PRIVACYREGLEMENT

Persoonsgegevens bij ProgresZorg

Uw privacy is voor ProgresZorg van groot belang. Wij houden ons dan ook aan de Algemene Verordening Gegevensbescherming, waarin is geregeld hoe met uw persoonsgegevens moet worden omgegaan. Hierin staat ook dat wij moeten kunnen aantonen dat wij ons aan de wet houden. Wij hebben de privacy van onze cliënten, medewerkers en anderen hoog in het vaandel staan. In dit reglement hebben wij de verplichtingen van ProgresZorg en de rechten van onze cliënten (of hun vertegenwoordigers) beschreven.

1. Begrippen

In dit reglement worden de volgende begrippen gebruikt.

- Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
- Bijzondere persoonsgegevens: persoonsgegevens die door de AVG als bijzondere categorie worden aangemerkt, waaronder gegevens over gezondheid.
- Verwerken: elke bewerking met betrekking tot persoonsgegevens, zoals verzamelen, vastleggen, raadplegen, gebruiken, verstrekken en verwijderen.
- U: de cliënt die zorg of begeleiding ontvangt van ProgresZorg.
- Vertegenwoordiger: degene die op grond van de wet of een schriftelijke volmacht namens u handelt (zie paragraaf 11).
- ProgresZorg: de zorgaanbieder die dit reglement hanteert en in beginsel verwerkingsverantwoordelijke is.

2. Toepassingsbereik en doel

Dit reglement is van toepassing op de verwerking van persoonsgegevens door ProgresZorg, zowel op papier als digitaal.
Het reglement beschrijft welke persoonsgegevens ProgresZorg verwerkt, voor welke doelen dit gebeurt, met wie gegevens kunnen worden gedeeld, hoe ProgresZorg gegevens beveiligt en welke rechten u heeft.
Dit reglement ziet in het bijzonder op persoonsgegevens van u en, voor zover relevant, van uw vertegenwoordiger, contactpersonen, partner en/of familieleden en (huis)artsen of andere behandelaren.

3. Verwerkingsverantwoordelijke en contact

ProgresZorg is verwerkingsverantwoordelijke voor de persoonsgegevens die zij verwerkt in het kader van de zorg- en dienstverlening, de bedrijfsvoering en het voldoen aan wettelijke verplichtingen.

Contactgegevens ProgresZorg:
Friesestraatweg 211A, Groningen
Telefoon: 06 41 76 80 97
E-mail: info@progreszorg.nl

Contactpersoon privacy:
Manisha Maduro-Ramlal
Telefoon: 06 41 76 80 97
E-mail: info@progreszorg.nl

4. Welke persoonsgegevens verwerkt ProgresZorg en waarvoor

ProgresZorg verwerkt alleen persoonsgegevens die noodzakelijk zijn voor de zorg- en dienstverlening, uw ondersteuning, de bedrijfsvoering en het voldoen aan wettelijke verplichtingen.

a. *Algemene persoonsgegevens en contactgegevens*
ProgresZorg verwerkt onder meer uw naam, geboortedatum en contactgegevens.
Ook kan ProgresZorg contactgegevens verwerken van een (wettelijk) vertegenwoordiger of contactpersoon.
Daarnaast kan ProgresZorg verzekerings- en indicatiegegevens en gegevens over verleende zorgproducten verwerken.
Voor zover relevant kan ProgresZorg gegevens verwerken over uw sociale netwerk.
Deze gegevens gebruikt ProgresZorg voor uitvoering van de zorgovereenkomst, communicatie en voor verantwoording en declaratie.

b. *Burgerservicenummer (BSN)*
ProgresZorg kan uw BSN verwerken wanneer dit wettelijk is voorgeschreven, onder meer voor identificatie en voor uitwisseling van gegevens binnen de zorgketen. Het gebruik van het BSN in de zorg is geregeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Wet gebruik burgerservicenummer in de zorg.

c. *Gezondheidsgegevens en begeleidingsgegevens*
ProgresZorg verwerkt gezondheids- en begeleidingsgegevens over u voor het vaststellen, toetsen, volgen en uitvoeren van de individuele zorg- en dienstverlening.

