



Privacyreglement voor familie, naasten, bezoekers, Buurtgenoten, en passanten

Naam instelling: Lister
Adres: Furkplateau 15, 3524 ZH Utrecht
Email: privacy@lister.nl
Telefoon: 030-2361099

Inhoudsopgave

1 Lister	4
2 Informatiebeveiliging en privacy	5
3 Soort gegevensverwerking	6
4 Uitgangspunten	7
5 Het delen van persoonsgegevens	8
6 Beveiliging	9
7 Website, cookies en social media	10
8 Camerabeleid	11
9 Uw rechten	12
Bijlage 1: Register van verwerkingen	13
1.1 Lister heeft de volgende verwerkingen opgenomen in haar verwerkingsregister:	13
Bijlage 2: Protocol Cameratoezicht	14
1.1 Inleiding	14
1.2 Verantwoordelijke	14
1.3 Mogelijke doelen van cameratoezicht	14
1.4 Toetsing & informatie	14
1.5 Bekijken van beelden	15
1.6 Afgeven van beelden	15
1.7 Bewaartermijn beelden	15
1.8 Beheer en beveiliging systeem	15
1.9 Overige bepaling	16

1 Lister

Lister is een Regionale Instelling voor Begeleid Wonen, gevestigd in Utrecht, haar werkgebied omvat Utrecht stad en de Lekstroomgemeenten. Lister biedt begeleiding thuis en wonen met zorg aan mensen vanaf 18 jaar met een psychische kwetsbaarheid en/of verslavingsproblematiek en zorgvragen op verschillende levensgebieden. Onze begeleiding is herstelondersteunend en gericht op ontwikkeling. De mens met zijn mogelijkheden en wensen, staat centraal.

Onderstaand beleid heeft betrekking op externe partijen. Bijvoorbeeld bezoekers, buurtgenoten, maar ook familie of naasten van cliënten en passanten.

Het privacybeleid voor cliënten en medewerkers van Lister is in aparte documenten vastgelegd.

2 Informatiebeveiliging en privacy

Binnen Lister wordt gevoelige informatie verwerkt. Dat wil zeggen dat we onder andere informatie over gezondheid of onderzoeksgegevens of bedrijfsinformatie vastleggen, bewaren en delen. We doen dit zorgvuldig. We zorgen ervoor dat de systemen waarin we gegevens verwerken goed beveiligd zijn en dat alleen de juiste mensen toegang hebben. Daarnaast zorgen we ervoor dat de mensen die met deze gegevens werken zich bewust zijn van hun verantwoordelijkheid en zich hiernaar gedragen.

Als Lister gegevens van u verwerkt is ze er verantwoordelijk voor dat dit op de juiste manier gebeurt. Dat wil zeggen dat Lister dit doet volgens de geldende Europese wetgeving op het gebied van privacy en informatiebeveiliging. De Functionaris Gegevensbescherming bij Lister geeft hier advies over en houdt hier toezicht op. Hier kunt u ook terecht als u vragen of klachten heeft over hoe Lister omgaat met uw gegevens.

Contactgegevens Functionaris gegevensbescherming

De functionaris gegevensbescherming is Joris van den Heuvel.

Hij is te bereiken op functionarisgegevensbescherming@lister.nl of 030-2361099.

3 Soort gegevensverwerking

Lister houdt een register bij met daarin de gegevens die zij verwerkt, de grondslag en het doel hiervan en welke bewaartermijn ze hanteert. Een overzicht van de verwerkingen in dit register vindt u terug in bijlage I. Als u vragen heeft over dit register kunt u contact opnemen met de Functionaris Gegevensbescherming.

