uitgevoerd en kan zelfs extern, door een verwerker uitgevoerd worden.

Om zorg te kunnen dragen voor de rechten van alle betrokkenen, investeert *<Dienst>* in verschillende, al dan niet technische trajecten. De communicatie en implementatie van dit beleid is een onderdeel dat kadert in het bewustwordingsproces rond de gevaren van elektronische informatie verwerking en hoe hier mee om te gaan.

Tevens wordt er permanent geïnvesteerd in technische oplossingen om de medewerkers, de cliënten en de eigen omgeving te beschermen.

Dit beleid wordt gedragen door de verschillende directies van *<Dienst>*.

# Data Privacy beleid

## Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden in het kader van informatie veiligheid worden als volgt beschreven:

|  |  |
| --- | --- |
| **Rol** | **Verantwoordelijkheden** |
| Directie Dienst | * Eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen *<Dienst>* * Stelt het beleid, de maatregelen en de procedures op het gebied van verwerking vast. |
| Functionaris gegevensbescherming | * houdt binnen *<Dienst>* toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming. * Geeft advies inzake de verwerkingen van persoonsgegevens. * Rapporteert rechtstreeks aan de Directie. |
| Leidinggevende | * Creëert bewustwording en de naleving van het beleid. * Ziet toe op de naleving van het beleid door zijn medewerkers. * Brengt periodiek het onderwerp privacy onder de aandacht in werkoverleggen.   Rapporteert onverwijld inbreuken op het Data Privacy beleid aan de functionaris gegevensbescherming. |
| IT-verantwoordelijke | * Werkt IT-operationele procedures uit, nodig om het Data Privacy beleid te ondersteunen, * Rapporteert onverwijld veiligheidsincidenten waarbij persoonsgegevens betrokken zijn aan de functionaris gegevensbescherming, * Rapporteert aan de Directie in het kader van bescherming van persoonsgegevens. |
| Gebruiker | * Zorgt ervoor dat hij/zij op de hoogte is van het Data Privacy beleid; * Past dit beleid toe op zijn/haar dagelijkse activiteiten; * Rapporteert inbreuken op het Data Privacy beleid en aan zijn/haar leidinggevende. |

## Bewustwording en training

Het zorgvuldig omgaan met persoonsgegevens is ieders verantwoordelijkheid. Er wordt van alle medewerkers verwacht dat ze zich integer gedragen. Het is niet aanvaardbaar dat door al dan

niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot materiële (zoals financiële schade, imagoschade, reputatie/stigmatisering) en/of immateriële schade (aantasting van de fysieke integriteit: verlies aan zelfstandigheid, gelijkheid, bewegingsvrijheid, ongestoord leven, autonomie) van personen.

Beleid en maatregelen zijn echter niet altijd voldoende om risico’s rond het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om bij *<Dienst>* het bewustzijn voortdurend aan te scherpen, zodat kennis van de risico’s wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd. Dit beleid moet dan ook uitgedragen worden door regelmatig terugkerende bewustwordingscampagnes.

## Beleidslijnen

### Grondslag, doelbinding en belangen-afweging

Het verwerken van persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 6 van de Algemene Verordening Gegevensbescherming. De verwerkingsverantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd.

Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de rechtmatigheid, behoorlijkheid en transparantie. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Het verwerken van bijzondere persoonsgegevens (gegevens betreffende iemands godsdienst of

levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een

vakvereniging en strafrechtelijke gegevens) is verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Er gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

*<Dienst>* treft de nodige maatregelen om te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. persoonsgegevens dienen na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie gebracht te worden. *<Dienst>* zal de persoonsgegevens na het verlopen van de bewaartermijn op adequate wijze vernietigen.

Bij projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren.

*<Dienst>* hanteert bij de implementatie de principes “Privacy by Design” en “Privacy by Default”.

Bij *<Dienst>* worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van persoonsgegevens te erkennen en daarnaar te handelen. Ook medewerkers voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

### Organisatie van de beveiliging

*<Dienst>* draagt zorg voor een afdoend beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies, niet-geoorloofde toegang of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er tevens op gericht onnodige en/of onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van *<Dienst>*.

### Documenteren van verwerkingen

Elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens wordt gedocumenteerd in een register van verwerkingen. Dit register wordt door de functionaris gegevensbescherming op regelmatige basis gecontroleerd.

Dit register omvat minstens:

* Contactgegevens verantwoordelijke & functionaris gegevensbescherming, betrokken verwerkers,
* Doeleinden van de verwerking,
* Soort persoonsgegevens,
* Ontvanger persoonsgegevens,
* Of er sprake is van doorgifte naar buitenland,
* Bewaringstermijnen,
* Overzicht van de beveiligingsmaatregelen.

Dit register moet steeds op eenvoudige vraag aan de ‘Commissie voor de Bescherming van de Persoonlijke Levenssfeer’ (CBPL ook privacycommissie genoemd) ter beschikking gesteld worden.

### Doorgifte aan derden

Indien *<Dienst>* persoonsgegevens laat verwerken door een verwerker, wordt de uitvoering van deze verwerkingen geregeld in een schriftelijke overeenkomst, de verwerkingsovereenkomst, tussen *<Dienst>*, als verwerkingsverantwoordelijke, en de verwerker.

*<Dienst>* verstrekt persoonsgegevens alleen aan derden binnen de Europese Economische Ruimte, als deze doorgifte is gebaseerd op een wettelijke grondslag en volgens de bepalingen van de Algemene Verordening Gegevensbescherming.

Doorgifte aan landen buiten de Europese Economische Ruimte is niet toegelaten zonder bijkomend advies van de CBPL.

