Beleid
Verwerking persoonsgegevens

Auteur: Lars Schiltmans

Datum: 24 juni 2016

Status: Definitief

Inhoudsopgave

1 Inleiding

Opslag en verwerking van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van Vivantes. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan cliënten, medewerkers en andere betrokkenen bij Vivantes, maar ook aan Vivantes zelf. Denk hierbij bijvoorbeeld aan identiteitsfraude.

Vivantes hecht veel waarde aan het beschermen van de persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van persoonsgegevens is de eindverantwoordelijkheid van de Raad van Bestuur van Vivantes dit begint echter bij het nemen van verantwoordelijkheid door iedereen die met deze soort gegevens te maken heeft bij de uitvoering van aan hun toebedeelde werkzaamheden.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt Vivantes haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en meent daarmee ook te voldoen aan de relevante privacywet- en regelgeving.

2 Definities

Term	Definitie
Beleid	Dit beleid met betrekking tot het verwerken van persoonsgegevens door Vivantes.
Betrokkene	Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.
Verantwoordelijke	De Raad van Bestuur van Vivantes die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Bewerker	Een door Vivantes ingeschakelde (derde) partij die ten behoeve van Vivantes persoonsgegevens verwerkt.
Persoonsgegeven	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.
Verwerking	Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens.
Derde	Ieder ander, niet zijnde de betrokkene, de verantwoordelijke of de bewerker, of enig persoon die onder rechtstreeks gezag valt van de verantwoordelijke of de bewerker en gemachtigd is om persoonsgegevens te verwerken.
Data-lek	Persoonsgegevens die in handen vallen van derden die geen toegang tot die gegevens (mogen) hebben.
Privacy Impact Assessment	Een tool dat helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

3 Reikwijdte en doelstellingen van het beleid

3.1 Reikwijdte van het beleid

Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Vivantes waaronder in ieder geval alle cliënten, medewerkers, gasten, bezoekers en externe relaties (o.b.v. inhuur en/of outsourcing), alsmede op andere betrokkenen waarvan Vivantes persoonsgegevens verwerkt.

In het beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde / systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Vivantes alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het beschermen van persoonsgegevens wordt breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.

Dit beleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van persoonsgegevens van betrokkene. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn.

3.2 Doelstellingen van het beleid

1. Het bieden van een kader: het beleid biedt een kader om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgestelde norm én om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen;
2. Het stellen van normen: de basis voor de beveiliging van persoonsgegevens is ISO 27001. Maatregelen worden daarnaast op basis van de kaders van de NEN7510 vormgegeven, dit is beschreven in de toolkit NEN7510;
3. Het nemen van de verantwoordelijkheid: door de vastgestelde uitgangspunten en de organisatie van het verwerken van persoonsgegevens vast te leggen voor iedere betrokkene;
4. Daadkrachtige implementatie van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen;
5. Compliant zijn met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van persoonsgegevens, mede ter vermijding van risico’s als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

4 Beleidsprincipes verwerking persoonsgegevens

4.1 Beleidsuitgangspunt en -principes

Algemeen beleidsuitgangspunt is dat de verwerking van persoonsgegevens in overeenstemming met de relevante wet- en regelgeving plaats vindt.

Om aan bovenstaand beleidsuitgangspunt te voldoen gelden de volgende principes:

- Een verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 8 van de Wet bescherming persoonsgegevens (Wbp);
- Persoonsgegevens worden alleen verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd;
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn;
- verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doel;
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn;
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen;
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen;
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen;
- Iedere betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van de in de afzonderlijke verwerkingen hem betreffende persoonsgegevens, en heeft het recht van verzet;
- Bij alle registraties op vrijwillige basis zal aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

5 Wet- en regelgeving

De verschillende wetten binnen de gezondheidszorg waar Vivantes mee te maken heeft en in aanraking komt, kun je grofweg onderscheiden in:

1. Wetgeving met betrekking tot de kwaliteit van de gezondheidszorg. Voorbeelden zijn:
   - Wet op de geneeskundige behandelovereenkomst (WGBO);
   - Wet op de beroepen in de individuele gezondheidszorg (BIG) inclusief Tuchtrecht;
   - Kwaliteitswet zorginstellingen (KZI);
   - Wet klachtrecht cliënten zorgsector (WKCZ);
   - Wet medezeggenschap cliënten zorgsector (WMCZ);
   - Wet Bijzondere Opnemingen Psychiatrische Ziekenhuizen (BOPZ).
2. Wetgeving met betrekking tot de financiering, planning en organisatie van de gezondheidszorg. Voorbeelden zijn:
   - Wet toelating zorginstellingen (WTZ);
   - Wet Marktordening Gezondheidszorg (WMG);
   - Wet Langdurige Zorg (WLZ);
   - Wet maatschappelijke ondersteuning (WMO);
   - Zorgverzekeringswet (Zvw);
   - Wet op de medische hulpmiddelen;
   - Gezondheidswet.
3. Overige wetgeving waar we in de zorg mee te maken hebben. Voorbeelden zijn:
   - Wet bescherming persoonsgegevens;
   - Wet gebruik burgerservicenummer in de zorg;
   - Wet gelijke behandeling op grond van handicap of chronische ziekte.

Bij Vivantes conformeert zich in haar bedrijfsvoering onverkort aan de bepalingen in de voor haar relevante wet- en regelgeving. Bijzondere aandacht gaat hierbij uit naar de onderstaande wetten:

A. Kwaliteitswet zorginstellingen. Vivantes heeft een kwaliteitszorgsysteem, waarin onder meer het zorgvuldig omgaan met gegevens van cliënten in meest brede zin in het (cliënt)registratieve proces is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (niet-) zorgpersoneel nageleefd en toegepast.
B. Wet bescherming persoonsgegevens. Vivantes heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van persoonsgegevens en nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking van data c.q. persoonsgegevens) geïmplementeerd door middel van dit beleid.
C. Archiefwet. Vivantes houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

6 Rollen en verantwoordelijkheden met betrekking tot verwerking persoonsgegevens

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken wordt een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

I. Raad van Bestuur. Is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens en stelt het beleid, de maatregelen en de procedures op het gebied van verwerking vast.
II. Portefeuillehouder beveiliging persoonsgegevens. Is degene die privacy in portefeuille heeft. Hij/zij is eindverantwoordelijk voor beveiliging van persoonsgegevens.
III. Functionaris gegevensbescherming. Vivantes heeft de mogelijkheid zelf een interne toezichthouder op de verwerking van persoonsgegevens aan te stellen. Deze toezichthouder wordt functionaris voor de gegevensbescherming (FG) genoemd. De FG houdt toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie. Bij het in werking treden van de Algemene Verordening Gegevensbescherming is de benoeming van een Functionaris voor de Gegevensbescherming (FG) verplicht.
IV. Systeemeigenaar. Is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het beleid. Dit betekent dat de systeemeigenaar er voor zorgt dat zowel nu, als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.
V. Leidinggevenden. Het creëren van bewustwording en de naleving van het beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:
    a. er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beleid;
    b. toe te zien op de naleving van het beleid door zijn medewerkers;
    c. periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

7 Implementatie beleid

De Raad van Bestuur is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt. Zij wordt aangemerkt als de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van Vivantes uitgevoerd. Het goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van Vivantes. Een goed corporate governance-beleid draagt zorg voor de rechten van alle betrokkenen.

7.1 Verdeling van de verantwoordelijkheden

Het zorgvuldig verwerken van persoonsgegevens dient gezien te worden als een lijnverantwoordelijkheid: dat betekent dat de lijnmanagers (afdelingshoofden/centrale stafdiensten) de primaire verantwoordelijk dragen voor een zorgvuldige verwerking van persoonsgegevens op hun afdeling/eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen.

Het zorgvuldig omgaan met persoonsgegevens is ieders verantwoordelijkheid. Er wordt van medewerkers en studenten verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van Vivantes of van individuen. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.