4 Uitgangspunten

Om te weten of gegevens verwerkt mogen worden zijn er wettelijk een aantal uitgangspunten geformuleerd. Lister volgt deze uitgangspunten:

- Legitimiteit: verwerking van gegevens vindt uitsluitend plaats voor zover dit wettelijk gerechtvaardigd is. Er moet een noodzaak zijn;
- Doelbinding: gegevens worden alleen verwerkt om het vastgestelde doel te bereiken. De gegevens worden niet gebruikt voor doeleinden die onverenigbaar zijn met (of niet herleidbaar zijn tot) het oorspronkelijke doel waarvoor de gegevens nodig zijn;
- Subsidiariteit: het vastgestelde doel kan niet met minder dan de verzamelde gegevens worden bereikt;
- Proportionaliteit: de verzamelde gegevens staan in verhouding tot het vastgestelde doel. Er worden geen onnodige gegevens verzameld;
- Integriteit: de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- Informatieveiligheid: de verzamelde gegevens staan op een veilige plek (conform NEN normen) en er wordt gezorgd voor adequate toegangsbeveiliging;
- Houdbaarheid: gegevens die niet langer nodig zijn, worden vernietigd (tenzij dit wettelijk anders is bepaald) of geanonimiseerd. Betrokkene heeft het recht om vergeten te worden (tenzij dit wettelijk anders is bepaald)

5 Het delen van persoonsgegevens

Lister deelt uw gegevens niet met anderen tenzij dit nodig is voor het uitvoeren van een overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die in opdracht van Lister gegevens van u verwerken sluiten wij een verwerkersovereenkomst af om te zorgen dat zij zorgvuldig en vertrouwelijk met uw gegevens omgaan. Lister blijft hier verantwoordelijk voor. Met partijen waarmee gegevens worden uitgewisseld worden gegevensuitwisselingsovereenkomsten afgesloten. Voor het delen van uw gegevens anders dan noodzakelijk en/of voortkomend uit een overeenkomst met u vraagt Lister altijd nadrukkelijk uw toestemming.

6 Beveiliging

Lister neemt het beschermen van vertrouwelijke gegevens serieus en doet er alles aan om uw privacy te waarborgen. Lister zorgt ervoor dat er technische en organisatorische maatregelen worden genomen om dit goed uit te voeren. Er wordt regelmatig gecontroleerd of deze maatregelen werken. De computersystemen en applicaties die Lister gebruikt worden beveiligd volgens de geldende standaarden. Er zijn maatregelen genomen om ook bij verlies of diefstal van apparatuur het ongewenst openbaar worden van gegevens tegen te gaan. Als u aanwijzingen heeft dat uw gegevens niet goed beveiligd zijn of er zijn aanwijzingen van misbruik van gegevens, neem dan contact op met de Functionaris Gegevensbescherming.

Externe medewerkers die worden ingehuurd hebben een geheimhoudingsplicht.

7 Website, cookies en social media

Lister maakt gebruik van cookies tijdens het bezoek op de website. Deze cookies bevatten geen informatie waarmee u als persoon geïdentificeerd kunt worden. Wel bevatten deze cookies informatie over uw bezoek aan deze website of over het gebruik van sociale media op deze website. Verder maakt Lister gebruik van Google Analytics om bezoekersstatistieken te verzamelen en rapportages daarvan samen te stellen, met als doel de website gebruiksvriendelijker te maken. Lister maakt gebruik van externe sites om functionaliteit toe te voegen aan de website van Lister. Zo voegt Lister geregeld video's in van YouTube. Lister biedt de mogelijkheid om artikelen te delen op sociale media door share-buttons van Facebook, Twitter en LinkedIn. Voor het invoegen van de share-buttons gebruikt Lister AddThis. Deze scripts legt Lister met cookies op uw computer vast om te zorgen dat uw gebruikservaring zo prettig mogelijk is, maar ook om het profiel dat deze bedrijven over u bijhouden te verrijken.

Tot slot maakt Lister gebruik van software om inzicht te krijgen in opinies op social media. Dit doet zij om tijdig te kunnen reageren op berichtgeving.

8 Camerabeleid

Lister gebruikt op enkele van haar locaties cameratoezicht. Ze doet dit onder strikte voorwaarden die opgenomen zijn in het camerabeleid. U vindt dit beleid in Bijlage II of u kunt het beleidsdocument opvragen bij de Functionaris Gegevensbescherming.

