Privacyreglement Villa Hooghe Heide

De aard van onze werkzaamheden brengt met zich mee dat wij veel persoonlijke gegevens van mensen gebruiken. Om de privacy van onze bewoners te waarborgen en om aan te geven hoe met persoonlijke gegevens wordt omgegaan, heeft Villa Hooghe Heide dit privacyreglement. In dit reglement worden de bepalingen die de wetgever stelt aan de verantwoorde omgang met en de bescherming van persoonsgegevens uitgewerkt.

Artikel 1
Algemene en begripsbepalingen

1.1 Tenzij hieronder uitdrukkelijk anders is bepaald worden termen in dit reglement gebruikt in de betekenis die de Wet Bescherming Persoonsgegevens daaraan toekent.
1.2 Persoonsgegevens: elk gegeven dat informatie bevat over een geïdentificeerde of identificeerbaar natuurlijk persoon.
1.3 Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens welke wordt of worden gebruikt voor de uitoefening van de zorg en dienstverlening van Villa Hooghe Heide
1.4 Gebruiker van persoonsgegevens: degene die als medewerker, bewerker of anderszins geautoriseerd is persoonsgegevens te gebruiken.
1.5 Medewerker: alle personen, werkzaam in de organisatie van Villa Hooghe Heide, al dan niet op basis van een arbeidsovereenkomst.
1.6 Betrokkene: degene van wie persoonsgegevens zijn opgenomen.
1.7 Opdrachtgever: een natuurlijk persoon (bewoner) of wettelijk vertegenwoordiger die aan Villa Hooghe Heide een opdracht tot dienstverlening heeft gegeven.
1.8 Bewoner: een natuurlijk persoon waarvan Villa Hooghe Heide direct dan wel via een wettelijk vertegenwoordiger een opdracht tot zorg en dienstverlening heeft gekregen.
1.9 Toegang tot persoonsgegevens: het autoriseren van personen, werkzaam in de organisatie van Villa Hooghe Heide, tot het kennisnemen en eventueel muteren van persoonsgegevens.
1.10 Verstrekken van persoonsgegevens aan derden: het bekend maken of ter beschikking stellen van persoonsgegevens buiten de organisatie van Villa Hooghe Heide
1.11 Derden: alle ingehuurde en niet tot de organisatie behorende personen, die voor kortere of langere tijd werkzaamheden verrichten in opdracht van Villa Hooghe Heide.

Artikel 2
Reikwijdte

2.1 Dit reglement is van toepassing op de verwerking van alle persoonsgegevens die direct betrekking hebben op de bewoners van Villa Hooghe Heide, tenzij uitdrukkelijk anders bepaald.

Artikel 3
Doel van de verwerking van persoonsgegevens

3.1 Doel van de verwerking van persoonsgegevens is het vastleggen van en het kunnen beschikken over gegevens, die noodzakelijk zijn voor de uitvoering van de met de bewoner overeen gekomen zorg.
3.2 Er worden geen persoonsgegevens verwerkt voor andere doeleinden dan in het reglement is aangegeven. Het verwerken van persoonsgegevens vindt alleen plaats overeenkomstig deze doelstelling.

Artikel 4
Verwerkingen van persoonsgegevens

4.1 De directie van Villa Hooghe Heide is aanspreekbaar voor het goed functioneren van de verwerking van de persoonsgegevens en voor de naleving van de bepalingen van dit reglement. Zijn/haar handelen, met betrekking tot de verwerking van de persoonsgegevens en de verstrekking van gegevens, wordt beperkt door dit reglement.

4.2 De directie van Villa Hooghe Heide is aansprakelijk voor eventuele schade als gevolg van het niet naleven van dit reglement. De directie van Villa Hooghe Heide is niet aansprakelijk, indien een opdrachtgever aansprakelijk is voor de verwerking van persoonsgegevens.

4.3 De directie van Villa Hooghe Heide treft de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de opgenomen gegevens. De directie draagt tevens zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de persoonsgegevens tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan.

Artikel 5
Toegang tot de persoonsgegevens

5.1 Alleen die medewerkers hebben toegang tot de persoonsgegevens voor zover dat noodzakelijk is voor hun taakuitoefening.

5.2 Eenieder die toegang heeft tot persoonsgegevens heeft een geheimhoudingsplicht ter zake van de gegevens waarvan hij/zij op grond van die toegang heeft kennisgenomen.

5.3 Alle ingehuurde en niet tot de organisatie behorende personen, die voor kortere of langere tijd werkzaamheden verrichten in opdracht van Villa Hooghe Heide met inzicht in de persoonsgegevens van bewoners en/of medewerkers dienen ofwel een verklaring in de overeenkomst te ondertekenen ofwel een verwerkersovereenkomst te ondertekenen gericht op de taken die zijn opgenomen in desbetreffende overeenkomst. **zie bijlage stroomschema verwerkersovereenkomst**

Artikel 6
Beveiliging van de persoonsgegevens

6.1 Er wordt zorgvuldig met persoonsgegevens omgegaan. Hiertoe worden de gegevens voldoende beveiligd.

Artikel 7
Verstrekking van gegevens

7.1 Tenzij zulks noodzakelijk is ter uitvoering van een wettelijk voorschrift of het een geval betreft als genoemd in artikel 7.3, is voor verstrekking van persoonsgegevens aan derden de gerichte schriftelijke toestemming van de betrokkene vereist.