d. *Medicatiegegevens*
ProgresZorg kan gegevens verwerken over voorgeschreven en toegediende medicatie, voor zover dit nodig is voor veilige zorg en verantwoording.

e. *Incidenten, kwaliteit en veiligheid*
ProgresZorg kan gegevens verwerken over incidenten, getroffen maatregelen en eventuele schade, voor kwaliteitsbewaking en het verbeteren van de veiligheid van cliënten en medewerkers.

f. *(Seksueel) grensoverschrijdend gedrag of misbruik*
Wanneer noodzakelijk voor zorg, nazorg, het voorkomen van herhaling of voor wettelijke verplichtingen, kan ProgresZorg gegevens verwerken over de toedracht en de ondernomen acties.

Grondslagen
ProgresZorg verwerkt persoonsgegevens op basis van wettelijke grondslagen.
Voor gewone persoonsgegevens gaat het meestal om uitvoering van de zorgovereenkomst, wettelijke verplichtingen of een gerechtvaardigd belang (zoals veiligheid en kwaliteitsbewaking).

Gezondheidsgegevens en andere bijzondere persoonsgegevens worden alleen verwerkt als de wet dit toestaat, bijvoorbeeld omdat verwerking nodig is voor het verlenen van zorg of begeleiding. Wanneer toestemming nodig is (bijvoorbeeld voor publicatie van foto's) wordt dit expliciet gevraagd.
Toestemming kan altijd worden ingetrokken; intrekking werkt voor de toekomst.

5. Overige (bijzondere) persoonsgegevens

ProgresZorg verwerkt in beginsel geen persoonsgegevens over godsdienst of levensovertuiging, seksuele gerichtheid, politieke opvattingen of ras.
Als verwerking van dergelijke gegevens aantoonbaar noodzakelijk is voor de zorg of begeleiding, of als een wettelijke uitzondering geldt, kan verwerking toch plaatsvinden.
Foto's worden alleen vastgelegd of gepubliceerd als dit nodig is voor de dienstverlening of als daarvoor uitdrukkelijke toestemming is gegeven.
Euthanasieverklaringen en reanimatieverklaringen worden alleen vastgelegd op uw verzoek, voor zover dit passend is binnen het dossier en de zorgverlening.
Voor veiligheid kan ProgresZorg signaleringsinformatie vastleggen (zoals agressie- of veiligheidsincidenten) wanneer dit noodzakelijk is voor veilige zorg. Daarbij wordt zo min mogelijk vastgelegd en alleen wat relevant is.

6. Hoe verkrijgt ProgresZorg de persoonsgegevens

De meeste gegevens ontvangt ProgresZorg van u en/of uw vertegenwoordiger bij de start van de zorg en gedurende de zorgverlening.
Daarnaast kan ProgresZorg, voor zover toegestaan, gegevens ontvangen van andere zorgaanbieders, verwijzers of ketenpartners.
Het dossier en/of begeleidingsplan vult zich gedurende de periode dat u bij ProgresZorg in zorg bent.

7. Met wie deelt ProgresZorg persoonsgegevens

ProgresZorg deelt uw persoonsgegevens niet met derden, tenzij dit nodig is voor de zorgverlening, de uitvoering van de zorgovereenkomst, het voldoen aan een wettelijke verplichting of wanneer toestemming is gegeven.

a. *Intern gebruik*
   Intern worden persoonsgegevens alleen gebruikt door medewerkers die deze gegevens nodig hebben voor hun werkzaamheden.
   ProgresZorg richt haar systemen en werkwijze zodanig in dat medewerkers alleen toegang hebben tot gegevens die passen bij hun rol.

b. *Delen binnen het zorgteam*
   Persoonsgegevens kunnen binnen het zorgteam worden gedeeld voor zover dit noodzakelijk is voor uw zorg en begeleiding of voor de organisatie van de zorg.

c. *Verplichte doorgifte en wettelijke verplichtingen*
   ProgresZorg kan verplicht zijn gegevens te delen met zorgkantoor, zorgverzekeraar en gemeenten, bijvoorbeeld voor declaraties en verantwoording.

