

# Privacyreglement Lichtpunten BV

## Inleiding

Dit reglement is van toepassing binnen Lichtpunten BV en heeft betrekking op de verwerkingen van gegevens van cliënten die bij Lichtpunten BV in zorg zijn. Dit reglement is van toepassing op zowel op papier als elektronische verwerking van gegevens.

## Definities

**Autoriteit Persoonsgegevens (AP):** de toezichhoudende autoriteit, de onafhankelijke instantie die erover waakt dat persoonsgegevens zorgvuldig en veilig worden verwerkt en zo nodig sancties kan opleggen als dat niet gebeurt.

**Bestand:** elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn.

**Betrokkene:** degene op wie een persoonsgegeven betrekking heeft, meestal de cliënt, of zijn (wettelijk) vertegenwoordiger.

**Bijzondere categorieën persoonsgegevens:** persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

**Derde:** elke persoon of instantie die geen betrokkene, verwerkingsverantwoordelijke, verwerker, of een persoon is die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is persoonsgegevens te verwerken.

**Functionaris voor gegevensbescherming (FG):** functionaris die door de zorgaanbieder moet of kan worden aangesteld voor het informeren en adviseren over en het toezicht houden op de toepassing en naleving van de AVG en andere gegevensbeschermingsbepalingen.

**Gezondheidsgegevens:** gegevens over de lichamelijke of geestelijke gezondheid van een persoon, waaronder gegevens over verleende gezondheidsdiensten, waarmee informatie over zijn gezondheidstoestand wordt gegeven;

**Inbreuk in verband met persoonsgegevens:** 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 anderszins verwerkte gegevens. Onder een 'datalek' valt dus niet alleen het vrijkomen (leken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

**Persoonsgegevens:** alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); 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 identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

**Pseudonimisering:** het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkenen kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

**Toestemming van de betrokkene:** door betrokkene, op goede informatie berustende, specifieke, in vrijheid en ondubbelzinnig gegeven toestemming waarbij betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt. Dat kan door middel van een schriftelijke of mondelinge verklaring of een ondubbelzinnige actieve handeling (zoals het elektronisch aanvinken van een hokje).

**Verwerker:** degene die in opdracht van en voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een externe hostingsfirma, saas-leverancier, kwaliteitsauditor of een extern salarisadministratiekantoor).

**Verwerking van persoonsgegevens:** alle 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 in een andere vorm beschikbaar stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

**Verwerkingsverantwoordelijke:** degene die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; meestal de bestuurder van de zorgaanbieder.

## **Verwerking van persoonsgegevens van cliënten**

Lichtpunten BV is verantwoordelijk voor de naleving van onderstaande beginselen en moet de naleving hiervan aantonen. Binnen Lichtpunten BV worden persoonlijke gegevens alleen verwerkt:

- Op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk, en transparant is;
- Voor gerechtvaardigde doeleinden, en niet voor andere doeleinden onverenigbaar met het doel welke is aangegeven voor de verzameling van de gegevens;
- Op basis van het dataminimalisatie principe, dat wil zeggen dat zorg draagt om de verzameling van persoonsgegevens te beperken tot wat noodzakelijk is voor het doeleinde waarmee zij verzameld worden;
- Indien zij juist zijn, hierbij worden redelijke maatregelen genomen om de controleren of dit het geval is;
- Na het nemen van de toepasselijke technische en organisatorische maatregelen om de verwerking van persoonlijke gegevens veilig te doen verlopen.

### **Rechtmatigheid van de verwerking**

De verwerking is alleen rechtmatig wanneer wordt voldaan aan een van de onderstaande voorwaarden:

- Betrokkene heeft toestemming gegeven voor het verwerken van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- De gegevensverwerking is noodzakelijk voor de uitvoering van de overeenkomst waarbij de betrokkene partij is, bijvoorbeeld de zorgovereenkomst;
- De gegevens worden verwerkt om de dossierplicht na te komen;
- Verwerkt persoonlijke gegevens van de betrokkene alleen na toestemming van de betrokkene. Hierbij worden de wettelijke verplichtingen in acht genomen.