7.2 Binnen de organisatie van Villa Hooghe Heide kunnen zonder toestemming van de betrokkene persoonsgegevens worden verstrekt, indien en voor zover dit voor hun taakuitoefening noodzakelijk is aan:

- Degenen die rechtstreeks betrokken zijn bij de actuele begeleiding van of advisering over de betrokkene dan wel op andere wijze rechtstreeks betrokken zijn bij de uitvoering van een concrete opdracht van een opdrachtgever;
- Personen die belast zijn met de directe vakinhoudelijke begeleiding van de betrokkene of personen die betrokken zijn bij behandeling van klachten van de betrokkene;
- De directie van Villa Hooghe Heide in verband met algemene verantwoordelijkheid als directie.

7.3 Buiten de organisatie van Villa Hooghe Heide kunnen zonder toestemming van de betrokkene persoonsgegevens worden verstrekt, indien en voor zover dit voor hun taakuitoefening noodzakelijk is, aan:
- Opdrachtgevers in het kader van de overeengekomen zorg- en dienstverlening;
- Personen die op grond van een daartoe gesloten overeenkomst, goedgekeurd door de verantwoordelijke, belast zijn met het onderhoud en de instandhouding van de apparatuur en programmatuur ten behoeve van de persoonsgegevens en indien voor zover toegang tot de gegevens noodzakelijk is voor hun taakuitoefening;

Artikel 8
Inzage van opgenomen gegevens

8.1 De betrokkene heeft recht op inzage in en afschrift van de op zijn/haar persoon betrekking hebbende persoonsgegevens.

8.2 Aan een verzoek als bedoeld in dit artikel wordt binnen tien werkdagen na ontvangst daarvan voldaan.

8.3 De door de betrokkene of zijn/haar gemachtigde gevraagde gegevens worden niet eerder verstrekt dan nadat, naar het oordeel van degene naar wie het verzoek is doorgeleid, voldoende vaststaat dat degene die de gegevens vraagt, de betrokkene of zijn/haar gemachtigde is. Dit dient plaats te vinden middels een deugdelijke legitimatie.

8.4 Villa Hooghe Heide kan weigeren aan een in dit artikel bedoeld verzoek te voldoen, voor zover dit noodzakelijk is wegens gewichtige belangen van anderen dan de verzoeker, de organisatie van de directie van Villa Hooghe Heide daaronder begrepen.

8.5 Inzage van de op zijn persoon betrekking hebbende persoonsgegevens door betrokkene, vindt uitsluitend plaats ten kantore van Villa Hooghe Heide in aanwezigheid van de directie , tenzij uitdrukkelijk anders bepaald.

Artikel 9
Aanvulling, correctie of vernietiging van opgenomen gegevens

9.1 Desgevraagd worden de opgenomen gegevens aangevuld met een door de betrokkene afgegeven verklaring met betrekking tot de opgenomen gegevens;

9.2 Zijn opgenomen gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift van de verwerking, dan dient de betrokkene een schriftelijk verzoek in van wat de aan te brengen correctie behelst;

9.3 Vernietiging blijft achterwege indien redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de betrokkene, alsmede voor zover bewaring op grond van een wettelijk voorschrift is vereist;

9.4 De directie draagt zorg dat een beslissing tot aanvulling, correctie of vernietiging zo spoedig mogelijk wordt uitgevoerd;

9.5 In geval van vernietiging van gegevens wordt in de gegevens een verklaring opgenomen dat op verzoek van betrokkene gegevens zijn vernietigd.

Artikel 10
Bewaartermijnen

10.1 Met inachtneming van eventuele wettelijke voorschriften stelt de verantwoordelijke vast hoelang de persoonsgegevens bewaard blijven. Tenzij anders bepaald, eindigt de bewaartermijn vijftien jaar na het laatste contact met de geregistreerde;

10.2 Indien de bewaartermijn is verstreken worden de betreffende persoonsgegevens uit de verwerkingen van persoonsgegevens verwijderd en vernietigd, zulks binnen een termijn van drie jaar.

Artikel 11
Klachten

11.1 Indien de betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of indien hij andere redenen heeft tot klagen, dient hij zich te wenden tot de klachten commissie van Villa Hooghe Heide

Artikel 12

Slotbepalingen

12.1 Onverminderd eventuele wettelijke bepalingen is dit reglement van kracht gedurende de gehele looptijd van de verwerkingen van persoonsgegevens;

12.2 Dit reglement kan gewijzigd worden bij besluit van de directie van Villa Hooghe Heide;

12.3 Dit reglement is per 17 oktober 2017 in werking getreden.

Privacy reglement - Bescherming persoons gegevens

Inleiding

In het onderstaande privacyreglement staat beschreven hoe in Villa Hooghe Heide wordt omgegaan met de gegevens die vallen onder de Wet Bescherming Persoonsgegevens. Het document heeft geen juridisch karakter, maar geeft een kader voor het handelen van medewerkers.