In bijzondere situaties kan ProgresZorg verplicht zijn gegevens te verstrekken aan andere instanties, bijvoorbeeld op grond van een wettelijke verplichting of een rechterlijke uitspraak.

d. *Inschakeling van verwerkers*
ProgresZorg kan gebruikmaken van software en ICT-diensten van leveranciers.
Als leveranciers persoonsgegevens verwerken in opdracht van ProgresZorg, sluit ProgresZorg een verwerkersovereenkomst met afspraken over beveiliging, geheimhouding en gebruik van persoonsgegevens.

e. *Overige doorgifte*
Als ProgresZorg gegevens wil verstrekken aan anderen, gebeurt dit alleen wanneer daarvoor een grondslag bestaat en, waar nodig, nadat toestemming is verkregen.

f. *Doorgifte buiten de Europese Economische Ruimte*
Door of namens ProgresZorg worden in beginsel geen gegevens verwerkt buiten de Europese Economische Ruimte. Als ProgresZorg toch persoonsgegevens doorgeeft naar landen buiten de Europese Economische Ruimte, gebeurt dit alleen wanneer de AVG dit toestaat en wanneer passende waarborgen zijn getroffen.

8. Beveiliging en geheimhouding

ProgresZorg neemt passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang en onrechtmatige verwerking.
Maatregelen kunnen onder meer zijn: persoonlijke accounts, tweestapsverificatie waar beschikbaar, logging, versleutelde overdracht waar passend en afgesloten opslag voor papieren dossiers.
Iedereen die bij ProgresZorg met persoonsgegevens werkt (waaronder medewerkers, vrijwilligers, stagiaires en ingehuurde krachten) heeft een geheimhoudingsplicht. ProgresZorg zorgt ervoor dat deze personen passend worden geïnstrueerd over de omgang met persoonsgegevens.

9. Bewaartermijnen

ProgresZorg bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor de gegevens zijn verzameld, tenzij een langere bewaartermijn voortvloeit uit een wettelijke verplichting of uit de zorg van een goed hulpverlener.
Uw dossier: ProgresZorg hanteert een bewaartermijn van minimaal 20 jaar, te rekenen vanaf de laatste wijziging in het dossier, tenzij langer bewaren noodzakelijk is.
Toedienlijsten en medicatieadministratie: gebruikte toedienlijsten worden in beginsel minimaal twee jaar bewaard.
Als langer bewaren redelijkerwijs nodig is (bijvoorbeeld bij incidenten, klachten of lopende procedures), kan langer bewaren passend zijn.
Overige gegevens worden verwijderd of vernietigd zodra ze niet meer nodig zijn, tenzij ook daarvoor een wettelijke bewaarplicht geldt.

10. Uw rechten

Op grond van de AVG heeft u verschillende rechten. Het gaat onder meer om het recht op inzage, rectificatie en aanvulling, het recht op wissing van persoonsgegevens, het recht op beperking van de verwerking, het recht op gegevensoverdraagbaarheid en het recht van bezwaar.
ProgresZorg beoordeelt ieder verzoek zorgvuldig en kan een verzoek (gedeeltelijk) weigeren wanneer dit is toegestaan, bijvoorbeeld ter bescherming van de rechten en vrijheden van anderen of vanwege wettelijke bewaarplichten.

U kunt uw verzoek indienen via de contactpersoon privacy (zie paragraaf 3).
ProgresZorg reageert in beginsel binnen één maand na ontvangst van uw verzoek.
Als uw verzoek complex is of als er meerdere verzoeken zijn, kan deze termijn met maximaal twee maanden worden verlengd. In dat geval ontvangt u binnen één maand bericht.
Bij inzage verstrekt ProgresZorg in beginsel kosteloos een eerste kopie van de persoonsgegevens waarop uw verzoek betrekking heeft.
Voor extra kopieën kan ProgresZorg een redelijke vergoeding vragen.
ProgresZorg kan vragen om legitimatie of aanvullende verificatie om te voorkomen dat gegevens aan de verkeerde persoon worden verstrekt.