### **Verwerking van gezondheidsgegevens**

Lichtpunten BV verwerkt geen gezondheidsgegevens in het kader van de zorgovereenkomst en het verstrekken van zorg en ondersteuning.

### **Gegevensverwerking door verwerker**

Lichtpunten BV heeft een verwerkersovereenkomst afgesloten met betrekking tot het verwerken van gegevens van cliënten. De verwerker van gegevens van cliënten van Lichtpunten BV hanteert adequate beveiligingsstandaarden.

### **Aansprakelijkheid verwerkingsverantwoordelijke en/of verwerker**

Eventuele aansprakelijkheid voor schade die voortvloeit uit toerekenbaar tekort schieten of niet voldoende naleven van de AVG is vastgelegd in onze verwerkersovereenkomst.

### **Geheimhoudingsplicht en verstrekking aan derden**

Lichtpunten BV neemt alle toepasbare gedragscodes en beroepscodes in acht met betrekking tot de geheimhoudingsplicht van de hulpverlener. Bij verstrekking van gegevens aan derden wordt de wet nageleefd. De verstrekking van gegevens aan derden vindt alleen plaats in het kader van de zorgverlening of ondersteuning en de correcte administratieve verwerking hiervan.

### **Bewaren van persoonsgegevens**

Lichtpunten BV zal zich inspannen om de papieren en elektronische persoonsgegevens op een veilige manier te bewaren, in overeenstemming met de Europese Privacywet: De Algemene Verordening Gegevensbescherming (AVG). Persoonsgegevens worden niet langer bewaard dan noodzakelijk om de doelen te bereiken waarvoor de gegevens werden verzameld en verwerkt.

Voor gezondheidsgegevens die binnen de zorgrelatie worden verwerkt, zoals het dossier van de cliënt, gelden verschillende bewaartermijnen. De bewaartermijnen worden nagekomen zoals opgenomen in de Wet Kwaliteit Klachten en Geschillen Zorg, waar Lichtpunten als zorgaanbieder onder valt.

### **Rechten van de betrokkene**

Betrokkenen kunnen kosteloos inzage opvragen in hun dossier. Verzoeken worden binnen een maand van een gepast antwoord voorzien.

### **Te verstrekken informatie**

Lichtpunten BV verstrekt in het geval van een inzageverzoek op een transparante en begrijpelijke manier de relevante informatie. Hierin is opgenomen:

- de periode gedurende welke de persoonsgegevens worden opgeslagen;
- de mogelijkheden om een verzoek om inzage, rectificatie, of verwijdering van persoonsgegevens of beperking van de hem betreffende verwerking, alsmede het recht op bezwaar en de het recht op gegevensoverdraagbaarheid.

Lichtpunten BV verwerkt de persoonsgegevens op basis van de toestemming van de cliënt, op basis van de uitoefening van de zorgovereenkomst en op basis van contract met opdrachtgevers. Deze toestemming kan de cliënt te allen tijde intrekken. Tevens heeft de cliënt te allen tijde recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

### **Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen**

Lichtpunten BV werkt samen met andere zorgverleners. Wanneer de persoonsgegevens van de betrokkene aan Lichtpunten BV zijn verstrekt door een derde, worden deze gegevens, en de bron hiervan, gedeeld met de betrokkene om de juistheid van de informatie te verifiëren.

### **Inzage en afschrift/kopie**

De betrokkene van twaalf jaar of ouder heeft het recht op inzage en een kopie van de op zijn persoon betrekking hebbende verwerkte gegevens. Is de betrokkene 16 jaar of ouder dan beslist de betrokkene zelf wie wel en niet inzage krijgt in de persoonsgegevens. Lichtpunten BV kan betrokkenen anders dan de cliënt zelf pas inzage geven in persoonlijke gegevens na uitdrukkelijke, schriftelijke toestemming.

### **Recht op rectificatie of aanvulling van persoonsgegevens**

De betrokkene heeft het recht om rectificatie aan te vragen van hem of haar betreffende persoonsgegevens die onjuist zijn. In het geval van een rectificatie wordt de betrokkene hiervan op de hoogte gesteld door de zorgaanbieder. Tevens heeft de betrokkene het recht om de zorgaanbieder te vragen bepaalde gegevens voor bepaalde personen af te schermen of toegang tot die gegevens te laten blokkeren. Het verzoek tot rectificatie of aanpassing van de gegevens wordt in het dossier opgeslagen.