- hoe om te gaan met een data lek, **zie bijlage protocol datalek.**

Dit document beschrijft voor de volgende situaties hoe met persoonsgegevens wordt omgegaan:

- Omgang met persoonsgegevens algemeen;
- privacy met betrekking tot email verkeer;
- Privacy met betrekking tot notulen;
- Privacy met betrekking tot bewonersbesprekingen;
- Privacy met betrekking tot het digitale zorgdossier: persoonsgegevens bewoners;
- Privacy met betrekking tot het digitale medicatie aftekensysteem;
- Privacy met betrekking tot personeelsgegevens.

Omgang met persoonsgegevens algemeen

De volgende algemene richtlijnen zijn van toepassing voor alle medewerkers van Villa Hooghe Heide

- De medewerker verzamelt alleen gegevens die nodig zijn voor de uitvoering van het werk
- De medewerker is verplicht om te zwijgen over alles wat hem of haar wordt toevertrouwd en wat als vertrouwelijke informatie kan worden gezien (geheimhoudingsplicht), ook al geeft de bewoner niet direct aan dat het geheim moet blijven. Dit houdt in dat de medewerker de informatie niet met niet derden kan en mag bespreken. Uitzondering op deze regel is de beschreven samenwerkingsverbanden in het privacy beleid[1] die betrekking hebben op zorginhoudelijke overdrachten.
- De medewerkers hanteren de 'Beroepscode voor verpleegkundigen en verzorgenden' [2] geheimhoudingsafspraak in de persoonlijke arbeidsovereenkomst de gedragscode[3] en de huisregels[4] waarin ook onderdelen over privacy zijn opgenomen
- Kasten waarin gegevens over bewoners of medewerkers worden bewaard zijn gesloten als er geen medewerkers in de ruimte aanwezig zijn
- Kasten waarin persoonsgegevens worden bewaard zijn na werktijd afgesloten
- Vertrouwelijke informatie over bewoners of medewerkers wordt in een afgesloten envelop gedaan
- Oude bewoner gegevens dienen vernietigd te worden. Er is een papierversnipperaar aanwezig

[1] Privacy beleid ondertekenen bij opname
[2] Beroepscode verpleegkundige en verzorgenden
[3] Gedragscode
[4] Huisregels
Documenten zijn te vinden in de kwaliteitshandboeken.

- Indien er een bekende of familielid van een medewerker in zorg is bij Villa Hooghe Heide, wordt dit besproken met de leiding gevende
- Adressen en telefoonnummers hangen niet zichtbaar in het kantoor
- Mails met meerdere geadresseerden worden in BCC verstuurd zowel voor bewoners als medewerkers/ vrijwilligers.

Privacy met betrekking tot e-mail verkeer

- E- mail verkeer met persoonlijke gegevens over zowel medewerkers als bewoners worden met Zivver verstuurd in een beveiligde omgeving waar een code voor ingesteld wordt voor de ontvanger. (AVG) De ontvanger kan via deze mail veilig een retourbericht versturen.

Privacy met betrekking tot notulen
De volgende richtlijnen zijn van toepassing voor het schrijven en verspreiden van notulen:

- De notulen dienen in neutrale termen beschreven te worden
- Notulen worden digitaal ondergebracht in de daarvoor bestemde mappen indien noodzakelijk alleen verspreid via het beveiligde medewerkersportaal.

Privacy met betrekking tot bewonersbesprekingen
De volgende richtlijnen zijn van toepassing bij een zorgoverleg / MDO

- Bij de bewonersbespreking zijn alleen medewerkers en externe zorgverleners aanwezig die direct met de zorg voor de bewoner te maken hebben
- De resultaten van de bewonersbespreking worden in het beveiligde ECD individueel beschreven en als document opgeslagen onder documenten.

Privacy met betrekking tot het zorgdossier (ONS)

Villa Hooghe Heide werkt met een elektronisch cliënten dossier (ECD) Wij werken met Nedap, een extern beveiligde server. Alleen zorgmedewerkers hebben rechten om met een persoonlijke inlogcode gegevens te verwerken en te lezen. Dit is afhankelijk van functie.

Opgeslagen persoonsgegevens van de bewoner

- Naam , adres en woonplaats
- Telefoonnummer
- Man / vrouw
- Geboortedatum
- Gegevens uit voorafgaande ziekte-en voorgeschiedenis
- Gegevens over actuele hulpbehoeften
- Gegevens over actuele hulpbehoeften
- Gegevens van belang voor de uitvoering en kwaliteit van de hulpverlening
- Verzekeringsgegevens

In overleg met de bewoner en de 1ste contactpersoon (meestal de beheerder van dit portaal) wordt een inlogcode via Carenzorgt aangereikt. (familieportaal) actuele gegevens kunne binnen deze beveiligde omgeving worden gelezen.

