Privacybeleid 2023-2024

Salios-voormalig Parkhuis

Naam organisatie	:	Salios-voormalig het Parkhuis
Document	:	Privacybeleid 2023-2024
Versienummer	:	1.2
Datum	:	3 oktober 2023
Classificatie	:	Intern vertrouwelijk

Versiebeheer

Datum	7 november 2023
Betreft	Mutaties in versie 1.2
Mutaties	• Tekstuele aanpassingen (minor changes) • CISO en Privacy officer opgenomen in organisatiestructuur • Rol, taak en positie beschreven van CISO en Privacy Officer

Inhoud

1. Inleiding

Het Parkhuis is een zorgorganisatie voor langdurige zorg aan mensen met dementie, Korsakov en gerontopsychiatrie. Dit betekent dat het Parkhuis omgaat met persoonsgegevens van cliënten en medewerkers. Het Parkhuis vindt het belangrijk dat met deze persoonsgegevens zorgvuldig wordt omgegaan. Het verwerken van persoonsgegevens brengt namelijk een grote verantwoordelijkheid met zich mee. Cliënten vertrouwen het Parkhuis persoonsgegevens toe. Misbruik van deze gegevens kan voor een cliënten én werknemer grote gevolgen hebben.
In dit Privacybeleid van het Parkhuis wordt beschreven hoe het Parkhuis omgaat met de verwerkingen van persoonsgegevens van betrokkenen. Het Parkhuis houdt zich hierbij aan de van toepassing zijnde wet- en regelgeving (*Algemene Verordening Gegevensbescherming en Uitvoeringswet AVG en andere nationale wet- en regelgeving en sectorspecifieke regels*) en richtlijnen van de Autoriteit Persoonsgegevens.
Dit Privacybeleid wordt periodiek onderhouden. Minimaal een keer per jaar wordt dit beleid getoetst op ontwikkelingen zoals nieuwe richtlijnen van de Autoriteit Persoonsgegevens en veranderingen in wet- en regelgeving. Het Parkhuis werkt hierbij met een beheer methodiek (EasyPrivacy, met een normenkader AVG) om in continuïteit aantoonbaar te maken dat het Parkhuis voldoet aan de privacy wet- en regelgeving. Het Parkhuis vindt het daarbij belangrijk transparant te zijn over de wijze van verwerkingen van persoonsgegevens en ziet dit als een onderscheidende kwaliteit in haar dienstverlening.

1.1. Toelichting Privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform de actuele wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Voor het parkhuis zijn dit voornamelijk cliënten en medewerkers (*dit noemen we 'betrokkenen'*). Onder verwerking van persoonsgegevens wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: *verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.*

1.2. Toelichting Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.
Deze aspecten zijn:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.

- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van de bedrijfsvoering. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.3. Vervlechting Informatiebeveiliging en Privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het Parkhuis heeft een apart Informatiebeveiligingsbeleid.

2. Doelstelling, reikwijdte en strategie van het beleid

2.1. Doel

Dit beleid is zo opgesteld dat het aan de vereisten van de wet- en regelgeving, met name de Algemene Verordening Gegevensbescherming (hierna: AVG), voldoet. Maar ook zodanig dat het past binnen de doelstellingen van het Parkhuis.
Dit beleid heeft tot doel:

- Het waarborgen van de continuïteit van de bedrijfsvoering.
- Beleidsregels te stellen aan het Parkhuis voor het verwerken van persoonsgegevens, zodat de privacy van betrokkenen (*cliënten en medewerkers*) gegarandeerd is en beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.
- Bij te dragen aan de transparantie van de regels die door het Parkhuis worden gehanteerd met betrekking tot de verwerking van persoonsgegevens.
- Om ervoor te zorgen dat het Parkhuis continu '*in control*' is over de persoonsgegevens die zij verwerkt in het kader van de (contractuele)verplichtingen.
- Een uitvoerend kader te scheppen om de naleving van de verantwoordingsplicht zoals gesteld in art. 5 en art. 24 AVG na te komen.

2.2. Reikwijdte

Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen. De privacyaspecten met betrekking tot de medewerkers worden opgenomen in de diverse regelingen van P&O (Cluster Staf).

De volgende uitgangspunten gelden hierbij:

- Het privacy beleid binnen het Parkhuis geldt voor alle medewerkers, vrijwilligers, leden Raad van Toezicht, externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle apparaten waarmee geautoriseerde toegang tot het netwerk verkregen kan worden.

- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van het Parkhuis. Het beleid heeft betrekking op gecontroleerde informatie, die door het Parkhuis zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop het Parkhuis kan worden aangesproken, zoals mailboxen van medewerkers en opslag van persoonsgegevens op mobiele media.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van het Parkhuis evenals op de daaraan ten grondslag liggende documenten en persoonsgegevens die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- Het Privacybeleid heeft raakvlakken met het:
    - Informatiebeveiligingsbeleid van het Parkhuis;
    - Informatiebeleidsplan; met als aandachtspunten aanschaf, beheer en gebruik van ICT- middelen.

2.3. Strategie

Er zijn drie pijlers voor het voeren van een effectief Privacybeleid: papier, mensen en techniek.
Papier bestaat uit het opstellen van beleid, procedures, richtlijnen en handleidingen. De pijler 'mensen' draait om bewustwording van risico's en de bewustwording van de waarde van informatie en het werken conform beleid en procedures. Bij 'techniek' is het van belang dat de juiste ICT-infrastructuur en -beveiliging aanwezig is zodat het beleid op een juiste manier door het Parkhuis kan worden uitgevoerd. Door het continu werken aan deze drie pijlers wil het Parkhuis een effectief beleid voeren, waarbij het Parkhuis haar verantwoordelijkheid invult voor het treffen van passende technische en organisatorische maatregelen teneinde te waarborgen en te kunnen aantonen dat de verwerking in overstemming is met de AVG.

