

## PRIVACYREGLEMENT

### Inhoudsopgave

Voorwoord .....	2
Privacybepalingen .....	3
1. Begripsbepalingen .....	3
2. Toepassingsgebied.....	3
3. Doel van de verwerking van persoonsgegevens .....	4
4. Verwerking van Persoonsgegevens .....	4
5. Geheimhoudingsplicht .....	4
6. Verzet .....	4
7. Recht op inzage, afschrift en dataportabiliteit van persoonsgegevens.....	5
8. Recht op correctie/verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens ..	5
9. Recht op vernietiging van persoonsgegevens.....	5
10. Bewaren .....	5
11. Beveiliging.....	5
12. Waar kunnen de persoonsgegevens worden vastgelegd.....	6
13. Meldplicht datalekken .....	6

## Voorwoord

Iedereen heeft recht op bescherming van zijn persoonlijke levenssfeer. Om die bescherming te waarborgen geef de Wet Algemene verordening gegevensbescherming (AVG) aan hoe we moeten omgaan met persoonsgegevens, wat de rechten zijn degene van wie persoonsgegevens worden verwerkt en wat de plichten zijn van degene die met de gegevens werkt.

Binnen Futuris Zorg en Werk werken we met persoonsgegevens van medewerkers, cliënten en sollicitanten. Met dit reglement willen we inzicht geven in de manier waarop wij met gegevensverwerking omgaan.

In dit reglement zijn de algemene privacy bepalingen rondom gegevensverwerking opgenomen en de rechten en plichten van partijen.

## Privacybepalingen

### 1. Begripsbepalingen

In dit reglement wordt verstaan onder:

- a. *Persoonsgegevens*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
- b. *Gezondheidsgegevens*: persoonsgegevens die direct of indirect betrekking hebben op de lichamelijke of de geestelijke gesteldheid van betrokkenen;
- c. *Verwerking van persoonsgegevens*: elke handeling of een 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 ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
- d. *Verstrekken van persoonsgegevens*: het bekend maken of ter beschikking stellen van gegevens
- e. *Bestand*: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
- f. *Verantwoordelijke*: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
- g. *Bewerker*: diegene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt;
- h. *Betrokkene*: degene op wie een persoonsgegeven betrekking heeft of zijn vertegenwoordiger;
- i. *Derde*: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, diegene(n) die onder gezag van de verantwoordelijke of de bewerker gemachtigd is / zijn om persoonsgegevens te verwerken;
- j. *Toestemming van betrokkene*: elke vrije, specifieke en op informatie berustende wilsuiting waarmee betrokkene aanvaardt dat de hem/haar betreffende persoonsgegevens worden verwerkt;
- k. *De Autoriteit Persoonsgegevens (AP)*: de organisatie die tot taak heeft toe te zien op de verwerking van persoonsgegevens krachtens de Wet Bescherming Persoonsgegevens;
- l. *AVG*: Algemene verordening gegevensbescherming;
- m. *Datalekken*: toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens die een inbreuk hebben op de beveiliging van persoonsgegevens, zonder dat dit de bedoeling was.

### 2. Toepassingsgebied

Dit reglement is van toepassing binnen Futuris Zorg en Werk BV en heeft betrekking op alle door of vanwege Futuris geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

### 3. Doel van de verwerking van persoonsgegevens

1. Persoonsgegevens worden in overeenstemming met de wet en dit reglement op behoorlijke en zorgvuldige wijze verwerkt en alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
2. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
3. Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.

### 4. Verwerking van persoonsgegevens

Persoonsgegevens mogen slechts worden verwerkt indien aan een van onderstaande voorwaarden is voldaan:

- A. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
- B. dit noodzakelijk is voor de uitvoering van de overeenkomst waarbij de betrokkene partij is, of voor handelingen die op verzoek van de betrokkene worden verricht en die noodzakelijk zijn voor het sluiten van een overeenkomst;
- C. dit noodzakelijk is om een wettelijke verplichting na te komen;
- D. dit noodzakelijk is ter bestrijding van ernstig gevaar voor de gezondheid van de betrokkene;
- E. dit noodzakelijk is met het oog op het belang van de verantwoordelijke of van een derde en het belang van degene van wie de gegevens worden verwerkt niet prevaleert.

### 5. Geheimhoudingsplicht

De gegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding zijn verplicht.