9 Uw rechten

Als u een vraag of klacht heeft over hoe Lister omgaat met uw persoonsgegevens kunt u dit altijd kenbaar maken. U kunt dit aangeven bij het locatie- of stafhoofd waar u mee te maken heeft of u kunt contact opnemen met de Functionaris Gegevensbescherming.

U heeft het recht op inzage, aanpassing of verwijdering van (een deel van) de gegevens die wij van u vastleggen, tenzij er een wettelijk bezwaar is. Als u een verzoek indient voor het doorsturen van de door Lister vastgelegde gegevens naar een andere partij, dan moet Lister indien mogelijk aan dit verzoek tegemoet komen.

Wij doen ons best om klachten zo goed mogelijk en naar tevredenheid van alle partijen op te lossen. Mocht u toch niet tevreden zijn over de afhandeling kunt u een klacht indienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens. We stellen het in dit geval wel op prijs als u eerst contact met ons opneemt om te kijken of we uw klacht in goed overleg kunnen oplossen. (<https://autoriteitpersoonsgegevens.nl/nl/voordat-u-een-klacht-indient>)

Bijlage 1: Register van verwerkingen

1.1 Lister heeft de volgende verwerkingen opgenomen in haar verwerkingsregister:

- Cliëntgegevens administreren
- Familie/naasten coaching administreren
- Cursistgegevens administreren
- Medewerkergegevens administreren
- Sollicitantgegevens administreren
- Vrijwilligersgegevens administreren
- Stagiaires administreren
- Administreren gegevens externe medewerkers
- Leden raad van toezicht administreren
- Administeren gegevens door vertrouwenspersonen en cliëntconsulenten
- Klachtgegevens van cliënten, wettelijke vertegenwoordigers en naastbetrokkenen administreren
- Cameratoezicht registreren
- Administreren gebruik infrastructuur en informatiesystemen
- Incidenten administreren
- Administreren governance gegevens
- Financiële mutaties administreren, begroten en rapporteren
- In- en verkoopgegevens en contractgegevens administreren
- Administreren van klachten in algemene zin van medewerkers en bezwaren ten aanzien van het Sociaal Plan
- Indienen en afhandelen schadeclaims bij verzekeringen
- Beeldbank beheren
- Administreren gegevens ten behoeve van de uitgifte van zakelijke wereldpassen / creditcards / online keys
- Wagenparkbeheer administreren
- Administreren verhuur van panden
- Administreren informatievoorziening derden op de website
- Verzamelen van opinies over Lister op social media

Bijlage 2: Protocol Cameratoezicht

1.1 Inleiding

In dit document zijn de afspraken vastgelegd met betrekking tot het gebruik van de geplaatste camera's, het bekijken van beelden en de opslag van beeldmateriaal.

Lister maakt op enkele plaatsen in de organisatie gebruik van cameratoezicht. Dit betreft locaties waar door de aard van de zorg extra inzet nodig is op het gebied van veiligheid.

1.2 Verantwoordelijke

Het locatiehoofd beslist of er op zijn locatie camera's worden geplaatst en voor welke doeleinden en met welke middelen. Voordat wordt overgegaan tot het installeren van camera's toetst de raad van bestuur deze beslissing op basis van een advies van de functionaris gegevensbescherming. Het locatiehoofd is verantwoordelijk voor de verwerking van de persoonsgegevens.

1.3 Mogelijke doelen van cameratoezicht

- Bewaking in verband met toegang en schade door vandalisme en diefstal;
- 24 uur toezicht;
- Herkenning of identificatie van personen die bij gebeurtenissen betrokken zijn geweest;
- Bevorderen van het gevoel van veiligheid;
- Preventie van onwenselijk gedrag;
- Ondersteuning bij opsporing van strafbare feiten;
- Ter beveiliging van een ieders eigendommen.

1.4 Toetsing & informatie

Bij alle locaties waar cameratoezicht aanwezig is, wordt dit duidelijk kenbaar gemaakt.