### **Recht op gegevensverwijdering**

De betrokkene heeft het recht om verwijdering van de op hem of haar betreffende persoonsgegevens aan te vragen. Dit is mogelijk op een van de volgende gronden:

- a) de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- b) de betrokkene trekt de toestemming waarop de verwerking berust in en er geen andere rechtsgrond is voor de verwerking;
- c) de persoonsgegevens zijn onrechtmatig verwerkt;
- d) op basis van een wettelijke verplichting, die op de zorgaanbieder rust, de persoonsgegevens moeten worden gewist.

Lichtpunten BV zal waar mogelijk dit verzoek honoreren, mits dit in strijd is met de wettelijke bewaarplicht. In dit geval zal de betrokkene op de hoogte stellen van de reden van de weigering van het verzoek.

In het geval dat Lichtpunten BV het verzoek tot verwijdering inwilligt, zullen alle ontvangers aan wie persoonsgegevens zijn verstrekt in kennis worden gesteld van de verwijdering van de persoonsgegevens. Tevens worden zij verzocht de persoonsgegevens welke zij van Lichtpunten BV hebben verkregen te wissen.

Een verzoek tot gegevensverwijdering mag alleen worden geweigerd indien dit in strijd is met de wet; een derde een aanmerkelijk belang heeft bij bewaring van de gegevens; de cliënt een procedure tegen de hulpverlener heeft aangespannen of het waarschijnlijk is dat hij dit zal doen; er vermoedens van kindermishandeling in de dossiergegevens staan (in lijn met de Meldcode Huiselijk Geweld en Kindermishandeling kunnen deze gegevens alleen op verzoek van het kind zelf wanneer het kind de leeftijd van 16 jaar heeft bereikt, worden verwijderd); Lichtpunten BV deze gegevens nodig heeft voor de instelling, uitoefening, of onderbouwing van een rechtsvordering; om redenen van algemeen belang op het gebied van volksgezondheid.

**Recht op gegevensoverdraagbaarheid** De betrokkene heeft het recht de hem betreffende persoonsgegevens, die aan Lichtpunten BV zijn verstrekt, in een gestructureerd, gangbare, en machine-leesbare vorm te verkrijgen en heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen. Waar mogelijk zal deze informatie direct aan de nieuwe zorgverlener toesturen. De uitoefening van dit recht doet geen afbreuk aan de rechten en vrijheden van anderen.

### **Vertegenwoordiging**

1. Bij een jeugdige jonger dan twaalf jaar en bij een wilsbekwame jeugdige van twaalf tot achttien jaar, oefent (oefenen) de ouder(s) met gezag of de voogd de rechten van de jeugdige uit, tenzij dit niet verenigbaar is met de zorg van een goede hulpverlener.
2. De wilsbekwame jeugdige van twaalf jaar of ouder oefent zelfstandig zijn rechten over zijn persoons- en gezondheidsgegevens uit. Vernietiging van gegevens over (vermoedens van) kindermishandeling vindt uitsluitend plaats met toestemming van een wilsbekwame jeugdige van zestien jaar en ouder.
3. Is de betrokkene ouder dan achttien jaar en wilsbekwaam ter zake, dan treedt als vertegenwoordiger voor hem op:
  - a) een (toegewezen) curator of mentor;
  - b) indien er geen curator of mentor is, de persoon die de cliënt schriftelijk heeft gemachtigd;
  - c) indien de persoonlijk gemachtigde ontbreekt of niet optreedt; de echtgenoot of levensgezel van de betrokkene;
  - d) indien de echtgenoot of levensgezel ontbreekt of niet optreedt: een kind, broer of zus van de betrokkene.

In het uiterste geval treedt de zorgaanbieder op als goed hulpverlener; hij zorgt er voor dat er zo snel mogelijk een wettelijk vertegenwoordiger voor betrokkene optreedt. Zo nodig, als familie of naaste dat niet kan of wil, verzoekt hij de rechter om een vertegenwoordiger te benoemen.