De volgende richtlijnen zijn van toepassing bij het gebruik van het zorgdossier van de bewoner

- De informatie uit het zorgdossier is alleen toegankelijk voor direct betrokken zorg- en dienstverleners, bewoner en 1ste contact persoon.
- Er wordt tijdens de dienst gerapporteerd. Na rapporteren/ lezen logt de zorgmedewerker uit zodat er geen derden in het systeem kunnen.
- Wordt een zorgmedewerker met dringende spoed weggeropen dan logt de medewerker uit. Er dient geen geopend scherm aan te staan indien er geen medewerker in de ruimte aanwezig is!
- Zorgmedewerkers kunnen ook buiten werktijden inloggen in het ecd. Het is verboden dit te doen in openbare ruimten. Thuis via de app. is toegestaan mits en geen anderen kunnen meekijken, en direct na lezen wordt er uitgelogd!
- Het zorgdossier wordt gebruikt om de zorg in kaart te brengen, afspraken vast te leggen en over te dragen naar andere betrokkenen bij de zorg. Als de bewoner naar de doelstelling vraagt wordt dit door de medewerker toegelicht
- De bewoner en / of zijn vertegenwoordiger is op de hoogte van de inhoud van het zorgdossier en de reden waarom het wordt bijgehouden
- De rapportage wordt zorgvuldig geformuleerd zonder waardeoordeel
- De rapportage wordt in het ECD automatisch door de medewerker geparafeerd
- Mocht een medewerker/ samenwerkende (para) medici in overleg onder naam van een andere medewerker rapporteren dan de mail of starten/ dan wel afsluiten met de naam van de rapporteur.
- De bewoner heeft het recht zijn dossier in te zien, of dit te laten lezen aan wie hij wil (mits de bewoner aantoonbaar een goed besluit kan nemen (Denk aan wilsbekwaamheid))
- De bewoner heeft het recht op het wijzigen of verwijderen van gegevens uit het zorgdossier. Het gaat om gegevens die niet juist, onvolledig of niet ter zaken doend zijn. Dit kan door een schriftelijk verzoek te sturen naar de directie. Binnen vier weken wordt de bewoner op de hoogte gesteld van de uitkomst hiervan. Bij een weigering moet hiervan de reden worden vermeld. Wanneer wordt ingegaan op het verzoek moet de informatie uit het dossier worden verwijderd.
- De medewerkers die in het dossier schrijven en lezen zijn aan de geheimhoudingsplicht gehouden
- Het is niet toegestaan onderdelen van het dossier te kopiëren (behalve wanneer de bewoner na het afsluiten van de zorg een kopie van het zorgdossier wil hebben)
- Het is niet toegestaan onderdelen uit het dossier van de bewoner te verwijderen zonder vraag van de bewoner en toestemming van de directie
- De bewoner is niet verplicht om informatie te geven. Wanneer de bewoner weigert bepaalde informatie te geven mag deze ook niet aan de vertegenwoordiger worden gevraagd. Uitzondering hierop is alleen als de bewoner de gevolgen van het niet verstrekken van informatie niet kan overzien
- De contactverzorgende/ verpleegkundige is verantwoordelijk voor het up to date houden van het zorgdossier
- Wanneer gegevens, in overleg met de bewoner, worden verstrekt aan derden in belang van de zorgverlening, dan wordt dit in het dossier vastgelegd
- Wanneer het zorgdossier moet worden ingezien door derden vanwege materiele controle dan wordt de bewoner/ 1ste contactpersoon hierover tijdig schriftelijk geïnformeerd en om toestemming gevraagd.
- Wanneer de zorg wordt beëindigd, dan wordt het dossier in het ECD archief volgens de wettelijke daarvoor staande termijn bewaard. Alle losse bestanden worden vernietigd.
- In bepaalde gevallen is het mogelijk dat, op verzoek van de bewoner, het zorgdossier wordt vernietigd. Dit gebeurt alleen als de bewoner hiertoe een schriftelijk verzoek indient bij de directie. De directie zorgt voor een juridisch juiste behandeling van het verzoek en stuurt indien

het dossier vernietigd wordt een aangetekende brief naar de bewoner waarin wordt vermeld dat op verzoek van de bewoner het dossier vernietigd is.
- Het zorgdossier blijft altijd eigendom van Villa Hooghe Heide.

Privacy met betrekking tot digitaal aftekenen van medicatie (N-Care)

- Het digitaal aftekenen van de medicatie is gericht op autorisaties gekoppeld aan functie en/of onder voorwaarden besproken met de directie/ teamleiders.
- Medewerkers dienen geautoriseerd te zijn voor het uitvoeren van handelingen in het digitale medicatie systeem.
- Het is verboden een persoonlijk wachtwoord te delen met een collega. (Ook al is deze geautoriseerd.)
- Het aftekenen van medicatie dient alleen onder eigen naam van de persoon die de verantwoordelijkheid heeft van het geven of toedienen van de medicatie plaats te vinden.
- De medewerker laat zich niet afleiden tijdens het medicatie proces.
- De medewerker zorgt dat het scherm afgeschermd/ dicht geklapt wordt bij afleiding. Laat he scherm nooit geopend achter.
- De medewerker volgt de gebruiksaanwijzingen van NCare en de instructies van de beheerders.
- De medewerker vraagt ondersteuning van een bevoegde collega bij problemen.
- De medewerker **logt** na gebruik van de digitale handelingen **altijd UIT!**