### Incidenten met betrekking tot persoons-gegevens

Elke inbreuk, per ongeluk of onrechtmatig, die leidt tot vernietiging, verlies, ongeoorloofde wijziging of toegang, of niet geautoriseerde vrijgave van persoonsgegevens is een incident met betrekking tot persoonsgegevens. Dit is dus ruimer dan enkel verlies van persoonsgegevens, ook een inbreuk op de beveiliging met gevolgen voor persoonsgegevens kan hiertoe ondergebracht worden.

Incidenten kunnen gemeld worden bij het meldpunt voor incidenten rond persoonsgegevens of in uitzonderlijke gevallen bij een vertrouwenspersoon of personeelsbegeleiding van *<Dienst>*.

Van elk incident en de afhandeling daarvan zal een registratie bijgehouden worden.

Een incident kan gemeld worden door een betrokkene, een verwerker of een personeelslid.

Incidenten worden zo veel mogelijk doorgezet naar de verantwoordelijke afdeling of persoon en

vervolgens conform de daarvoor vastgestelde procedures afgehandeld. De functionaris gegevensbescherming wordt steeds op de hoogte gebracht van incidenten met mogelijke gevolgen voor persoonsgegevens.

Alle incidenten waarbij persoonsgegevens betrokken zijn (of kunnen zijn), moeten gedocumenteerd worden in een logboek, conform de vereisten van de Algemene Verordening Gegevensbescherming. Dit logboek omvat minstens volgende elementen:

* + Aard van de inbreuk,
  + Categorieën van betrokkenen en van persoonsgegevens,
  + Aantal betrokkenen (bij benadering),
  + Waarschijnlijke gevolgen van de inbreuk,
  + Voorgestelde of genomen maatregelen.

Als de persoonsgegevens van betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van *<Dienst>* ernstig in gevaar zijn, wordt in ieder geval de Directie en de functionaris gegevensbescherming op de hoogte gesteld.

Incidenten met waarschijnlijk risico op de rechten en vrijheden van betrokkenen, moeten tevens binnen 72u gemeld worden aan de CBPL en indien er sprake is van een waarschijnlijk hoog risico, moeten ook de betrokkenen op de hoogte worden gebracht.

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportering daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens.

### Rechten van betrokkenen

*<Dienst>* beoogt de verwerking van persoonsgegevens van cliënten, medewerkers en andere

betrokkenen door middel van *data privacy disclaimer* mede te delen. Daarnaast beoogt *<Dienst>* in overeenstemming met de wet, alle betrokkenen onder bepaalde omstandigheden rechten te verschaffen waarmee zij de aan hen toebehorende persoonsgegevens naar behoren kunnen beschermen.

Iedere betrokkene heeft recht op inzage in hem betreffende verwerkte persoonsgegevens. Een verzoek hiertoe kan schriftelijk worden ingediend bij *<E-mailadres van de instelling | Adres van de Dienst>*. Een verzoek tot inzage van minderjarigen die de leeftijd van 18 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger. *<Dienst>* draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.

Indien gegevens worden verwerkt, bevat de mededeling van *<Dienst>* een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van de doeleinden van de verwerking, de categorieën van gegevens waarop verwerking betrekking heeft en de categorieën van ontvangers, alsmede beschikbare informatie over herkomst van de gegevens en de termijn van bewaring van gegevens. Iedere eerste aanvraag kan kosteloos worden ingediend. Bijkomende vragen tot informatie kunnen echter leiden tot administratieve kosten in rekening gebracht bij de betrokkene.

Iedere betrokkene kan met betrekking tot over hem opgenomen persoonsgegevens bij *<Dienst>* van deze gegevens verzoeken die te wijzigen, verbeteren of aan te vullen. Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige Opt-in procedure worden aangeboden.

Indien opgenomen persoonsgegevens van de betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de verwerking onvolledig zorgt de verwerkingsverantwoordelijk voor een verbetering van deze gegevens. Bovendien worden derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld.

Indien de betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij *<Dienst>*.

# Naleving en controle

De Directie behoudt het recht om controles betreffende de naleving van de gedragsregels uit te voeren of te laten uitvoeren. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De functionaris gegevensbescherming initieert eventueel in samenwerking met de veiligheidsconsulent en/of de interne auditor de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens

Bij misbruiken en inbreuken op de beleidslijnen kan de Directie gepaste sancties opleggen (zie Arbeidsreglement).

De bovenstaande voorwaarden zijn niet van toepassing wanneer gerechtelijke autoriteiten gegevens van een bepaald medewerker opvorderen in het kader van een opsporingsonderzoek of een gerechtelijk onderzoek.

# Verklarende woordenlijst

TBD

|  |  |
| --- | --- |
| **Term** | **Definitie** |
| Betrokkene | Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft. |
| Opt-in | Procedure waarbij de betrokkene expliciet de keuze moet maken om in te stappen. |
| Opt-out | Deze regeling houdt in dat betrokkenen niets hoeven te doen om mee te doen met de regeling, maar de mogelijkheid hebben ervan af te zien. |
| Persoonsgegevens | Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon. |
| Privacy by default | Ontwikkelingsprincipe waarbij waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid en integriteit standaard ingesteld zijn. |
| Privacy by design | Het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens. |
| Verwerker | Een door de Dienst ingeschakelde (derde) partij die ten behoeve van de Dienst persoonsgegevens verwerkt. |
| Verwerking | Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens. |
| Verwerkingsverantwoordelijke | Bestuurlijk orgaan dat het doel van en middelen voor de  verwerking van persoonsgegevens vaststelt. |

1. 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 [↑](#footnote-ref-1)