Gegevensbeschermingsbeleid

GEGEVENS CAR Impuls VZW

Inhoudstafel

1 Het belang van gegevensbescherming

CAR Impuls VZW hecht grote waarde aan het juist beschermen van de gegevens die zij verwerkt, in het bijzonder persoonsgegevens. Middels dit beleid wil CAR Impuls VZW op strategisch niveau vastleggen op welke wijze gegevens beschermd worden, welke verantwoordelijkheden hierrond zijn toegewezen en welke prioriteiten CAR Impuls VZW heeft bepaald rond de bescherming van gegevens.

In het bijzonder wil CAR Impuls VZW de gegevens van klanten en de persoonsgegevens die zij ter beschikking stellen, beschermen tegen:

- verlies: gegevens zijn niet meer beschikbaar
- lekken: gegevens komen in verkeerde handen terecht
- fouten: gegevens zijn niet correct, bijvoorbeeld verouderd of onvolledig
- niet toegankelijk: op het moment van de zorg zijn gegevens niet toegankelijk
- onterecht inkijken: ingekeken door personen die hiertoe niet gemachtigd zijn
- het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde
- verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen

De directie wil in dit beleid een beroep doen op iedereen die betrokken is bij de elektronische en papieren verwerking om samen, vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle dienstverlening aan te bieden, de verwerking van persoonsgegevens correct te laten verlopen.

Dit beleidshandboek gaat dieper in op de bescherming van de persoonlijke levenssfeer van en meer in het bijzonder, de informationele privacy. Dit beleidshandboek dient als norm voor het verwerken van alle persoonsgegevens door CAR Impuls VZW. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentienorm voor audit en controle. Het beleidshandboek biedt elke belanghebbende, medewerker of betrokken externe een inzage in het gegevensbeschermingsbeleid en de manier waarop we omgaan met gevoelige persoonsgegevens.

Het handboek is tevens geschreven voor iedereen die een functie heeft binnen CAR Impuls VZW waarbij persoonsgegevens verwerkt worden. Ze gebruiken (delen van) dit beleidshandboek voor het ontwerpen van procedures en richtlijnen voor medewerkers en externen, zoals ICT-leveranciers. De relevante onderdelen van dit beleidshandboek worden verwerkt in overeenkomsten met cliënten, personeel en leveranciers.

2 Toepassingsgebied

Het is de directie die bij start van de arbeidsovereenkomst conform de voorhanden zijnde procedure bepaalt tot welke applicaties en met welke rechten de medewerker toegang mag krijgen.

Daarnaast is er een autorisatiematrix om de specifieke toegangen te beheren.

Cliënteninformatie:

- Cliëntenzorg: Het stellen van een diagnose, het verstrekken van (medische, paramedische, verpleegkundige en psycho-sociale) zorg of behandelingen aan de betrokkene of een verwant of het beheer van de dienstverlening, in het belang van de betrokkene;

- Cliëntenregistratie: Het registreren van gegevens van cliënten voor interne door de overheid opgelegde doeleinden, evenals voor onderzoeks- behandelings- en beleidsdoeleinden, evenals het opvolgen van de prestaties van cliënten met het oog op facturering;

- Geneesmiddelenbeheer: Verwerkingen met betrekking tot het voorschrijven, opvolgen en/of toedienen van geneesmiddelen;

- Cliëntenadministratie en zorgkwaliteit: Verzameling en verwerking van alle gegevens met betrekking tot medische en paramedische diagnostische en therapeutische praktijken toegediend aan de cliënten met als doel de zorgkwaliteit te verbeteren;

- Klachtenbehandeling: Het registreren van persoonsgegevens van cliënten en/of hun vertrouwenspersonen teneinde te kunnen bemiddelen bij de aangebrachte klachten. Het registreren van klachten.

Personeelsinformatie:

- Alle medewerkers die in de uitoefening van hun functie in contact komen met persoonlijke gegevens, en in het bijzonder de HR medewerkers die met personeelsgegevens in contact komen, zullen een confidentialiteitsclausule ondertekenen als addendum aan hun contract.

- Alle sollicitanten, vrijwilligers, stagiaires die met personeelsgegevens in contact komen, zullen een confidentialiteitsclausule ondertekenen als addendum.