Privacy met betrekking tot medewerker gegevens

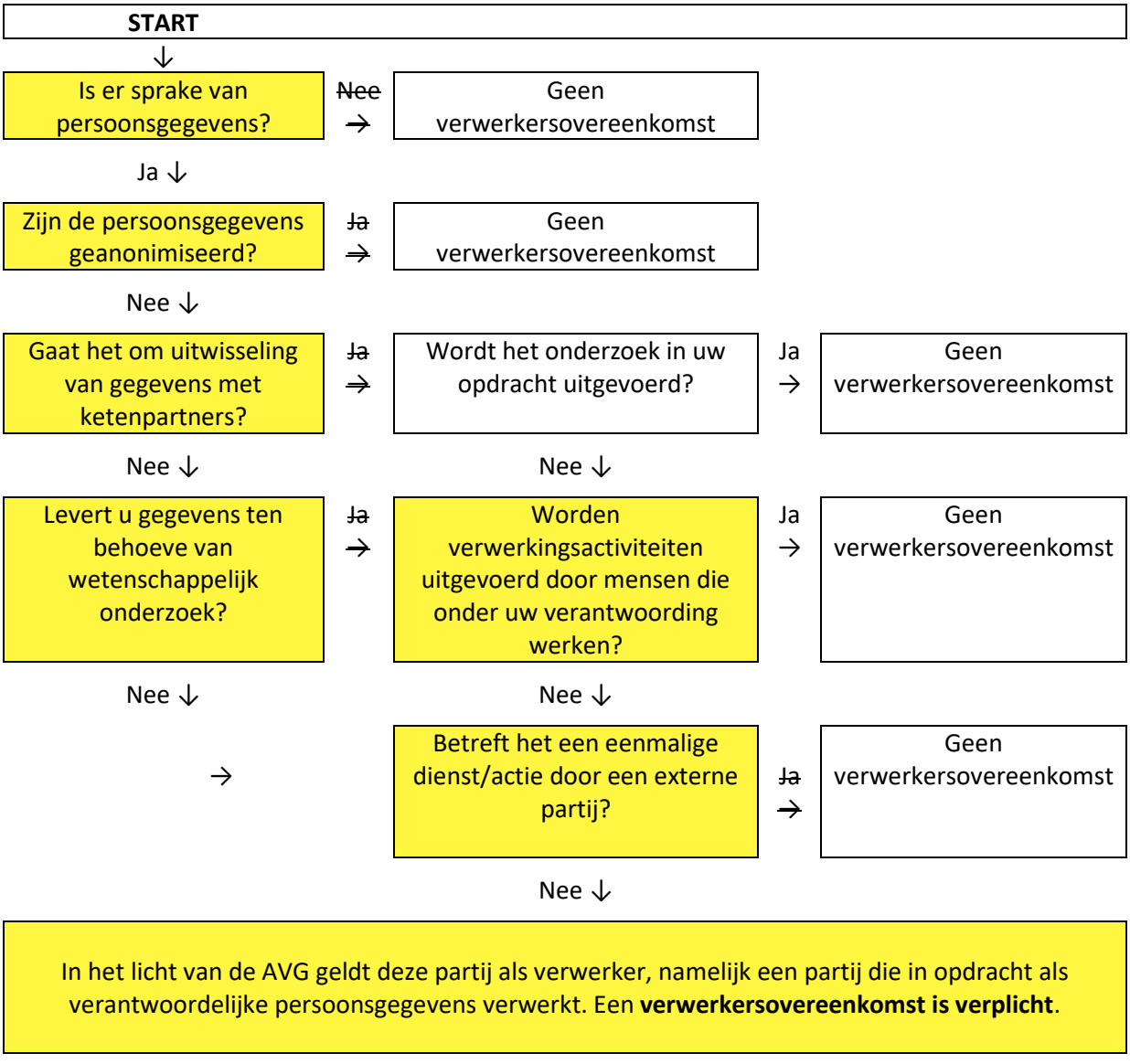
De volgende richtlijnen zijn van toepassing voor het opvragen / gebruiken van gegevens van medewerkers

- Bij indiensttreding wordt een medewerker alleen gevraagd naar relevante informatie
- De medewerker is niet verplicht om informatie te verstrekken over seksuele geaardheid, politieke voorkeur, ras, lidmaatschap van een vakbond, deze vragen worden bij een sollicitatiegesprek niet gesteld
- De gegevens over medewerkers worden bewaard in een afgesloten archiefkast onder beheer van de directie.
- De directie houdt het dossier van de medewerker actueel
- In het medewerker dossier zijn de volgende items opgenomen:
    - Sollicitatiebrief en CV
      naam, adres, telefoonnummer, gender, geboortedatum, e mailadres.
    - Arbeidsovereenkomst met de medewerker
    - VOG
    - Functiebeschrijving
    - Kopie identiteitsbewijs van de medewerker
    - Gegevens mbt salarisadministratie
      Loonbelasting, banknummer,
    - Kopieën van diploma's en certificaten
    - Verslagen van functioneringsgesprekken
    - Ziekmeldingen, verloop ziekteproces en correspondentie hierover
    - Contactgegevens in geval van nood
- Medewerkers hebben recht op inzage in hun personeelsdossier
- De medewerker kan altijd schriftelijk het verzoek doen tot verwijdering uit of correctie van het personeelsdossier. Het gaat om gegevens die niet juist, niet volledig of niet ter zaken doende worden bevonden.