### 6. Verzet

1. De betrokkene kan zich verzetten tegen verwerking van hem betreffende persoonsgegevens op grond van persoonlijke omstandigheden.
2. Binnen 4 weken na ontvangst van het verzet wordt beoordeeld of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is, beëindigt hij terstond de verwerking. Indien de betrokkene het niet eens is met de beslissing, heeft de betrokkene het recht bezwaar te maken tegen opnamen van persoonsgegevens.

## 7. Recht op inzage, afschrift en dataportabiliteit van persoonsgegevens

1. De betrokkene heeft het recht kennis te nemen van de op zijn persoon betrekking hebbende verzamelde en verwerkte gegevens. Hij dient daartoe een (schriftelijk) verzoek om inzage te doen.
2. De gevraagde inzage en/of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen 4 weken, plaatsvinden of respectievelijk worden verstrekt.
3. Recht op inzage of afschrift kan worden geweigerd voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander. Slechts in uitzonderingsgevallen zal het belang van een ander dan de betrokkene prevaleren.
4. In geval van een verzoek om een afschrift van de persoonsgegevens van betrokkene heeft de betrokkene in verband met dataportabiliteit het recht een afschrift van de persoonsgegevens te ontvangen in een vorm die het voor betrokkene makkelijk maakt om zijn gegevens te hergebruiken en door te geven.

## 8. Recht op correctie/verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens

1. De betrokkene kan verzoeken om verbetering/correctie, aanvulling, verwijdering, gedeeltelijke verwijdering of afscherming van de op hem betrekking hebbende gegevens indien deze feitelijk onjuist voor het doel van de verwerking, onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift verwerkt zijn/worden.
2. De verzoeker wordt zo spoedig mogelijk, doch binnen 4 weken na ontvangst van het verzoek, schriftelijk bericht of, en dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.
3. De verantwoordelijke die op verzoek persoonsgegevens heeft verbeterd, aangevuld, verwijderd of afgeschermd, is verplicht aan derden aan wie de gegevens daaraan voorafgaand zijn verstrekt, zo spoedig mogelijk kennis te geven van de verbetering, aanvulling, verwijdering of afscherming, tenzij dit onmogelijk blijkt of een onevenredige inspanning vraagt.

## 9. Recht op vernietiging van persoonsgegevens

1. De betrokkene kan heeft het recht te verzoeken om vernietiging van de op hem betrekking hebbende gegevens. Daarvoor dient hij een schriftelijk gemotiveerd verzoek in te dienen.
2. Het verzoek tot vernietiging kan slechts geweigerd worden indien bewaring op grond van een wettelijk voorschrift vereist is, dan wel redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene.

3. De betreffende gegevens worden uiterlijk binnen drie maanden na daartoe strekkend verzoek vernietigd. Deze beslissing wordt schriftelijk aan de betrokkene mede gedeeld.

## 10. Bewaren

1. Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.
2. Persoonsgegevens mogen langer worden bewaard dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, wanneer zij geanonimiseerd worden of voor zover ze uitsluitend voor historische, statische of wetenschappelijke doeleinden worden bewaard.
3. De verantwoordelijke stelt vast hoe lang de opgenomen persoonsgegevens bewaard blijven.
4. De bewaartermijn is in beginsel 15 jaar, te rekenen vanaf datum dat de begeleiding is beëindigd.

## 11. Beveiliging

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de ten uitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich mee brengen.

## 12. Waar kunnen persoonsgegevens worden vastgelegd

- Elektronisch cliëntendossier
- Papieren cliëntendossier
- Financiële en administratieve gegevens
- Klachtenregistratie en klachtenbehandeling
- Archiefregistratie
- Kwaliteitsbewaking

## 13. Meldplicht datalekken

1. De verantwoordelijke is verplicht ernstige datalekken binnen 72 uur te melden bij de Autoriteit Persoonsgegevens (AP). Dit is het geval wanneer het datalek een waarschijnlijke kans op nadelige gevolgen heeft of kan hebben voor de bescherming van persoonsgegevens.
2. De verantwoordelijke stelt de betrokkene onverwijld in kennis van het datalek indien er sprake is van een hoog risico op een inbreuk op de persoonlijke levenssfeer.

3. De melding aan het AP en eventueel de betrokkene omvat in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
4. De melding omvat tevens een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.
5. De melding aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.
6. Indien de verantwoordelijke geen melding aan de betrokkene doet, kan het AP, indien het van oordeel is dat inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog melding doet.
7. De verantwoordelijke houdt een overzicht bij van iedere ernstige datalek/inbreuk. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk alsmede de tekst van de melding aan de betrokkene.

## STROOMSCHEMA MELDPPLICHT DATALEKKEN