3. Definities

De volgende definities worden gehanteerd:

- **AP**: Autoriteit Persoonsgegevens, toezichthouder als bedoeld in artikel 51 AVG.
- **AVG**: Algemene Verordening Persoonsgegevens.
- **Bestand**: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is, dan wel verspreid op functionele of geografische gronden.
- **Betrokkene**: degene op wie een Persoonsgegeven betrekking heeft. Voor het Parkhuis voornamelijk cliënten en medewerkers.

- **Bijzondere persoonsgegevens**: Persoonsgegevens waaruit iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Daarnaast ook 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.
- **CFW**: Control Framework. Dit is een methodiek waarbij via een geautomatiseerd systeem door middel van een normenkader met beheersmaatregelen, periodieke controles worden uitgevoerd. EasyPrivacy is een geautomatiseerd control framework. Hierbij worden de uitkomsten van de controles in het systeem vastgelegd en kan de FG en het management via een PDCA (*Plan Do Check Act*) cyclus continu monitoren of aan de verplichtingen wordt voldaan en waar bijgestuurd moet worden.
- **Data Protection Impact Assessment (DPIA)**: '*Gegevensbeschermingseffectbeoordeling*' in het Nederlands. Een DPIA wordt uitgevoerd voorafgaand aan de verwerking van persoonsgegevens en bevat een gegevensverwerkingsanalyse, een beoordeling van de noodzaak en evenredigheid van de verwerking en inventariseert de risico's die met de verwerking zijn verbonden alsmede de beheersmaatregelen om deze risico's te verkleinen.
- **Derde**: de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkings-verantwoordelijke vallen of door de verwerker gemachtigd zijn om de gegevens te verwerken.
- **FG**: Functionaris Gegevensbescherming als bedoeld in Afdeling 4 AVG, art. 37 e.v.
- **Inbreuk in het geval van 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.
- **Informatiebeveiligingsbeleid:** dit is het beleid waarin het Parkhuis uitwerkt op welke wijze zij de informatie en persoonsgegevens heeft beveiligd tegen ongeoorloofde toegang, met als doel inbreuken op de beveiliging te voorkomen.
- **Ontvanger:** de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig Uniewetgeving of nationale wetgeving, gelden echter niet als ontvangers; de verwerking van deze gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.
- **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand

van een identificatiemiddel, zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die persoon.

- **Pseudonimisering**: het verwerken van persoonsgegevens op zodanige wijze dat de gegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er 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 betrokkene**: elke vrije, specifieke, op informatie berustende en ondubbelzinnige wilsuiting waarmee de Betrokkene, door middel van hetzij een verklaring hetzij een ondubbelzinnige actieve handeling, aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.
- **Uitvoeringswet AVG**: de uitwerking van de AVG met speciale onderwerpen, zoals van toepassing voor nationale Nederlandse wetgeving, zoals BSN-nummer.
- **Verwerkingsverantwoordelijke**: de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij Uniewetgeving of nationale wetgeving, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
- **Verwerker**: de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke (*Het Parkhuis*) persoonsgegevens verwerkt.
- **Verwerking**: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
- **Verwerking van Persoonsgegevens**: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder verzamelen, vastleggen, ordenen, bewaren, wijzigen, raadplegen, gebruiken, verstrekken en vernietigen.

4. Uitgangspunten

4.1. Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij het Parkhuis zijn:

- Privacybescherming dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming.
- De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen.
- Binnen het Parkhuis is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- Het Parkhuis is als rechtspersoon eigenaar van de persoonsgegevens die onder haar verantwoordelijkheid worden verwerkt.
- Persoonsgegevens hebben een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij het Parkhuis geclassificeerd. De classificatie is het uitgangspunt voor de te nemen beveiligingsmaatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen het Parkhuis wil beschermen en de benodigde investeringen en maatregelen. Deze classificatie is uitgewerkt in het Informatiebeveiligingsbeleid.
- Het Parkhuis sluit met alle leveranciers verwerkersovereenkomsten af als zij persoonsgegevens ontvangen van het Parkhuis.
- Privacybescherming is bij het Parkhuis een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing van beleid, procedures en richtlijnen gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij het Parkhuis vanaf de start rekening gehouden met informatiebeveiliging en privacy.

4.2. Uitgangspunten privacy

De uitgangspunten met betrekking tot de omgang van persoonsgegevens bij het Parkhuis zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze in verhouding staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere

gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Behoorlijk en transparant**: het Parkhuis legt aan betrokkenen op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
6. **Vertrouwelijkheid**: er zijn passende organisatorische en technische beveiligingsmaatregelen getroffen zodat een passende beveiliging van de verwerking van Persoonsgegevens is gegarandeerd. Persoonsgegevens zijn beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
7. **Verantwoordingsplicht**: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van bovenstaande uitgangspunten (beginselen) en kan dit aantonen.

5. Wet- en regelgeving

In onderstaande overzicht is de relevante wet- en regelgeving voor het Parkhuis in verband privacy weergegeven:

- Algemene Verordening Gegevensbescherming
- Uitvoeringswet AVG
- Europees Verdrag voor de Rechten van de Mens
- Auteurswet
- Telecommunicatiewet (inclusief de bijbehorende besluiten)
- Burgerlijk Wetboek (WGBO)
- Sector specifieke regelgeving, zoals de NEN 7510, 12 en 13 en NTA 7516

Gedragscodes en richtlijnen

- Gedragscode mobiele telefonie, e-mail, internet en sociale media
- Procedure camerabewaking
- Beroepsregels van BIG geregistreerde medewerkers

6. Verwerkingen van persoonsgegevens

In dit hoofdstuk is beschreven welke persoonsgegevens door het Parkhuis worden verwerkt, wat de grondslag daarvan is, hoe deze gegevens worden verkregen en wat er met de gegevens wordt gedaan. Bijzondere persoonsgegevens komen in het volgende hoofdstuk aan bod.