Camera's zijn zichtbaar opgehangen. Het gebruik van een verborgen camera is alleen in zeer uitzonderlijke gevallen toegestaan. Voordat dit middel ingezet wordt moet in alle gevallen een data protection impact assessment gedaan worden. Camera's zijn alleen toegestaan als een camera noodzakelijk¹ is om het gestelde doel te bereiken.

Er moet een (schriftelijke) afweging zijn gemaakt waarin beschreven staat waarom deze is opgehangen en welke afwegingen er gemaakt zijn ten aanzien van de privacy van betrokkenen.

Zowel de hoofddoelen als de nevedoelen moeten hierbij genoemd worden. Daarnaast moet bepaald worden welk soort camera of softwaretechniek in het concrete geval gerechtvaardigd is om in te zetten. Ook de juridische grondslag van het ophangen van de camera moet omschreven zijn.

¹ regeling beleidsregels cameratoezicht 1.4

Zowel de afweging voor het gebruik van gewone camera's als het gebruik van verborgen camera's dient vooraf getoetst te worden door de RvB die hierin ondersteunt wordt door de FG.

1.5 Bekijken van beelden

Een locatiehoofd heeft toestemming voor het bekijken van opgeslagen camerabeelden. Opgeslagen camerabeelden kunnen uitsluitend in opdracht van en in het bijzijn van het locatiehoofd of een daartoe vanwege specifieke expertise gemandateerde medewerker bekeken worden. Het locatiehoofd beoordeelt, na afstemming met de functionaris gegevensbescherming, verzoeken voor het bekijken van de camerabeelden door belanghebbenden. Belanghebbenden zijn slachtoffers in de zin van een vorm van agressie of geweld, zowel fysiek geweld als psychisch of seksueel geweld, vernieling en / of diefstal van eigendommen. Als er sprake is van een strafbaar feit kan Lister de beelden gebruiken bij het doen van aangifte. Personen die op basis van camerabeelden als 'verdachte / dader' worden aangemerkt worden hiervan op de hoogte gesteld en krijgen de gelegenheid de desbetreffende beelden te bekijken. Het moment van inzage wordt door Lister bepaald en hangt af van het onderzoek.

1.6 Afgeven van beelden

Als de politie een redelijk vermoeden heeft dat de camera beelden bevat van een strafbaar feit kan ze deze beelden bij Lister opvragen als er een machtiging is afgegeven door het openbaar ministerie om deze te vorderen. Camerabeelden worden verder alleen afgegeven aan derden als dit noodzakelijk is vanwege een vitaal belang. Dit wordt ter beoordeling voorgelegd aan de RvB/FG

1.7 Bewaartermijn beelden

De beelden worden maximaal 28 dagen bewaard. Indien er in die periode geen incidenten zijn gemeld of hebben plaatsgevonden worden de beelden vernietigd. Beelden van een incident worden tot uiterlijk het moment waarop dit incident is afgehandeld bewaard. Camerabeelden die gebruikt worden in het kader van onderzoek, waarvan aangifte is gedaan bij de politie, worden pas vernietigd na overleg met de politie. De wettelijke termijn van 28 dagen is dan niet van toepassing.

1.8 Beheer en beveiliging systeem

Om beheer en beveiliging te kunnen waarborgen loopt de aanschaf en installatie van camerasystemen via de afdeling I&A. Medewerkers van de afdeling I&A zijn zonder aanvullende mandatering alleen gerechtigd benodigde apparatuur te installeren en te controleren op het functioneren van het systeem. Bekijken van beelden is niet toegestaan. De afdeling controleert ieder half jaar het functioneren van de beeldregistratie en het bewaren van beelden.

1.9 Overige bepaling

In situaties waarin dit protocol niet voorziet, beslist de RvB/FG. Als om een dringende reden van bovenstaande afspraken moet worden afgeweken, wordt de functionaris gegevensbescherming hiervan direct op de hoogte gesteld.