3 De organisatie van gegevensbescherming

Bevoegdheid	Als verantwoordelijke voor de verwerking, ligt de bevoegdheid van dit beleid bij CAR Impuls VZW, vertegenwoordigd door de directie. De directeur is verantwoordelijk voor het formuleren en vaststellen van, en het toezien op, de naleving van de beleidsprincipes binnen CAR Impuls VZW, hierbij ondersteund door de Raad van Bestuur en Algemene Vergadering.
Verantwoordelijke uitvoerder	Het bestuur fungeert als formeel beslissingsplatform voor gegevensbescherming. Het bestuur is bevoegd om beslissingen te nemen die betrekking hebben op volgende aspecten: • De risicoanalyse en bijhorende methodiek; • Het ontwikkelen van het gegevensbeschermingsbeleid en de bijhorende richtlijnen; • De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan)

- De structurele reactie op gegevensbeschermingsproblemen en –adviezen (binnen de 3 maanden);

Het aanspreekpunt informatieveiligheid

Het aanspreekpunt informatieveiligheid treedt op als contactpersoon voor de DPO aangesteld vanuit de Federatie. Hij/zij draagt niet de eindverantwoordelijkheid i.v.m. het naleven van de AVG. Deze ligt bij de directie en het bestuur.
Het aanspreekpunt kent idealiter de aard van de data waarover het CAR Impuls VZW beschikt en de datastromen.
Het aanspreekpunt helpt mee aan het bewustmakingsproces over hoe het CAR Impuls VZW veilig moet omgaan met persoonsgegevens en helpt mee om samen met directie en het bestuur het informatieveiligheids- en privacybeleid toe te passen.
Daarnaast zal hij/zij de nodige documenten opstellen waaronder het register van verwerkingsactiviteiten, om aan te tonen dat het CAR Impuls VZW aan de AVG voldoet en is hij/zij het eerste aanspreekpunt bij gegevenslekken.

De medewerker

Iedereen (intern of extern) die gegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, …), doet dit volgens de beleidsprincipes uit dit beleidshandboek. De gebruiker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Is verantwoordelijk voor de persoonsgegevens 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.
- Leeft artikel 458 van het Strafwetboek na: De gebruiker respecteert het (gedeeld) beroepsgeheim.

ICT-medewerker of key user

De ICT-medewerker of key user zijn, bovenop de verantwoordelijkheden voor de gebruiker, verantwoordelijk voor:

- De implementatie van de technische maatregelen.
- De veiligheidsinstellingen te implementeren in lijn met dit beleidshandboek.
- De veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen te melden het aanspreekpunt.
- Te fungeren als expert. Vanuit deze rol neemt hij/zij deel aan de identificatie zowel als aan de remediëring van de gegevensbeschermingsrisico’s.

ICT-leverancier

De ICT-leverancier heeft dezelfde verantwoordelijkheden als deze van een ICT-medewerker. Bijkomstig:

- Wijst hij op veiligheidsrisico’s van geleverde toepassingen.
- Wijst de instelling op de op te nemen veiligheidstaken.
- Streeft naar een transparant gegevensbeschermingsbeleid door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

4 Scope van het gegevensbeschermingsbeleid

Dit beleid is van toepassing voor de gehele levensduur van informatie binnen het CAR Impuls VZW, van het verkrijgen van informatie tot de uiteindelijke verwijdering van informatie binnen de organisatie, voor:

- Alle personeelsleden, zowel interne medewerkers als externen voor bepaalde of onbepaalde duur.
- Alle bedrijfsmiddelen en informatieverwerkende systemen beheerd door CAR Impuls VZW, evenals systemen beheerd door externen ten behoeve van informatieverwerkingen voor het CAR Impuls VZW zoals databases, informatie ongeacht de drager ervan, netwerken, datacenters, etc.
- Alle verwerkingsactiviteiten, zowel als verwerkingsverantwoordelijke als verwerker.

Voor bepaalde domeinen of processen binnen CAR Impuls VZW kunnen aanvullende richtlijnen of procedures worden uitgewerkt die in detail omschrijven welke maatregelen genomen worden om het gewenste niveau van gegevensbescherming te bereiken. Dit beleid is de kapstok waar alle andere richtlijnen of procedures onder vallen.