11. Vertegenwoordiging

Als u niet in staat of bevoegd bent om zelfstandig uw rechten uit te oefenen, handelt uw vertegenwoordiger namens u volgens de wettelijke regels.
ProgresZorg kan vragen om bewijs van vertegenwoordiging (bijvoorbeeld gezag, een beschikking of een schriftelijke volmacht).

a. *Minderjarigen*
   - Jonger dan 12 jaar: vertegenwoordiging door ouders met gezag of de voogd.
   - 12 tot en met 15 jaar: u en uw ouders/voogd treden gezamenlijk op, als u in staat bent tot een redelijke waardering van uw belangen.
     Als u niet in staat bent tot een redelijke waardering van uw belangen, treden uw ouders/voogd op als vertegenwoordiger.
   - 16 of 17 jaar: u oefent uw rechten in beginsel zelfstandig uit, als u in staat bent tot een redelijke waardering van uw belangen.
     Als u niet in staat bent tot een redelijke waardering van uw belangen, treden uw ouders/voogd op als vertegenwoordiger.
     Ouders/voogd worden voor informatieverstrekking en inzage in beginsel als derden beschouwd.
     Informatieverstrekking aan ouders/voogd gebeurt alleen als de wet dit toestaat of als u daarmee instemt.

b. *Volwassenen die wilsonbekwaam zijn*
   Als u 18 jaar of ouder bent en niet in staat kan worden geacht tot een redelijke waardering van uw belangen, treedt als vertegenwoordiger op, in de volgende volgorde.
   - de curator of mentor (indien een maatregel is ingesteld);
   - de persoonlijk gemachtigde (schriftelijk aangewezen);
   - de echtgenoot, geregistreerd partner of andere levensgezel;
   - een ouder, kind, broer of zus, grootouder of kleinkind.

De vertegenwoordiger betracht de zorg van een goed vertegenwoordiger en betrekt u zoveel mogelijk bij beslissingen.

12. Datalekken en meldplicht

Een datalek is een inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens.
Als ProgresZorg een datalek constateert, neemt ProgresZorg direct maatregelen om het datalek te stoppen en de gevolgen te beperken.
ProgresZorg registreert ieder datalek in een intern datalekregister.

Als melding bij de Autoriteit Persoonsgegevens verplicht is, doet ProgresZorg dit zonder onredelijke vertraging en, waar mogelijk, uiterlijk binnen 72 uur.
Een melding blijft achterwege als het niet waarschijnlijk is dat het datalek een risico inhoudt voor uw rechten en vrijheden.
Als het datalek waarschijnlijk een hoog risico inhoudt, informeert ProgresZorg u onverwijld.
ProgresZorg heeft een Datalek-protocol opgesteld waarin een en ander verder is uitgewerkt.

13. Klachten

Als u vindt dat ProgresZorg niet op de juiste manier omgaat met uw persoonsgegevens, kunt u contact opnemen met de contactpersoon privacy (zie paragraaf 3).
Ook kunt u een klacht indienen via de klachtenregeling van ProgresZorg, zoals vermeld op de website.
Daarnaast heeft u het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

14. Wijzigingen en inzage

ProgresZorg kan dit reglement aanpassen wanneer wet- en regelgeving of de werkwijze daarom vraagt.
De meest recente versie is beschikbaar via ProgresZorg. Op verzoek kan een papieren versie worden verstrekt.

Privacyreglement ProgresZorg, december 2025

BIJLAGE: DATALEK-PROTOCOL[1]

Bij een datalek geldt het volgende protocol:

1. Zorg voor overzicht op de situatie.
2. Neem onmiddellijk maatregelen om het datalek te stoppen en de schade van het datalek te beperken. Schat daarbij ook de risico's in.
3. Bepaal of het datalek wel of niet moet worden gemeld aan de Autoriteit Persoonsgegevens. Zo ja, dan doen we dit zo snel mogelijk.
4. Bepaal of de betrokkenen wel of niet geïnformeerd moeten worden. Zo ja, dan doen we dit zo snel mogelijk.
5. Registreer het datalek in het interne datalekregister.