- Het antwoord op dit verzoek dient binnen vier weken schriftelijk gegeven te worden, een weigering dient gemotiveerd te worden.

Verwerkersovereenkomst, beslisboom

Wanneer maak je wel en wanneer maak je geen verwerkersovereenkomst? Onderstaande beslisboom is ontleend aan een publicatie van de LHV en is een handig hulpmiddel.



Persoonsgegevens

Persoonsgegevens zijn gegevens die herleidbaar zijn tot een individu. zoals namen, adressen, telefoonnummers.

Ketenpartners

Ketenpartners, zoals huisarts, SOG, apotheek zijn geen ‘verwerkers’. Zij zijn verwerkingsverantwoordelijk. De ketenpartners zijn in kaart gebracht en de samenwerkingsafspraken zijn vastgelegd.

Onderzoek en analyse

Een partij heeft opdracht gekregen om een analyse uit te voeren op bestanden met persoonsgegevens of om een onderzoek uit te voeren. In dat geval geldt deze partij als verwerker, waarmee een verwerkersovereenkomst wordt afgesloten. Deze partij die is ingehuurd, heeft geen eigen doel heeft met de analyse of het onderzoek. Als onderzoek onder verantwoordelijkheid van deze derde plaatsvindt, dan geldt deze partij niet als verwerker.

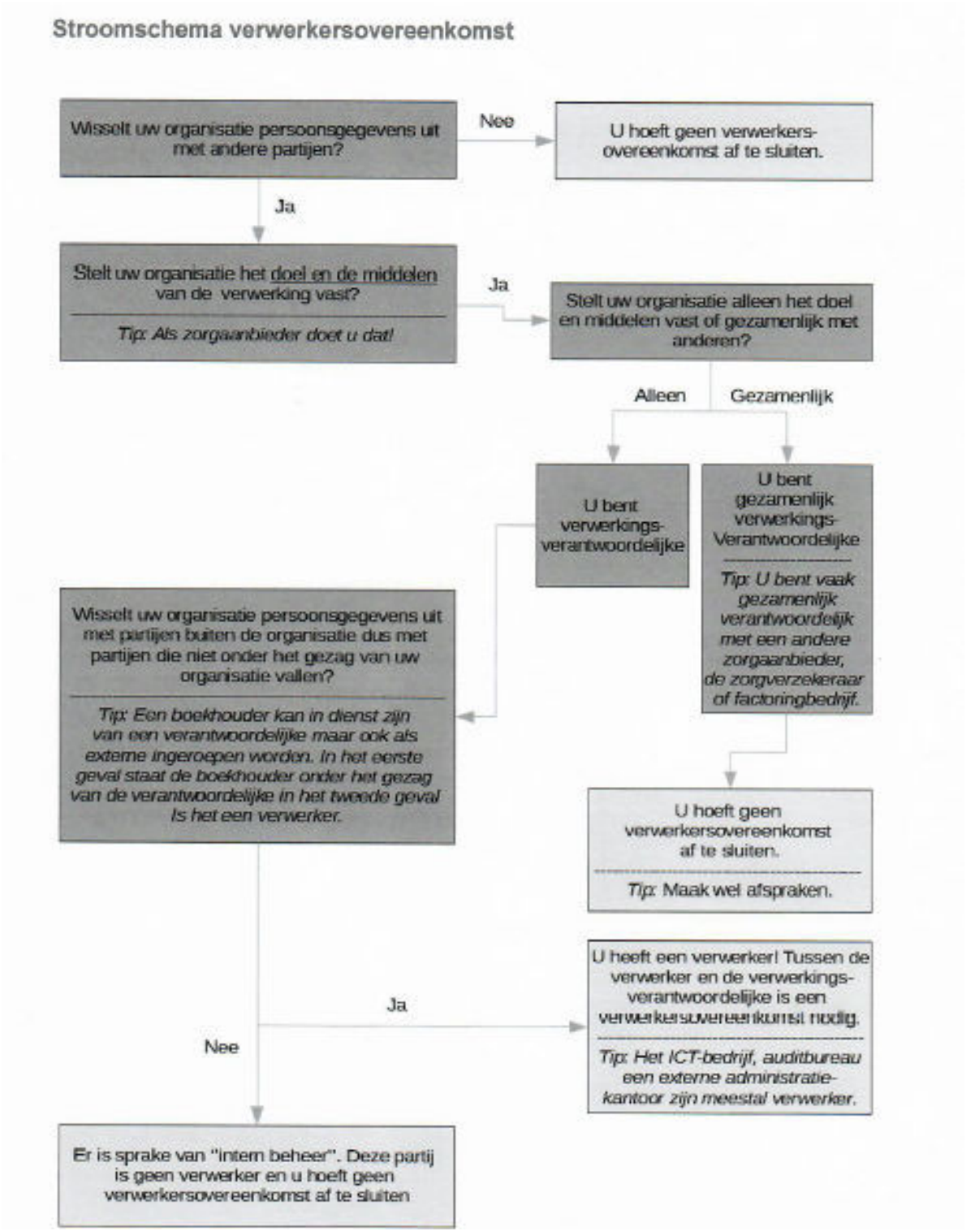
Medewerkers

Medewerkers, al dan niet in vaste dienst zijn geen verwerkers.

Dienstverleners

Een bedrijf dat bestanden met persoonsgegevens kan inzien, geldt als verwerker. Bijvoorbeeld een bedrijf dat de server verhuurt of de software onderhoudt. Met dit bedrijf is een verwerkersovereenkomst afgesloten.

Toelichting[5]



[5] Juridisch bureau Eldermans en Geerts

Datalek

Doel:

- Weten wat een datalek is;
- Een datalek voorkomen;
- Wat te doen bij een datalek.

Verantwoordelijk: Functionaris gegevensbeveiliging.[6]

- Directie: j.luiten@villahoogheheide.nl

Wat is een datalek

Meest voorkomende datalekken

De meest voorkomende datalekken incidenten zijn waarbij persoonsgegevens per ongeluk bij een verkeerde ontvanger terecht komen. Dit kan zijn omdat een brief verkeerd wordt bezorgd, omdat een e-mail naar een verkeerd e-mailadres wordt verstuurd of omdat een klant in een klantportaal de gegevens van iemand anders ziet. Ook verloren USB sticks en verloren of gestolen laptops en telefoons zijn veel voorkomende datalekken. Het gaat dus zeker niet alleen om cybercrime!

Beveiliging van persoonsgegevens hoe deze te organiseren: * zie privacy reglement en privacy reglement - bescherming persoonsgegevens.

De meldplicht datalekken houdt verband met de verplichting om persoonsgegevens adequaat te beveiligen tegen verlies of onrechtmatige verwerking. Deze verplichting houdt niet alleen in dat IT systemen of verbindingen technisch beveiligd zijn, maar ook dat er organisatorische maatregelen zijn genomen binnen de organisatie. Denk aan waarborgen binnen de administratieve processen, zoals autorisaties en logging, bewustwording bij medewerkers en afspraken over de omgang met bijzondere persoonsgegevens, zoals medische gegevens of Burger Service Nummers.

- Bij het per ongeluk vrijkomen van privacy gevoelige informatie dient dit per omgaande gemeld te worden aan de leidinggevende.

De leiding gevende beoordeeld het datalek en maakt een rapportage op het daarvoor beschikbare Excel datalekregister.

- [6] Vanaf 1 januari 2016 bestaat de verplichting voor alle organisaties om datalekken aan de Autoriteit Persoonsgegevens te melden.

Maatregelen Autoriteit Persoonsgegevens

Een melding van een datalek is vertrouwelijk en de Autoriteit Persoonsgegevens doet daar geen uitspraken over. Als de Autoriteit Persoonsgegevens een melding van een datalek ontvangt kan zij de volgende acties ondernemen:

- contact opnemen om de informatie in een melding te verifiëren of aan te vullen;
- de organisatie verplichten om betrokkenen, degene op wie de persoonsgegevens betrekking hebben, te informeren;
- voorlichting geven en organisaties wijzen op beveiligingsrisico's;
- een onderzoek instellen; of
- overgaan tot handhaving.

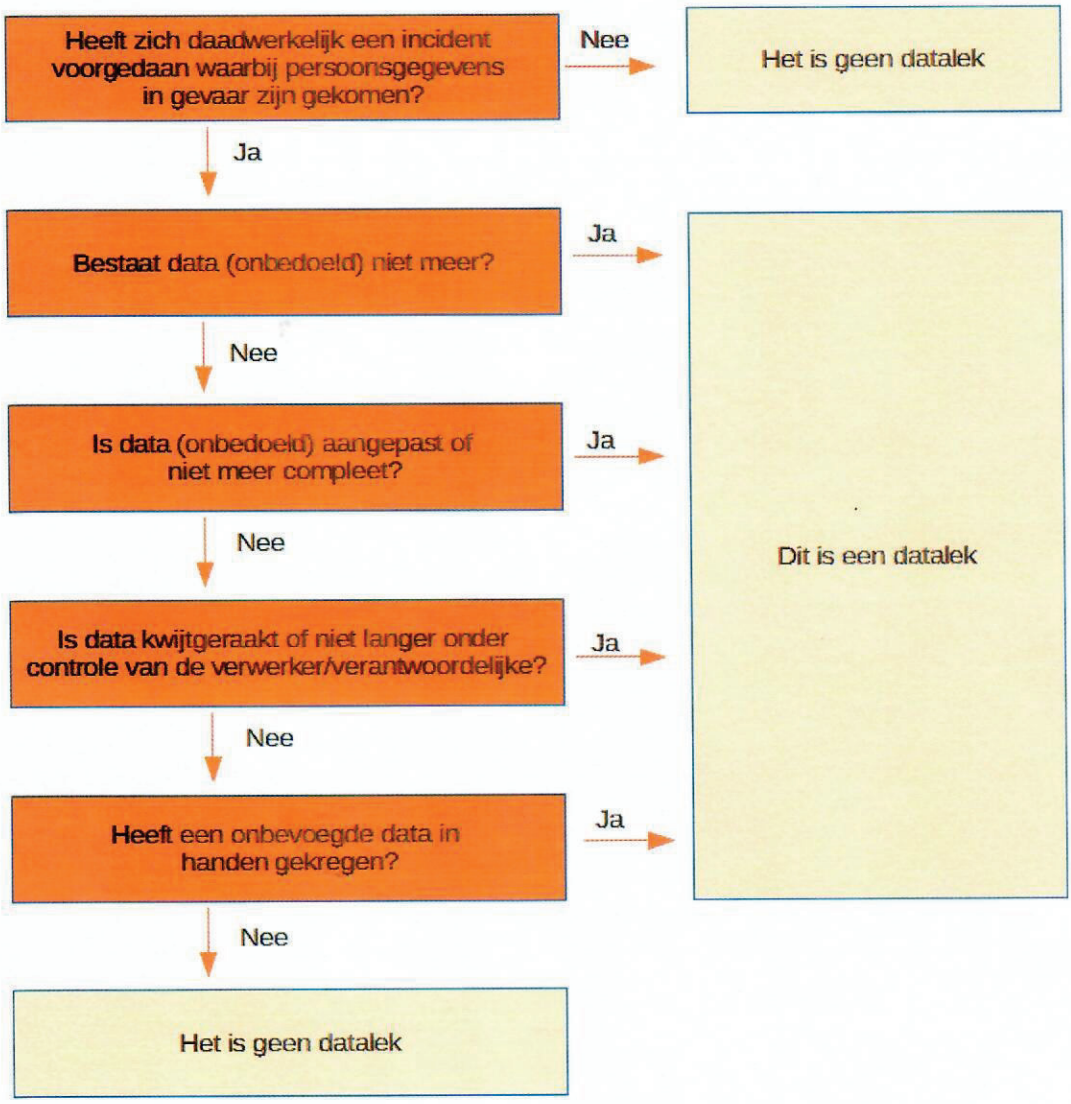
Actie nodig: De Autoriteit Persoonsgegevens kan ook handhavend optreden. Naast een last onder dwangsom kan zij sinds 1 januari 2016 ook boetes opleggen oplopend tot € 820.000 of zelfs 10% van de jaaromzet. Die boete kan ook worden opgelegd aan de bestuurder. Wilt u weten of binnen uw organisatie de beveiliging van persoonsgegevens in orde is of dat uw procedure voor de meldplicht datalekken voldoet aan de eisen van de Autoriteit Persoonsgegevens?

Functionaris Gegevensbescherming: In de AVG worden de volgende taken genoemd voor een FG van een organisatie:

- De betrokken partijen binnen een organisatie informeren en adviseren wat de verplichtingen zijn op het gebied van privacy.
    - Het geven van advies over en ondersteuning bij het uitvoeren van een PIA (Privacy Impact Assessment) is een belangrijk voorbeeld hiervan, dat specifiek in de AVG wordt genoemd.
    - Ook het verzorgen van interne trainingen, opleidingen of voorlichtingsmateriaal valt hieronder.
- Toezien op:
    - de naleving van de AVG en andere wetgeving op het gebied van privacy.
    - het interne beleid van de organisatie.
- De FG is geen toezichthouder met corrigerende bevoegdheden. Het gaat meer om het controleren, meekijken, rapporteren en bespreken van zaken die niet goed gaan bij de eindverantwoordelijken. De verwerkingsverantwoordelijke blijft eindverantwoordelijk als er niet volgens de privacywet wordt gehandeld, de FG is niet persoonlijk verantwoordelijk of aansprakelijk.
- Samenwerken met de toezichthoudende Autoriteit (de Autoriteit Persoonsgegevens in Nederland). De FG is het eerste aanspreekpunt voor de AP. Omgekeerd mag de FG ook het AP (gratis) raadplegen om informatie te krijgen over rechtmatige verwerkingen. De Functionaris Gegevensbescherming dient bij het uitvoeren van zijn taken rekening te houden met de risico's die verbonden zijn aan de verwerkingen, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden.

- Raadpleeg middels het stroomschema om vast te stellen of er sprake is van een datalek en wat te doen. **Zie bijlagen**

Stroomschema datalek



Stroomschema melden datalek bij de AP en de betrokkene(n)