Gezien de belangrijke rol van de ICT-leveranciers bij het opzetten van de ICT-omgeving om gegevens te verwerken, legt het beleidshandboek hiervoor ook de beleidsprincipes vast.

5 Bewerkers van cliëntenbestanden en hun bevoegdheden

Alle medewerkers van het CAR Impuls VZW die voor de uitvoering van hun taken toegang nodig hebben tot persoonsgegevens, zijn ertoe gehouden het vertrouwelijk karakter van de betrokken gegevens strikt in acht te nemen.

De volgende personen zijn belast met de bewerking van de persoonsgegevens van cliënten, binnen de perken van hun opdracht en de doeleinden eigen aan deze opdracht (niet limitatief):

• De medewerkers zijn verantwoordelijk voor de verzameling en de verwerking van de persoonsgegevens van de cliënten in de afdelingen waarin zij werkzaam zijn. Zij zijn eveneens verantwoordelijk voor de door hen gemachtigden (vb stagiaires).

• De personeelsleden van het secretariaat en de administratie staan in voor het verwerken van de persoonsgegevens in de cliëntenbestanden. Er is aandacht voor het doorsturen van attesten, verslagen, …. Deze kunnen enkel naar de patiënt zelf worden verstuurd, of naar die zorgverstrekkers die de patiënt schriftelijk heeft doorgegeven.

• De personeelsleden van de dienst onthaal, facturatie en boekhouding staan in voor het verwerken van de persoonsgegevens in de cliëntenbestanden, voor factureringsdoeleinden, medische registratie, debiteurenopvolging en beleidsinformatie.

• De personeelsleden van de dienst ICT staan in voor de technische verwerking van persoonsgegevens tot geanonimiseerde gegevens met het oog op door de overheid opgelegde doeleinden. Daarnaast komen zij in contact met persoonsgegevens in het kader van probleemoplossende werkzaamheden, interne efficiëntieverhoging of gelijkaardige toepassingen.

• De personeelsleden verbonden aan een patiëntbegeleidende dienst staan in voor de verwerking van de persoonsgegevens. Bijzondere aandacht wordt besteed aan het verstrekken van persoonsgegevens vanuit de therapie. Deze kunnen enkel worden verstrekt aan de patiënt zelf of aan de ouders, leerkracht en/of ondersteuner indien de patiënt hiervoor vooraf zijn uitdrukkelijke toestemming heeft verleend. Het verstrekken van persoonsgegevens vanuit de therapie mag alleen indien dit noodzakelijk is en als dat verenigbaar is met het doel waarvoor de gegevens zijn verzameld.

• De personeelsleden van de ombudsdienst staan in voor de verwerking van de persoonsgegevens in de cliëntenbestanden, in het kader van de ombudsfunctie.

6 Interne en externe raadpleging van de cliëntenbestanden, rechten en plichten van de bewerkers

6.1 Intern

• De interne raadpleging en bewerking van de cliëntenbestanden geschiedt door de personen zoals omschreven punt 5. Dit recht is echter beperkt in het kader van hun opdracht en de verwerkers hebben geen toegang tot de persoonsgegevens die niet noodzakelijk zijn voor de uitvoering van hun opdracht.

• Bij de verwerking van de persoonsgegevens hebben de verwerkers de plicht op de persoonsgegevens eerlijk en rechtmatig te verwerken. Ze hebben de plicht om de persoonsgegevens niet te verwerken dan voor de doeleinden zoals vermeld in punt 5 van dit regelement.

• Interne auditoren kunnen met het oog op kwaliteitscontrole cliëntendossiers of applicaties inkijken. Dit is gekoppeld aan een geheimhoudingsverklaring.

• Bovendien zijn de verwerkers bij de verwerking van de persoonsgegevens betreffende de gezondheid tot geheimhouding verplicht en staan ze onder het toezicht van de directeur, de medisch directeur en het aanspreekpunt informatieveiligheid.