Een uitwerking van dit protocol is hieronder opgenomen:

Stap 1: Overzicht krijgen bij datalek
De eerste stap bij een datalek is zorgen voor overzicht op de situatie, zodat de juiste vervolgstappen genomen kunnen worden. Daarvoor moet allereerst duidelijk zijn om wat voor soort datalek het gaat.

Zodra bekend is om wat voor soort datalek het gaat, dan helpen de volgende vragen om verder overzicht te krijgen op de situatie:

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En is het datalek nog steeds gaande?
- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn gelekt? Bijvoorbeeld naam, adres, e-mailadres en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het?
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Is er zicht op wie die onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?
- Welke maatregelen zijn vooraf getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Stap 2: Beperken schadelijke gevolgen datalek
Hoe de gevolgen van een datalek beperkt kunnen worden, hangt volledig af van de situatie. Ten eerste moet het datalek onmiddellijk gestopt worden als het nog bestaat. Daarnaast moeten er maatregelen worden genomen om de negatieve gevolgen te beperken.

Voorbeelden van maatregelen om schade bij een datalek te beperken zijn:

- Een laptop, tablet of smartphone op afstand wissen of versleutelen.
- Een gepubliceerd bestand offline halen.

[1] Bij het opstellen van dit protocol is gebruik gemaakt van de informatie van de Autoriteit Persoonsgegevens over wat te doen bij datalekken.

- Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd. Hoewel op basis van zo'n bevestiging niet 100% zeker is dat de gegevens gewist zijn, kan het wel worden meegenomen in de risico-inschatting.
- De toegang tot een account of clouddienst op afstand blokkeren.
- Wanneer de verplichting bestaat om de betrokkenen te informeren, dan aangeven wat zij zelf kunnen doen om de schade te beperken.

Diepgaand onderzoek bij complexe datalekken
Soms is er sprake van een complex datalek. Dan is het vaak nodig om een diepgaand digitaal forensisch onderzoek uit te voeren om de ernst en omvang van het lek vast te stellen. En vervolgens te bepalen welke maatregelen genomen moeten worden om de gevolgen van het datalek te beperken en om nieuwe, soortgelijke datalekken te voorkomen.

Als er sprake is van een complex datalek, bijvoorbeeld een datalek door ransomware, en binnen de organisatie is niet bekend wat te doen, dan wordt een expert ingeschakeld. Bijvoorbeeld een digitaal forensisch expert.

Stap 3: Melden datalek en informeren betrokkenen
Er kan een verplichting zijn om het datalek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Ook kan er een verplichting zijn om de betrokkenen te informeren over het datalek. Er moet worden beoordeeld of dit het geval is, zie daarvoor de handleiding van de Autoriteit Persoonsgegevens op
https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-wel-of-niet-melden

Stap 4: Registreren datalek in datalekregister
Volgens de AVG is het opstellen en bijhouden van een datalekregister verplicht. Hierin wordt bijgehouden welke datalekken er in de organisatie zijn geweest. In het register moeten alle datalekken worden vastleggen die zich binnen de organisatie hebben afgespeeld. Ook de datalekken die niet aan de Autoriteit Persoonsgegevens zijn gemeld.

Het doel van het datalekregister is dat de organisatie:
- leert van eerdere datalekken en bewust is van datalekken die in het verleden hebben plaatsgevonden;
- effectieve maatregelen neemt om de kans op nieuwe, soortgelijke datalekken te verminderen;
- met het datalekregister aan de Autoriteit Persoonsgegevens kan laten zien dat de organisatie zich houdt aan de meldplicht datalekken.

Vorm en inhoud datalekregister
Er is geen eis aan de vorm van het register, zolang het maar de wettelijk verplichte informatie bevat. Over elk datalek wordt ten minste de volgende informatie vermeld:
- de feiten over het datalek, zoals de oorzaak, wat er precies is gebeurd en om welke persoonsgegeven het gaat;
- de gevolgen van het datalek;
- de corrigerende maatregelen die zijn genomen.

De datalekregistratie wordt meegenomen bij de organisatiebeoordeling die jaarlijks plaatsvindt, om zo als onderdeel van een 'plan-do-check-act'-cyclus te worden gebruikt om te leren van fouten.