7.2 Inpassing in de instellingsgovernance / Afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt ingevuld in het DT.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld in het MT.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Het operationeel niveau wordt ingevuld in het locatie-overleg.

7.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn voortdurend aan te scherpen, zodat kennis van risico’s wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van de Functionaris voor de Gegevensbescherming | de Security Officer.

7.4 Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De Functionaris voor de gegevensbescherming initieert gezamenlijk met de Information Security Officer en de interne auditor de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekort schieten, dan kan Vivantes de betrokken verantwoordelijke medewerkers een sanctie op te leggen, binnen de kaders van de cao en de wettelijke mogelijkheden.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten Vivantes maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

8 Rechtmatige en zorgvuldige verwerking van persoonsgegevens

8.1 Grondslag, doelbinding en belangenafweging

Het Verwerken van persoonsgegevens moet gebaseerd zijn op een van de wettelijke gronden zoals beschreven in artikel 8 van de Wet bescherming persoonsgegevens. De verantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Vivantes treft de nodige maatregelen om te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

Bij projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren. Vivantes hanteert bij de implementatie het principe van “Privacy by Design”. Dit betekent dat er bij het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, stelselmatig aandacht wordt besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

8.2 Melden en documenteren van verwerkingen

De verwerking van persoonsgegevens wordt door Vivantes gemeld in de openbare registers van het Autoriteit Persoonsgegevens. Verwerkingen die onder het bereik van het zogenaamde Vrijstellingsbesluit vallen zijn, mits voldaan is aan alle vereisten van het Vrijstellingsbesluit, uitgezonderd van de meldingsplicht.]

De verwerkingen worden voldoende gedocumenteerd en gepubliceerd op voor de betrokkenen toegankelijke media met vermelding van het doel van de registratieregistraties en de verantwoordelijken.

8.3 De organisatie van de beveiliging

Vivantes draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem.

8.4 Geheimhouding

Bij Vivantes worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

8.5 Bewaartermijnen/ vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor ze zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie gebracht te worden. Vivantes zal de persoonsgegevens

na het verlopen van de bewaartermijn vernietigen of, indien de persoonsgegevens bestemd zijn voor historische of statistische doeleinden, in een archief bewaren.

8.6 Bijzondere persoonsgegevens

Het verwerken van Bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder Bijzondere persoonsgegevens vallen gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke gegevens.

8.7 Doorgifte persoonsgegevens aan derden

8.7.1 Uitbesteden van verwerking aan een bewerker

Indien Vivantes persoonsgegevens laat verwerken door een bewerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen Vivantes als verantwoordelijke en de bewerker.

8.7.2 Doorgifte persoonsgegevens binnen de Europese Unie

Vivantes verstrekt persoonsgegevens alleen aan derden, als deze doorgifte is gebaseerd op een wettelijke grondslag (de Wbp principiële gronden voor gegevensverwerking, artikel 8).

Met betrekking tot Bijzondere persoonsgegevens worden deze niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

8.7.3 Doorgifte persoonsgegevens buiten de Europese Unie (inclusief de EEA)

Vivantes verstrekt persoonsgegevens alleen aan derden die zich bevinden in een land buiten de Europese Unie indien dat land in zijn geheel of dat bedrijf/die instelling specifiek een passend beschermingsniveau waarborgt. Als passend beschermingsniveau hanteert Vivantes:

- De algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie;
- Safe harbor principles voor bedrijven in de Verenigde Staten, gepubliceerd door de Europese Commissie i.s.m. de US Department of Commerce.

Vivantes verstrekt persoonsgegevens alleen aan landen zonder passend beschermingsniveau, waar zij een vergunning van de Minister van Veiligheid & Justitie heeft verkregen, dan wel o.b.v. een modelcontract (als opgesteld door de Europese Commissie) een contract is aangegaan. In beide gevallen voorziet Vivantes het CBP van een melding van doorgifte naar een land buiten de EU.

(Niet limitatieve) lijst van derden aan wie Vivantes persoonsgegevens doorgeeft:

- Novicare
- Managementinstituut Nederland
- Synthra

9 Incidenten met betrekking tot persoonsgegevens

Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen Vivantes is een incident. De bekendste vorm van zo'n incident is een data-lek. Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

9.1 Melding en registratie

Incidenten moeten gemeld worden bij in Ultimo [type melding: incident persoonsgegevens]. Van elk incident en de afhandeling daarvan zal een registratie bijgehouden worden.

Een incident kan gemeld worden door een betrokkene, een bewerker of een derde.

9.2 Afhandeling

Incidenten worden zo veel mogelijk doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures afgehandeld.

Als de persoonsgegevens van betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van Vivantes ernstig in gevaar zijn, wordt in ieder geval de Raad van Bestuur en indien aanwezig ook de Functionaris Gegevensbescherming op de hoogte gesteld.

Indien sprake is van ernstige data-lekken worden deze conform de in de relevante wet- en regelgeving opgenomen specifieke bepalingen over data-lekken afgehandeld.

9.3 Evaluatie

Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage over incidenten met betrekking tot persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van de Raad van Bestuur en, indien aanwezig, die van de Functionaris Gegevensbescherming .

9.4 Bijzondere omstandigheden / Calamiteiten

Om voorbereid te zijn op (de dreiging tot) incidenten op het gebied van persoonsgegevens in bijzondere omstandigheden heeft Vivantes een Privacy Incident Response Team ingesteld.

Dit team heeft als voornaamste taak om te acteren bij incidenten met persoonsgegevens in die gevallen waarbij de staande organisatie een incident niet via de standaard procedures kan oplossen. Dit kan zijn omdat het incident plaatsvindt buiten de reguliere openingstijden, in een periode waarbij de reguliere bedrijfsprocessen verstoord zijn of omdat de aard van het incident vraagt om noodmaatregelen en/of specifieke mandaten om deze maatregelen uit te voeren.

Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben spreken we van een data-lek.

Het PIRT-team werkt volgens een door de Raad van bestuur vastgestelde procedure en heeft bijzondere mandaten die overeenkomen met de mandaten van de Functionaris Gegevensbescherming , indien benoemd, waarbij het team altijd achteraf verantwoording moet afleggen waarom en op welke wijze het team van deze mandaten gebruik heeft gemaakt.

Het team heeft een directe link naar de Raad van Bestuur als verantwoordelijke in het kader van de relevante wet- en regelgeving.

10 Rechten van betrokkenen

10.1 Informatieplicht

10.1.1 Algemene mededeling

Vivantes beoogt de verwerking van persoonsgegevens van cliënten, medewerkers en andere betrokkenen door middel van algemene kennisgeving in dit Beleid verwerking persoonsgegevens mede te delen. Daarnaast beoogt Vivantes in overeenstemming met de wet, alle betrokkenen onder bepaalde omstandigheden rechten te verschaffen waarmee zij de aan hen toebehorende persoonsgegevens naar behoren kunnen beschermen.

Vivantes verstrekt de betrokkene tenminste het volgende:

- De identiteit en contactgegevens van de voor verwerking verantwoordelijke en, in voorkomend geval, de Functionaris Gegevensbescherming;
- De specifieke doeleinden van verwerking waarvoor de persoonsgegevens zijn bestemd alsook informatie betreffende de beveiliging van verwerking;
- De periode gedurende welke de persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen;
- Het bestaan van het recht om van de verantwoordelijke toegang tot en rectificatie of wissen van persoonsgegevens betreffende de betrokkene te verlangen;
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens.

10.2 Mededeling van aanpassingen

Indien het beleid ingrijpend wordt aangepast dan wel verandert, deelt Vivantes deze algemeen mede, om zorgvuldige en behoorlijke verwerking te waarborgen.

10.3 Recht op inzage

10.3.1Verzoek tot inzage

Iedere betrokkene heeft recht op inzage in hem betreffende verwerkte persoonsgegevens. Een verzoek hiertoe kan schriftelijk worden ingediend bij Vivantes.

Een verzoek tot inzage van minderjarigen die de leeftijd van 16 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger.

10.3.2 Termijn

Op het verzoek wordt zo spoedig mogelijk, doch uiterlijk binnen twee weken na indiening schriftelijk gereageerd. Vivantes draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.

10.3.3 Mededeling

Indien gegevens worden verwerkt, bevat de mededeling van Vivantes een volledig overzicht daarvan in begrijpelijke vorm, een omschrijving van de doeleinden van de verwerking, de categorieën van gegevens waarop verwerking betrekking heeft en de categorieën van ontvangers, alsmede beschikbare informatie over herkomst van de gegevens en de termijn van bewaring van gegevens.

10.3.4 Kosten

Iedere aanvraag kan kosteloos worden ingediend.

10.4 Recht op verbetering, aanvulling, verwijdering of afscherming

10.4.1 Verzoek tot verbetering, aanvulling verwijdering of afscherming

Iedere betrokkene kan met betrekking tot over hem opgenomen persoonsgegevens bij Vivantes van deze gegevens verzoeken die te wijzigen, verbeteren, aan te vullen, te verwijderen of af te schermen.

Een verzoek tot verbetering, aanvulling, verwijdering of afscherming van minderjarigen die de leeftijd van 16 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger.

10.4.2 Termijn

Vivantes deelt binnen twee weken na ontvangst van het verzoek schriftelijk aan de betrokkene mede of zijn verzoek gegrond is.

10.5 Kennisgeving

Indien opgenomen persoonsgegevens van de betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, verbetert de gegevensbeheerder (dat kan zowel de functioneel beheerder als de verwerker zijn) deze gegevens.

Bovendien worden derden aan wie de gegevens, voorafgaand aan de correctie, zijn verstrekt hiervan in kennis gesteld. De verzoeker mag opgave verzoeken van degene aan wie Vivantes deze mededeling heeft gedaan.

10.5.1 Termijn voor uitvoering

De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

10.6 Recht van verzet

10.6.1 Gronden voor verzet

In verband met zijn of haar persoonlijke omstandigheden, mag iedere betrokkene verzet aantekenen tegen verwerking bij Vivantes, als deze verwerking plaatsvond op grond van:

a) de vervulling van een publiekrechtelijke taak van de gegevensbeheerder;

b) de behartiging van het gerechtvaardigd belang van Vivantes of van een derde aan wie de gegevens worden verstrekt.

10.6.2 Termijn

Vivantes beoordeelt binnen twee weken na ontvangst van het verzet of deze gerechtvaardigd is. Indien het verzet gerechtvaardigd is, treft Vivantes maatregelen die nodig zijn om de verwerking de beëindigen.

10.6.3 Kosten

De kosten die Vivantes hiervoor berekent, bedragen nihil.

10.7 Rechtsbescherming

10.7.1 Algemene klachten

Indien de betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit reglement jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij Vivantes.

10.7.2 Bezwaarmogelijkheden na indienen algemene klacht

Indien het antwoord van Vivantes voor de betrokkene niet leidt tot een voor hem acceptabel resultaat, heeft de betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

10.7.3 Bezwaarmogelijkheden na afwijzing van een verzoekschrift tot inzage

Indien Vivantes afwijzend heeft beslist op een verzoek tot inzage in of verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens, of Vivantes heeft het verzoek van de betrokkene afgewezen, heeft de betrokkene de mogelijkheid een verzoekschriftprocedure te starten bij de kantonrechter.

10.7.4 Termijn indienen bezwaar

Het bezwaarschrift wordt binnen zes weken na ontvangst van het antwoord van Vivantes ingediend bij de kantonrechter. Indien Vivantes niet binnen de gestelde termijn heeft geantwoord, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend.

Tot slot

Dit beleid is vastgesteld door de Raad van Bestuur van Vivantes d.d. 1 november 2016.

Een review van het beleid maakt onderdeel uit van de plan-do-check-act cyclus van Vivantes. Daarin is ook een controle op de effectiviteit van de maatregelen opgenomen.

Aanpassingen van dit beleid worden gepubliceerd in MMS.