6.2 Extern

Binnen het kader van art. 7, lid 4 W.B.P.L[1]. zijn volgende categorieën van instanties gerechtigd tot het verkrijgen van gegevens uit de cliëntenbestanden:

• Verzekeringsinstellingen voor zover opgelegd door of krachtens de wet of met toestemming van de patiënt;

• De betrokken cliënten of hun aangestelde - mits ondertekend aanvraagformulier inzage en afschrift cliëntendossier;

• Overheidsinstanties die door een overheidsbeslissing daartoe gemachtigd zijn;

• Externe zorgverstrekkers van de patiënt met toestemming van de patiënt;

• Andere instanties, voor zover opgelegd door of krachtens de wet of met toestemming van de patiënt;

• Software en hardware leveranciers ter ondersteuning. Hiervoor wordt een specifieke verklaring ondertekend (gegevensverwerkersovereenkomst) om de privacy van deze data te garanderen.

7 De aard van de verwerkte gegevens en de wijze waarop ze verkregen worden

De aard van de gegevens zijn als volgt vastgelegd:

- Identificatiegegevens, waaronder het rijksregisternummer
- Financiële en administratieve gegevens met betrekking tot opname en facturatie, waaronder het lidmaatschap van het ziekenfonds

[1] Wet op de Bescherming van de Persoonlijke Levenssfeer

- Medische, paramedische en verpleegkundige gegevens, opgesplitst volgens:

  - medische gegevens
  - verpleegkundige gegevens
  - paramedische gegevens
  - geneesmiddelen
  - psychosociale en relevante familiale gegevens
  - andere gegevens noodzakelijk voor het uitvoeren van de doeleinden bepaald of opgelegd door de wet (gerechtelijke gegevens)

8 Het beheer van risico's

CAR Impuls VZW brengt de risico's inzake gegevensbescherming in kaart aan de hand van een risico analyse. Deze werd uitgevoerd op basis van volgende criteria (toetsingskader):

- De richtlijnen met betrekking tot de informatiebeveiliging van persoonsgegevens, zoals deze werden gepubliceerd door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer
- De Algemene Verordening Gegevensbescherming
- De ISO 27001 norm rond informatiebeveiliging

De analyse brengt operationele, tactische en technische risico's in kaart. De bevindingen uit de risico analyse werden besproken en worden opgenomen in een actieplan om de gevonden risico's te behandelen. Hierin onderkent CAR Impuls VZW vier mogelijk risicobehandelingen:

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

Alle nodige voorzieningen worden getroffen ter bevordering van de juistheid en volledigheid van de opgenomen gegevens. Tevens worden de nodige technische en organisatorische maatregelen getroffen ter beveiliging van de cliëntenbestanden tegen verlies of aantasting van de gegevens en tegen ongeoorloofde kennisneming, wijziging of verstrekking daarvan.

Het doel is dat de risico analyse jaarlijks wordt herzien.

Jaarlijks zullen eveneens sensibiliseringscampagnes worden gehouden voor de medewerkers van CAR Impuls VZW

Aangezien de CAR Impuls VZW over een grote hoeveelheid gevoelige data beschikt, heeft de ICT dienst een autorisatiematrix uitgewerkt waarin per departement en per dienst is aangegeven welke rol welke bevoegdheid heeft op vlak van digitale toegangen.

9 Bewaartermijnen

• Met inachtneming van eventuele wettelijke voorschriften geldt, te rekenen vanaf het laatste ontslag of de laatste behandeling van de patiënt, voor de persoonsgegevens die identificatie toelaten, een bewaartermijn van (niet limitatief):

- 10 jaar voor de facturatiegegevens uit de cliëntenbestanden die dienen als boekhoudkundig verantwoordingsstuk;

- 30 jaar voor de medische gegevens;

- 1 jaar voor de afgehandelde dossiers van de ombudsdienst (na opmaak jaarverslag).

• Indien de bewaartermijn is verstreken, worden de betreffende persoonsgegevens uit de bestanden verwijderd en vernietigd, binnen een termijn van één jaar.

• Vernietiging blijft evenwel achterwege wanneer:

- de bewaring vereist is op grond van een wettelijk voorschrift;

- de bewaring redelijkerwijze belangrijk wordt geacht vanuit medisch oogpunt of vanuit de levensverwachting van de patiënt, of vanuit de verdediging van zijn rechtmatige belangen of die van zijn rechtverkrijgenden;

- over de bewaring overeenstemming bestaat tussen de patiënt en de behandelende arts, bij ontstentenis, de medisch directeur.

Indien betreffende gegevens zodanig bewerkt zijn dat herleiding tot individuele personen redelijkerwijze onmogelijk is, kunnen zij in geanonimiseerde vorm bewaard blijven.

10 Rechten en mogelijkheden van verweer van de patiënt in het kader van de bescherming van de persoonlijke levenssfeer

• De patiënt, die zijn identiteit bewijst, heeft het recht vanwege de verantwoordelijke voor de verwerking kennis te krijgen van:

- het al dan niet bestaan van verwerkingen van op hem betrekking hebbende gegevens,

- de doeleinden van deze verwerkingen,

- de categorieën gegevens waarop deze verwerkingen betrekking hebben,

- de categorieën ontvangers aan wie de gegevens worden verstrekt,

- de gegevens zelf die worden verwerkt en alle beschikbare informatie over de oorsprong van die gegevens tenzij de inzage van deze gegevens via de wet van het recht op inzage worden uitgesloten.

• Eenieder mag zich kosteloos en zonder enige motivering verzetten tegen het verwerken van gegevens met het oog op direct marketing.

• Bij de verzameling van persoonsgegevens die op de patiënt betrekking hebben, wordt deze omtrent de in art. 4 W.B.P.L. vermelde topics geïnformeerd via de website van het CAR Impuls VZW.

• Bovendien heeft elke patiënt het recht om hetzij op rechtstreekse wijze, hetzij met behulp van een beroepsbeoefenaar in de gezondheidszorg, kennis te krijgen van de persoonsgegevens die betreffende zijn gezondheid worden verwerkt. Deze aanvraag tot inzage of afschrift dient gericht te worden tot de algemene directie.

• Indien de patiënt van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere redenen tot klagen heeft omtrent de bescherming van diens persoonlijke levenssfeer, kan deze zich steeds wenden tot de in §5 vermelde perso(o)n(en) en tot de directie.

• Onverminderd alle hierboven opgesomde interne rechts- en verweermiddelen, kan de patiënt zich overeenkomstig de art. 13, 14 en 63 e.v. W.B.P.L. respectievelijk wenden tot de Voorzitter van de Rechtbank van Eerste Aanleg en tot de Commissie voor de bescherming van de Persoonlijke Levenssfeer, Hoogstraat 139 – 1000 BRUSSEL

11 Beleidsdoelstellingen voor gegevensbescherming

Het CAR Impuls VZW, zowel in haar rol als verwerkingsverantwoordelijke als verwerker:

1. Is transparant over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene, de cliënten als naar de toezichthouders. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer de persoonsgegevens worden uitgewisseld.
2. Verwerkt enkel de gegevens die relevant zijn voor het uitvoeren van haar 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 CAR Impuls VZW. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel, waar nodig aan de hand van een gegevensbeschermingseffectbeoordeling (DPIA[2]).
3. Verwerkt enkel de persoonsgegevens die strikt noodzakelijk voor de uitvoering van de activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.
4. Kijkt toe op de integriteit van de persoonsgegevens gedurende de ganse 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 bij 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. CAR Impuls VZW bewaakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.
8. Waakt er actief over dat bij het verwerken van de persoonsgegevens voor een welbepaald doel, de rechten en vrijheden (bijvoorbeeld recht op verzekerbaarheid, recht op zorg) van de betrokkene gevrijwaard blijven.
9. 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. CAR Impuls VZW leeft bijgevolg alle wettelijke en normerende kaders na (i.e. zowel Vlaamse, Federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van andere duidelijk in kaart gebracht.
10. Kan aantonen dat het alle beleidsdoelstellingen naleeft, conform de wettelijke bepalingen. Deze verantwoordingsplicht wordt bewaakt door interne toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.

12 Inwerkingtreding en wijzigingen

Deze versie van het privacybeleid treedt in werking op 25 mei 2018.

[2] Data Protection Impact Assessment