Zijn we er klaar voor?

De verwerking van persoonsgegevens van cliënten getoetst aan de Wbp en de AVG

Surplus Welzijn

Jasper van Gorp

29 mei 2017, ‘s-Hertogenbosch

Zijn we er klaar voor?

De verwerking van persoonsgegevens van cliënten getoetst aan de Wbp en de AVG

Auteur:	Jasper van Gorp
Studentnummer:	2064596
Opleiding:	HBO-Rechten
Onderwijsinstelling:	Juridische Hogeschool Avans-Fontys, te ’s-Hertogenbosch
Afstudeerorganisatie:	Surplus Welzijn, te Etten-Leur
Stagementor:	Mr. W.C.J. van de Kar
Eerste docent:	Mr. M.M.J. van den Haspel
Tweede docent:	Mr. B.C.M. Hooijdonk
Afstudeerperiode:	Februari 2017 – mei 2017

Voorwoord

Voor u ligt mijn onderzoeksrapport dat geschreven is in het kader van het afsluiten van mijn studie HBO-Rechten aan de Juridische Hogeschool Avans-Fontys te ’s-Hertogenbosch. Van februari tot en met mei 2017 heb ik gewerkt aan dit onderzoek. Het onderzoek was een uitdaging. Binnen de organisatie Surplus Welzijn was het regelmatig zoeken om de juiste persoon te vinden die mijn vragen kon beantwoorden. Mijn stagementor Wilma van de Kar heeft mij daar enorm bij geholpen. Ik wil haar daarom ook bedanken voor haar hulp en feedback gedurende dit onderzoek. Daarnaast wil ik Maria van den Haspel van de Juridische Hogeschool Avans-Fontys bedanken voor haar begeleiding gedurende het afstuderen en de feedback op mijn ingeleverde stukken. Ook wil ik de medewerkers van Surplus Welzijn en Surplus bedanken voor de medewerking. Zonder hen was dit onderzoek niet tot stand gekomen.

Tot slot wil ik de organisatie bedanken dat ze mij de kans heeft geboden dit onderzoek te kunnen doen. Ik ben hen erg dankbaar voor deze aangename en leerzame periode.

Ik wens u veel plezier bij het lezen van mijn onderzoeksrapport.

Jasper van Gorp
’s-Hertogenbosch, 29 mei 2017

Inhoud

Samenvatting

Surplus Welzijn is een organisatie die het welzijn van mensen stimuleert en bijdraagt aan een leefbare omgeving. De organisatie heeft veel verschillende afdelingen. Dit onderzoek richt zich op de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening van de locatie Etten-Leur. Doordat bij deze afdeling sprake is van het verwerken van persoonsgegevens is de Wet bescherming persoonsgegevens van toepassing. Vanaf 25 mei 2018 is er een nieuw wettelijk kader voor het verwerken van persoonsgegevens binnen de gehele Europese Unie. Op die datum is de Algemene verordening gegevensbescherming van toepassing.

In dit onderzoeksrapport staat vermeld welke eisen de wettelijke eisen het huidige en toekomstig wettelijk kader stelt aan de verwerking van persoonsgegevens van cliënten door Surplus Welzijn. Daarnaast is ook vermeld wat het huidige beleid van de organisatie is en hoe in de praktijk wordt omgegaan met het verwerken van persoonsgegevens. Uiteindelijk zijn de bevindingen getoetst aan de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming.

Uit het onderzoek is gebleken dat er verschillende bepalingen uit de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming worden overtreden door Surplus Welzijn. De organisatie heeft bijvoorbeeld geen beleid hoe zij om gaat met een datalek. Ook heeft men geen bewerkingsovereenkomst met de bewerker van de persoonsgegevens afgesloten. Door Surplus Welzijn zijn geen instructies opgesteld hoe de medewerkers om dienen te gaan met de verwerking van persoonsgegevens van hun cliënten. Hierdoor is het veelvuldig voorgekomen dat er te veel persoonsgegevens door de medewerkers worden geregistreerd.

Door de inwerkingtreding van de Algemene verordening gegevensbescherming in 2018 gaan er nieuwe verplichtingen voor de organisatie bij komen. De verwerkingsverantwoordelijke moet er voortaan voor zorgen dat wordt voldaan aan de documentatieplicht. De organisatie moet aan kunnen tonen dat zij voldoet aan de Algemene verordening gegevensbescherming. Daarnaast is de organisatie verplicht om een privacy impact assessment uit te voeren zodat privacyrisico's kunnen worden blootgelegd. Dit draagt ook bij aan het vermijden en verminderen van privacyrisico's. De cliënten van Surplus Welzijn krijgen ook enkele nieuwe rechten. Zij hebben voortaan het recht op de beperking van de verwerking, recht op gegevensoverdraagbaarheid en het recht op de vergetelheid.

In dit onderzoek worden verschillende aanbevelingen aangedragen die ervoor kunnen zorgen dat de organisatie in de toekomst aan de wettelijke eisen voor de verwerking van persoonsgegevens voldoet. De belangrijkste aanbeveling is het updaten van het Privacyreglement dat de organisatie 'heeft'. Dit is opgesteld in 2011 en nooit officieel vastgesteld. Andere belangrijke aanbevelingen die voortvloeien uit dit onderzoek zijn: het opstellen en afsluiten van een bewerkingsovereenkomst met softwareleverancier Regas, beleid opstellen hoe de medewerkers en de organisatie moeten omgaan met een datalek en medewerkers bewustwording geven van de risico's die de verwerking van persoonsgegevens met zich mee brengen.

Voor de organisatie is het van belang om de aanbevelingen op te volgen. Men kan namelijk een boete krijgen van de Autoriteit Persoonsgegevens als men het huidige beleid voortzet en daardoor bepalingen uit de Wet bescherming Persoonsgegevens en/of de Algemene verordening gegevensbescherming overtreden.

Afkortingen

AVG	Algemene verordening gegevensbescherming
Bestuurder	Lid van de Raad van Bestuur
Boetebeleidsregels	Boetebeleidsregels Autoriteit Persoonsgegevens 2016
FG	Functionaris voor de gegevensbescherming
ICT-Beveiligingsrichtlijnen	ICT-Beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie
Medewerkers	Beroepskrachten, vrijwilligers en eventueel stagiaires van Surplus Welzijn
PIA	Privacy impact assessment
Privacyreglement	Privacyreglement van Surplus Welzijn
Surplus Welzijn	De afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening in Etten-Leur
Wbp	Wet bescherming persoonsgegevens
Wpr	Wet persoonsregistratie

Hoofdstuk 1 Inleiding

§ 1.1 Beschrijving organisatie

Surplus is een organisatie voor comfort, welzijn, wonen en zorg. De organisatie heeft verschillende dochterstichtingen in West- en Midden-Brabant. Een van deze dochterstichtingen is Surplus Welzijn.[1] Surplus Welzijn is gevestigd in zeven gemeentes en bestaat uit verschillende afdelingen. De organisatie bevordert het welzijn van mensen en draagt bij aan een leefbare maatschappij.[2]

Het uitgevoerde onderzoek heeft betrekking op de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening van de locatie Etten-Leur. Deze afdelingen zullen in het onderzoek vermeld worden als Surplus Welzijn.

§ 1.2 Probleembeschrijving

De beroepskrachten, vrijwilligers en stagiairs van Surplus Welzijn (hierna: medewerkers) helpen mensen met verschillende problemen. In het computersysteem Regas worden de contactgegevens van de cliënt opgeslagen. Daarnaast wordt bij elk bezoek van de cliënt vermeld wat er is gedaan om het probleem van de cliënt op te lossen. Door het registreren van de persoonsgegevens houdt Surplus Welzijn zich bezig met het verwerken van persoonsgegevens. De cliënten worden door de afdelingen doorverwezen als het probleem beter opgelost kan worden door een andere afdeling. De afdelingen delen onderling ook informatie over cliënten.

Doordat Surplus Welzijn bezig is met het verwerken van persoonsgegevens is de Wet bescherming persoonsgegevens (hierna: Wbp) van toepassing. De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG)[3].[4] Op 1 september 2001 is die wet in werking getreden. Organisaties die persoonsgegevens verwerken worden verplicht passende beveiligings- en beheersmaatregelen te nemen. Zo mogen persoonsgegevens – kort gezegd – worden verzameld en verwerkt, als daarvoor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen zijn vastgesteld. De betrokkenen moeten door de organisaties op de hoogte worden gesteld wat zij gaan doen met de persoonsgegevens.[5]

Sinds 1 januari 2016 is de Wbp uitgebreid met de Wet meldplicht datalekken en de uitbreiding boetebevoegdheid Cbp. De meldplicht datalekken houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens[6] zodra zij een ernstig datalek hebben.[7] De verantwoordelijke moet de betrokkene op de hoogte stellen van het datalek. Dit is alleen van toepassing als de inbreuk waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene.[8]

In het verleden had de Autoriteit Persoonsgegevens een zeer beperkte mogelijkheid om boetes op te leggen. Door de inwerkingtreding van de Wet meldplicht datalekken en de uitbreiding boetebevoegdheid Cbp heeft de Autoriteit Persoonsgegevens nu de bevoegdheid

---

[1] www.surplus.nl.
[2] Surplus 2015, p. 4.
[3] Richtlijn 95/46/EG van het Europees Parlement en de raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
[4] www.autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten (klik op: *Wet bescherming persoonsgegevens*).
[5] www.duthler.nl/nl (zoek op: *Wet bescherming persoonsgegevens*).
[6] Bij de inwerkingtreding heette deze organisatie College bescherming persoonsgegevens.
[7] www.autoriteitpersoonsgegevens.nl/ (zoek op: *Meldplicht datalekken*).
[8] Goudsmit, *Bb* 2015/53, afl. 16, p. 184.

om voor de meeste overtredingen van de Wbp een boete van maximaal € 820.000 op te leggen.[9]

In december 2015 hebben het Europees Parlement en de Raad overeenstemming bereikt over een nieuw wettelijk kader voor de bescherming van persoonsgegevens. Dit nieuwe wettelijke kader is de Algemene verordening gegevensbescherming[10] (hierna: AVG). Door de vernieuwingen van de AVG moeten de persoonsgegevens beter beschermd worden.[11] Voorbeelden van vernieuwingen zijn de versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden voor organisaties en dezelfde stevige bevoegdheden voor alle Europese privacytoezichthouders.[12]

De AVG is vanaf 25 mei 2018 van toepassing.[13] Vanaf dan geldt er nog maar één privacywet in de hele Europese Unie. De Wet bescherming persoonsgegevens geldt dan niet meer.[14]

Doordat er een aantal veranderingen op het gebied van privacyrecht zijn doorgevoerd en de inwerkingtreding van de AVG wil Surplus Welzijn weten of zij voldoet aan de huidige privacywetgeving. Daarnaast wil de organisatie weten welke gevolgen de inwerkingtreding van de AVG heeft voor het beleid en de praktijk.

Tijdens dit onderzoek zal worden onderzocht of het beleid van Surplus Welzijn voldoet aan de huidige privacywetgeving. Dit geldt zowel voor het beleid dat de organisatie wil voeren, als voor de wijze waarop er door de werknemers van de organisatie in de praktijk invulling wordt gegeven aan het te voeren beleid. Daarnaast zal worden ingegaan op de veranderingen die Surplus Welzijn zal moeten ondergaan om zich aan te passen aan de AVG.

§ 1.3 Centrale vraag

Uit de probleembeschrijving is de volgende centrale vraag naar voren gekomen: Welke aanbevelingen voor de wijze waarop de afdelingen sociaal raadsliedenwerk, schuldhulpverlening en maatschappelijk werk van Surplus Welzijn in Etten-Leur, persoonsgegevens van cliënten verwerken, vloeien voort uit een toets van het privacybeleid en de praktijk bij deze afdelingen, aan de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming?

§ 1.4 Deelvragen

Om tot een goede beantwoording van de centrale vraag over te gaan, zullen eerst de volgende deelvragen worden beantwoord:

1. Welke eisen gelden er voor Surplus Welzijn vanuit de Wet bescherming persoonsgegevens voor de verwerking van persoonsgegevens van cliënten?
2. Welke wijzigingen brengt de inwerkingtreding van de Algemene verordening gegevensbescherming voor Surplus Welzijn met zich mee voor de verwerking van persoonsgegevens van cliënten ten opzichte van de Wet bescherming persoonsgegevens?
3. Welke eisen stelt het beleid van de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening aan de verwerking van persoonsgegevens van cliënten?

---

[9] Goudsmit, *Bb* 2015/53, afl. 16, p. 185.
[10] Verordening (EU) 2016/679.
[11] Hijmans, *NJ* 2016, afl. 16, p. 1094.
[12] www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving (klik op: *Algemene verordening gegevensbescherming*).
[13] Artikel 99 lid 2 AVG.
[14] www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving (klik op: *Algemene verordening gegevensbescherming*).

4. Hoe wordt door de beroepskrachten en vrijwilligers van de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening in de praktijk invulling gegeven aan het beleid voor de verwerking van persoonsgegevens van cliënten?
5. In hoeverre is het beleid en de praktijk van de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening in overeenstemming met de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming?

§ 1.5 Doelstelling

Het doel van dit onderzoek is om uiterlijk 29 mei 2017 een onderzoeksrapport te overhandigen aan mevrouw mr. W.C.J. van de Kar waarin aanbevelingen worden gegeven hoe Surplus Welzijn ervoor kan zorgen dat het privacybeleid en de praktijk in overeenstemming komen met de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming.

§ 1.6 Onderzoeksstrategieën, methoden en bronnen

Hieronder zal besproken worden welke onderzoeksstrategie(en), methoden en bronnen zijn toegepast voor het beantwoorden van de betreffende deelvraag.

- Welke eisen gelden er vanuit de Wet bescherming persoonsgegevens voor de verwerking van persoonsgegevens?

- Welke wijzigingen brengt de inwerkingtreding van de Algemene verordening gegevensbescherming met zich mee ten opzichte van de Wet bescherming persoonsgegevens?

Voor het beantwoorden van deze deelvragen is gebruik gemaakt van rechtsbronnen- en literatuuronderzoek. Het huidige wettelijk kader voor de verwerking van persoonsgegevens is de Wbp. Deze wet is grondig geanalyseerd. Daarnaast is er gekeken welke wettelijke bepalingen voor de organisatie van toepassing zijn. Om een beter beeld te krijgen van de eisen uit de Wbp voor Surplus Welzijn is ook gebruik gemaakt van literatuur, kamerstukken, internetbronnen en handleidingen.

Naast het huidige wettelijk kader is ook het toekomstig wettelijk kader onderzocht. Er is voornamelijk gekeken welke bepalingen uit de AVG relevant zijn voor Surplus Welzijn en welke gevolgen die met zich mee brengen. Hiervoor is tevens gebruik gemaakt van literatuur, internetbronnen en handleidingen.

De Wbp en de AVG zijn ook met elkaar vergeleken. Een aantal bepalingen van de Wbp komen ook terug in de AVG. Sommige bepalingen komen letterlijk terug en andere met dezelfde strekking. Er is gekozen om alleen bepalingen uit de AVG mee te nemen in dit onderzoek die ingrijpend zijn gewijzigd. Hiervoor is gekozen omdat er meer literatuur beschikbaar is over de Wbp. Hierdoor is het mogelijk om een goede analyse te maken welke wettelijke vereisten voor de organisatie van toepassing zijn.

- Welke eisen stelt het beleid van de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening aan de verwerking van persoonsgegevens van cliënten?

Het beleid van Surplus Welzijn omtrent het verwerken van persoonsgegevens is geraadpleegd voor het beantwoorden van deze deelvraag. Dit was voornamelijk het Privacyreglement van Surplus Welzijn. Om een completer beeld te krijgen van het Privacyreglement is ook een van de auteurs daarvan geïnterviewd. Daarnaast is er gevraagd om werkinstructies omtrent dit onderwerp in te mogen zien. Deze waren echter niet beschikbaar.

- Hoe wordt door de beroepskrachten en vrijwilligers van de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening in de praktijk invulling gegeven aan het beleid voor de verwerking van persoonsgegevens van cliënten?

Om een goed antwoord te kunnen formuleren op deze deelvraag is gebruik gemaakt van casestudy. Bij casestudy worden vaak meerdere onderzoeksmethoden gecombineerd.[15] Bij dit onderzoek is gebruik gemaakt van interviews en een steekproef. Per afdeling zijn twee medewerkers geïnterviewd om na te gaan hoe zij omgaan met het verwerken van persoonsgegevens van cliënten. De werknemers zijn geïnterviewd aan de hand van een semigestructureerde vragenlijst. De geïnterviewde medewerkers zijn at random gekozen.

Voor het technische gedeelte van dit onderzoek zijn drie medewerkers van de afdeling ICT geïnterviewd. De vragen die de medewerkers van de onderzochte afdeling en ICT niet konden beantwoorden, zijn voorgelegd aan een lid van de Raad van Bestuur.

Naast de interviews is een steekproef toegepast in computersysteem Regas. In totaal zijn zesentwintig dossiers onderzocht. Uit alle beschikbare dossiers in Regas heeft een selectie plaatsgevonden. Deze dossiers zijn at random geselecteerd. Er is gekozen om te zoeken op de naam van een client. Als eerste letter zijn verschillende letters uit het alfabet ingevuld. De tweede letter was steeds de a. Er is bijgehouden welke dossiers zijn onderzocht. Hierdoor is het uitgesloten dat twee keer hetzelfde dossier werd gebruikt voor deze steekproef. Het doel van deze steekproef was om te analyseren welke persoonsgegevens van de cliënten door de medewerkers worden verwerkt.

- In hoeverre is het beleid en de praktijk van de afdelingen sociaal raadsliedenwerk, maatschappelijk werk en schuldhulpverlening in overeenstemming met de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming?

Voor het beantwoorden van deze deelvraag is gekeken welke juridische vereisten er zijn en of er door de organisatie is voldaan aan de wettelijke vereisten. Hiervoor is gebruik gemaakt van een analyse.

§ 1.7 Methodische verantwoording

Om het onderzoek af te bakenen zijn er een aantal keuzes gemaakt. Een van de keuzes is om niet te onderzoeken welke wettelijke eisen er gesteld worden aan het verstrekken van persoonsgegevens aan derden. De bepalingen komen, voor de volledigheid, wel terug in het Privacyreglement, maar zijn niet behandeld in de toetsing van het wettelijk kader aan de praktijk. Hiervoor is gekozen omdat de opdrachtgever daaraan geen prioriteit stelde en vanwege het geringe tijdsbestek van dit onderzoek.

Daarnaast is gekozen om alleen de voor de organisatie relevante bepalingen uit te lichten in de hoofdstukken. Dit onderzoeksrapport is geschreven voor Surplus Welzijn en de organisatie heeft alleen belang bij relevante bepalingen uit de Wbp en AVG die van toepassing zijn de organisatie. Indien er sprake is van een wettelijke bepaling die door de komst van de AVG vervalt, wordt deze kort weergegeven. Dit omdat deze bepaling in het nieuwe wettelijk kader voor de verwerking van de persoonsgegevens niet meer van toepassing is en dus niet relevant meer is voor de organisatie.

Het praktijkonderdeel van dit onderzoek is vooral tot stand gekomen door middel van interviews. Per onderzochte afdeling zijn twee medewerkers geïnterviewd. Door de beperkte

[15] Van Schaaijk 2011, 81.

looptijd van dit onderzoek, was het niet mogelijk om meer medewerkers per afdeling te interviewen. In totaal hebben zes interviews plaatsgevonden bij de onderzochte afdelingen.

De afgenomen interviews zijn opgenomen en uitgetypt. De geïnterviewden hebben aanvullingen kunnen geven op het verslag. Daarna zijn allen akkoord gegaan met de tekst zoals deze is weergegeven in de bijlages.

Hoofdstuk 2 De Wet bescherming persoonsgegevens

De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens (95/46/EG). Deze wet is sinds 1 september 2001 van toepassing. Door de inwerkingtreding van de Wbp is de Wet persoonsregistratie (hierna: Wpr) komen te vervallen. In de Wbp is zoveel mogelijk vastgehouden aan het beschermingsniveau van de Wpr.[16]

In dit hoofdstuk zullen alleen onderwerpen aan bod komen die relevant zijn voor Surplus Welzijn.

§ 2.1 Reikwijdte en toepassingsgebied Wbp

De Wbp is van toepassing op geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens en ook op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn daarin opgenomen te worden.[17] Het is voornamelijk voor dit onderzoek van belang of er sprake is van het verwerken van persoonsgegevens. Deze begrippen staan namelijk centraal in de Wbp.[18] Hieronder is weergegeven wat wordt verstaan onder deze begrippen.

Persoonsgegevens

In de Wbp wordt onder persoonsgegeven het volgende verstaan: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.[19] De informatie moet dus direct over iemand gaan of naar een persoon te herleiden zijn.[20] Voorbeelden van persoonsgegevens zijn namen, adressen, woonplaatsen, telefoonnummers en postcodes met huisnummers.

Verwerken

Het hele proces dat een persoonsgegeven doormaakt vanaf het moment van ontvangst tot de vernietiging wordt verwerken genoemd. Iedere handeling of geheel van handelingen met betrekking tot persoonsgegevens valt daaronder.[21] Voorbeelden van handelingen die worden gezien als verwerking zijn verzamelen, bewaren, bijwerken, wijzigen en raadplegen.[22]

§ 2.2 Begrippen

In de Wbp worden een aantal begrippen gebruikt. Hieronder zullen de begrippen worden weergegeven die van belang zijn voor dit onderzoek.

Verantwoordelijke/bestuurder

Dit is degene die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. Dit kan een persoon of instantie zijn.[23] De verantwoordelijke bepaalt om welke verwerking het gaat, welke persoonsgegevens de organisatie verwerkt, voor welk doel de persoonsgegevens worden verwerkt en hoe de verwerking door de organisatie wordt uitgevoerd.[24] In de praktijk is de verantwoordelijke bij Surplus Welzijn een lid van de Raad van Bestuur. In dit onderzoek zal gebruik worden gemaakt van de term bestuurder in plaats van verantwoordelijke.

---

[16] Kranenborg en Verhey 2011, p. 57.
[17] Artikel 2 lid 1 Wbp.
[18] Berkvens en Prins 2007, p. 28.
[19] Artikel 1 sub a Wbp.
[20] www.autoriteitpersoonsgegevens.nl/ (zoek op: *wat zijn persoonsgegevens*).
[21] Kranenborg en Verhey 2011, p. 65.
[22] Artikel 1 sub b Wbp.
[23] www.autoriteitpersoonsgegevens.nl (zoek op: *wat zijn persoonsgegevens* en klik op: *wie is de verantwoordelijke en wie de betrokkene bij het verwerken van persoonsgegevens?*).
[24] www.autoriteitpersoonsgegevens.nl (zoek op: *wat zijn persoonsgegevens* en klik op: *wie is de verantwoordelijke en wie de betrokkene bij het verwerken van persoonsgegevens?*).

Bestand
Onder een bestand wordt een geheel van gegevens verstaan. Deze gegevens moeten betrekking hebben op verschillende personen. Het systeem moet geordend zijn en de gegevens moeten onderlinge samenhang vertonen. Een voorbeeld van een bestand is een geordende dossierkast.[25]

Betrokkene/cliënt
De betrokkene is degene waarover de persoonsgegevens gaan.[26] In de praktijk bij Surplus Welzijn is de betrokkene de cliënt. In dit onderzoek zal daarom gebruik worden gemaakt van de term cliënt in plaats van betrokkene.

Bewerker/Regas
De bewerker is degene die ten behoeve van de bestuurder persoonsgegevens verwerkt, zonder dat hij rechtstreeks onder het gezag van de bestuurder staat.[27] De bewerker staat buiten de organisatie van de bestuurder en deze moet de persoonsgegevens verwerken onder verantwoordelijkheid van de bestuurder.[28] In de praktijk worden de persoonsgegevens verwerkt door de organisatie Regas. Hierdoor wordt in dit onderzoek gebruik gemaakt van de term Regas in plaats van bewerker.

Bijzondere persoonsgegevens
Dit zijn gegevens die betrekking hebben op iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en persoonsgegevens met betrekking tot het lidmaatschap van een vakvereniging.[29]

Datalek
Een datalek is de toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van de organisatie. Hieronder valt ook de onrechtmatige verwerking van persoonsgegevens.[30] Onder onrechtmatige verwerking vallen aantasting van de gegevens, onbevoegde kennisneming, aanpassing of verstrekking daarvan.[31]

Toestemming van een cliënt
De toestemming van een cliënt is elke vrije, specifieke, heldere, ondubbelzinnige en op informatie berustende wilsuiting waarmee een cliënt akkoord gaat met de verwerking van zijn persoonsgegevens.[32] Aan de toestemming van een cliënt worden een aantal eisen gesteld. Zo moet de cliënt zijn wil in vrijheid kunnen uiten. Daarnaast moet hij de bedoeling hebben om toestemming te geven voor bepaalde gegevensverwerking. Tot slot moet de cliënt een goede afweging kunnen maken. Hij dient daarom te beschikken over de benodigde informatie.[33]

§ 2.3 Verwerking van persoonsgegevens

Aan de verwerking van persoonsgegevens worden een aantal eisen gesteld in de Wbp. De persoonsgegevens moeten namelijk in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.[34] Dit geldt voor alle handelingen met betrekking tot de

[25] Sauerwein en Linnemann 2002, p. 15.
[26] Artikel 1 sub f Wbp.
[27] Artikel 1 sub e Wbp.
[28] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 61.
[29] Berkvens en Prins 2007 p. 36.
[30] www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/ (klik op: *meldplicht datalekken*).
[31] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 98.
[32] Artikel 1 sub i Wbp.
[33] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 65.
[34] Artikel 6 Wbp.

verwerking van de persoonsgegevens.[35] Daarnaast moeten de persoonsgegevens conform welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.[36] Met welbepaald en uitdrukkelijk omschreven wordt bedoeld dat er geen gegevens mogen worden verzameld zonder een doelomschrijving. De doelomschrijving moet duidelijk zijn.[37] Door de organisaties waarop de Wbp van toepassing is, zullen dus doeleinden moeten worden opgesteld. Het is niet toegestaan om persoonsgegevens te verwerken op een manier die in strijd is met de doeleinden waarvoor ze zijn verkregen.[38]

De doeleinden zijn bepalend voor de hoeveelheid en de soort van gegevens die onderwerp van de verwerking zijn.[39] Er zal bij de verwerking daarom altijd rekening gehouden moeten worden met de doeleinden van de verwerking. De persoonsgegevens mogen pas worden verwerkt indien zij toereikend, ter zake dienend en niet bovenmatig zijn.[40] Aan de vereisten van toereikend wordt voldaan als er een noodzaak bestaat om te beschikken over voldoende informatie.[41] Onder ter zake dienend en niet bovenmatig wordt verstaan dat er niet meer persoonsgegevens mogen worden verwerkt dan nodig is voor het doel van de verwerking.[42]

Naast de eisen aan de doeleinden, is het voor organisaties niet vanzelfsprekend dat zij persoonsgegevens mogen verwerken. Een organisatie mag persoonsgegevens verwerken indien[43]:

- de cliënt of zijn wettelijk vertegenwoordiger daarvoor ondubbelzinnige toestemming voor de toestemming heeft verleend;
- de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de cliënt partij is;
- de verwerking noodzakelijk is voor de uitvoering van een wettelijke verplichting van de bestuurder;
- de verwerking noodzakelijk is ter bescherming van een vitaal belang van de cliënt;
- de verwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak;
- de verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang.

Daarnaast moet bij elke verwerking worden voldaan aan de beginselen van proportionaliteit en subsidiariteit. Met proportionaliteit wordt bedoeld dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokken cliënt niet onevenredig mag zijn in verhouding tot het te dienen doel. Het subsidiariteitsbeginsel houdt in dat er gekozen moet worden voor een wijze van verwerken die het minst nadelig voor de cliënt is.[44]

Tot slot geldt er nog de eis dat de bestuurder maatregelen moet treffen om ervoor te zorgen dat persoonsgegevens juist en nauwkeurig zijn.[45] De persoonsgegevens moeten dus regelmatig worden gecontroleerd. Zo kan worden voorkomen dat er onjuiste persoonsgegevens van de cliënt beschikbaar zijn.

---

[35] Kranenborg en Verhey 2011, p. 81.
[36] Artikel 7 Wbp.
[37] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 79.
[38] Artikel 9 lid 1 Wbp.
[39] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 96.
[40] Artikel 11 lid 1 Wbp.
[41] Kranenborg en Verhey 2011, p. 97.
[42] Kranenborg en Verhey 2011, p. 97.
[43] Artikel 8 sub a tot en met f Wbp.
[44] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 80.
[45] Artikel 11 lid 2 Wbp.

§ 2.4 Verwerking van bijzondere persoonsgegevens

In beginsel is het verboden om de bijzondere persoonsgegevens te verwerken.[46] Op dit verbod gelden wel een aantal uitzonderingen. Deze uitzonderingen zijn terug te vinden in de artikelen 17 tot en met 24 Wbp. Hieronder zal kort ingegaan worden op de uitzonderingen.

Godsdienst of levensovertuiging

Het verbod voor de verwerking van gegevens betreffende de godsdienst of levensovertuiging van een persoon geldt, kort gezegd, niet voor kerkgenootschappen, genootschappen op geestelijke grondslag of andere instellingen op godsdienstige of levensbeschouwelijke grondslag.[47]

Ras

In uitzonderlijke situaties is het toegestaan om gegevens te verwerken over iemands ras. Dit is alleen toegestaan voor identificatiedoeleinden of in het kader van een voorkeursbeleid.[48] Indien er sprake is van een voorkeursbeleid gelden er nog extra vereisten.

Gezondheid

De Wbp noemt een aantal groepen van instellingen die gegevens over de iemands gezondheid mogen verwerken. Het gaat dan om ziekenhuizen, instellingen voor maatschappelijke dienstverlening, verzekeraars, speciale scholen, reclasseringsinstellingen, de Raad voor de Kinderbescherming, (gezins-) voogdijinstellingen, bestuursorganen en uitvoeringsinstellingen die bepaalde socialezekerheidswetten uitvoeren. [49]

Algemene uitzonderingen

Indien de bovenstaande specifieke uitzonderingen niet van toepassing zijn, kan een beroep worden gedaan op de algemene uitzonderingen. Deze uitzonderingen gelden voor alle bijzondere persoonsgegevens. Het is wel toegestaan om bijzondere persoonsgegevens te verwerken als de cliënt uitdrukkelijke toestemming heeft gegeven, de cliënt de gegevens zelf duidelijk openbaar heeft gemaakt of de verwerking noodzakelijk is voor het vaststellen, uitoefenen of verdedigen van een recht in een gerechtelijke procedure.[50] [51]

Burgerservicenummer

Het burgerservicenummer is een bijzonder persoonsgegeven omdat het een uniek en tot de persoon herleidbaar nummer is. Het burgerservicenummer is een nummer dat bij de wet is voorgeschreven om een persoon te identificeren. Het mag daarom alleen gebruikt worden voor de uitvoering of voor de doeleinden van een betreffende wet. Het is toegestaan een burgerservicenummer te registreren op grond van de Wet gebruik burgerservicenummer in de zorg en de Wet algemene bepalingen burgerservicenummer. Op grond van deze wetten is het voor bijvoorbeeld zorgaanbieders en overheidsinstellingen toegestaan om een burgerservicenummer te verwerken. Het verbod op het verwerken van het burgerservicenummer kan niet worden omzeild door de toestemming van een cliënt.[52]

§ 2.5 Rechten cliënten

Recht op kennisneming

De cliënt kan de bestuurder verzoeken om hem mede te delen welke persoonsgegevens van hem worden verwerkt.[53] De bestuurder dient een zo volledig mogelijk overzicht te

[46] Artikel 16 Wbp.
[47] Sauerwein en Linnemann 2002, p. 48.
[48] Artikel 18 Wbp.
[49] Sauerwein en Linnemann 2002, p. 49.
[50] Artikel 23 Wbp.
[51] Sauerwein en Linnemann 2002, p. 50.
[52] www.autoriteitpersoonsgegevens.nl (zoek op: *burgerservicenummer*).
[53] Artikel 35 lid 1 Wbp.

verstrekken met inlichtingen over het doel, de aard van de gegevens, de ontvangers en de herkomst van de gegevens.[54] [55] De bestuurder moet dit binnen vier weken mededelen aan de cliënt.[56]

Recht op correctie
Als een cliënt gebruik heeft gemaakt van zijn recht op kennisneming, kan hij de bestuurder verzoeken om zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.[57] De bestuurder dient binnen vier weken te reageren op dit verzoek. Als hij het verzoek afwijst, moet hij dit beargumenteren.[58]

Recht van verzet
Als persoonsgegevens van een cliënt verwerkt worden omdat het noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak of het noodzakelijk is voor de behartiging van het gerechtvaardigd belang van de bestuurder heeft een cliënt het recht op verzet.[59] Een cliënt heeft dan het recht om de organisatie te vragen om de persoonsgegevens niet meer te gebruiken. De cliënt kan altijd het verzet aantekenen tegen de verwerking in verband met zijn persoonlijke omstandigheden. Op dit verzoek moet binnen vier weken gereageerd worden.[60]

§ 2.6 Verplichtingen bestuurder

Bewaartermijn
De persoonsgegevens van cliënten mogen niet langer woorden bewaard dan noodzakelijk is voor de realisatie van de doeleinden waarvoor ze zijn verzameld. Als het doel door de organisatie is bereikt, moet de gegevensverwerking in principe worden beëindigd.[61] Het is toegestaan om de persoonsgegevens langer te bewaren als dit gebeurt voor historische, statistische of wetenschappelijke doeleinden. De bestuurder dient er wel voor te zorgen dat de gegevens alleen voor die doeleinden worden gebruikt.[62] In de Wbp is geen termijn vastgelegd hoe lang persoonsgegevens bewaard mogen blijven.

Beveiliging
De bestuurder dient de persoonsgegevens te beveiligen tegen verlies of een vorm van onrechtmatige verwerking. Dit dient de bestuurder te doen door het nemen van passende technische en organisatorische maatregelen.[63] Bij technische maatregelen kan worden gedacht aan de logische en fysieke maatregelen in en rondom de informatiesystemen. Voorbeelden hiervan zijn toegangscodes, vastlegging van gebruik en een back-up. Met organisatorische maatregelen worden maatregelen bedoeld voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens. Voorbeelden hiervan zijn toekenning en deling van verantwoordelijkheden en bevoegdheden, werkinstructies, cursussen en calamiteitenplannen.[64] Zoals eerder aangegeven moet het wel gaan om passende technische en organisatorische maatregelen. Aan gevoelige gegevens worden zwaardere beveiligingseisen gesteld. Dit komt omdat er sprake moet zijn van proportionaliteit tussen de aard van de gegevens en de beveiligingsmaatregelen.[65]

[54] Artikel 35 lid 2 Wbp.
[55] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 158.
[56] Artikel 35 lid 1 Wbp.
[57] Artikel 36 lid 1 Wbp.
[58] Artikel 36 lid 2 Wbp.
[59] Artikel 40 lid 1 Wbp.
[60] www.autoriteitpersoonsgegevens.nl (zoek op: *recht van verzet*).
[61] Kranenborg en Verhey 2011, p. 99.
[62] Artikel 10 lid 2 Wbp.
[63] Artikel 13 Wbp.
[64] Kranenborg en Verhey 2011, p. 99.
[65] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 99.

Informatieplicht
Als de persoonsgegevens van de cliënt zelf worden verkregen, moet aan de cliënt voor de verkrijging bekend worden gemaakt wie de bestuurder is en geïnformeerd worden over de verwerkingsdoeleinden.[66] Daarnaast zal gekeken moeten worden of er verdere informatie moet worden verstrekt in het kader van het garanderen van een behoorlijke en zorgvuldige gegevensverwerking.[67]

Meldingsplicht
De bestuurder is verplicht een verwerking van persoonsgegevens te melden bij de Autoriteit Persoonsgegevens.[68]

Meldplicht datalekken
Indien er sprake is van een datalek dient de bestuurder dit direct te melden bij de Autoriteit Persoonsgegevens. Na de ontdekking van een datalek mag er enige tijd genomen worden voor nader onderzoek. De organisatie heeft dan de mogelijkheid om een onnodige melding te voorkomen.[69]

Niet alle datalekken moeten door de bestuurder worden gemeld aan de Autoriteit Persoonsgegevens. Een organisatie deze alleen melden als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen van de bescherming van persoonsgegevens. Om te bepalen of hiervan sprake is, moeten onderstaande vragen worden beantwoord:

- Zijn er persoonsgegevens van gevoelige aard gelekt?
- Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Als een van deze bovenstaande vragen met ‘ja’ kan worden beantwoord, is er sprake van een datalek die gemeld moet worden aan de Autoriteit Persoonsgegevens.[70] Die melding kan gedaan worden via de website van de Autoriteit Persoonsgegevens.[71]

Een cliënt moet op de hoogte worden gesteld van het datalek als er sprake is van (waarschijnlijk) ongunstige gevolgen voor zijn privéleven.[72] De organisatie moet dan vermelden wat de aard van de inbreuk is, de instanties waar de cliënt meer informatie over de inbreuk kan krijgen en de maatregelen die worden aanbevolen om de negatieve gevolgen van de inbreuk te beperken.[73]

Daarnaast dient de organisatie een overzicht bij te houden van alle datalekken waarvoor een meldplicht bij de Autoriteit Persoonsgegevens geldt. In de Wbp is niet beschreven hoe lang deze gegevens bewaard moeten blijven. De Autoriteit Persoonsgegevens geeft aan dat eruit moet worden gegaan van een bewaartermijn van minimaal één jaar.[74]

Verwerking door Regas
Als de bestuurder de persoonsgegevens laat verwerken door Regas, moet Regas zorg dragen voor voldoende waarborgen. Deze waarborgen hebben betrekking op technische en

[66] Sauerwein en Linnemann 2002, p. 34.
[67] Kranenborg en Verhey 2011, p. 120.
[68] Kranenborg en Verhey 2011, p. 116.
[69] Autoriteit Persoonsgegevens 2015, p. 31.
[70] Autoriteit Persoonsgegevens 2015, p. 24.
[71] www.datalekken.autoriteitpersoonsgegevens.nl/actionpage?0
[72] www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken (klik op: *moet ik alle datalekken melden aan de betrokkene?*).
[73] Artikel 34a lid 3 Wbp.
[74] Autoriteit Persoonsgegevens 2015, p. 46.

organisatorische maatregelen. Op de naleving van die maatregelen moet de bestuurder toezicht houden.[75] De bestuurder moet Regas voldoende duidelijk maken hoe moet worden omgegaan met de persoonsgegevens.[76] Er moet daarom sprake zijn van een overeenkomst tussen de bestuurder en Regas.[77] Deze overeenkomst wordt ook wel de bewerkingsovereenkomst genoemd. In die overeenkomst moeten in ieder geval bepalingen staan omtrent de geheimhoudingsplicht, de vertrouwelijkheid, de beveiliging van de gegevensverwerking en de meldplicht indien er sprake is van een inbreuk op de beveiliging.[78]

§ 2.7 Verplichtingen personen onder gezag bestuurder

Als een werknemer onder gezag van een bestuurder of Regas handelt, brengt dit verschillende verplichtingen met zich mee. Men mag, in beginsel, de persoonsgegevens van een cliënt slechts verwerken in opdracht van de bestuurder.[79]

De werknemers die onder het gezag van de bestuurder persoonsgegevens verwerken, zijn verplicht tot geheimhouding van die persoonsgegevens. Als een wettelijk voorschrift hem verplicht tot mededeling of uit hun taak de noodzaak tot mededeling voortvloeit, geldt deze geheimhoudingsplicht niet.[80]

§ 2.8 Boetebevoegdheid Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens houdt toezicht op organisaties die zich bezighouden met het verwerken van persoonsgegevens. Zij zien toe op de correcte naleving van de bepalingen uit de Wbp.[81] Als een organisatie handelt in strijd met de Wbp, kan de Autoriteit Persoonsgegevens een boete opleggen.[82]

De hoogte van de boete is afhankelijk van de soort overtreding. Om de hoogte van de boete te kunnen bepalen zijn de Boetebeleidsregels Autoriteit Persoonsgegevens 2016 (hierna: Boetebeleidsregels) opgesteld. Daarin is een onderscheid gemaakt in overtredingen met een wettelijk boetemaximum van € 820.000, € 900.000 en € 20.500.

<u>Hoogte boete</u>

In bijlage 1 van de Boetebeleidsregels is een lijst opgenomen voor welke overtreding het boetemaximum van € 820.000 geldt. In de lijst met overtredingen is een onderscheid gemaakt in categorieën. Het onderscheid ziet er als volgt uit:

Categorie	**Boetebandbreedte**
Categorie I	Tussen € 0 en € 200.000
Categorie II	Tussen € 120.000 en € 500.000
Categorie III	Tussen € 350.000 en € 820.000

De overtredingen waarvoor een wettelijk boetemaximum van € 900.000 kan worden opgelegd, zijn terug te vinden in bijlage 2 van de Boetebeleidsregels. In die bijlage is ook een overzicht opgenomen tot welke categorieën de overtredingen behoren.

---

[75] Artikel 14 lid 1 Wbp.
[76] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 99.
[77] Artikel 14 lid 2 Wbp.
[78] Artikel 14 lid 3 sub a tot en met c Wbp.
[79] Artikel 12 lid 1 Wbp.
[80] Sauerwein en Linnemann 2002, p. 29.
[81] Artikel 51 Wbp.
[82] www.autoriteitpersoonsgegevens.nl (zoek op: *CBP krijgt boetebevoegdheid en wordt Autoriteit Persoonsgegevens*).

Categorie	Boetebandbreedte
Categorie I	Tussen € 0 en € 250.000
Categorie II	Tussen € 150.000 en € 600.000
Categorie III	Tussen € 360.000 en € 900.000

In de derde bijlage van de Boetebeleidsregels zijn overtredingen opgenomen die worden bestraft met een boete met een wettelijk boetemaximum van € 20.500. Ook deze overtredingen zijn onderverdeeld in verschillende categorieën.

Categorie	Boetebandbreedte
Categorie I	Tussen € 0 en € 12.500
Categorie II	Tussen € 7.500 en € 20.500

Om de exacte boete voor de organisatie te kunnen bepalen, zijn factoren in de Boetebeleidsregels opgenomen waar de Autoriteit Persoonsgegevens rekening mee houdt bij de oplegging van de boete. Zoals de ernst van de overtreding. Bij het bepalen van de ernst wordt rekening gehouden met de volgende factoren[83]:

- de aard en de omvang van de overtreding;
- de duur van de overtreding;
- de impact van de overtreding op de betrokkene(n) en/of de maatschappij;
- de verwijtbaarheid van de organisatie;
- de omstandigheden waaronder de overtreding is gepleegd;
- de financiële mogelijkheden van de organisatie.

Boeteverhogende omstandigheden

De Autoriteit Persoonsgegevens kan een boete van tien procent van de jaaromzet van de organisatie opleggen als een boete van € 820.000 geen passende straf is. Naast deze mogelijkheid heeft de Autoriteit Persoonsgegevens ook de gelegenheid om de boete te verhogen als een overtreder al eerder dezelfde of een vergelijkbare overtreding heeft begaan.[84] Tot slot kan de Autoriteit Persoonsgegevens de boete verhogen als de overtredende organisatie het onderzoek heeft tegengewerkt of belemmerd.[85]

Boeteverlagende omstandigheden

In de Boetebeleidsregels zijn omstandigheden opgenomen die in ieder geval zorgen voor de verlaging van de boete. De boete wordt verlaagd als[86]:

- de overtreder meer medewerking verleent dan waartoe hij wettelijk verplicht is;
- de overtreder op eigen initiatief de overtreding heeft beëindigd voor of bij de bekendwording van het onderzoek;
- de overtreder op eigen initiatief de schade heeft vergoed die de overtreding veroorzaakt.

Bindende aanwijzing

In veel gevallen legt de Autoriteit Persoonsgegevens niet meteen een boete op. Er zal dan een bindende aanwijzing worden gegeven. De Autoriteit Persoonsgegevens zal dan aangeven wat er van de overtreder wordt verwacht op grond van de Wbp. De overtreder wordt in staat gesteld om de overtreding geheel of gedeeltelijk ongedaan te maken.[87] De

[83] Artikel 6 lid 1 tot en met 3 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[84] Artikel 9 lid 1 sub a Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[85] Artikel 9 lid 1 sub b Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[86] Artikel 10 sub a tot en met c Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[87] *Kamerstukken II* 2014/2015, 33662, nr. 9, p.4.

Autoriteit Persoonsgegevens kan een termijn stellen waarbinnen de aanwijzingen moeten zijn opgevolgd.[88] Als de aanwijzingen niet worden opgevolgd, kan er alsnog een boete worden opgelegd.[89] Een bindende aanwijzing kan niet worden opgelegd als er sprake is van een opzettelijke overtreding of een overtreding die het gevolg is van ernstige verwijtbare nalatigheid.[90]

[88] Artikel 66 lid 3 Wbp.
[89] Artikel 66 lid 5 Wbp.
[90] Artikel 66 lid 4 Wbp.

Hoofdstuk 3 De algemene verordening gegevensbescherming

In Brussel werd op 27 april 2016 door het Europees parlement en de Raad de AVG vastgesteld. Die verordening komt in de plaats van de nu geldende privacyrichtlijn van de Europese Unie.[91] Het doel van de verordening is het niveau van bescherming van persoonsgegevens te verhogen. De AVG moet zorgen voor hetzelfde niveau van bescherming in alle lidstaten en een versterking van de rechten van een cliënt.[92]

Doordat er sprake is van een verordening is deze rechtstreeks toepasbaar op de lidstaten van de Europese Unie. Voor het privacyrecht heeft dit als gevolg dat de Wbp komt te vervallen als de AVG van toepassing is vanaf 25 mei 2018. Inmiddels is een concept Uitvoeringswet AVG opgesteld. Deze Uitvoeringswet AVG is niet meegenomen voor het beantwoorden van de deelvraag aangezien daar weinig relevante informatie in staat met betrekking tot de punten die in dit hoofdstuk worden besproken. Alleen de voor de organisatie relevante veranderingen zullen worden besproken.

§ 3.1 Begrippen

In de definities van de Wbp zijn een aantal kleine veranderingen gekomen door de inwerkingtreding van de AVG. De bewoording van sommige begrippen is iets aangepast. De strekking van de definities is nog wel hetzelfde gebleven. Een voorbeeld is de definitie van persoonsgegevens. In de Wbp werd nog gesproken over ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. In de AVG is dit ‘alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon’.

In de AVG hebben sommige begrippen een andere naam gekregen. Zo wordt de ‘verantwoordelijke’ in de AVG de ‘verwerkingsverantwoordelijke’ genoemd en ‘bewerker’ is ‘verwerker’ geworden. In dit hoofdstuk zal vastgehouden worden aan de termen cliënt, Regas en bestuurder zoals eerder omschreven.

Hieronder zullen relevante definities voor dit onderzoek worden weergegeven die nieuw zijn of ingrijpend zijn veranderd.

<u>Inbreuk in verband met persoonsgegevens</u>

Een begrip dat met de komst van de AVG geïntroduceerd wordt, is het begrip inbreuk in verband met persoonsgegevens. Hiermee wordt een inbreuk op de beveiliging bedoeld die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang verwerkte persoonsgegevens.[93] In de Wbp was niet bepaald wat er verstaan werd onder een inbreuk in verband met persoonsgegevens.

<u>Toestemming</u>

Met toestemming wordt bedoeld elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee een cliënt door middel van een verklaring of een ondubbelzinnige actieve handeling de op hem betreffende verwerking van persoonsgegevens aanvaardt.[94] Als de verwerking berust op de toestemming van een cliënt, moet de bestuurder kunnen aantonen dat een cliënt toestemming heeft gegeven voor de verwerking.[95] Het verschil met de Wbp zit in het feit dat het moet gaan over een ondubbelzinnige wilsuiting en dat de toestemming aangetoond moet worden door de bestuurder. Dit was voorheen niet opgenomen in de wet- en regelgeving.

---

[91] De Jong, *AA* 2016, p. 770.
[92] De Vries en Goudsmit, *NJB* 2016, p. 1553.
[93] Artikel 1 lid 12 AVG.
[94] Artikel 1 lid 11 AVG.
[95] Artikel 7 lid 1 AVG.

Profilering
In de Wbp is geen bepaling opgenomen omtrent profilering. Door gebruik te maken van profilering worden (persoons)gegevens verzameld, geanalyseerd en gecombineerd. De cliënten kunnen dan ingedeeld worden in bepaalde categorieën.[96] Een organisatie mag alleen gebruik maken van profilering indien er sprake is van een van de rechtsgronden voor de verwerking van persoonsgegevens. Daarnaast zijn de beginselen voor de gegevensbescherming ook van toepassing.[97]

Pseudonimisering
Hiermee wordt bedoeld dat persoonsgegevens op een bepaalde manier worden verwerkt die ervoor zorgt dat zij niet meer aan een specifieke cliënt kunnen worden gekoppeld zonder aanvullende gegevens.[98] De persoonsgegevens worden dan vervangen door een code of een sleutel. Alleen degene die de sleutel heeft of de code weet, kan de bewerking omkeren.[99] In de Wbp waren geen bepalingen opgenomen omtrent het gebruik maken van pseudonimisering.

§ 3.2 Rechten cliënten

Door de inwerkingtreding van de AVG blijven de rechten van de cliënten, die bestonden op grond van de Wbp, bestaan. Verder worden er in de AVG nieuwe rechten toegekend aan de cliënten. Hieronder zullen de nieuwe rechten worden weergegeven.

Recht op beperking van de verwerking
In bepaalde gevallen kan een cliënt gebruik maken van zijn recht op beperking van de verwerking. Door dit recht kunnen bijvoorbeeld geselecteerde gegevens tijdelijk niet beschikbaar zijn of van een website worden verwijderd.[100] Een cliënt kan gebruik maken van dit recht indien[101]:

- men de juistheid van de persoonsgegevens betwist (de bestuurder wordt in de gelegenheid gesteld de juistheid van de persoonsgegevens te controleren);
- de verwerking van de persoonsgegevens onrechtmatig is en een cliënt niet wil dat zijn gegevens worden verwijderd;
- de bestuurder de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden, maar de cliënt de persoonsgegevens wel nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Recht op gegevensoverdraagbaarheid
De cliënt heeft het recht om aan de bestuurder verstrekte persoonsgegevens over te dragen aan een andere bestuurder. De cliënt dient zijn gegevens te verkrijgen in een gestructureerde, gebruikelijke en machine leesbare vorm.[102] In de Wbp was geen bepaling opgenomen die betrekking had op het digitaal overdragen van persoonsgegevens naar andere organisaties.

Recht op vergetelheid
De cliënt had, op grond van de Wbp, al het recht om te verzoeken tot het verwijderen van zijn persoonsgegevens. Door de inwerkingtreding van de AVG wordt dit recht uitgebreid met het recht op vergetelheid. Dit geeft de cliënt de mogelijkheid de bestuurder te verzoeken iedere koppeling naar, kopie of weergave van de persoonsgegevens van de cliënt die door

[96] www.autoriteitpersoonsgegevens.nl (zoek op: *profilering*).
[97] Overweging 72 AVG.
[98] Artikel 4 lid 5 AVG.
[99] www.justitia.nl/privacy/privacy-by-design.html.
[100] De Vries en Goudsmit, *NJB* 2016, p. 1557.
[101] Artikel 18 lid 1 sub a tot en met c AVG.
[102] Artikel 20 lid 1 sub a en b AVG.

de bestuurder openbaar zijn gemaakt te wissen. Als het verzoek door de bestuurder wordt gehonoreerd, moeten derden door hem op de hoogte worden gesteld. Dit is echter alleen mogelijk als de verwerking berust op de toestemming van een cliënt of als er sprake is van een automatische verwerking.[103]

§ 3.3 Verplichtingen bestuurder

De bestuurder heeft door de inwerkingtreding van de AVG een aantal nieuwe verplichtingen gekregen. Deze worden hieronder weergegeven.

Documentatieplicht

In de AVG wordt meer nadruk gelegd op de verantwoordelijkheid van organisaties zelf om de wet na te leven. Ook moeten zij kunnen aantonen dat zij zich aan de wet houden. Op grond van de Wbp was dit nog niet het geval. De organisaties krijgen door de inwerkingtreding van de AVG een documentatieplicht. Dit houdt in dat zij met documenten moeten kunnen aantonen dat zij de juiste organisatorische en technische maatregelen hebben genomen om aan de AVG te voldoen.[104] De maatregelen omvatten een passend gegevensbeschermingsbeleid dat door de bestuurder zal worden uitgevoerd.[105] De documentatieplicht is neergelegd in artikel 30 AVG. In dat artikel is aangegeven dat de bestuurder een register van de verwerkingsactiviteiten dient bij te houden. Dit register dient de volgende gegevens te bevatten[106]:

- de naam en contactgegevens van de bestuurder;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van cliënten en persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de voorgenomen bewaartermijn;
- een beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Informatieplicht

In de Wbp had de bestuurder al de verplichting om zijn identiteit kenbaar te maken aan de cliënten. Daarnaast moet een cliënt geïnformeerd worden over de verwerkingsdoeleinden. Door de komst van de AVG is de informatieplicht uitgebreid en moeten er meer gegevens aan de cliënt worden verstrekt op het moment dat de persoonsgegevens worden verzameld. De cliënt moet ook op de hoogte gesteld worden van[107]:

- de vertegenwoordiger van de bestuurder;
- de functionaris voor de gegevensbescherming (hierna: FG);
- de gerechtvaardigde belangen van de bestuurder;
- de ontvangers van de persoonsgegevens;
- de bewaartermijn van de persoonsgegevens;
- de rechten die hem toekomen;
- de mogelijkheid tot het indienen van een klacht bij de Autoriteit Persoonsgegevens.

Privacy impact assessment

Door een privacy impact assessment (hierna: PIA) uit te voeren, worden privacyrisico's van nieuwe en huidige verwerkingen van persoonsgegevens bloot gelegd. Daarnaast draagt het bij aan het vermijden en verminderen van privacyrisico's. Er wordt dan op consequente wijze

[103] De Jong, *AA* 2016, p. 772.
[104] www.autoriteitpersoonsgegevens.nl (zoek op: *belangrijkste verschillen verordening gegevensbescherming*).
[105] Artikel 24 lid 2 AVG.
[106] Artikel 30 lid 1 sub a tot en met g AVG.
[107] Artikel 13 lid 2 sub a tot en met f AVG.

duidelijk gemaakt hoe groot de kans is dat de privacy van een cliënt wordt geschaad, waar deze risico's zich voordoen en welke gevolgen daaraan verbonden zijn.[108] Een PIA is met name vereist als er[109]:

- systematisch en uitvoerig persoonlijke aspecten worden geëvalueerd;
- op grote schaal bijzondere persoonsgegevens worden verwerkt;
- op grote schaal en systematisch mensen worden gevolgd in een publiek toegankelijk gebied.

In de beoordeling moet een omschrijving worden opgenomen van voorgenomen verwerkingen, de verwerkingsdoeleinden, een oordeel van de noodzakelijkheid en evenredigheid van de verwerkingen, de risico's voor de rechten en vrijheden van een cliënt en de voorgenomen maatregelen om de risico's aan te pakken.[110]

In de Wbp was de verplichting tot het doen van een PIA niet opgenomen.

Meldplicht datalekken

In de Wbp moesten alleen ernstige lekken worden gemeld bij de toezichthouder. Door de inwerkingtreding van de AVG moeten bijna alle datalekken aan de Autoriteit Persoonsgegevens worden gemeld. Een datalek hoeft niet gemeld te worden als de bestuurder kan aantonen dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich mee brengt. Een cliënt moet direct op de hoogte worden gesteld van inbreuken die 'waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen'.[111]

Privacy by design en privacy by default

De termen privacy by design en privacy by default zijn al langer in gebruik. Met de komst van de AVG zijn deze begrippen opgenomen in de wet- en regelgeving omtrent het verwerken van persoonsgegevens. In de AVG worden deze begrippen in het Nederlands vertaald als gegevensbescherming door ontwerp en door standaardinstellingen.[112] Met privacy by design wordt bedoeld dat er bij het ontwerpen van producten en diensten gezorgd moet worden dat de persoonsgegevens worden beschermd. De verplichting tot privacy by default houdt in dat er technische en organisatorische maatregelen moeten worden genomen om ervoor te zorgen dat er alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel dat de organisatie wil bereiken.[113]

Verwerking door Regas

Aan de bewerkingsovereenkomst tussen Regas en de bestuurder worden, door de inwerkingtreding van de AVG, extra eisen gesteld. In de bewerkingsovereenkomst moeten onder andere de volgende punten zijn vermeld[114]:

- doeleinden van de gegevensverwerking;
- de aard van de verwerkte persoonsgegevens;
- de beveiliging van de (persoons)gegevens;
- de uitvoering van audits;
- of er bij de beëindiging van de verwerking de data wordt vernietigd of teruggezonden naar de bestuurder.

[108] NOREA 2015, p. 9.
[109] www.autoriteitpersoonsgegevens.nl (zoek op: *Europese verordening* en klik op: *wanneer moet ik straks een PIA uitvoeren?*).
[110] Artikel 35 lid 7 sub a tot en met d AVG.
[111] De Vries en Goudsmit, *NJB* 2016, p. 1559.
[112] De Vries en Goudsmit, *NJB* 2016, p. 1559.
[113] www.autoriteitpersoonsgegevens.nl (zoek op: *hoe kan ik me voorbereiden op de AVG*).
[114] Artikel 28 lid 3 sub a tot en met h AVG.

§ 3.4 Functionaris voor gegevensbescherming

Een FG is iemand die toezicht houdt op de verwerking van persoonsgegevens van een organisatie. In de Wbp waren er nog geen wettelijke grondslagen wanneer een organisatie verplicht is een FG aan te nemen. Door de inwerkingtreding van de AVG is een organisatie verplicht een FG aan te stellen als[115]:

- de verwerking van persoonsgegevens verricht wordt door een overheidsinstantie of overheidsorgaan (geldt niet voor gerechten bij de uitoefening van hun rechterlijke taken);
- een bestuurder of Regas hoofdzakelijk is belast met verwerkingen die grootschalige regelmatige en systematische observatie van cliënten vereisen.
- een bestuurder of Regas hoofdzakelijk grootschalige verwerkingen uitvoert met betrekking tot bijzondere persoonsgegevens, persoonsgegevens omtrent strafrechtelijke veroordelingen of strafbare feiten.

Eisen aan de FG

De FG dient te beschikken over meer dan gemiddelde kennis over het privacyrecht en de praktijk van de gegevensbescherming. Hij moet ook verstand hebben van informatietechnologie en informatiebeveiliging en kennis hebben van de organisatie en de branche van de organisatie.[116]

Taken van de FG

De voornaamste taak van de FG is het toezicht houden op de naleving van de bepalingen uit de AVG door de organisatie.[117] De FG moet op zijn minst[118]:

- de bestuurder informeren en adviseren over de verplichtingen die de bestuurder heeft op grond van de AVG;
- advies verstrekken over een PIA en de uitvoering daarvan, als dat aan hem gevraagd wordt;
- samen werken met de Autoriteit Persoonsgegevens;
- dienen als contactpersoon voor de Autoriteit Persoonsgegevens.

§ 3.5 Boetebevoegdheid Autoriteit Persoonsgegevens

In de Wbp was het mogelijk om een boete op te leggen indien er sprake was van een overtreding van een bepaling uit die wet. Met de komst van de AVG is het maximale boetebedrag € 20.000.000 of vier procent van de totale wereldwijde jaaromzet.[119] Dit is een flinke stijging ten opzichte van de boetes die opgelegd konden worden vanuit de Wbp.

In de AVG zijn een aantal criteria opgesomd waarmee rekening wordt gehouden bij het opleggen van de boete en de hoogte daarvan. Er wordt onder andere rekening gehouden met[120]:

- de aard, ernst en duur van de inbreuk;
- de opzettelijke of nalatige aard van de inbreuk;
- de genomen maatregelen om de schade van de cliënt te beperken.

De Autoriteit Persoonsgegevens kan een organisatie waarschuwen als de voorgenomen verwerking waarschijnlijk niet in overeenstemming is met de AVG.[121]

---

[115] Artikel 37 lid 1 sub a tot en met c AVG.
[116] www.autoriteitpersoonsgegevens.nl (zoek op: *functionaris voor de gegevensbescherming (FG)*).
[117] Autoriteit Persoonsgegevens 2017, p. 15.
[118] Artikel 39 lid 1 sub a tot en met e AVG.
[119] Artikel 83 lid 5 AVG.
[120] Artikel 83 lid 2 sub a tot en met c AVG.

Hoofdstuk 4 Het privacybeleid

In dit hoofdstuk is beschreven hoe de organisatie wil dat er om wordt gegaan met het verwerken van persoonsgegevens van de cliënten. Surplus Welzijn heeft namelijk een Privacyreglement opgesteld. Deze zal hieronder ook terugkomen. Daarnaast zal in worden gegaan op de meldplicht datalekken en de bewerkingsovereenkomst vanuit de praktijk.

§ 4.1 Privacyreglement van Surplus Welzijn

In het Privacyreglement van Surplus Welzijn (hierna: Privacyreglement) is opgenomen dat het reglement van toepassing is op persoonsregistraties binnen Surplus Welzijn.[122] Een persoonsregistratie is een verzameling van gegevens die op diverse personen betrekking heeft en waartussen een onderling verband bestaat. Deze moeten in het kader van de hulp- of dienstverlening zijn verzameld. Uit een interview met een beleidsmedewerker[123] is naar voren gekomen dat de persoonsregistratie het aanmeldformulier in Regas is dat ingevuld moet worden als een nieuwe cliënt geregistreerd wordt in het systeem.

In het Privacyreglement staat vermeld dat het een conceptversie is. Uit een interview met een beleidsmedewerker[124] is gebleken dat het Privacyreglement nooit formeel is goedgekeurd door het managementteam. Het Privacyreglement is wel het enige document dat binnen de organisatie betrekking heeft op het verwerken van persoonsgegevens van cliënten. Daarom is dit document gebruikt voor dit onderzoek.

§ 4.1.1 Begrippen Privacyreglement toegepast in de praktijk

Persoonsgegevens

Dit zijn naar natuurlijke personen herleidbare gegevens. Deze gegevens kunnen op verschillende manieren worden vastgelegd. Dit kan audiovisueel, geautomatiseerd of schriftelijk.[125] In de praktijk is dit het veld waar de persoonsgegevens worden vermeld bij een eerste contact met een cliënt.

Houder van de persoonsregistratie

In de praktijk is dit een lid van de Raad van Bestuur (hierna: bestuurder). De bestuurder is degene die gezag heeft over de persoonsregistratie en verantwoordelijk is voor de naleving van het Privacyreglement.[126]

Beheerder van de persoonsregistratie*

Dit is de persoon die dagelijkse zorg draagt voor (een gedeelte van) de persoonsregistratie. Dit zijn in de praktijk de medewerkers. Zij staan onder verantwoordelijkheid van de bestuurder.[127]

Bewerker van de persoonsregistratie

Dit is de persoon of organisatie die het geheel of een gedeelte van de faciliteiten onder zich heeft waarmee de persoonsregistratie wordt uitgevoerd. De bewerker mag geen deel uitmaken van de organisatie en niet de houder zijn van de persoonsregistratie.[128] Bij Surplus Welzijn worden de persoonsregistraties bewerkt door Regas.

---

[121] Artikel 58 lid 2 sub a AVG.
[122] Artikel II Privacyreglement.
[123] Zie bijlage 7.
[124] Zie bijlage 7.
[125] Artikel I Privacyreglement.
[126] Artikel III Privacyreglement.
[127] Artikel I Privacyreglement.
[128] Artikel I Privacyreglement.

Gebruiker van de persoonsregistratie*
Dit is een persoon die geautoriseerd is om de persoonsregistratie in te voeren en/of wijzigingen aan te brengen of kennis te nemen van de persoonsregistratie.[129] In de praktijk zijn dit de medewerkers van Surplus Welzijn.

Geregistreerde
De persoon waarvan persoonsgegevens zijn opgenomen in de persoonsregistratie wordt de geregistreerde genoemd.[130] In de praktijk worden persoonsgegevens van cliënten opgenomen.

* In de praktijk zijn de medewerkers zowel de gebruiker als de beheerder van de persoonsregistraties. In dit hoofdstuk zal de gebruiker/beheerder omschreven worden als 'de medewerkers'.

§ 4.1.2 Doelomschrijving
Volgens artikel II van het Privacyreglement zijn persoonsregistraties hulp- en dienstverleningsgegevens. Deze hulp- en dienstverleningsgegevens worden alleen verzameld in het kader van het verwezenlijken van de doelstelling van de hulp- en dienstverlening aan de cliënt. Daarnaast worden de persoonsgegevens verzameld in het kader van beleidsvoering van de instelling, de organisatie- en beheerstaken van de instelling en het uitvoeren van onderzoek voor de hulp- en dienstverlening.[131]

In het privacyreglement is ook vermeld dat er niet meer gegevens in de registratie worden opgeslagen of bewaard dan voor het doel van de persoonsregistratie nodig is.[132]

§ 4.1.3 Verkrijgen van cliëntgegevens
In het Privacyreglement staat dat als een persoonsregistratie wordt aangemaakt, de cliënt door middel van een folder daarvan op de hoogte wordt gebracht. In die folder staat de reden waarom dit gebeurt en welke aanpak er gehanteerd wordt.[133]

Als de organisatie gegevens van een cliënt bij derden wil opvragen, moet de cliënt daar eerst toestemming voor geven.[134]

§ 4.1.4 Verplichtingen bestuurder
De bestuurder heeft een aantal taken toegewezen gekregen in het Privacyreglement. Zo dient hij zorg te dragen voor een doelmatig beheer van de hulp- en dienstverleningsgegevens, een zorgvuldige handelswijze van de gegevens bij het verkrijgen en verstrekken van die gegevens en een zorgvuldige handelswijze van de gegevens bij het uitoefenen van de rechten van de cliënten.[135]

§ 4.1.5 Verplichtingen medewerkers van Surplus Welzijn
De medewerkers moeten volgens het Privacyreglement zorgen voor de verkrijging, bewerking en het opslaan van de hulp- of dienstverleningsgegevens. Verder voeren zij de werkzaamheden uit waarvoor de bestuurder zorg draagt.[136]

---

[129] Artikel I Privacyreglement.
[130] Artikel I Privacyreglement.
[131] Artikel II Privacyreglement.
[132] Artikel II Privacyreglement.
[133] Artikel VII lid 1 Privacyreglement.
[134] Artikel VII lid 1 Privacyreglement.
[135] Artikel III lid 1 sub a tot en met c Privacyreglement.
[136] Artikel III lid 2 Privacyreglement.

§ 4.1.6 Verwerkte gegevens

In de bijlage van het Privacyreglement is vermeld welke gegevens de persoonsregistratie maximaal mag bevatten. Er worden in het begin alleen algemene cliëntgegevens opgenomen. Dit zijn gegevens zoals de contactgegevens, BSN-nummer, burgerlijke staat, leefverband, nationaliteit, inkomensbron en huisarts. Verder is het toegestaan om in het dossier aan verslaglegging te doen, een verslag op te nemen over ontvangen consulten en/of samenwerkingscontracten met derden, briefwisseling met en over de cliënt, gegevensverwerking aan derden en gegevens als die van belang zijn voor de realisatie en kwaliteit van de hulp- of dienstverlening.[137]

§ 4.1.7 Opslag van gegevens

De dossiers en gegevensverzamelingen moeten, volgens het Privcyreglement, worden opgeslagen op een plek die afsluitbaar en/of beveiligd is. Dit betekent dat er gezorgd moet worden voor afsluitbare kasten of kamers waar de dossiers veilig bewaard kunnen worden. Het ordenen van de opslag van de gegevens wordt aan de medewerkers toevertrouwd. De opslag van de gegevens moet overzichtelijk en nauwkeurig zijn. De opslag dient zo te zijn ingericht dat deze makkelijk toegankelijk is indien een cliënt een van zijn rechten uitoefent. De cliëntgegevens mogen niet onder elke voorwaarde uit de persoonsregistratie worden gelicht. Dit mag alleen indien er sprake is van toestemming van de medewerkers (beheerder) en alleen voor interne verwerking. Na het gebruik moeten de medewerkers de gegevens zo snel mogelijk opbergen in het dossier.[138]

§ 4.1.8 Aanmelding College Bescherming Persoonsgegevens

In artikel V van het Privacyreglement is vermeld dat de registratie van de cliënten aangemeld is bij het College Bescherming Persoonsgegevens (nu Autoriteit Persoonsgegevens). Tevens is vermeld onder welk nummer deze aanmelding is gedaan.

§ 4.1.9 Toegankelijkheid persoonsregistratie

In beginsel hebben alleen de medewerkers toegang tot de persoonsregistratie. Dit is niet van toepassing als[139]:

- een dringende crisis het noodzakelijk maakt dat een andere hulpverlener wordt ingeschakeld;
- de hulp- of dienstverlening wordt overgedragen (de cliënt dient hiervan op de hoogte te worden gesteld);
- een medewerker weigert veranderingen of verbeteringen aan te brengen in de gegevens van de cliënt. De bestuurder heeft dan toegang tot de persoonsregistratie. Dit kan ook in het geval van de algemene verantwoordelijkheid van de bestuurder.

Daarnaast hebben de medewerkers van de instelling (niet-hulpverleners) ook toegang tot de persoonsregistratie. Zij hebben alleen toegang voor zover dit vereist is voor de uitoefening van hun functie.

§ 4.1.10 Rechten van cliënten

<u>Recht op inzage</u>

Een cliënt kan een verzoek doen tot inzage in zijn hulp- en dienstverleningsgegevens. Dit verzoek dient schriftelijk ingediend te worden bij de bestuurder. Bij de inzage van de gegevens is altijd een medewerker aanwezig. Daarnaast heeft een cliënt ook recht op afschriften uit zijn dossier.[140]

---

[137] Artikel IV Privacyreglement.
[138] Artikel V Privacyreglement.
[139] Artikel VI lid 1 sub a tot en met d Privacyreglement.
[140] Artikel VII lid 3 Privacyreglement.

Recht op correctie
Een cliënt heeft het recht om de gegevens in zijn dossier te laten verbeteren, aan te vullen of te verwijderen. Als een cliënt dit wil, moet hij een schriftelijk verzoek indienen bij de bestuurder. Als er gegevens worden gewijzigd, dient de bestuurder de wijzigingen door te geven aan derden aan wie de gegevens zijn verstrekt.

Na afloop van het hulp- of dienstverleningstraject aan een cliënt kan hij verzoeken om zijn gegevens te laten vernietigen of anonimiseren. Als het verzoek is ingediend, heeft de bestuurder twee maanden de tijd om daarop te reageren. Als het verzoek wordt afgewezen, moet beargumenteerd worden waarom dit is gebeurd.[141]

§ 4.1.11 Bewaring en vernietiging
De cliëntgegevens in het dossier worden tot tien jaar na afloop van de hulp- en dienstverlening bewaard. Dit is niet mogelijk indien een wettelijk voorschrift zich daartegen verzet. Na afloop van de bewaartermijn zullen de gegevens worden vernietigd. Deze vernietiging moet binnen een jaar na afloop van de bewaartermijn. Surplus Welzijn hoeft niet te voldoen aan de eisen tot vernietiging als er een klacht bij de bestuurder is ingediend, de cliënt een schriftelijk verzoek heeft gedaan waarin hij een van zijn rechten wil uitoefenen of na een daartoe strekkende uitspraak op basis van een aangespannen gerechtelijke procedure.[142] Het Privacyreglement biedt ook de mogelijkheid om geanonimiseerde gegevens te bewaren.[143]

§ 4.1.12 Geheimhoudingsplicht
De medewerkers hebben, volgens het Privacyreglement, een geheimhoudingsplicht ten opzichte van iedereen. Deze geheimhoudingsplicht geldt ook als de medewerker niet meer werkzaam is bij Surplus Welzijn.[144]

§ 4.2 Meldplicht datalekken
Om een datalek te voorkomen, is in januari 2016 een mededeling[145] geplaatst op het intranet van Surplus Welzijn. In die mededeling staat vermeld dat de medewerkers zorgvuldig dienen om te gaan met hun apparatuur en dat niemand anders het wachtwoord mag weten. Er wordt ook afgeraden om persoonsgegevens van cliënten naar of van emailadressen van Hotmail of Gmail te sturen. Daarnaast wordt er geattendeerd op het feit dat er gevaren zijn als je vanaf een externe computer inlogt in het systeem. Tevens worden nog enkele tips gegeven.

Als een medewerker bijvoorbeeld een laptop van de organisatie verliest, moet diegene zo snel mogelijk contact opnemen met de afdeling ICT. Die afdeling kan er dan voor zorgen dat de informatie geblokkeerd wordt en kan maatregelen nemen. Tot slot wordt er om bewustwording gevraagd welke informatie er gedeeld wordt op sociale media. Er wordt aangeraden om communicatiekanalen van Surplus te gebruiken wanneer je met een collega wil overleggen over cliënten.

Bij de afdeling ICT is navraag gedaan hoe omgegaan wordt met een datalek. De manager ICT gaf in een interview[146] aan dat in het tweede kwartaal van 2017 gestart wordt met het

[141] Artikel VII lid 4 Privacyreglement.
[142] Artikel VII lid 5 Privacyreglement.
[143] Artikel VII lid 5 Privacyreglement.
[144] Artikel VII lid 6 Privacyreglement.
[145] Zie bijlage 4.
[146] Zie bijlage 11.

project Meldplicht Datalekken. De bestuurder gaf in het interview[147] aan dat er momenteel geen beleid is ontwikkeld hoe de organisatie omgaat als er sprake is van een datalek.

§ 4.3 Bewerkingsovereenkomst

Surplus Welzijn heeft momenteel geen bewerkingsovereenkomst met Regas. Deze informatie is verkregen uit een interview met de bestuurder.[148] De manager ICT gaf aan dat Surplus Welzijn bezig is met het ontwikkelen van een weerbare bewerkingsovereenkomst met onder andere Regas.

[147] Zie bijlage 12.
[148] Zie bijlage 12.

Hoofdstuk 5. Het verwerken van persoonsgegevens in de praktijk

Om het verwerken van persoonsgegevens in de praktijk te kunnen onderzoeken, zijn een zes medewerkers van Surplus Welzijn geïnterviewd. Daarnaast zijn nog drie medewerkers van de afdeling ICT geïnterviewd om een goed beeld te krijgen van de digitale praktijk.

§ 5.1 De aanmelding van een nieuwe cliënt

Bij het eerste cliëntcontact wordt de cliënt geregistreerd in het systeem Regas. Uit interviews is gebleken dat een cliënt niet altijd op de hoogte is van een registratie in Regas.[149] Sommige medewerkers registreren een cliënt in het systeem zonder te vertellen dat dit gebeurt en waarom. Uit interviews blijkt tevens dat niet alle medewerkers een goed beeld hebben waarom persoonsgegevens van de cliënten worden verwerkt.

Informatieplicht

In het Privacyregelement is een bepaling opgenomen dat cliënten geïnformeerd worden als er persoonsgegevens van hen wordt verwerkt. Dit zou gebeuren door middel van een folder. De afdelingen sociaal raadsliedenwerk en schuldhulpverlening hebben een gezamenlijke folder en de afdeling maatschappelijk werk heeft een eigen folder. Deze folders zijn toegevoegd in bijlage 6 en 7. In die folders staat voornamelijk aangegeven met welke problemen de cliënten geholpen kunnen worden bij de betreffende afdelingen. In deze folders wordt niet vermeld dat er een persoonsregistratie wordt aangelegd en daarmee dus persoonsgegevens worden verwerkt. Er wordt ook niet verwezen naar een eventueel Privacyreglement. Dit zou volgens de geïnterviewde beleidsmedewerker wel op de folders moeten staan. In hetzelfde interview is aangegeven dat er in het verleden gebruik werd gemaakt van inlegvellen met daarop de rechten en plichten van een cliënt. Die inlegvellen zijn gedurende dit onderzoek niet aangetroffen in de folders of op de plek waar de folders te raadplegen zijn.

Tijdens de interviews met de medewerkers is gevraagd naar de werkwijze als een nieuwe cliënt zich aanmeldt bij Surplus Welzijn. De deelnemers aan de interviews hebben niet aangegeven dat zij daarbij gebruik maken van een folder. Deze folders[150] zijn wel te raadplegen in de wachtruimtes en de spreekkamers van de bij dit onderzoek betrokken afdelingen. De cliënt heeft dus de mogelijkheid om op eigen initiatief deze folders te raadplegen. Deze folders worden niet standaard overhandigd.

Uit de interviews met de medewerkers is ook gebleken dat de cliënten niet altijd op de hoogte zijn van de registratie in Regas. Drie van de zes geïnterviewden geeft aan dit niet aan een cliënt mede te delen.

Verwerkte (bijzondere) persoonsgegevens

Om een aanmelding compleet te maken, moet en kan de medewerker een aantal (bijzondere) persoonsgegevens invullen op een persoonskaart in Regas. Om te bepalen welke gegevens van een cliënt worden verwerkt, heeft er een steekproef plaatsgevonden in de verschillende dossiers in Regas.[151] De resultaten van de onderzochte dossiers worden hieronder weergegeven.

Gegevens	Persoonsgegevens	Bijzondere persoonsgegevens	Verplicht	Niet aangetroffen*
Achternaam	**X**		**X**	
Tussenvoegsel	**X**			
Voornaam	**X**			

[149] Zie bijlage 8.
[150] Zie bijlage 5 en 6.
[151] Zie bijlage 2.

Roepnaam	X		X	
Voorletters	X			
Geslacht	X		X	
Geboortedatum	X			
BSN		X		
Titel	X		X	
Aanhef	X		X	
Land	X		X	
Postcode	X		X	
Adres	X		X	
Woonplaats	X		X	
Gemeente	X		X	
Telefoonnummer	X			
Mobiel	X			
Fax	X			X
Email	X			
Homepage	X			X
Algemene informatie	X			
Foto		X		X

§ 5.2 Verwerken van persoonsgegevens gedurende hulpverleningstraject

Tijdens het hulpverleningstraject wordt in Regas geregistreerd wat er besproken is (en welke handelingen er zijn verricht) tijdens het cliëntencontact. Niet iedere afdeling doet dat op dezelfde manier. De afdeling maatschappelijk werk heeft namelijk een andere inrichting van Regas dan de afdeling sociaal raadsliedenwerk. Bij maatschappelijk werk worden uitgebreidere gegevens gevraagd omtrent de hulpvragen. Bij de afdeling sociaal raadsliedenwerk kan een medewerker zelf bepalen wat hij in het dossier zet. Over het algemeen wordt er in de dossiers hetzelfde vermeld door de medewerkers van de verschillende afdelingen. Hierdoor is er geen onderscheid gemaakt in de verschillende afdelingen.

Managementinformatie

Bij de registratie van een cliëntcontact of handeling moeten de medewerkers een extra lijst met gegevens over een cliënt invullen. Zij zijn verplicht om de volgende punten over een cliënt te registreren: het geslacht, de leeftijdscategorie, de etnische achtergrond, de verblijfstatus, het samenlevingsverband, de (hoofd)bron van inkomsten en de hoogte van het inkomen. Voor maatschappelijk werk wordt nog gevraagd wie de huisarts van de cliënt is, waar de huisarts zijn kantoor heeft en of de cliënt woont op Fort Oranje. Deze ingevulde gegevens worden gebruikt als managementinformatie. Deze gegevens worden verstrekt aan de stakeholders van Surplus Welzijn (in dit geval de gemeente). Deze gegevens worden echter niet anoniem geregistreerd. Deze gegevens worden aan een cliënt gekoppeld.

Op de website van de Autoriteit Persoonsgegevens is de aanmelding van de registratie van de persoonsgegevens van cliënten opgezocht. Bij die melding heeft Surplus Welzijn (toen nog Stichting Markenlanden) aangegeven dat zij anonieme gegevens verstrekt aan subsidieverstrekkers.[152] Hier wordt dus de managementinformatie voor gebruikt. Deze gegevens worden dus wel anoniem verstrekt, maar worden niet anoniem opgeslagen. Ze worden opgeslagen in het dossier van een cliënt. De bestuurder gaf in het interview aan dat

[152] www.collegebeschermingpersoonsgegevens.nl/asp/orsearch.asp (zoek op: *meldingsnummer 1037758*).

deze informatie ook gebruikt wordt voor het opstellen van een jaarverslag en het constateren van trends.[153]

Documenten van cliënten
Aan twee medewerkers van Surplus Welzijn is gevraagd of zij toegang wilden verschaffen tot hun computeraccount bij Surplus Welzijn. Hierdoor was het mogelijk om te controleren welke cliëntgegevens de medewerkers op hun computer hebben staan. Op beide accounts zijn verschillende gegevens van cliënten aangetroffen. Het gaat dan om bijvoorbeeld loonstroken of de ingevulde belastingaangiftes. Deze documenten worden gedownload om de cliënten inzicht te geven in hun situatie of om ze te printen.

§ 5.3 Doeleinden

Het hoofddoel van de verwerking van persoonsgegevens is het verwezenlijken van de doelstelling van de hulp- en dienstverlening aan de cliënt.[154] De geïnterviewde medewerkers reageren tijdens het interview wisselend op de vraag wat het doel is van het registreren in Regas. Sommige medewerkers denken dat dit voornamelijk is 'voor de cijfers die het bestuur zal moeten aandragen'. Andere medewerkers bekijken deze vraag vanuit een ander oogpunt en zien dat dit bijdraagt aan de dienst- en hulpverlening aan de cliënt.

§ 5.4 Verrichte handelingen met de persoonsgegevens

Op de persoonskaart in Regas worden de contactgegevens gevraagd van een cliënt. Doordat deze gegevens geregistreerd worden, kan een van de medewerker altijd contact opnemen met de cliënt of op huisbezoek gaan.

Als een cliënt geregistreerd is, wordt door de medewerkers van Surplus Welzijn een dossier opgebouwd. Door de medewerkers wordt in Regas een samenvatting opgenomen van het gesprek met de cliënt. Daarin worden zowel adviezen als verrichte handelingen vermeld.

Niet iedere cliënt wordt steeds door dezelfde medewerker te woord gestaan. Hierdoor komt het voor dat de medewerkers de gegevens uit het dossier raadplegen om te zien wat er besproken is met de cliënt.

§ 5.5 Rechten van cliënten

Recht op inzage
Uit interviews is gebleken dat de medewerkers niet allemaal dezelfde mening hebben over het recht van inzage.[155] Drie medewerkers zouden de cliënt meteen inzage geven in het dossier. Zij staan open voor een transparante manier van werken. Twee andere medewerkers denken daar eerst goed over na of bespreken dat met een leidinggevende. Een andere medewerker weet dat er binnen Surplus Welzijn richtlijnen voor zijn. Uit het interview blijkt duidelijk dat ze op de hoogte is van wat er in het Privacyreglement bepaald is over het recht van inzage van een cliënt.

De geïnterviewde medewerkers reageren wisselend op de vraag of zij afschriften van het dossier mee zouden geven aan de cliënten. Twee medewerkers zouden dit meteen doen. Drie medewerkers zouden dit verzoek voorleggen aan een leidinggevende om te bepalen of dit wordt gehonoreerd. Een medewerker is niet bereid om een cliënt afschriften te verstrekken.

[153] Zie bijlage 12.
[154] Artikel II Privacyreglement.
[155] Zie bijlage 8.

Recht op correctie
Uit de interviews is gebleken dat de geïnterviewde medewerkers niet altijd gehoor zouden geven aan het verzoek tot wijziging van de geregistreerde gegevens.[156] Vier van de zes medewerkers zullen met de cliënt in gesprek gaan om te achterhalen waarom de gegevens gewijzigd moeten worden. Een medewerker is niet bereid om gespreksinhoudelijke informatie te wijzigen. Een andere medewerker zou dit eerst overleggen met zijn leidinggevende.

Bij het recht op correctie hoort ook het verwijderen van persoonsgegevens. Vier van de zes geïnterviewde medewerkers zou een cliënt doorverwijzen naar een leidinggevende als een cliënt vraagt om zijn persoonsgegevens te verwijderen. Twee medewerkers zijn bereid om zelf deze persoonsgegevens uit het dossier te verwijderen.

Recht op verzet
Een cliënt heeft de mogelijkheid om gebruik te maken van zijn recht op verzet. Daardoor verzoekt hij de organisatie om zijn persoonsgegevens niet meer te gebruiken. Een dergelijk verzoek zou door twee geïnterviewde medewerkers gehonoreerd worden. Drie medewerkers zouden dit verzoek voorleggen aan hun leidinggevende. Een medewerker zou hierover met de cliënt in gesprek gaan.[157]

Recht op beperking van de verwerking
Uit een interview met de functioneel applicatie beheerder is gebleken dat het technisch gezien niet mogelijk is te voorkomen dat de dossiers gewijzigd of verwijderd worden.[158]

Recht op gegevensoverdraagbaarheid
Uit een interview is gebleken dat het niet mogelijk om de gegevens van Surplus Welzijn binnen Regas over te dragen aan een andere organisatie. De functioneel applicatie beheerder geeft aan dat Surplus Welzijn een hele specifieke inrichting heeft in Regas. [159] De organisatie die de persoonsgegevens dan wil ontvangen, heeft waarschijnlijk niet hetzelfde systeem of een andere inrichting. Hierdoor kunnen zij geen gebruik maken van de data van Surplus Welzijn. Het is wel mogelijk om de dossiers uit te printen en op te sturen.

Recht op vergetelheid
Hoe dit recht in de praktijk ten uitvoer wordt gebracht, is niet nader onderzocht. De overdracht van persoonsgegevens aan derden is niet bij dit onderzoek betrokken. Hierdoor is er geen zicht op hoe dit recht in de praktijk ten uitvoer wordt gelegd.

§ 5.6 Verplichtingen bestuurder

Bewaartermijn
Bij Surplus Welzijn wordt gebruik gemaakt van een bewaartermijn van tien jaar. Tijdens een steekproef in de dossiers zijn er geen dossiers aangetroffen die de bewaartermijn van tien jaar overtreffen. De geïnterviewde beleidsmedewerker heeft aangegeven dat Surplus Welzijn sinds 2011 of 2012 gebruik maakt van Regas.[160] Hierdoor zullen er nog geen dossiers beschikbaar zijn die de bewaartermijn hebben overschreden. Uit het interview met de functioneel applicatie beheerder is gebleken dat de dossiers in Regas oneindig worden bewaard. Er zijn dus geen afspraken gemaakt over het vernietigen van dossiers.

[156] Zie bijlage 8.
[157] Zie bijlage 8.
[158] Zie bijlage 9.
[159] Zie bijlage 9.
[160] Zie bijlage 7.

Uit het interview met een medewerker is gebleken dat de papieren dossiers van de afdeling formulierenteam sinds 2014 bewaard worden.[161] Uit een controle van de papieren dossiers is echter gebleken dat het oudste dossier is aangemaakt in 2013.

Beveiliging computers

Om toegang te krijgen tot de computers van Surplus Welzijn moeten de medewerkers inloggen op Citrix Xenapp. De Xenapp is een applicatievirtualisatieoplossing die helpt bij het optimaliseren van de productiviteit met universele toegang tot virtuele apps, desktops en data vanaf elk apparaat.[162] Door in te loggen op Citrix worden de medewerkers toegelaten op het gesloten netwerk van Surplus Welzijn. Bijna alle medewerkers hebben hun eigen gebruikersnaam en wachtwoord om in te loggen op de computers. Sommige medewerkers gebruiken inlogcodes van andere collega's omdat zij geen eigen account hebben. Per 21 maart 2017 is het verplicht om elke negentig dagen het wachtwoord van de Citrix Xenapp te veranderen. Een aantal medewerkers hebben aangegeven dat zij hun wachtwoord door dit beleid hebben moeten wijzigen.

Uit een interview met een ICT-medewerker[163] is gebleken dat er elke nacht een back-up wordt gemaakt van het hele netwerk en de mail van Surplus Welzijn. Daarnaast maakt de organisatie ook gebruik van een virusscanner en een spamfilter. De manager ICT geeft nog aan dat Surplus Welzijn gebruik maakt van een managed Firewal en een Proxy-server.[164]

De functioneel applicatiebeheerder heeft aangegeven dat Surplus Welzijn jaarlijks wordt gecontroleerd op het gebied van databeveiliging.[165] Dit gebeurt door verschillende accountants.

De computers van Surplus Welzijn staan in kamers die afgesloten kunnen worden. Er is gedurende dit onderzoek verschillende keren geconstateerd dat de werknemers van Surplus Welzijn hun kamer verlaten zonder de deur op slot te doen of de computer te vergrendelen. Hierdoor is het mogelijk dat onbevoegde personen toegang krijgen tot (gevoelige) gegevens van de cliënten. Wel is er meermaals geconstateerd dat de computers en werkkamers van Surplus Welzijn aan het eind van de dag afgesloten zijn.

Beveiliging digitale dossiers

Als een medewerker gebruik wil maken van de digitale dossiers zal hij moeten inloggen op de webversie van het computersysteem Regas. Het is niet noodzakelijk om bij Surplus Welzijn aanwezig te zijn om toegang te krijgen tot Regas.

De werknemers hebben bijna allemaal een eigen inlogcode en wachtwoord voor Regas. Sommige, voornamelijk nieuwe of tijdelijke, medewerkers gebruiken inlogcodes van collega's. De betreffende collega is dan wel aanwezig en weet dat er gebruikt wordt gemaakt van zijn inlogcodes.

Het systeem zelf voldoet aan de ICT-Beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie (hierna ICT-Beveiligingsrichtlijnen).[166] De ICT-Beveiligingsrichtlijnen vormen een handleiding voor het veiliger ontwikkelen, aanbieden en beheren van webapplicaties.[167] Daarnaast geeft Regas aan dat ze voldoen aan de eisen van de NEN-7510 en dat alle data versleuteld worden via

[161] Zie bijlage 8.
[162] www.citrix.nl/ (zoek op: *Xenapp*).
[163] Zie bijlage 10.
[164] Zie bijlage 11.
[165] Zie bijlage 9.
[166] www.regas.nl/veiligheid
[167] www.ncsc.nl (zoek op: *vernieuwde ICT-beveiligingsrichtlijnen voor Webapplicaties*).

SSL.[168] De NEN-7510 geeft richtlijnen en uitgangspunten voor een organisatie in de gezondheidszorg. De richtlijnen en uitgangspunten hebben betrekking op het bepalen, instellen en in stand houden van maatregelen die getroffen moeten worden voor de beveiliging van informatievoorzieningen.[169] Doordat de data via SSL worden versleuteld, zijn ze onleesbaar voor derden.[170]

Beveiliging papieren dossiers
Tijdens de interviews is gebleken dat alleen de medewerkers van het formulierenteam gebruik maken van papieren dossiers.[171] Die dossiers worden op een later moment in Regas geregistreerd. De werknemers van het formulierenteam vinden een papieren dossier handiger om aantekeningen te maken bij een huisbezoek. Aan het eind van de dag worden de kasten met de dossiers afgesloten. Uit meerdere controles is gebleken dat beide kasten zijn afgesloten indien er niemand van het formulierenteam aanwezig is. De kamer waar de kasten in staan, is ook aan het eind van de dag afgesloten.

Meldplicht datalekken
De geïnterviewde medewerkers zouden dit melden bij de afdeling ICT of een leidinggevende.[172] Bij de geïnterviewde medewerkers is dit nog niet aan de orde geweest.

Documentatieplicht
Op dit moment wordt er door Surplus Welzijn nog niet bijgehouden of zij aan de huidige wet- en regelgeving voldoen. De geïnterviewde beleidsmedewerker geeft aan dat hij nog aan het onderzoeken is hoe Surplus Welzijn zich het best kan voorbereiden op het moment dat de AVG van toepassing is (25 mei 2018).

§ 5.7 Verplichtingen personen onder gezag bestuurder

Toegankelijkheid dossiers
Niet iedere werknemer kan alles van een cliënt zien in het dossier. De medewerkers van Surplus Welzijn kunnen wel zien of een cliënt geregistreerd is. Zij zien dan de persoonskaart met de contactgegevens van een cliënt. De medewerkers hebben niet allemaal onbeperkt toegang tot het dossier van een cliënt. Om dat te voorkomen, wordt er gebruik gemaakt van autorisaties. Uit een interview met de functioneel applicatiebeheerder is gebleken dat er gebruikersgroepen zijn ingericht. Per gebruikersgroep is dan geregeld of de medewerkers inzage of bewerkingsrechten hebben.

De functioneel applicatiebeheerder heeft aangegeven dat de accounts van werknemers die uit dienst zijn, worden geblokkeerd.[173] De leidinggevende van de oud-werknemer moet daarvoor een formulier invullen. De afdeling ICT is op dit gebied wel afhankelijk van de consequentheid van de betreffende leidinggevende.

Geheimhoudingsplicht
Om te kunnen controleren of de werknemers op de hoogte zijn van een geheimhoudingsplicht, is bij de afdeling P&O een standaardarbeidsovereenkomst opgevraagd.[174] Er is nadrukkelijk gevraagd om een contract die de werknemers van Surplus Welzijn tekenen bij het begin van hun werkzaamheden. In artikel 13 van de standaardarbeidsovereenkomst is de geheimhoudingsplicht van de werknemer opgenomen.

[168] www.regas.nl/veiligheid
[169] www.nen.nl (zoek op: *medische informatica informatiebeveiliging in de zorg*).
[170] www.netsupport.nl/2_internet/35_hosting-e-mail-en-beveiliging (klik op: *versleutelde internetverbinding (SSL)*.
[171] Zie bijlage 8.
[172] Zie bijlage 8.
[173] Zie bijlage 9.
[174] Zie bijlage 3.

Daarin is bepaald dat de werknemer een geheimhoudingsplicht heeft ten opzichte van de aan hem toevertrouwde gegevens die hij bij de uitoefening van zijn functie te weten komt. Deze plicht richt zich specifiek op de belangen van de werkgever en zijn cliënten. Doordat de werknemers van Surplus Welzijn deze arbeidsovereenkomst tekenen voordat zij in dienst treden bij de organisatie, kan ervan uit worden gegaan dat zij op de hoogte zijn van de geheimhoudingsplicht.

Tijdens de interviews met de werknemers is ook gevraagd of zij een beroepsgeheim hebben. Elke medewerker gaf aan dat hij of zij een beroepsgeheim heeft en dus niet naar buiten zal treden met de informatie over een cliënt. Opmerkelijk is wel dat een aantal geïnterviewden expliciet aangeeft daar niet voor getekend te hebben.

Hoofdstuk 6 Het privacybeleid en de praktijk van Surplus Welzijn getoetst aan de Wbp en de AVG

§ 6.1 Toepasselijkheid Wbp

Zoals aangegeven is in hoofdstuk 5 worden diverse gegevens zoals contactgegevens van cliënten geregistreerd en opgeslagen in Regas. De contactgegevens van cliënten zijn persoonsgegevens. Het opslaan van de contactgegevens van cliënten is een handeling die in de Wbp wordt gezien als verwerken.[175] Hierdoor is er sprake van het verwerken van persoonsgegevens en is de Wbp van toepassing voor Surplus Welzijn.[176]

§ 6.1.1 Verwerking van persoonsgegevens

Doeleinden

Zoals eerder is aangegeven worden de persoonsgegevens verwerkt voor het verwezenlijken van de doelstelling van de hulp- en dienstverlening aan de cliënt. Dit is in het eerste opzicht een vrij brede doelstelling. Dit komt omdat het Privacyreglement geschreven is voor geheel Surplus Welzijn en niet alleen de afdelingen die vallen onder het bereik van dit onderzoek. Onder Surplus Welzijn in Etten-Leur vallen negentien afdelingen.[177] Er wordt ook gebruik gemaakt van interne verwijzingen. Als een cliënt die bekend is bij bijvoorbeeld sociaal raadsliedenwerk beter geholpen kan worden bij maatschappelijk werk, zullen de werknemers de cliënten doorverwijzen naar die afdelingen.

Naast het hoofddoel worden in het Privacyreglement ook andere doelen genoemd. De gegevens worden namelijk ook verzameld met het oog op de beleidsvoering van de instelling, de organisatie- en beheerstaken van de instelling en het (doen) verrichten van onderzoek voor de hulp- en dienstverlening. Dit zijn concrete doelstellingen die in overeenstemming zijn met de Wbp.

In paragraaf 5.2 is aangegeven dat er in sommige gevallen loonstroken of ingevulde belastingaangiften van cliënten worden opgeslagen door individuele werknemers. Het opslaan van dergelijke gegevens draagt niet bij aan de doeleinden die Surplus Welzijn heeft geformuleerd. Dit is daarom dan ook niet toegestaan.

Rechtmatigheid van de verwerking

In het Privacyreglement wordt geen grondslag voor de verwerking genoemd. Een beleidsmedeweker heeft wel in het interview[178] aangegeven dat het gedaan wordt voor de interne dossiervorming. De verwerking van de persoonsgegevens is voor de organisatie noodzakelijk om reguliere bedrijfsactiviteiten te kunnen verrichten. Surplus Welzijn verwerkt, in dat geval, persoonsgegevens omdat het noodzakelijk is voor de behartiging van het gerechtvaardigd belang van de bestuurder.[179] [180] Als Surplus Welzijn niet aan dossiervorming zou doen, kunnen zij de cliënt niet goed helpen omdat er niet terug kan worden gekeken wat er in de voorgaande keren is besproken of gedaan. Hierdoor is het voor de organisatie toegestaan om persoonsgegevens van cliënten te verwerken.

Verwerkte persoonsgegevens

De meeste gegevens die geregistreerd worden op de persoonskaart bij de aanmelding van een nieuwe cliënt zijn noodzakelijk voor het doel dat de organisatie wil behalen met het verwerken van persoonsgegevens. De enige uitzondering is de mogelijkheid tot het registreren van de homepage van een cliënt. Het registreren van de homepage draagt niet

[175] Artikel 1 lid 1 sub b Wbp.
[176] Artikel 4 lid 1 Wbp.
[177] www.surpluswelzijn.nl (klik op: *Etten-Leur*).
[178] Zie bijlage 5.
[179] *Kamerstukken II* 1997/1998, 25892, nr. 3, p. 63.
[180] Artikel 8 sub f Wbp.

bij aan het verwezenlijken van het doel van Surplus Welzijn. De registratie van de homepage is daarom bovenmatig en niet toegestaan op grond van de Wbp.[181]

§ 6.1.2 Bijzondere persoonsgegevens

Gezondheid

In beginsel is het verboden om gegevens over de gezondheid van een cliënt te registreren. Voor Surplus Welzijn geldt echter een uitzondering. In artikel 21 lid 1 sub a Wbp is bepaald dat het voor (onder andere) maatschappelijke dienstverlening is toegestaan om persoonsgegevens over iemands gezondheid te verwerken. Het verwerken van deze bijzondere persoonsgegevens is alleen toegestaan als dit gebeurt met het oog op een goede behandeling of verzorging van een cliënt.[182] Aangezien Surplus Welzijn zich bezighoudt met maatschappelijke dienstverlening is het voor de organisatie toegestaan om persoonsgegevens over iemands gezondheid te verwerken. Hiermee handelt Surplus Welzijn in overeenstemming met de Wbp.

Ras

Regas biedt de mogelijkheid om een foto van een cliënt te registreren als hij voor het eerst wordt aangemeld bij Surplus. Een foto is een bijzonder persoonsgegeven omdat je daaruit iemands ras kan afleiden.[183] In bepaalde gevallen is het registreren van het ras toegestaan.

Aangezien het registreren van de foto niet bijdraagt aan de doelstelling van de verwerking van persoonsgegevens van Surplus Welzijn zal niet verder in worden gegaan in welke gevallen het registreren van de foto wel is toegestaan. In de dossiers is geen enkele foto aangetroffen van een cliënt. Hierdoor is het mogelijk om de doelstelling te realiseren zonder het registreren van een foto. Op dit punt handelt de organisatie in overeenstemming met de Wbp.

Burgerservicenummer

Door de medewerkers wordt regelmatig het BSN van een cliënt geregistreerd. Zoals in hoofdstuk 2 is aangegeven, is het BSN een bijzonder persoonsgegeven. Het verwerken hiervan is in sommige gevallen wel toegestaan. Deze gevallen zijn bepaald in de Wet gebruik burgerservicenummer in de zorg en de Wet algemene bepalingen burgerservicenummer. Deze wetten zijn voor Surplus Welzijn niet van toepassing omdat men geen zorgaanbieder of overheidsorgaan is. Hierdoor is het verboden voor de organisatie om het BSN van een cliënt te verwerken. Surplus Welzijn handelt, door het registreren van het BSN, in strijd met de Wbp.

§ 6.1.3 Rechten van cliënten

Recht op kennisneming

De cliënten hebben, op grond van de Wbp, het recht om te weten welke persoonsgegevens van hen verwerkt worden. Er dient een zo volledig mogelijk overzicht verstrekt te worden. In het Privacyreglement wordt deze mogelijkheid ook geboden. De cliënten hebben het recht om inzage te krijgen in hun hulp- of dienstverleningsgegevens. Ook is aangegeven dat de cliënt recht heeft op afschriften van het dossier. In het Privacyreglement staat geen termijn vermeld waarbinnen gereageerd moet worden op het verzoek van de cliënt. In het reglement staat niet wat de afschriften moeten bevatten. De Wbp spreekt over een zo volledig mogelijk overzicht met inlichtingen over het doel, de aard van de gegevens, de ontvangers en de herkomst van de gegevens. Deze bepaling uit het Privacyreglement is dus gedeeltelijk in overeenstemming met de Wbp.

[181] Artikel 11 lid 1 Wbp.
[182] Artikel 21 lid 1 sub a Wbp.
[183] Artikel 16 Wbp.

In de praktijk zijn er geen werkinstructies aangetroffen hoe er om dient te worden gegaan met een dergelijk verzoek. De geïnterviewde medewerkers geven hier ieder op hun eigen manier invulling aan.

Recht op correctie
Bij Surplus Welzijn is het mogelijk om een verzoek in te dienen tot verbetering, aanvulling of verwijdering/vernietiging van de persoonsgegevens. Deze bepaling is bijna volledig in overeenstemming met hetgeen bepaald is in de Wbp. De Wbp heeft bepaald dat binnen vier weken op een dergelijk verzoek gereageerd moet worden. Volgens het Privacyreglement moet binnen twee maanden op een dergelijk verzoek gereageerd worden. Deze bepaling is dus niet volledig in overeenstemming met de Wbp.

Voor dit verzoek van een cliënt zijn ook geen werkinstructies aangetroffen. De medewerkers gaan hier op een verschillende manier mee om.

Recht van verzet
Het recht van verzet komt niet terug in het Privacyreglement. Doordat voor dit verzoek geen instructie is opgesteld hoe de medewerkers daarmee om dienen te gaan, geven zij ieder op hun eigen manier invulling aan dit verzoek.

§ 6.1.4 Verplichtingen bestuurder

Bewaartermijn
Bij Surplus Welzijn worden de dossiers tien jaar bewaard na afloop van de hulp- en dienstverlening. Een jaar na afloop van die bewaartermijn vindt de vernietiging plaats. In de Wbp is geen concrete bewaartermijn opgenomen. De organisatie dient zelf te kijken hoe lang de gegevens nodig zijn voor het doel waarvoor ze worden gebruikt of verzameld zijn.[184] In het Privacyreglement is niet geformuleerd waarom de gegevens nog tien jaar bewaard worden na afloop van het hulp- en dienstverleningstraject. Ook is er niet bepaald waar de bewaarde gegevens nog voor worden gebruikt. Daarom kan er geconcludeerd worden dat Surplus Welzijn op dit moment niet voldoet aan de wettelijke eisen voor de bewaartermijn van persoonsgegevens.

Technische beveiligingsmaatregelen
Op het eerste oogpunt lijken de computers goed beveiligd door Surplus Welzijn. Er zijn een aantal technische beveiligingsmaatregelen getroffen om ervoor te zorgen dat er veilig gebruik van kan worden gemaakt. Surplus Welzijn gebruikt namelijk een virusscanner, spamfilter, back-ups en wachtwoorden.

De digitale dossiers worden door Regas beveiligd. Tijdens dit onderzoek is het niet mogelijk geweest om te controleren of deze beveiliging echt plaatsvindt. Regas heeft wel aangegeven dat zij een aantal beveiligingsmaatregelen heeft getroffen om veilig persoonsgegevens te kunnen verwerken in het systeem.

Over het algemeen zijn er voldoende technische beveiligingsmaatregelen getroffen. De opmerking verdient wel dat sommige medewerkers inlogcodes van andere medewerkers gebruiken. Dit is een aandachtspunt voor Surplus Welzijn. Hierdoor kunnen sommige medewerkers op het account van een andere medewerker hun gang gaan zonder dat daar de juiste persoon over kan worden aangesproken.

Organisatorische beveiligingsmaatregelen
Er is geconstateerd dat de medewerkers van Surplus Welzijn hun kamer verlaten zonder dat deze op slot is of dat de computer is vergrendeld. Hierdoor kunnen persoonsgegevens van de cliënten vrijkomen zonder dat dit de bedoeling is van de organisatie. Dit wordt ook wel

[184] www.autoriteitpersoonsgegevens.nl (zoek op: *bewaren van persoonsgegevens*).

een datalek genoemd. Hierdoor zijn er onvoldoende organisatorische beveiligingsmaatregelen getroffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verkrijging. Surplus Welzijn zal ervoor moeten zorgen dat de medewerkers meer bewust zijn van de risico's wat het handelen met zich mee brengt.

Informatieplicht
De cliënten hebben, op grond van de Wbp, het recht om te weten welke persoonsgegevens van hen verwerkt worden. Er dient een zo volledig mogelijk overzicht verstrekt te worden. In het Privacyreglement wordt deze mogelijkheid ook geboden. De cliënten hebben het recht om inzage te krijgen in hun hulp- of dienstverleningsgegevens. Ook is aangegeven dat de cliënt recht heeft op afschriften van het dossier. In het Privacyreglement staat geen termijn vermeld binnen welke termijn de bestuurder moet reageren. In reglement staat niet wat de afschriften moeten bevatten. De Wbp spreekt over een zo volledig mogelijk overzicht met inlichtingen over het doel, de aard van de gegevens, de ontvangers en de herkomst van de gegevens. Op dit punt voldoet de organisatie niet aan de Wbp.

In de praktijk is geconstateerd dat de geïnterviewde medewerkers niet actief gebruik maken van de folders. Door de medewerkers wordt ook niet altijd aan de cliënt verteld dat zij worden geregistreerd in Regas. Hierdoor handelt Surplus Welzijn zowel op het gebied van het beleid als de praktijk in strijd met de Wbp.

Meldingsplicht
In het Privacyreglement staat vermeld dat Surplus Welzijn de verwerking van persoonsgegevens heeft aangemeld bij de Autoriteit Persoonsgegevens. In het Wbp Meldingenregister is terug te vinden dat Surplus Welzijn (toen nog Stichting de Markenlanden) gemeld heeft dat er persoonsgegevens van cliënten worden verwerkt. Op dit punt handelt de organisatie in overeenstemming met de Wbp.

Meldplicht datalekken
Een beleid omtrent de melding van een datalek bij Surplus Welzijn ontbreekt. Hierdoor voldoet Surplus Welzijn niet aan de Wbp.

Verwerking door Regas
Doordat er geen bewerkingsovereenkomst is met Regas, handelt Surplus Welzijn in strijd met de Wbp.

§ 6.1.5 Verplichtingen personen onder gezag bestuurder

Toegankelijkheid
In het Privacyreglement is bepaald op welke manier de medewerkers toegang hebben tot de persoonsgegevens in Regas. Zij kunnen deze registreren en raadplegen. Hiermee geeft de bestuurder de opdracht tot het verwerken van de persoonsgegevens van de cliënten. In de praktijk is dit geregeld door middel van autorisaties. Door de afdeling ICT is bepaald welke personen toegang hebben tot welke persoonsgegevens en dossiers van cliënten. Op dit punt voldoet Surplus Welzijn aan de bepalingen uit de Wbp. In de praktijk gebruiken sommige medewerkers inlogcodes van anderen. Hierdoor wordt dit niet altijd even consequent nageleefd.

Geheimhoudingsplicht
De geheimhoudingsplicht van de medewerkers is terug te vinden in de arbeidsovereenkomsten en het Privacyreglement. De medewerkers geven ook allen zelf aan dat zij een geheimhoudingsplicht hebben. Hierdoor wordt door Surplus voldaan aan de vereisten uit de Wbp omtrent de geheimhoudingsplicht van personen onder het gezag van de bestuurder.

§ 6.1.6 Vereisten waaraan momenteel niet aan wordt voldaan (Wbp)

Hieronder is een schema opgenomen aan welke wettelijke verplichtingen de organisatie niet voldoet en hoe hoog de boete is die zij daarvoor kunnen ontvangen van de Autoriteit Persoonsgegevens.[185]

Overtreden bepaling	**Boetebrandbreedte**
Inhoud kennisgeving datalek aan Autoriteit Persoonsgegevens	Tussen € 0 en € 200.000
Inhoud kennisgeving datalek aan cliënt	Tussen € 0 en € 200.000
Wijze van kennisgeving aan cliënt over datalek	Tussen € 0 en € 200.000
Beslistermijn correctieverzoek	Tussen € 120.000 en € 500.000
Beslistermijn inzagerecht	Tussen € 120.000 en € 500.000
Beveiligingsverplichting	Tussen € 120.000 en € 500.000
Bijhouden overzicht inbreuken	Tussen € 120.000 en € 500.000
Bovenmatige gegevensverwerking	Tussen € 120.000 en € 500.000
Informatieplicht	Tussen € 120.000 en € 500.000
Overschrijden bewaartermijn	Tussen € 120.000 en € 500.000
Meldplicht datalekken aan Autoriteit Persoonsgegevens	Tussen € 120.000 en € 500.000
Meldplicht datalekken aan cliënt	Tussen € 120.000 en € 500.000
Recht van verzet	Tussen € 120.000 en € 500.000
Te verstrekken informatie bij informatieplicht	Tussen € 120.000 en € 500.000
Gebruik burgerservicenummer	Tussen € 350.000 en € 820.000
Verbod verwerking bijzonder persoonsgegevens	Tussen € 350.000 en € 820.000

§ 6.2 Toepasselijkheid AVG

De AVG is, net als de Wbp, van toepassing op het verwerken van persoonsgegevens. In § 6.1 is er aangegeven dat er sprake is van het verwerken van persoonsgegevens. Hierdoor zal daar in dit hoofdstuk niet verder op in worden gegaan. In de komende paragrafen worden alleen de wijzigingen van de AVG ten opzichte van de huidige wet- en regelgeving besproken.

§ 6.2.1 Rechten cliënten

Recht op beperking van de verwerking en gegevensoverdraagbaarheid

Deze verplichtingen zijn (nog) niet opgenomen in het Privacyreglement. Hierover zijn binnen de organisatie (nog) geen regels bepaald hoe invulling gegeven moet worden aan dergelijke verzoeken van cliënten. In de praktijk is de uitvoering van deze rechten ook niet mogelijk. Dit zal aangepast moeten worden om in de toekomst te kunnen voldoen aan de AVG.

Recht op vergetelheid

In het Privacyreglement is de mogelijkheid tot het verwijderen van hulp- en dienstverleningsgegevens opgenomen. Hiervoor kan een cliënt een verzoek indienen bij de bestuurder. Als het verzoek wordt gehonoreerd, wordt dit ook doorgegeven aan derden die de gegevens hebben ontvangen. Deze bepaling is in overeenstemming met artikel 17 lid 2 AVG. Deze bepaling is, zoals in hoofdstuk 5 is aangegeven, niet verder onderzocht.

[185] Artikel 2 lid 1 en 2, 3 lid 1 en 2 jo. artikel 4 lid 1 en 2 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.

§ 6.2.2 Verplichtingen bestuurder

Documentatieplicht

De beleidsmedewerker heeft tijdens het interview aangegeven dat er op dit moment nog niet is voldaan aan de documentatieplicht uit artikel 30 AVG.

Informatieplicht

Zoals eerder is aangegeven voldoet de organisatie niet aan de informatieplicht uit de Wbp. Met de komst van de AVG wordt deze informatieplicht uitgebreid. Aan die plicht voldoet de organisatie op dit moment niet.

Privacy impact assessment

In hoofdstuk 3 is de PIA besproken. Privacyrisico's van bestaande en nieuwe verwerkingen worden blootgelegd. Ook draagt het bij aan het vermijden en verminderen van privacyrisico's. In de AVG worden een aantal gronden genoemd wanneer een PIA moet worden uitgevoerd. Een van die gronden is de grootschalige verwerking van bijzondere persoonsgegevens. Bij Surplus Welzijn is hiervan sprake omdat van iedere cliënt de etnische achtergrond registreren bij het aanmaken van een handeling in Regas. Aangezien dit gedurende een langere periode gebeurt, dit gevoelige persoonsgegevens zijn en op veel verschillende locaties van Surplus Welzijn, kan er geconcludeerd worden dat de organisatie zich bezighoudt met grootschalige verwerking van bijzondere persoonsgegevens. Hierdoor zal de organisatie een PIA moeten uitvoeren.

Meldplicht datalekken

In paragraaf 6.1.4 is aangegeven dat een beleid voor een melding van een datalek ontbreekt. Hierdoor voldoet Surplus Welzijn nog niet aan de vereisten die de AVG stelt voor het melden van een datalek.

Verwerking door Regas

Zoals al eerder is aangegeven, heeft Surplus Welzijn geen bewerkingsovereenkomst met Regas. Hierdoor voldoet Surplus Welzijn niet aan de vereisten van de AVG.

§ 6.2.3 Profilering

Door de medewerkers worden persoonsgegevens van cliënten opgeslagen. Sommige van deze gegevens worden gebruikt voor managementinformatie. Zoals in hoofdstuk 5 is aangegeven, worden deze gegevens gebruikt voor het opstellen van een jaarverslag en het constateren van trends. Surplus Welzijn maakt daarom een analyse van de persoonsgegevens. Hierdoor is er sprake van profilering. Dit is alleen toegestaan als er sprake is van een van de rechtsgronden van de verwerking van persoonsgegevens. Daarvan is hier geen sprake. Daarom is het voor Surplus Welzijn niet toegestaan om gebruik te maken van profilering.

§ 6.2.4 Functionaris voor de gegevensbescherming

Voor Surplus Welzijn is het niet noodzakelijk om een FG aan te stellen. Zij zijn namelijk geen overheidsinstantie/orgaan en houden zich niet bezig met stelselmatige observatie. De organisatie houdt zich wel bezig met het verwerken van bijzondere persoonsgegevens. Dit is echter niet de hoofdtaak van de bestuurder. De verwerking van de persoonsgegevens is een nevenactiviteit.[186]

Op grond van de AVG is niet verplicht om een FG aan te stellen. Een beleidsmedewerker en de bestuurder hebben aangegeven dat Surplus Welzijn wel een FG gaat aanstellen. Hierdoor staan de eisen en taken van de FG wel vermeld in dit onderzoeksrapport.

[186] Autoriteit Persoonsgegevens 2017, p. 5.

§ 6.2.5 Vereisten waaraan momenteel niet aan wordt voldaan (AVG)

Naast het overtreden van de bepalingen uit de Wbp overtreedt Surplus Welzijn ook een paar bepalingen uit de AVG. Hieronder is een overzicht opgenomen welke bepalingen er uit de AVG zijn overtreden. De bepalingen die op grond van de Wbp zijn overtreden, komen niet terug in dit overzicht.

Overtreden bepaling	**Maximale boete**
Documentatieplicht	€ 10.000.000
PIA	€ 10.000.000
Recht op gegevensoverdraagbaarheid	€ 20.000.000
Recht op beperking van de verwerking	€ 20.000.000

Hoofdstuk 7 Aanbevelingen en plan van aanpak

§ 7.1 Aanbevelingen

Gedurende dit onderzoek is er gezocht naar een passend antwoord op de volgende centrale vraag: welke aanbevelingen voor de wijze waarop de afdelingen sociaal raadsliedenwerk, schuldhulpverlening en maatschappelijk werk van Surplus Welzijn in Etten-Leur, persoonsgegevens van cliënten verwerken, vloeien voort uit een toets van het privacybeleid en de praktijk bij deze afdelingen, aan de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming? Hieronder zijn aanbevelingen opgenomen die voortvloeien uit dit onderzoek. Deze aanbevelingen zouden ervoor kunnen zorgen dat Surplus Welzijn in de toekomst wel voldoet aan het wettelijk kader voor de verwerking van persoonsgegevens.

Aanbevelingen die voortvloeien uit de toets van de Wbp aan het beleid en de praktijk

Bewerkingsovereenkomst

Momenteel heeft Surplus Welzijn geen bewerkingsovereenkomst met Regas. Naar aanleiding van dit onderzoek wordt aanbevolen om op korte termijn een adequate bewerkingsovereenkomst af te sluiten met Regas. Daarin zullen in ieder geval bepalingen moeten worden opgenomen over de geheimhoudingsplicht, de vertrouwelijkheid, de beveiliging van de gegevensverwerking en de meldplicht datalekken.

Bewustwording medewerkers

Uit de interviews is gebleken dat de medewerkers onvoldoende op de hoogte zijn van het wettelijk kader van de verwerking van persoonsgegevens van cliënten en het Privacyreglement. Om ervoor te zorgen dat de medewerkers niet bovenmatige persoonsgegevens van cliënten registreren, zullen zij ingelicht moeten worden door de organisatie. Dit kan door middel van werkinstructies of cursussen. Hierdoor wordt er in de toekomst voorkomen dat er te veel (bijzondere) persoonsgegevens worden verwerkt en dus in strijd wordt gehandeld met het wettelijk kader. Daarnaast zullen de medewerkers op de hoogte gebracht moeten worden hoe zij een datalek kunnen voorkomen en welke handelingen zij dienen te verrichten als er zich een datalek voordoet bij de organisatie.

Informatieplicht

De cliënten dienen op de hoogte te worden gesteld van het feit dat er persoonsgegevens van hen worden verwerkt. Zoals eerder aangegeven zou dit door middel van folders moeten gebeuren. Dit gebeurt momenteel echter niet. Om een cliënt toch op de hoogte te stellen van het feit dat er persoonsgegevens worden verwerkt, kan de organisatie ervoor kiezen om voortaan te gaan werken met toestemmingsformulieren. De toestemmingsformulieren moeten de identiteit van de bestuurder en de doeleinden van de verwerking bevatten.

Inlogcodes

Surplus Welzijn dient ervoor te zorgen dat iedere medewerker een eigen inlogcode heeft voor de toegang tot de computers en Regas. Dit geldt ook voor invalkrachten en stagiaires. Hierdoor kan de organisatie beter controleren wie welke handelingen heeft verricht. Als een medewerker handelingen heeft verricht die volgens de organisatie niet toegestaan zijn, kan de juiste persoon daarover worden aangesproken.

Vernieuw het Privacyreglement

Het huidige Privacyreglement is gedateerd en nooit officieel vastgesteld. Daarom is het van belang dat de organisatie een nieuw privacybeleid opstelt. Daarin zal de organisatie onder andere moeten vermelden hoe zij omgaat met de rechten van een cliënt, hoe de bewaartermijn wordt nageleefd en hoe er om moet worden gegaan met een datalek. Daarnaast dient de organisatie ook regelmatig te controleren of dit beleid op een juiste manier wordt uitgevoerd. Dit kan de organisatie doen door middel van interne of externe audits.

Bij interne audits controleren eigen medewerkers andere afdelingen van Surplus Welzijn of zij voldoen aan het afgesproken beleid. De medewerkers die de interne audits uitvoeren, worden auditoren genoemd en hebben daarvoor een speciale opleiding of training gevolgd. Zij geven de organisatie een advies welke verbeterpunten er nog zijn. Surplus Welzijn zou ook kunnen kiezen voor een externe organisatie die de audit uitvoert.

Aanbevelingen die voortvloeien uit de toets van de AVG aan het beleid en de praktijk

Documentatieplicht

Uit het onderzoek is naar voren gekomen dat de organisatie momenteel niet voldoet aan de documentatieplicht uit de AVG. De documentatieplicht houdt in dat de organisatie zelf moet aan tonen dat zij de juiste maatregelen hebben genomen om aan de AVG te voldoen. Surplus Welzijn zal daarom een document moeten opstellen waarin de volgende punten naar voren komen:

- de naam en contactgegevens van de bestuurder;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van cliënten en persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de beoogde bewaartermijn;
- een beschrijving van de technische en organisatorische beveiligingsmaatregelen.

FG aanstellen

Uit dit onderzoek is gebleken dat Surplus Welzijn niet verplicht is om een FG aan te stellen. De organisatie is dit wel van plan. Dit blijkt onder andere uit het interview met de bestuurder. De organisatie moet daarom wel rekening houden met de wettelijke voorwaarden en taken van een FG. Hierdoor wordt Surplus Welzijn aangeraden om alvast te oriënteren welk functieprofiel de toekomstig FG moet hebben. Aangezien de FG als toezichthouder onafhankelijk moet zijn, wordt aangeraden om een externe FG aan te stellen. Hiermee wordt voorkomen dat de organisatie de schijn wekt van belangenverstrengeling.

Informatieplicht

Zoals hierboven is aangegeven moeten er toestemmingsformulieren komen om te voldoen aan de informatieplicht uit de Wbp. Om aan de informatieplicht uit de AVG te voldoen, moeten de voorgenomen toestemmingsformulieren uitgebreid worden met de volgende gegevens:

- de identiteit van de vertegenwoordiger van de bestuurder;
- de identiteit van de FG;
- de gerechtvaardigde belangen van de bestuurder;
- de ontvangers van de persoonsgegevens;
- de bewaartermijn van de persoonsgegevens;
- de rechten de cliënten toekomen;
- de mogelijkheid tot het indienen van een klacht bij de Autoriteit Persoonsgegevens.

Deze toestemmingsformulieren moeten door de organisatie bewaard worden en een kopie kan verstrekt worden aan de cliënt.

PIA uitvoeren

Uit dit onderzoek is gebleken dat Surplus Welzijn een PIA moet uitvoeren aangezien zij zich bezighouden met grootschalige verwerking van bijzondere persoonsgegevens. Door het uitvoeren van de PIA wordt gekeken welke privacyrisico's van toepassing zijn voor Surplus Welzijn. Daarnaast kan gekeken worden op welke wijze de privacyrisico's verminderd kunnen worden. Op de website van de Beroepsorganisatie van IT-auditors NOREA is een

handreiking beschikbaar voor de uitvoering van een PIA. In die handreiking is ook een vragenlijst geformuleerd.

Privacy by design en privacy by default
Als gekeken is welke privacyrisico's er zijn bij Surplus Welzijn dient de organisatie deze op een juiste manier af te dekken. Daarbij dient de organisatie rekening te houden met privacy by design en privacy by default. Hierdoor wordt gezorgd voor een juiste beveiliging van de persoonsgegevens bij het ontwerpen van producten of diensten. Er moeten technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat er alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor de specifieke doeleinden van de organisatie.

Een technische maatregel die in ieder geval door Surplus Welzijn genomen moet worden is het aanpassen van Regas. Uit dit onderzoek is namelijk gebleken dat er niet wordt voldaan aan het beginsel van dataminimalisatie. Er is sprake van bovenmatige gegevensverwerking. Om dit in de toekomst te voorkomen is het van belang dat het veld waarin de persoonsgegevens worden vermeld, wordt verkleind. Hierdoor is de kans kleiner dat medewerkers persoonsgegevens registreren die niet noodzakelijk zijn voor de hulp- en dienstverlening aan een cliënt. Hiermee wordt voorkomen dat er sprake is van bovenmatige verwerking van persoonsgegevens. De gegevens die niet geregistreerd hoeven te worden zijn foto's, faxnummer, burgerservicenummer en homepage.

Een andere technische maatregel is het anoniem registreren van managementinformatie. Uit dit onderzoek is gebleken dat de organisatie de managementinformatie op een manier verwerkt die herleidbaar is tot een cliënt. Deze informatie wordt door de organisatie alleen gebruikt voor het jaarverslag en om te verantwoorden aan de subsidieverstrekkers. Hierdoor is het niet noodzakelijk om deze gegevens op te slaan op een manier die herleidbaar is tot een cliënt. Als deze gegevens anoniem worden verwerkt, zijn ze niet herleidbaar tot een natuurlijk persoons en is de Wbp en de AVG niet van toepassing.

Uit dit onderzoek is gebleken dat de computers niet worden altijd vergrendeld als een medewerker niet aanwezig is. De organisatie zou kunnen instellen dat de computers automatisch worden vergrendeld na een bepaalde tijdsduur. Dit is dan ook een derde technische maatregel die de organisatie zou kunnen treffen.

Vernieuw het Privacyreglement
In het nieuwe Privacyreglement zullen ook bepalingen moeten worden opgenomen hoe om wordt gegaan met de nieuwe rechten van een cliënt.

Algemene aanbevelingen
Indien aan bovenstaande is voldaan is het van belang dat huidige en toekomstige medewerkers goed op de hoogte worden gebracht van het nieuwe beleid en de werkwijzen in de praktijk. Het is van belang dat vanuit het management sturing plaatsvindt dat dit beleid ook wordt ingevoerd op de verschillende afdelingen. Daarnaast is regelmatig evaluatie en bijstelling noodzakelijk. De risico's voor Surplus Welzijn zijn vrij groot indien dit beleid onvoldoende wordt uitgevoerd en geborgd.

Aanvullend onderzoek
Het verstrekken van persoonsgegevens aan derden is niet meegenomen in dit onderzoek. Hierdoor is het onduidelijk of de organisatie wel aan deze wettelijke eisen voldoet. Het wordt daarom ook aangeraden om aanvullend onderzoek te doen of de organisatie op dit punt wel voldoet aan de huidige en toekomstige wet- en regelgeving omtrent het verstrekken van persoonsgegevens aan derden. Bij het schenden van die bepalingen kan de Autoriteit Persoonsgegevens ook boetes opleggen.

§ 7.2 Plan van aanpak

In de vorige paragraaf zijn een aantal aanbevelingen geformuleerd. Het zal voor de organisatie niet gemakkelijk zijn om alle aanbevelingen zo snel mogelijk op te volgen. Surplus Welzijn zal als eerst moeten zorgen dat men aan de Wbp voldoet. Dat is namelijk het huidige wettelijk kader. Als dit gerealiseerd is, moet de organisatie ervoor zorgen dat men uiteindelijk voldoet aan de AVG. Hierdoor is een prioriteitenlijst opgesteld welke aanbevelingen als eerste moeten worden opgevolgd.

Als allereerste zal Surplus Welzijn een bewerkingsovereenkomst moeten afsluiten met Regas. Dit is een vereiste waaraan een organisatie moet voldoen als zij de persoonsgegevens laat verwerken door een andere organisatie.

Als tweede zal de organisatie toestemmingsformulieren voor het verwerken van persoonsgegevens gaan ontwikkelen. Hierdoor wordt in de toekomst wel voldaan aan de informatieplicht die geldt op grond van de Wbp (en AVG). De organisatie dient daarbij wel rekening te houden met de extra vereisten die gaan gelden op het moment dat de AVG in werking treedt. Om de organisatie een helpende hand te bieden, is een voorbeeld toestemmingsformulier opgesteld. Dit is opgenomen in bijlage 13.

Vervolgens zal de organisatie moeten zorgen voor voldoende inlogcodes voor iedere medewerker en dat de computers naar verloop van tijd automatisch vergrendelen. Hiervoor zal de afdeling ICT zorg voor dragen. Daarnaast dienen zij ervoor te zorgen dat het veld, waarin persoonsgegevens worden vermeld, verkleind wordt en dat de managementinformatie voortaan anoniem wordt vastgelegd.

Daarna zal de organisatie het Privacyreglement, wat zij in conceptversie heeft, grondig moeten aanpassen. Dit reglement moet worden aangepast om in de toekomst te voldoen aan de AVG. Als dit is gebeurd, zal de organisatie de medewerkers op de hoogte moeten stellen van het geformuleerde beleid. De medewerkers zijn zich dan bewust welke acties zij moeten ondernemen als een cliënt bijvoorbeeld gebruik maakt van zijn recht op inzage. Hierdoor wordt ook privacy bewustwording gecreëerd.

Nadat de medewerkers op de hoogte zijn gebracht van het Privacyreglement zal de organisatie moeten zorgen dat er wordt voldaan aan de documentatieplicht. Met documenten moet men aantonen dat de organisatie aan de AVG voldoet.

Tot slot zal de organisatie een PIA moeten uitvoeren. Daaruit zullen privacyrisico's voortvloeien die van toepassing zijn voor de organisatie en hoe die verminderd kunnen worden. Bij de aanpassingen die de organisatie dan nog zal gaan doen, moet zij rekening houden met privacy by design en privacy by default.

De organisatie zal wel haast moeten maken bij het volgen van deze aanbevelingen. Surplus Welzijn zal ervoor moeten zorgen dat zij op 25 mei 2018 voldoet aan de privacywetgeving die dan van toepassing is.

Bronnenlijst

Literatuur

Berkvens en Prins 2007
J.M.A. Berkvens en J.E.J. Prins, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007.

De Jong, *AA* 2016
J.P. de Jong, 'De Algemene verordening gegevensbescherming', *AA* 2016, afl. 10, p. 770-773.

De Vries & Goudsmit, *NJB* 2016
H.H. de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming', *NJB* 2016, afl. 22, p. 1553-1560.

Goudsmit, *Bb* 2015/53
M. Goudsmit, 'Wet meldplicht datalekken en uitbreiding boetebevoegdheid CBP', *Bb* 2015/53, afl. 16, p. 184-185.

Hijmans, *NJB* 2016
H. Hijmans, 'De bescherming van persoonsgegevens: De taak van de Europese Unie de rechtsstaat inhoud te geven en de rol van de onafhankelijke autoriteiten', *NJB* 2016, afl. 16, p. 1092-1098.

Kranenborg en Verhey 2011
H.R. Kranenborg en L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.

Van Schaaijk 2011
G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*', Den Haag: Boom Juridische Uitgevers 2011.

Handleidingen

Autoriteit Persoonsgegevens 2015
Autoriteit Persoonsgegevens, *De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp): Beleidsregels voor toepassing van artikel 34a van de Wbp*, Den Haag: Autoriteit Persoonsgegevens 2015.

Autoriteit Persoonsgegevens 2017
Autoriteit Persoonsgegevens, *Richtlijnen voor functionarissen voor de gegevensbescherming (FG's)*, Den Haag: Autoriteit Persoonsgegevens 2017.

NOREA 2015
NOREA, *Privacy impact assessment (PIA): introductie, handreiking en vragenlijst*, Amsterdam: NOREA 2015.

Sauerwein en Linnemann 2002
L.B. Sauerwein en J.J. Linneman, *Handleiding Wet bescherming persoonsgegevens*, Den Haag: Ministerie van Justitie 2002.

Verslagen

Surplus 2015
Surplus, *Jaardocument Surplus 2015*, Zevenbergen: Surplus 2015.

Elektronische bronnen
Www.autoriteitpersoonsgegevens.nl

Www.citrix.nl

Www.collegebeschermingpersoonsgegevens.nl

Www.datalekken.autoriteitpersoonsgegevens.nl

Www.duthler.nl

Www.justitia.nl

Www.ncsc.nl

Www.nen.nl

Www.netsupport.nl

Www.regas.nl

Www.surplus.nl

Www.surpluswelzijn.nl

Parlementaire documenten
Kamerstukken II 1997/1998, 25892, nr. 3.

Kamerstukken II 2014/2015, 33662, nr. 9.