6.1. Persoonsgegevens

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze door het Parkhuis verwerkt. Dit betekent o.a. dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen.
De belangrijkste categorieën persoonsgegevens die Het Parkhuis verwerkt zijn persoonsgegevens van haar cliënten en van haar medewerkers.
In het register van verwerkingsactiviteiten is een gedetailleerd overzicht te vinden van de persoonsgegevens die Het Parkhuis verwerkt.

Hoe worden de bovenstaande gegevens verkregen?

In geval van de cliëntgegevens worden persoonsgegevens rechtstreeks verschaft door de cliënt dan wel door de hiertoe gemachtigde vertegenwoordigers. Tevens worden persoonsgegevens verstrekt met schriftelijke gerichte toestemming van betrokkene door derden.

Persoonsgegevens van medewerkers (personeel, vrijwilligers en externe inhuur) worden verkregen van de direct betrokkenen, dan wel via een broker of een leverancier (denk aan een arbodienst in het kader van verzuim, pensioenverzekeraar, e.d.).

6.2. Verwerkingen

Het Parkhuis onderscheidt de volgende kernverwerkingsactiviteiten ('diensten'), waarvan is geïnventariseerd welke persoonsgegevens noodzakelijk zijn voor een goede uitvoering van deze dienst.

1. Uitvoeren van de zorgovereenkomst ten behoeve van de cliënten die gebruik maken van de zorgverlening van het Parkhuis.
2. Uitvoeren van de personeelsadministratie (t.b.v. medewerkers, vrijwilligers en inleners) van Het Parkhuis.
3. Uitvoeren van wettelijke verplichtingen voor zover dat nodig is voor een verantwoorde uitvoering van de financiële administratie ten behoeve van de bedrijfsdoelstellingen van het Parkhuis.
4. Het verwerken van persoonsgegevens voor wat betreft een veilige omgeving. Het Parkhuis verwerkt bijvoorbeeld persoonsgegevens op basis van een gerechtvaardigd belang inzake de beveiliging van objecten via camera's.

Voor wat betreft de verwerking van persoonsgegevens zal het Parkhuis dit doen met inachtneming van de wet- en regelgeving alsmede de richtlijnen van de Autoriteit Persoonsgegevens.
Het Parkhuis verwerkt niet meer persoonsgegevens dan noodzakelijk is. Tevens zijn alleen de persoonsgegevens die nodig zijn voor de werkzaamheden van medewerkers voor de betreffende medewerkers beschikbaar. Op deze wijze geeft het Parkhuis invulling aan het '*need to know*' principe.

6.2.1 Register van verwerkingsactiviteiten

Het Parkhuis houdt conform art. 30 en art. 5 lid 2 AVG een verwerkingsregister bij waarin alle soorten persoonsgegevens en verwerkingen worden bijgehouden.
Per verwerkingsactiviteit wordt het volgende in het verwerkingsregister geregistreerd:

- de naam en contactgegevens van de verantwoordelijke;
- de doeleinden van de gegevensbewerking;
- een beschrijving van de categorieën betrokkenen;
- een beschrijving van de categorie persoonsgegevens;
- de categorie ontvangers;
- indien van toepassing een vermelding van een verstrekking van persoonsgegevens aan een derde land of internationale organisatie;
- de bewaartermijnen;
- een algemene beschrijving van de beveiligingsmaatregelen.

Het verwerkingsregister is de basis voor de 'datamapping' binnen Het Parkhuis, waarmee overzicht wordt gecreëerd van de gegevens die binnen de verschillende processen en

systemen worden verwerkt, aan wie deze gegevens worden verstrekt en welke gegevens door verwerkers worden verwerkt.

6.3. Doel van de verwerkingen

De doelen waarvoor het Parkhuis persoonsgegevens worden verwerkt zijn de volgende:

1. Het uitvoeren van de zorgleveringsovereenkomst (cliënten);
2. Het uitvoeren van de arbeidsovereenkomst (medewerkers);
3. Het borgen van een veilige omgeving voor cliënten en medewerkers;
4. Het nakomen van wettelijke verplichtingen, zoals fiscale verplichtingen.

Het Parkhuis draagt er zorg voor dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt. Persoonsgegevens worden alleen verwerkt door personen die uit hoofde van ambt, beroep of wettelijk voorschrift, dan wel krachtens een geheimhoudingsovereenkomst tot geheimhouding zijn verplicht.

6.4. Grondslagen

Persoonsgegevens worden door het Parkhuis conform artikel 6 en artikel 9 AVG slechts verwerkt als er sprake is van minimaal één van de volgende grondslagen:

1. De betrokkene heeft voor de verwerking van persoonsgegevens voor een of meer specifieke doeleinden zijn toestemming verleend. Deze grondslag geldt voor cliënten waarbij uitwisseling plaatsvindt met andere partijen.
2. De verwerking van persoonsgegevens is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is. Deze grondslag geldt voor cliënten waarbij uitvoering plaatsvindt van de zorgovereenkomst.
3. De verwerking van persoonsgegevens is noodzakelijk om een wettelijke verplichting na te komen waaraan het Parkhuis onderworpen is. Deze grondslag geldt voor o.a. medewerkers in het kader van fiscale verplichtingen.
4. De gegevensverwerking is noodzakelijk om de vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen. Deze grondslag geldt alleen in noodsituaties.
5. De gegevensverwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van het Parkhuis of een derde, tenzij het belang van de betrokkenen prevaleert. Deze grondslag geldt bijvoorbeeld voor het beveiligen van objecten.

6.5. Verstrekkingen aan derden

Het Parkhuis verstrekt in het kader van de dienstverlening aan haar cliënten persoonsgegevens aan derden. In het register van verwerkingen is een volledige opsomming opgenomen, waarin tevens een onderscheid is gemaakt tussen:

- Derden met wie gegevensuitwisseling plaats kan vinden, zonder dat daar een aanvullende overeenkomst onderligt (*zoals bijvoorbeeld: CIZ, Ziekenhuizen, Gemeentelijke instellingen en andere overheidsorganen als Belastingdienst, UWV en Officier van Justitie*).

- Derden met wie cliëntgegevens worden uitgewisseld, waarbij deze partij als zelfstandige verwerkingsverantwoordelijke wordt aangemerkt als bijvoorbeeld: leveranciers van zorgmiddelen alsmede andere behandelaars.
- Derden die verwerkingen uitvoeren in opdracht van Het Parkhuis. Met deze partijen is een verwerkersovereenkomst opgesteld.

6.6. Beveiliging

Het Parkhuis is zich bewust van het cruciale belang van de beveiliging van persoonsgegevens voor de betrokkene. Persoonsgegevens van de betrokkenen zijn beveiligd met adequate organisatorische en technische middelen die zijn vastgelegd in het Informatiebeveiligingsbeleid van het Parkhuis.

6.7. Cameratoezicht

Het Parkhuis heeft het recht bewakingscamera's te gebruiken om gebouwen en eigendommen te beveiligen. Middels borden worden medewerkers en derden geïnformeerd over het feit dat specifieke gedeelten van het Parkhuis terrein en gebouw worden gefilmd. Beelden worden niet langer opgeslagen dan nodig is en worden alleen gebruikt in geval dit uit oogpunt van een beveiligingsincident noodzakelijk is.

6.8. Verwerkersovereenkomsten

Het Parkhuis sluit met partijen die namens het Parkhuis verwerkingen verrichten een verwerkingsovereenkomst. In deze verwerkersovereenkomst zijn alle verplichtingen vastgelegd waaraan een verwerker op grond van geldende wet- en regelgeving (*art. 28 AVG*) moet voldoen. Daarnaast is opgenomen welke persoonsgegevens worden uitgewisseld, de verantwoordelijkheden van beide partijen, wat de beveiligingseisen zijn en wat de procedure is ingeval van een datalek.

7. Bijzondere persoonsgegevens

Art. 24 AVG stelt dat organisatorische en technische maatregelen getroffen moeten worden.
Het doel van deze technische en organisatorische maatregelen is om de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren. Omdat het Parkhuis ook bijzondere gegevens verwerkt zijn hiertoe speciale organisatorische en technische maatregelen getroffen. Deze staan volledig uitgeschreven in het Informatiebeveiligingsbeleid van het Parkhuis.

8. Toegang tot de persoonsgegevens

De toegang tot de persoonsgegevens binnen het Parkhuis is geregeld via een zogenaamde autorisatiematrix (bijlage 3). Dit betekent dat uitgewerkt is welke medewerkers (rollen en taken/verantwoordelijkheden) met welke persoonsgegevens mogen werken.

Hierbij geldt als uitgangspunt welke medewerkers persoonsgegevens objectief gezien nodig hebben voor een goede uitvoering van hun functie. Deze autorisatiematrix wordt periodiek onderhouden en binnen het Parkhuis wordt regelmatig gecontroleerd of de autorisaties conform het beleid zijn toegepast.

9. Organisatie

De organisatie van Privacy en Informatiebeveiliging gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.
Dit hoofdstuk beschrijft hoe dit binnen het Parkhuis is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen

9.1. Rollen en functies rondom Privacy

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij het Parkhuis een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

9.2. Richtinggevend

De bestuurder is eindverantwoordelijk voor het Privacybeleid en Informatiebeveiligingsbeleid en stelt in samenspraak met het MT het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor privacy- en informatiebeveiligingsbeleid is gemandateerd aan de Clustermanager Ondersteunend Bedrijf.

9.3. Sturend

Bij de Clustermanager Ondersteunend Bedrijf is de sturende rol op gebied van Privacy belegd. Deze functionaris geeft terugkoppeling en advies aan de Bestuurder en het MT en stuurt de medewerkers aan op uitvoerend niveau. De Manager Ondersteunend bedrijf draagt zorg voor:

- Vertalen van beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling.
- Bewaking van uniforme uitvoering van de privacywet binnen Het Parkhuis.

- Governance en aanspreekpunten voor incidenten op het gebied van informatiebeveiliging en privacy en de verdere coördinatie van afhandeling van incidenten binnen Het Parkhuis.

De Clustermanager Ondersteunend Bedrijf wordt hierbij ondersteunt door:

Functionaris voor Gegevensbescherming
De FG houdt binnen het Parkhuis toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. FG heeft regelmatig overleg met de Manager Ondersteunend Bedrijf. De rol van de FG is verder uitgewerkt in hoofdstuk 9.5.

CISO
De CISO is in opdracht van de Clustermanager Ondersteunend bedrijf verantwoordelijk voor het uitvoeren en toepassen van het Informatiebeveiligingsbeleid. Daarnaast houdt de CISO als onafhankelijke functionaris binnen het Parkhuis toezicht op de toepassing en naleven van de maatregelen op het gebied van informatiebeveiliging. De CISO heeft regelmatig overleg met de Manager Ondersteunend Bedrijf en de FG.

Privacy Officer

De Privacy Officer is in opdracht van de Clustermanager Ondersteunend bedrijf verantwoordelijk voor het uitvoeren en toepassen van het Privacybeleid en Informatiebeveiligingsbeleid. De Privacy Officer houdt toezicht op de toepassing en het naleven van de maatregelen op het gebied van gegevensbescherming.

De Privacy Officer heeft regelmatig overleg met de Manager Ondersteunend Bedrijf en de FG.

Domeinverantwoordelijke / proceseigenaar
Binnen het Parkhuis zijn er verschillende domeinen/processen, zoals ICT, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, beleid, et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze Privacy en Informatiebeveiliging daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren (conform de ICT beheersorganisatie) de volgende specifieke taken:

- Verantwoordelijk voor het beheer van de ICT middelen (*zoals een applicatie voor de zorg*) en het vaststellen en onderhouden van een autorisatiematrix.

- Samen met functioneel beheer en ICT-beheer zien zij erop toe dat regelmatig wordt gecontroleerd dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

9.4. Uitvoerend

- **Teamleider Administratie en Automatisering**
  De Teamleider administratie en automatisering is het technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.
- **Functioneel applicatie beheerder**
  De functioneel applicatie beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert deze zijn of haar taken uit.
- **Leidinggevende**
  Naleving van privacy en het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:
  - er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van het beveiligingsbeleid;
  - toe te zien op de naleving van het Privacy- en Informatiebeveiligingsbeleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
  - periodiek het onderwerp Privacy- en Informatiebeveiligingsbeleid onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
  - als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde privacy onderwerpen.

- **Medewerker**
  Alle medewerkers hebben verantwoordelijkheid met betrekking tot privacy en informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het Personeelshandboek en de Gedragscode ICT- en internetgebruik.
  Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
  Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de OR).

9.5. Functionaris voor de gegevensbescherming

Conform de wettelijke verplichting van artikel 37 AVG heeft Het Parkhuis een FG aangesteld. Het Parkhuis vindt het van belang dat de FG makkelijk te bereiken is.

9.5.1. Profiel FG

De FG moet zijn weg binnen de organisatie kennen. Daarbij moet hij/zij kennis hebben van de processen waarbij persoonsgegevens worden verwerkt. De FG moet deskundig zijn op het gebied van wetgeving en de praktijk inzake gegevensbescherming op een niveau dat passend is bij de gevoeligheid en complexiteit en de hoeveelheid gegevens die het Parkhuis verwerkt. Gezien de omvang van het Parkhuis is minimaal een hbo-niveau met een aanvullende privacy opleiding passend. De FG heeft kennis van essentiële AVG-onderwerpen zoals de rechten van betrokkenen, privacy by default en design, informatiebeveiliging, documentatieplicht en datalekken. Integriteit, onafhankelijke taakuitoefening en het stimuleren van privacy compliance staan voor de FG hoog in het vaandel.

De FG heeft de bevoegdheden zoals vastgelegd in het FG Statuut.

Binnen het Parkhuis is een profiel vastgesteld door HR.

9.5.2. Taken FG

De volgende taken zijn binnen het Parkhuis aan de FG toebedeeld:

- houdt toezicht op de naleving van de AVG en van het beleid van het Parkhuis op het gebied van gegevensbescherming met inbegrip van de toewijzing van verantwoordelijkheden, bewustwording en opleiding van het bij de verwerking betrokken personeel;
- werkt samen met de Autoriteit Persoonsgegevens en fungeert als contactpunt voor de AP;
- controleert inventarisaties van gegevensverwerkingen;
- handelt vragen en klachten af over gegevensverwerking van betrokkenen;
- controleert interne regelingen;
- adviseert over (nieuwe) processen, producten, diensten, technologie en beveiliging (privacy by design);
- adviseert met betrekking tot de noodzaak een DPIA en ziet toe op de uitvoering daarvan;
- adviseert en informeert het Parkhuis en de werknemers die de persoonsgegevens verwerken over hun verplichtingen die volgen uit de AVG en/of andere privacy regelgeving;
- kan input leveren bij het opstellen of aanpassen van een gedragscode;
- moet compliance van de organisatie op het gebied van de AVG bevorderen;
- rapporteert jaarlijks aan Bestuurder & MT.
- adviseert over audits en DPIA’s;
- fungeert als schakel tussen de organisatie en belanghebbenden, zoals de toezichthouder en de betrokkenen;
- mag contact opnemen met, en advies vragen aan de toezichthoudende autoriteit.

De FG houdt bij de uitoefening van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

9.5.3. Positie FG binnen het Parkhuis

De FG is door de Bestuurder benoemd in een benoemingsbesluit dat de rol, taken en verantwoordelijkheden alsmede positie van de FG respecteert.
De AVG vereist dat de FG "*naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens*". De FG heeft binnen het Parkhuis geen positie die ertoe leidt dat hij het doel en middelen voor de verwerking van persoonsgegevens bepaalt.
De FG is binnen het Parkhuis een gesprekspartner aangaande het verwerken van persoonsgegevens. Het is van belang dat de FG zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen. Wanneer de FG direct geïnformeerd en geraadpleegd wordt, is het makkelijker de AVG na te leven en wordt privacy by design vormgegeven.

Het Parkhuis ondersteunt de FG op de volgende manier:

- de FG wordt ondersteund bij de vervulling van zijn taken door hem of haar toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid;
- betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten;
- de FG heeft een regulier overleg met de CISO / Privacy Officer en Manager Ondersteunende Diensten en informeert de organisatie over nieuwe ontwikkelingen op het gebied van privacy en adviseert bij beslissingen met gevolgen voor gegevensbescherming;
- de FG heeft rechtstreeks toegang tot het raad van bestuur en de raad van toezicht;
- aan de mening van de FG wordt een passende waarde gehecht. Bij een verschil in mening wordt vastgelegd waarom er van het advies van de FG wordt afgeweken;
- de FG wordt onmiddellijk geraadpleegd bij een datalek of een ander incident van dien aard.

Art. 38 AVG schrijft voor dat de FG geen instructies ontvangt met betrekking tot de uitvoering van zijn taken. De FG dient in staat te zijn om zijn taken en verplichtingen onafhankelijk te vervullen. De FG kan niet ontslagen of gestraft worden voor de uitvoering van zijn taken als FG.[1] De autonomie van de FG houdt echter niet in dat zijn

[1] De FG kan wél rechtmatig ontslagen worden als hier andere redenen aan ten grondslag liggen dan het uitvoeren van zijn taken als FG en als dit op basis van een gebruikelijke beleidsregel is en uit hoofde van de toepasselijke nationale

beslissingsbevoegdheid verder gaat dan zijn taken onder artikel 39 AVG. Het Parkhuis, de Raad van Bestuur, blijft verantwoordelijk voor de naleving van de privacywetgeving en moet kunnen aantonen dat deze nageleefd wordt. Indien het Parkhuis een beslissing neemt die niet aan de AVG voldoet en niet met het advies van de FG overeenkomt, dient de FG de gelegenheid geboden te worden zijn afwijkende mening duidelijk te maken aan de Bestuurder.

9.6. Privacy Officer

Het Parkhuis heeft een Privacy Officer aangesteld. Het Parkhuis vindt het van belang dat de Privacy Officer makkelijk te bereiken is.

9.6.1. Profiel Privacy Officer

De Privacy Officer moet zijn weg binnen de organisatie kennen. Daarbij moet hij/zij kennis hebben van de processen waarbij persoonsgegevens worden verwerkt. De Privacy Officer moet deskundig zijn op het gebied van gegevensbescherming en privacy. Gezien de omvang van het Parkhuis is minimaal een hbo-niveau met een aanvullende opleiding op het gebied van gegevensbescherming passend. De Privacy Officer heeft kennis van essentiële AVG-onderwerpen alsmede informatiebeveiliging, waaronder cyber security.

Binnen het Parkhuis is een profiel vastgesteld door HR: Adviseur informatiebeveiliging en AVG.

9.6.2. Taken Privacy Officer

De volgende taken zijn binnen het Parkhuis aan de Privacy Officer toebedeeld:

- maakt beleid en richtlijnen en procedures op het gebied van privacy;
- houdt toezicht op de naleving van (interne) regels op het gebied van de AVG met inbegrip van de toewijzing van verantwoordelijkheden, bewustwording en opleiding van het bij de verwerking betrokken personeel;
- werkt samen met de FG in het kader van toezicht;
- is verantwoordelijk voor inventarisaties van gegevensverwerkingen;
- stelt interne regelingen op;
- adviseert over (nieuwe) processen, producten, diensten, technologie en beveiliging (privacy by design);
- adviseert en informeert het Parkhuis en de werknemers over privacy;
- rapporteert per kwartaal aan Bestuurder & MT.
- adviseert over audits en DPIA’s;
- fungeert als schakel tussen de organisatie en belanghebbenden.

contractenwet, arbeidswet en het strafrecht dat ook voor elke andere medewerker of aannemer zou gelden (bijvoorbeeld in geval van diefstal, fysieke, psychologische of seksuele intimidatie of soortgelijke zware misdragingen).

9.6.3. Positie Privacy Officer binnen het Parkhuis

De Privacy Officer zal "*naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens*".
Het is van belang dat de Privacy Officer zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen. Wanneer de Privacy Officer direct geïnformeerd en geraadpleegd wordt, is het makkelijker de AVG na te leven en wordt privacy by design vormgegeven.

Het Parkhuis ondersteunt de Privacy Officer op de volgende manier:

- de Privacy Officer wordt ondersteund bij de vervulling van zijn taken door hem of haar toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid;
- betrokkenen kunnen met de Privacy Officer contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten;
- aan de mening van de Privacy Officer wordt een passende waarde gehecht. Bij een verschil in mening wordt vastgelegd waarom er van het advies van de Privacy Officer wordt afgeweken;
- de CISO / Privacy Officer wordt onmiddellijk geraadpleegd bij een datalek of een ander incident van dien aard.

De Privacy Officer dient in staat te zijn om zijn taken en verplichtingen onafhankelijk te vervullen. Het Parkhuis, de Raad van Bestuur, blijft verantwoordelijk voor de mate waarin het Parkhuis voldoet aan de vereisten op het gebied van Informatiebeveiliging en moet kunnen aantonen dat aan de minimale eisen van informatiebeveiliging wordt voldaan.

10. Rechten van betrokkenen

De AVG geeft betrokkenen diverse rechten. In dit hoofdstuk is uitgewerkt hoe het Parkhuis hieraan invulling geeft.

10.1. Recht op informatie

Het Parkhuis is wettelijk verplicht informatie te geven aan betrokkenen van wie zij persoonsgegevens verwerkt. Zij moet betrokkenen informeren welke persoonlijke gegevens zij verwerkt en met welk doel. Op het moment dat de persoonsgegevens door het Parkhuis worden verwerkt, rust op het Parkhuis de plicht om de betrokkene te informeren. De regels van art. 12, 13 en 14 AVG worden hierbij in acht genomen.
Het Parkhuis verleent deze informatie via het privacy statement op de website en ook via de privacyverklaring rechtstreeks aan de betrokkene op het moment dat het Parkhuis de persoonsgegevens gaat verwerken. De privacyverklaring is opgenomen als bijlage 4.

10.2. Recht op inzage

Een betrokkene kan bij het Parkhuis een verzoek indienen om een overzicht van verwerkingen op te vragen. Het Parkhuis zal de betrokkene binnen een maand laten weten:

- of het Parkhuis zijn persoonsgegevens gebruikt, en zo ja:
- om welke gegevens het gaat;
- wat het doel is van het gebruik alsmede de bewaartermijnen;
- aan wie het Parkhuis (*derden; buiten Het Parkhuis*) de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens.

Het verzoek kan naar avg@hetparkhuis.nl worden gestuurd. De medewerker die het verzoek behandelt kan eventueel advies bij de FG opvragen. Indien er twijfel is over de identiteit van betrokkene moet deze net als bij het recht op inzage een kopie van het identiteitsbewijs kunnen tonen. Na vaststelling van de identiteit wordt de kopie van het identiteitsbewijs gewist.

10.3. Recht op rectificatie

Indien uit het verstrekte overzicht blijkt dat de persoonsgegevens feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd met een wettelijk voorschrift, kan de betrokkene schriftelijk om verbetering, aanvulling, verwijdering en/of afscherming van het/de betreffende persoonsgegeven(s) verzoeken. Binnen een maand zal het Parkhuis laten weten of er aan dit verzoek gehoor wordt gegeven. Als er niet of niet volledig aan het verzoek wordt voldaan zal het Parkhuis dit schriftelijk toelichten. Wijzigingen kunnen schriftelijk of per e-mail worden doorgeven. Indien er twijfel is over de identiteit van betrokkene moet deze net als bij het recht op inzage een kopie van het identiteitsbewijs kunnen tonen. Na vaststelling van de identiteit wordt de kopie van het identiteitsbewijs gewist.

10.4. Recht op gegevenswissing en bezwaar

Het Parkhuis wist persoonsgegevens van betrokkene zonder onredelijke vertraging, o.a. indien:

- persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- de betrokkene zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat;
- de persoonsgegevens onrechtmatig verwerkt zijn.

In het hoofdstuk bewaartermijnen staat hoe lang het Parkhuis persoonsgegevens van betrokkenen bewaart.
De betrokkene heeft ook het recht om bezwaar aan te tekenen tegen het gebruik van zijn persoonsgegevens. Dit kan als er sprake is van met zijn specifieke situatie verband

houdende redenen, tenzij het Parkhuis dwingende gerechtvaardigde gronden heeft om de gegevens wel te verwerken.
Het Parkhuis laat binnen een maand gemotiveerd weten of het verzoek wordt gehonoreerd.

10.5. Recht op beperking van de verwerking

Indien de juistheid van persoonsgegevens door de betrokkene worden betwist, de verwerking onrechtmatig is, de betrokkene de gegevens nodig heeft, dan wel de betrokkene bezwaar heeft gemaakt, dan kan betrokkene een beroep doen op dit recht.
Het Parkhuis laat binnen een maand gemotiveerd weten of het verzoek wordt gehonoreerd.

10.6. Recht op overdraagbaarheid van gegevens

Betrokkenen hebben het recht om de persoonsgegevens die het Parkhuis van de betrokkene verwerkt te verkrijgen in een gestructureerde, gangbare en machine leesbare vorm. Betrokkenen hebben vervolgens het recht om deze gegevens over te dragen of rechtstreeks te laten overdragen, zonder daarbij gehinderd te worden tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hem zelf verstrekte gegevens.
Als betrokkenen van dit recht gebruik willen maken dan kunnen zij per e-mail een verzoek indienen. De betrokkene ontvangt vervolgens per e-mail in PDF formaat de informatie.

10.7. Klachten gerelateerd aan de verwerking van persoonsgegevens

Klachten betreffende de bescherming van de privacy van de betrokkene worden behandeld via de procedure ‘Rechten van betrokkenen’ van het Parkhuis. Hierbij wordt vermeld dat de betrokkene zich na afhandeling van de klacht zich kan wenden tot de Autoriteit Persoonsgegevens.

11. Incidenten en datalekken

Organisaties die een meldingsplichtig datalek hebben, moeten dit conform art. 33 AVG melden bij de AP en volgen art. 34 AVG in bepaalde gevallen ook aan de betrokkenen van wie de gegevens gelekt zijn. In dit hoofdstuk is te lezen hoe het Parkhuis met de meldingsplicht omgaat.

11.1. Procedure Meldplicht Datalekken

Het Parkhuis meldt datalekken zonder onredelijke vertraging, en indien mogelijk binnen 72 uur 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. De Autoriteit Persoonsgegevens heeft hierover

beleidsregels bekendgemaakt. Daarin heeft de toezichthouder uiteengezet wat volgens haar een datalek of inbreuk op de beveiliging van persoonsgegevens is en wanneer zo'n datalek moet worden gemeld bij het meldloket en bij de betrokkene die het aangaat. Het Parkhuis heeft een procedure Meldplicht Datalekken (bijlage 2) waarin staat beschreven welke stappen moeten worden ondernomen op het moment dat er een vermoeden van een datalek is. Deze procedure Meldplicht Datalekken is op de beleidsregels van de AP gebaseerd.

11.2. Crisisteam

Het Parkhuis heeft een Crisisteam. Dit team bestaat uit de Bestuurder, Manager Ondersteunend Bedrijf, Manager Zorg en Communicatieadviseur. Dit crisisteam wordt ook ingeschakeld ten tijde van een zeer groot beveiligingsincident waarbij de zorg continuïteit en/of het imago van het Parkhuis op het spel staat, om de te nemen maatregelen op het gebied van communicatie en IT (beveiliging) te bespreken en te beslissen of de FG ingeschakeld moet worden. In het beleid en procedure datalekken staat nader beschreven hoe en wanneer dit team ingeschakeld wordt. De CISO/Privacy Officer heeft geen standaard plek in het Crisisteam, maar wordt, indien het incident dit vereist, als adviseur toegevoegd.

12. Bewaartermijnen

Om een goede administratie bij te kunnen houden, moet een organisatie bepaalde persoonsgegevens kunnen bewaren. Er zijn op de grond van de AVG geen concrete bewaartermijnen voor persoonsgegevens. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren. Het Parkhuis dient zich af te vragen of er redenen zijn op grond waarvan persoonsgegevens vastgelegd kunnen blijven. Bepalend hierbij is uit uitgangspunt dat persoonsgegevens niet langer bewaard worden dan strikt noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor de gegevens zijn verzameld en worden verwerkt. Wel gelden er op basis van andere wetten minimale en maximale bewaartermijnen.

Het schema bewaartermijnen is opgenomen in bijlage 5.

Bewaartermijnen met betrekking tot werknemers zijn te vinden in het personeelsbeleid.

13. Data Protection Impact Assessments

Voorafgaand aan nieuwe verwerkingen en na belangrijke aanpassingen van bestaande verwerkingen beslist het Parkhuis of zij een Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling in het Nederlands, hierna: DPIA) uitvoert. Het Parkhuis voert een DPIA uit als de verwerking gelet op de aard, de omvang, de context

en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene. De FG kan adviseren een DPIA uit te laten voeren.

De DPIA bevat een analyse van de beoogde verwerking, de doeleinden, de noodzaak, de grondslagen, mogelijke risico's voor de betrokkene en waarborgen die het Parkhuis treft om eventuele risico's te mitigeren. Degene die betrokken zijn bij de ontwikkeling van een nieuw product of een review, voeren de DPIA uit. De uitvoerders winnen (indien nodig) advies in bij de FG. Alle DPIA's worden zorgvuldig gearchiveerd, zodat altijd alle afwegingen van risico's en de bescherming van de belangen van betrokkenen zijn terug te vinden.

14. Privacy by design en default

Technologische ontwikkelingen gaan sneller dan ooit. Daarvan kan iedereen profiteren. Organisaties zoals het Parkhuis maar zeker ook cliënten en medewerkers die gebruik kunnen maken van nieuwe producten en diensten. Nog meer dan voorheen is het belangrijk om ook bij innovatieve ontwikkelingen van meet af aan actief rekening te houden met de privacyaspecten van een dergelijke technologische ontwikkeling. Als uitgangspunt geldt dat persoonsgegevens niet zonder meer door het Parkhuis mogen worden verwerkt maar uitsluitend wanneer dit noodzakelijk is voor een gerechtvaardigd doel, proportioneel is en hierbij wordt uitgegaan van dataminimalisatie en de gekozen werkwijze zo min mogelijk inbreuk maakt op de bescherming van persoonsgegevens. Dit vergt een juiste omgang met en gebruik van persoonsgegevens en daarmee een niet aflatende inzet van het Parkhuis, zowel bij aanvang van een nieuwe verwerkingsmethode alsook nadien. Bij de ontwikkeling van nieuwe diensten zal er daarom ook altijd een DPIA worden uitgevoerd en zal er advies bij de FG worden ingewonnen.
Doel hierbij is om de juiste technische en organisatorische maatregelen te treffen, om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor de diverse specifieke doelen.

15. Controle en rapportage

Het opstellen van dit Privacybeleid is een van de eerste stappen in het proces om 'in control' te zijn over de verwerking van persoonsgegevens binnen het Parkhuis. Artikel 5 lid 2 en 24 AVG schrijft voor dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de verplichtingen uit hoofde van de AVG en deze kan aantonen ('*verantwoordingsplicht*'). Daarom is het Parkhuis er met alleen het documenteren nog niet. Beleid dient niet alleen te worden vastgesteld door beleidsbepalers maar dient vooral te worden uitgevoerd door de organisatie. Privacy bewustzijn in alle lagen van de organisatie is daarom belang.

In dit hoofdstuk wordt uitgewerkt hoe het Parkhuis invulling geeft aan voorlichting en bewustzijn en wat de maatregelen zijn om in continuïteit te kunnen aantonen dat het Parkhuis privacy compliant is.

15.1. Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij het Parkhuis het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, externe inhuurkrachten en samenwerkingspartners.

15.2. Control Framework en normenkader Privacy

Het Parkhuis kiest ervoor om met EasyPrivacy te werken om in continuïteit te kunnen vaststellen of het Parkhuis privacy compliant is. Op deze wijze kan met geautomatiseerde controles periodiek worden gekeken of de wettelijke verplichtingen worden nageleefd. Hierbij maakt het Parkhuis gebruik van het privacy normenkader zoals opgenomen in EasyPrivacy. Daarin zijn normen en beheersmaatregelen uitgeschreven. Door deze periodiek te controleren en te monitoren, ontstaat een dashboard waarbij kan worden aangetoond in welke mate het Parkhuis voldoet aan dit normenkader.
Deze methodiek stelt tevens de externe accountant in staat te beoordelen in hoeverre het Parkhuis aan haar wettelijke verplichtingen op het gebied van Privacy voldoet en hoe zij de risico's beheerst.

15.3. Periodieke rapportage

Via de methodiek van EasyPrivacy kan de FG periodiek monitoren in hoeverre het Parkhuis de AVG naleeft. Vervolgens rapporteert de FG jaarlijks de status hiervan aan Bestuurder van het Parkhuis. De Bestuurder kan op basis van de monitoringsrapportage en aanbevelingen besluiten nemen om al dan niet bij te sturen, indien dit noodzakelijk is.

Bijlage 1: Register van verwerkingsactiviteiten van Het Parkhuis
Register van verwerkingsactiviteiten is opgesteld en valt onder beheer van Manager Ondersteunend bedrijf. De meest actuele versie is raadpleegbaar bij de security en/of privacy officer.

Bijlage 2: Procedure Meldplicht Datalekken
Procedure meldplicht datalekken is opgesteld. De meest actuele versie maakt onderdeel uit van het kwaliteitshandboek en is daar raadpleegbaar.

Bijlage 3: Autorisatiematrix
De autorisatie matrix en het beheer van autorisaties is opvraagbaar bij de Teamleider administratie en automatisering.

Bijlage 4: Privacyverklaring
Dit betreft de manier waarop Het Parkhuis invulling geeft aan haar verplichtingen m.b.t. art. 12, 13 en 14 AVG. Op de website van het parkhuis staat de meest recente verklaring opgenomen die is opgesteld conform AVG vereisten.

Bijlage 5: Bewaartermijnen
In het register van verwerkingsactiviteiten staan de bewaartermijnen per categorie van gegevens opgenomen.