## **Veilige verwerking van persoonsgegevens**

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, als ook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de zorgaanbieder passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.
2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de hierboven bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de zorgaanbieder wordt uitgevoerd.
3. Het aansluiten bij goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen kan worden gebruikt als element om aan te tonen dat de verplichtingen van de zorgaanbieder zijn nagekomen.

**Gegevensbescherming door Privacy by design en default** Lichtpunten BV, rekening houdende met de techniek, uitvoeringskosten en de aard, omvang, en context van de verwerking, treft maatregelen om minimale gegevensverwerking op een doeltreffende manier uit te voeren. treft passende technische en organisatorische maatregelen om data minimalisatie te bevorderen. De gegevensverwerker waarmee Lichtpunten BV een verwerkersovereenkomst heeft hanteert de wettelijke normen om aan te tonen dat aan de voorschriften is voldaan.

**Medewerking verlenen aan/samenwerken met de Autoriteit Persoonsgegevens** Lichtpunten BV en de verwerker en, in voorkomend geval, hun vertegenwoordigers, werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

**Beveiliging van de verwerking** Lichtpunten BV zal adequate beveiligingsmaatregelen treffen, evenals de verwerker die in opdracht van Lichtpunten BV gegevens verwerkt. Waar mogelijk kan dit de onder meer het volgende omvatten:

- a) de pseudonimisering en versleuteling van persoonsgegevens;
- b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, met name als gevolg van vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

### **Melding van een inbreuk in verband met persoonsgegevens aan de Autoriteit Persoonsgegevens en het datalekkenregister.**

1. Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de zorgaanbieder dit zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, wordt de vertraging toegelicht (gemotiveerd).
2. De verwerker informeert de zorgaanbieder zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens.
3. In de melding aan de Autoriteit Persoonsgegevens wordt ten minste het volgende omschreven of meegedeeld:
  - a) de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
  - b) de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
  - c) de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
  - d) de maatregelen die de zorgaanbieder heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
4. Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.
5. De zorgaanbieder houdt alle inbreuken in verband met persoonsgegevens bij in een overzicht, met inbegrip van de feiten omtrent die inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de Autoriteit Persoonsgegevens in staat de naleving van dit artikel te controleren.

### **Melding van een inbreuk in verband met persoonsgegevens aan de betrokkenen (datalekken melden aan de betrokkene)**

1. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de zorgaanbieder de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.
2. De bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens en ten minste de in het vorige artikel bedoelde gegevens en maatregelen.
3. De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:
  - a) de zorgaanbieder heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
  - b) de zorgaanbieder heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
  - c) de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

4. Indien de zorgaanbieder de inbreuk in verband met persoonsgegevens nog niet aan de betrokkene heeft gemeld, kan de Autoriteit Persoonsgegevens, na beraad over de kans dat de inbreuk in verband met persoonsgegevens een hoog risico met zich meebrengt, de zorgaanbieder daartoe verplichten of besluiten dat aan een van de in lid 3 van dit artikel, bedoelde voorwaarden is voldaan.

### **Functionaris gegevensbescherming**

Lichtpunten BV heeft een functionaris gegevensbescherming aangewezen vanwege de bijzondere categorieën data die verwerkt worden.

Betrokkenen kunnen contact opnemen met de functionaris gegevensbescherming over aangelegenheden die verband houden met de verwerking van hun persoonsgegevens. De functionaris gegevensbescherming zal dit met vertrouwelijkheid en integriteit behandelen.

### **Taken van de functionaris gegevensbescherming**

De functionaris gegevensbescherming vervult de volgende taken:

- a. de zorgaanbieder of de verwerker en de werknemers die verwerken, informeren en adviseren over hun verplichtingen uit hoofde van de privacywetgeving (de AVG en andere gegevensbeschermingsbepalingen zoals uit sectorspecifieke wet- en regelgeving);
- b. toezien op naleving van deze AVG, van andere gegevensbeschermingsbepalingen en van het beleid van de zorgaanbieder of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- c. desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan;
- d. optreden als contactpunt voor de Autoriteit Persoonsgegevens inzake met verwerking verband houdende aangelegenheden, met inbegrip van de voorafgaande raadpleging, en, waar passend, overleg plegen over enige andere aangelegenheid.

De functionaris voor gegevensbescherming houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden