Zorg voor privacy!

‘Een praktijkgericht juridisch onderzoek naar de huidige en nieuwe privacywet- en regelgeving’

Zeggelaan 110
4844 SK Terheijden
www.sovak.nl

Bo le Sage
SOVAK
Waalwijk, 30 mei 2016

Zorg voor privacy!

‘Een praktijkgericht juridisch onderzoek naar de huidige en nieuwe privacywet- en regelgeving’

Auteur:	**Bo le Sage (2069512)**
Onderwijsinstelling:	**Juridische Hogeschool Avans-Fontys te Tilburg**
Afstudeerorganisatie:	**SOVAK**
Afstudeermentor:	**De heer D. Koreman**
1e docent:	**Mevrouw mr. C.A.M. van der Voort**
2e docent:	**Mevrouw mr. N. Vermijs**
Afstudeerperiode:	**Februari 2016 – mei 2016**

Waalwijk, 30 mei 2016

Voorwoord

Voor u ligt het onderzoeksrapport ‘Zorg voor privacy!’ welke is geschreven in het kader van de afsluiting van mijn opleiding HBO Rechten aan de Juridische Hogeschool te Tilburg. Van januari tot en met mei heb ik dit onderzoek uitgevoerd en geschreven in opdracht van SOVAK. De vraag die in dit onderzoeksrapport centraal staat is: *‘Welke aanpassingen nodig zijn in het beleid en de werkwijze van SOVAK als gevolg van de invoering van de AVG en de Meldplicht datalekken en uitbreiding boetebevoegdheid, ten aanzien van de verwerking van persoonsgegevens van cliënten?*’.

De uitvoering en uiteenzetting van dit onderzoek waren niet altijd even makkelijk. Via deze weg wil ik daarom ook graag mijn stagementor Dennis Koreman bedanken voor alle hulp die hij mij heeft geboden bij het tot stand brengen van dit onderzoeksrapport. Ook wil ik graag mijn stagedocent Caro van der Voort bedanken voor de begeleiding tijdens mijn afstuderen en haar feedback op mijn stukken.

Tot slot wil ik graag mijn dank uitspreken aan SOVAK voor het bieden van een leerzame afstudeertijd. Uiteraard wil ik ook alle collega’s bij SOVAK bedanken voor de aangename samenwerking en hun medewerking aan mijn onderzoeksrapport.

Ik wens u veel plezier bij het lezen van het onderzoeksrapport ‘Zorg voor privacy!’.

Bo le Sage,

Waalwijk, mei 2016

Inhoudsopgave

Bijlagen

Samenvatting

SOVAK is een zorginstelling die zich richt op het bieden van zorg en ondersteuning aan mensen met een verstandelijke beperking. SOVAK beschikt over enorm veel persoonsgegevens van cliënten. Het waarborgen van de privacy van cliënten is belangrijk, omdat het gaat om een kwetsbare doelgroep. De wet- en regelgeving omtrent privacy spelen derhalve een grote rol in een organisatie zoals SOVAK. De huidige privacyregelgeving, de Wet bescherming persoonsgegevens (hierna Wbp), is gebaseerd op de Europese Richtlijn uit 1995. Gezien de technische ontwikkelingen is de snelheid en hoeveelheid waarin gegevens worden verzameld enorm gestegen. De richtlijn uit 1995 biedt onvoldoende waarborgen om de privacy van individuen optimaal te beschermen. De Europese Commissie heeft daarom in 2012 de Algemene verordening gegevensbescherming gepresenteerd (hierna AVG). De AVG is formeel aangenomen op 27 april 2016 en zal in 2018 in werking treden. De verordening zal de Wbp volledig vervangen. Om vooruit te lopen op de AVG is op 1 januari 2016 de Wet meldplicht datalekken en de uitbreiding boetebevoegdheid AP opgenomen in de Wbp.

Dit onderzoeksrapport geeft een overzicht aan SOVAK in hoeverre het beleid en de werkwijze van SOVAK met betrekking tot het verwerken van persoonsgegevens voldoet aan de huidige privacyregelgeving en welke aanpassingen er nodig zijn ten opzichte van de nieuwe privacyregelgeving.

Uit onderzoek is gebleken dat SOVAK nog niet geheel voldoet aan de bepalingen uit de Wbp. De in de wet voorgeschreven bewaartermijnen worden niet nageleefd en de beveiligingsmaatregelen op organisatorisch gebied schieten te kort. De beveiligingsmaatregelen spelen derhalve een grote rol met het oog op de Meldplicht datalekken. Een tekortschietende beveiliging brengt namelijk een grote kans op datalekken met zich mee. De meldplicht datalekken verplicht organisaties voortaan om datalekken te melden wanneer deze ernstige nadelige gevolgen kunnen hebben. Tevens is uit onderzoek gebleken dat de AVG een aantal nieuwe verplichtingen met zich mee brengt. Zo wordt SOVAK verplicht een functionaris voor de gegevensbescherming aan te stellen, het privacybeleid aan te passen en een Privacy Impact Assesment uit te voeren. Daarnaast introduceert de AVG de algemene documentatieverplichting en wordt de informatieplicht uitgebreid. Ook worden er nieuwe rechten voor betrokkenen gepresenteerd. Zij hebben voortaan het recht om vergeten te worden en het recht op dataportabiliteit. Tenslotte is het toestemmingscriterium voor de gegevensverwerking aangescherpt. SOVAK zal voortaan toestemming moeten vragen aan de betrokkene om persoonsgegevens te mogen verwerken.

De belangrijkste aanbeveling is om meer privacybewustzijn in de organisatie te creëren door middel van het opstellen van werkinstructies en protocollen. Uit onderzoek is namelijk naar voren gekomen dat medewerkers onvoldoende op de hoogte zijn van de verplichtingen die voortvloeien uit de privacywetgeving. Dit zal tevens bijdragen aan het beveiligingsniveau op organisatorisch gebied. Daarnaast is het belangrijk dat in het kader van de Meldplicht datalekken een datalekbeleid en datalekprotocol worden opgemaakt. Het datalekbeleid kan helpen bij het snel en adequaat handelen wanneer een datalek wordt geconstateerd. Een datalekprotocol daarentegen zorgt ervoor dat de medewerkers zich bewust worden van het risico op datalekken. Een datalekprotocol kan helpen om menselijke fouten zoveel mogelijk te voorkomen.

Het is van groot belang om te voldoen aan de eisen die de privacywetgeving stelt. De bevoegdheid voor het opleggen van boetes is namelijk enorm uitgebreid. Wanneer niet wordt voldaan aan de bepalingen uit de privacywetgeving kan de toezichthouder boetes opleggen tot € 1.000.000,- en tot 0,5% tot 2% van de wereldwijze jaaromzet.

Lijst van afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
EU	Europese Unie
EVRM	Europees Verdrag tot Bescherming van de Rechten van de Mens
FG	Functionaris voor de gegevensbescherming
GW	Grondwet
IVBP	Verdrag Inzake Burgerrechten en Politie rechten
PIA	Privacy Impact Assessment
POS	Persoonlijk ondersteuningsplan
UVRM	Universele Verklaring voor de Rechten van de Mens
VN	Verenigde Naties
Wbp	Wet bescherming persoonsgegevens
Wet Bopz	Wet bijzondere opnemingen in psychiatrische ziekenhuizen
WGBO	Wet op de geneeskundige behandelingsovereenkomst
Wpr	Wet persoonsregistratie

Begrippenlijst Wbp

Persoonsgegeven
Het begrip persoonsgegeven wordt in de wet omschreven als '*elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*'. Onder elk gegeven wordt niet alleen informatie in geschreven tekst verstaan, maar ook informatie in beeld en geluid.[1] De persoon waar de gegevens betrekking op hebben moet identificeerbaar zijn. Een persoon is identificeerbaar als naar aanleiding van het gegeven de identiteit van de persoon zonder te veel inspanning kan worden vastgesteld. De gegevens moeten een natuurlijk persoon betreffen. Is de persoon niet identificeerbaar of gaat het niet om een natuurlijk persoon, dan is het gegeven geen persoonsgegeven.

Verwerking
In de wet wordt het begrip verwerking omschreven als: *'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens'*. Dit is een niet uitputtende lijst van handelingen die als verwerking moeten worden aangemerkt. De voorwaarde is wel dat er sprake moet zijn van een feitelijke macht over de gegevens.[2]

Bestand
Onder het begrip bestand wordt verstaan: '*elk gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen'*. Dit wil zeggen dat de gegevens onderlinge samenhang moeten hebben en dat het systeem systematisch toegankelijk moet zijn. Een bestand kan geautomatiseerde of niet-geautomatiseerde verwerkingen bevatten. Als het gaat om niet-geautomatiseerde verwerkingen, dan vallen alleen bestanden binnen de reikwijdte van de Wbp. Een ongestructureerd cliëntdossier valt dus niet onder reikwijdte van de Wbp. Een gesystematiseerde verzameling van een cliëntdossier wel. [3]

Verantwoordelijke
De verantwoordelijke wordt gedefinieerd als: '*de natuurlijke persoon, rechtspersoon, bestuursorgaan of ieder ander die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.'* De verantwoordelijke is verantwoordelijk voor de gehele verwerking van persoonsgegevens. Het gaat om degene die formeel bevoegd is om beslissingen te nemen en niet om degene die feitelijk de beslissingen neemt.[4]

Betrokkene
De 'betrokkene' is degene op wie een persoonsgegeven betrekking heeft. Eenmaal aangemerkt als betrokkene kan beroep worden gedaan op verschillende rechten die in de Wbp zijn neergelegd.

Bewerker
De bewerker is omschreven als degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen. De bewerker is dus een persoon of instelling die buiten de organisatie van de verantwoordelijke staat. De bewerker treedt op ten behoeve van de verantwoordelijke. Hij handelt dus onder

[1] Kranenborg & Verhey 2011, p. 60
[2] Kranenborg & Verhey 2011, p. 66
[3] Kranenborg & Verhey 2011, p. 67
[4] Kranenborg & Verhey 2011, p. 76

diens verantwoordelijkheid. Dit betekent dat hij uitsluitend gegevens verwerkt volgens de instructies van de verantwoordelijke.[5]

Derde
Een derde is iedereen met uitzondering van: de betrokkene, de verantwoordelijke, de bewerker en personen die onder rechtstreeks gezag van de verantwoordelijke of bewerker bevoegd zijn persoonsgegevens te verwerken. Het begrip ‘derde’ speelt een rol bij het verstrekken van bepaalde gevoelige gegevens.[6]

Autoriteit persoonsgegevens
Dit is het bestuursorgaan dat in Nederland toezicht houdt op organisaties die persoonsgegevens verwerken. Dit bestuursorgaan werd tot 2016 het College bescherming persoonsgegevens genoemd.

[5] Kranenborg & Verhey 2011, p. 76
[6] Kranenborg & Verhey 2011, p. 77

1. Inleiding

§ 1.1 Organisatiebeschrijving

SOVAK is een organisatie die actief is in het bieden van zorg en ondersteuning aan mensen met een verstandelijke beperking. Het is een organisatie met ongeveer 900 medewerkers, 500 vrijwilligers en 700 cliënten. Het doel van de organisatie is het bijdragen aan de kwaliteit van het bestaan van de mensen die aan de zorgen van SOVAK zijn toevertrouwd. SOVAK ondersteunt cliënten, volwassenen, kinderen en ouderen van alle niveaus bij wonen, werken en vrijetijd. SOVAK wil met name uitblinken in de zorg voor cliënten met ernstige meervoudige beperkingen, zeer ernstige beperkingen in combinatie met gedragsproblemen, autisme en voor oudere cliënten. De diensten die SOVAK aanbiedt zijn onder andere: verblijf, dagbesteding en buitenschoolse opvang. SOVAK biedt ook diverse behandelingen aan door middel van een deskundig team dat bestaat uit fysiotherapeuten, ergotherapeuten, logopedisten, gedragsdeskundigen, artsen voor verstandelijk gehandicapten en geestelijk verzorgers. De voorzieningen van SOVAK worden aangeboden op verschillende locaties in Noord-Brabant.[7]

§ 1.2 Probleembeschrijving

SOVAK heeft in haar bedrijfsvoering dagelijks te maken met het verwerken van persoonsgegevens. De persoonsgegevens worden voornamelijk verzameld en verwerkt ter ondersteuning en instandhouding van de zorg- en dienstverlening aan cliënten. SOVAK heeft veel gegevens van cliënten beschikbaar, zowel persoonlijke als medische gegevens. De regels omtrent het verwerken en beschermen van persoonsgegevens spelen derhalve een grote rol in de organisatie.

Sinds de totstandkoming van de nationale en Europese privacyregels, de richtlijn uit 1995 en de Wet bescherming persoonsgegevens (hierna Wbp) uit 2001, is de snelheid en hoeveelheid waarin gegevens worden verzameld en gedeeld enorm gestegen. Door de snelle technologische ontwikkelingen zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. [8] De Europese Commissie heeft daarom enkele jaren geleden geconstateerd dat de huidige privacywetgeving aan herziening toe is. Deze herziening zal ook haar impact hebben op de zorgsector. De Europese Unie (hierna EU) wil de privacy van Europese burgers beter beschermen via een nieuwe Algemene Verordening Gegevensbescherming (hierna AVG).

In januari 2012 heeft de Europese Commissie voorstellen gepresenteerd voor een herziening van de Europese privacywetgeving. Op 17 december 2015 hebben de Europese Commissie, het Parlement en de Raad een akkoord bereikt over de herziening van de huidige privacywetgeving. Tijdens de uitvoering van dit onderzoek, namelijk op 14 april 2016, heeft het Europees Parlement ingestemd met de AVG. Deze zal in werking treden na publicatie in het Europees Publicatieblad. De verordening wordt dan direct van kracht in de EU en dus ook in Nederland. Nederland heeft na de publicatie nog twee jaar om de verordening te implementeren in de Nederlandse wetgeving.

Daarnaast is op 1 januari 2016 het Wetsvoorstel Meldplicht Datalekken in werking getreden. Dit wetsvoorstel is een uitbreiding van de huidige Wbp. De wijzigingen zien op de meldplicht bij datalekken en de uitbreiding van de boetebevoegdheden van de Autoriteit Persoonsgegevens (hierna AP). De meldplicht datalekken houdt in dat beveiligingsincidenten met betrekking tot persoonsgegevens direct gemeld moeten worden bij de AP. Wanneer een datalek niet wordt gemeld of andere wettelijke bepalingen uit de Wbp niet worden nageleefd, heeft de AP de bevoegdheid om een bestuurlijke boete op te leggen.

[7] <www.sovak.nl>
[8] COM(2012)/0011 definitief.

Naar aanleiding van de voorgestelde AVG en de invoering van de Meldplicht datalekken en uitbreiding boetebevoegdheid wil SOVAK weten welke gevolgen dit met zich meebrengt voor de organisatie. In de organisatie worden in de dagelijkse praktijk veel gegevens van cliënten verwerkt. Het is voor SOVAK belangrijk dat er een duidelijke richtlijn komt voor de organisatie hoe er dient te worden omgegaan met de veranderingen in de privacywetgeving en met name op het gebied van de Meldplicht datalekken. In dit onderzoek wordt alleen ingegaan op de gegevensverwerking van cliënten en niet op de gegevensverwerking van eigen medewerkers. De reden hiervan is dat de gegevens van cliënten een groter risico met zich meebrengen als het gaat om datalekken. In de organisatie zijn veel medewerkers dagelijks met (bijzondere) gegevens van cliënten bezig. Om deze reden is het van belang dat er een draaiboek wordt opgesteld voor medewerkers, waarin wordt aangegeven wat een datalek is en hoe er mee dient te worden omgegaan. Daarnaast is het huidige beleid van SOVAK verouderd ten opzichte van de nieuwe wetgeving.

In dit onderzoek wordt uiteengezet wat de AVG, de Meldplicht datalekken en de uitbreiding boetebevoegdheid met zich meebrengen ten aanzien van de verwerking van persoonsgegevens. Om de gevolgen van de nieuwe wetgeving toe te lichten, is het noodzakelijk om alvorens een goed beeld te schetsen van de huidige wetgeving. De handelswijze van SOVAK zal daarom summier worden getoetst aan de Wbp, omdat niet duidelijk is of het huidige beleid van SOVAK voldoet aan de Wbp. In dit onderzoek draait het voornamelijk om de wijzigingen in de privacywetgeving. Ten slotte worden er aanbevelingen gegeven in hoeverre SOVAK haar beleid moet aanpassen en op welke manier de organisatie kan voldoen aan de gewijzigde privacywetgeving.

§ 1.3 Centrale vraag

De centrale vraag luidt als volgt: *'Welke aanpassingen zijn nodig in het beleid en de werkwijze van SOVAK als gevolg van de invoering van de AVG en de Meldplicht datalekken en uitbreiding boetebevoegdheid, ten aanzien van de verwerking van persoonsgegevens van cliënten?'.*

§ 1.4 Deelvragen

Uit de centrale vraag zijn de volgende deelvragen ontstaan:

- Welke eisen stelt de huidige Wbp aan de verwerking van persoonsgegevens?
- Wat houdt de Meldplicht datalekken in?
- Welke wijzigingen in de privacywetgeving vloeien voort uit AVG?
- Wat is de huidige wijze van verwerken van persoonsgegevens binnen SOVAK?
- Welke tekortkomingen bestaan er in het huidige beleid en de huidige werkwijze van SOVAK ten aanzien van de Wbp (inclusief de meldplicht datalekken en uitbreiding boetebevoegdheid) en de AVG?

§ 1.5 Doelstelling

Op 30 mei 2016 wordt een onderzoeksrapport aan SOVAK overhandigd, waarin aanbevelingen worden gegeven in hoeverre SOVAK haar beleid en werkwijze, ten aanzien van de verwerking van persoonsgegevens, moet aanpassen met daarbij een werkinstructie voor medewerkers van de woongroepen en activiteitencentra, waarin de verplichtingen die uit de Meldplicht datalekken voortvloeien zijn neergelegd, zodat SOVAK voldoet aan de nieuwe privacywetgeving.

§ 1.6 Onderzoeksmethodiek

In deze paragraaf wordt per deelvraag uiteengezet welke onderzoeksstrategie, bronnen en methoden worden gebruikt bij de beantwoording van de deelvraag.

- Welke eisen stelt de huidige Wbp aan de verwerking van persoonsgegevens

- Wat houdt de Meldplicht datalekken in?
- Welke wijzigingen in de privacywetgeving vloeien voort uit de AVG?

De onderzoeksstrategie die voor het beantwoorden van deze deelvragen is gebruikt is het rechtsbronnen- en literatuuronderzoek. Er zijn verschillende bronnen bestudeerd zoals de wet, verdragen, literatuur en documenten. In dit onderzoek staan voornamelijk de Wbp inclusief de Meldplicht datalekken en uitbreiding boetebevoegdheid AP en de AVG centraal. Daarnaast zal is gebruik gemaakt van actuele literatuur, omdat actuele literatuur voor dit onderwerp het meest bruikbaar is. Tevens zijn kamerstukken, beleidsregels en handleidingen over de privacywetgeving onder de loep genomen. Deze stukken zijn allemaal inhoudelijk geanalyseerd om zo overbodige informatie te voorkomen. Alle bruikbare informatie is geïnterpreteerd en verwerkt in dit onderzoeksrapport. Daarnaast is de tekst van de AVG vergeleken met de Wbp om erachter te komen wat er verandert of wijzigt in de wetgeving met komst van de AVG. Voor deze strategie, methoden en bronnen is gekozen omdat deze het meest effectief zijn bij het beantwoorden van deze deelvragen. Daarnaast wordt er uitsluitend gebruik gemaakt van betrouwbare bronnen. De bronnen worden zorgvuldig geselecteerd door te kijken naar de herkomst van de bron. Wanneer er informatie uit een bron wordt gebruikt, is dat terug te vinden in de voetnoot.

- Wat is de huidige wijze van verwerken van persoonsgegevens binnen SOVAK?

De onderzoeksstrategie die voor het beantwoorden van deze deelvraag wordt gebruikt is de casestudy. Tijdens de casestudy zijn de werkwijze en het beleid van de organisatie in beeld gebracht door middel van verschillende onderzoeksmethoden. De onderzoeksmethoden die tijdens de casestudy zijn gebruikt zijn onder andere: het afnemen van interviews bij de afdelingen cliëntservice, de woongroepen en het activiteitencentrum. Het analyseren van verschillende documenten behorend tot de organisatie zoals beleidsregels, werkinstructies en protocollen. Door deze onderzoeksmethoden wordt er een volledig beeld gevormd van de werkwijze van de organisatie en in hoeverre medewerkers zich bewustzijn van de regels omtrent privacybescherming. Ook wordt er door deze onderzoeksmethoden meer inzicht verworven in de wijze waarop het in de praktijk gaat en welke vragen er spelen bij medewerkers omtrent de vernieuwde privacywetgeving. De onderzoeksstrategie casestudy is het meest effectief om deze deelvraag te beantwoorden. Deze deelvraag is alleen te beantwoorden via een onderzoek naar de praktijksituatie. Deze strategie, bronnen en methoden zijn daarnaast ook het meest efficiënt, omdat de omvang van het praktijkonderzoek past binnen het tijdsbestek van dit onderzoek. Er zijn bijvoorbeeld maar twee woongroepen en één groep op het activiteitencentrum geïnterviewd.

- Welke tekortkomingen bestaan er in het huidige beleid en de huidige werkwijze van SOVAK ten aanzien van de Wbp, inclusief de meldplicht datalekken en uitbreiding boetebevoegdheid, en de AVG?

Bij het beantwoorden van deze deelvraag wordt het recht toegepast op de praktijk. De beantwoording geschiedt via empirisch onderzoek. De informatie voortgevloeid uit de eerste twee deelvragen is geanalyseerd en met elkaar vergeleken. Dit is de meest effectieve manier om er achter te komen welke leemten er bestaan in het huidige beleid en de huidige werkwijze van SOVAK ten opzichte van de nieuwe privacywetgeving.

2. Privacy door de jaren heen

In 1948 is op internationaal niveau voor het eerst aandacht besteed aan de rechten van de mens. Door de Verenigde Naties (hierna: VN) is toen de Universele verklaring voor de Rechten van de Mens (hierna: UVRM) opgesteld. In art. 12 van deze verklaring is het recht op bescherming van de persoonlijke levenssfeer neergelegd. Deze verklaring was slechts een aanbeveling en daarom niet juridisch bindend. Om deze reden besloot de VN art. 12 vast te leggen in een verdrag, namelijk het Internationaal Verdrag inzake Burgerrechten en Politieke rechten (hierna: IVBP). In het IVBP is het recht op bescherming van de persoonlijke levenssfeer neergelegd in art. 17, dat bijna identiek is aan art. 12 UVRM.[9] Vervolgens werd in 1950 door de Raad van Europa het Europees Verdrag tot bescherming van de Rechten van de Mens opgesteld (hierna: EVRM). Art. 8 van dit verdrag is afgeleid van art. 12 UVRM. Art. 8 EVRM voorziet in het recht op respect voor privé- en familieleven, woning en correspondentie. Toch vond de Raad van Europa, in het licht van de moderne wetenschap en technologie, dat art. 8 EVRM niet voldoende bescherming bood aan het privéleven van burgers.[10] Het recht op eerbiediging van het privéleven is vervolgens ook uitgewerkt in het Verdrag van Straatsburg, dat in 1981 in werking is getreden. Dit verdrag heeft de basis gelegd voor de Europese privacybescherming.

Op nationaal niveau werd in 1972 de Staatscommissie Koopmans ingesteld om te adviseren over nut en noodzaak van wetgeving op het gebied van persoonsregistratie. De werkzaamheden van de Staatscommissie hebben uiteindelijk geleid tot de Wet persoonsregistratie (hierna: Wpr). De Wpr was de eerste Nederlandse wet die als doel had: het beschermen van persoonsgegevens. Deze wet is in 1989 in werking getreden. In de tussentijd heeft er in 1983 ook een grondwetswijziging plaatsgevonden. Vanaf nu was het recht op bescherming van de persoonlijke levenssfeer ook geregeld in art. 10 van de Grondwet (hierna: GW).[11] Momenteel is de basis van de huidige privacywetgeving de Europese privacyrichtlijn die in 1995 tot stand is gekomen.[12] Deze richtlijn bouwt voort op het Verdrag van Straatsburg met als doel het harmoniseren van de nationale wetgeving, zodat een gelijkwaardig beschermingsniveau wordt gewaarborgd.

De Wpr is naar aanleiding van deze richtlijn vervangen door de Wbp. Daarnaast is de Wbp gebaseerd op art. 10 GW en art. 8 EVRM. Een richtlijn bevat doelstellingen waar alle lidstaten van de Europese Unie aan moeten voldoen. Het beoogde resultaat staat vast maar de Europese lidstaten mogen zelf bepalen hoe ze de richtlijn uitwerken. Daarbij kan rekening worden gehouden met de specifieke situatie in eigen land. De privacywetgeving is dus in verschillende Europese lidstaten op een andere manier geïmplementeerd. Dit betekent dat in elke Europese lidstaat interpretatie- en implementatie verschillen zijn als het gaat om privacy.

De Europese Commissie heeft enkele jaren geleden geconstateerd dat de huidige richtlijn, ondanks het feit dat de algemene principes en rechten nog steeds van kracht zullen blijven, aan herziening toe is vanwege de snelle ontwikkelingen op het gebied van verwerken van persoonsgegevens.[13] In januari 2012 heeft de Europese Commissie de AVG gepresenteerd. Anders dan de huidige wet- en regelgeving, die gebaseerd is op de Europese Richtlijn, richt het nieuwe voorstel zich op een Europese verordening. Een verordening hoeft niet afzonderlijk geïmplementeerd te worden, maar is rechtstreeks toepasselijk in elke lidstaat. De directe werking van de verordening brengt, in tegenstelling tot de richtlijn, uniformiteit in de Europese lidstaten met zich mee. Dit verkleint de kans op interpretatie- en

[9] Berkvens & Prins 2007, p. 9
[10] Kranenborgh & Verhey 2011, p. 12
[11] Brouwer 2002, p. 20
[12] Richtlijn 95/46/EG (*PbEG* 1995, L 281/31)
[13] https://autoriteitpersoonsgegevens.nl/ (zoek op: *Europese privacyverordening*)

implementatieverschillen. De AVG op 24 april 2016 aangenomen door de Europese Commissie en zal in 2018 in werking treden voor alle lidstaten.

3. Wet bescherming persoonsgegevens

In deze paragraaf wordt het wettelijk kader van de Wbp beschreven. De doelstelling en beginselen, zoals nu in de Wbp vermeld, blijven met de komst van de AVG gelden. Het is van belang om te weten hoe de huidige wetgeving is opgezet om op die manier makkelijker in te kunnen zien welke veranderingen en vernieuwingen de invoering van de privacyverordening met zich meebrengt. Daarnaast wordt een duidelijk en volledig beeld geschetst ten aanzien van het toetsingskader.

§ 3.1 Toepassing van de Wbp

Het toepassingsgebied van de Wbp wordt bepaald door het begrip 'verwerken van persoonsgegevens'. Onder verwerken van persoonsgegevens valt het gehele proces vanaf de verzameling tot het moment van vernietiging.[14] De Wbp is van toepassing op de (gedeeltelijk) geautomatiseerde verwerking van persoonsgegevens. Een voorbeeld hiervan is een computersysteem waarin persoonsgegevens opgeslagen en te raadplegen zijn. Ook niet geautomatiseerde verwerkingen van persoonsgegevens vallen onder de Wbp, mits de gegevens zijn opgenomen in een bestand of bestemd zijn om daarin te worden opgenomen. De handmatige verwerking moet systematisch zijn ingedeeld en betrekking hebben op meerdere personen. De Wbp legt verplichtingen op aan de verantwoordelijke en kent rechten toe aan de betrokkene. De verantwoordelijke kan de verwerking van persoonsgegevens ook uitbesteden aan een ander. Deze wordt dan de bewerker genoemd.[15] [16]

§ 3.2 Voorwaarden voor verwerking

Bij het verwerken van persoonsgegevens moet de verantwoordelijke een aantal wettelijke beginselen in acht nemen. In art. 6 en 7 Wbp zijn de algemene regels voor de rechtmatigheid van de verwerking van persoonsgegevens opgenomen. Persoonsgegevens moeten te allen tijde in overeenstemming met de wet en op behoorlijke en zorgvuldige manier worden verwerkt. [17] Daarnaast mogen persoonsgegevens alleen worden verwerkt voor welbepaalde, uitdrukkelijk omgeschreven en gerechtvaardigde doeleinden. Zonder precieze doelomschrijving mogen persoonsgegevens niet worden verwerkt.[18] Uit art. 9 Wbp blijkt dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Er dient rekening te worden gehouden met het verband tussen het doel waarvoor de verantwoordelijke de gegevens gaat gebruiken en het doel waarvoor de gegevens zijn verkregen.[19] Tevens mogen de gegevens, gelet op het doel waarvoor ze worden verwerkt, niet bovenmatig, toereikend en ter zake dienend zijn. ''Niet bovenmatig'' wil zeggen dat er geen gedetailleerde gegevens mogen worden verwerkt als dat voor het doel niet noodzakelijk is. Met ''toereikend'' wordt bedoelt dat er ook niet te weinig gegevens mogen worden verwerkt, omdat er dan een onterecht beeld van betrokkene kan ontstaan. ''Ter zake dienend'' houdt in dat alle gegevens die noodzakelijk zijn voor het doel moeten worden verwerkt.[20] Tenslotte heeft de verantwoordelijke een wettelijke verplichting om maatregelen te treffen opdat de gegevens juist en nauwkeurig zijn.[21] Dit wordt ook wel het kwaliteitsbeginsel genoemd.

Zoals eerder vermeld, is in art. 7 Wbp neergelegd dat persoonsgegevens alleen mogen worden verwerkt voor gerechtvaardigde doeleinden. Art. 8 Wbp bevat een limitatieve opsomming van de verschillende grondslagen. Elke gegevensverwerking of categorie van

[14] De Vries & Rutgers 2012, p. 24
[15] De Vries & Rutgers 2012, p. 26
[16] Ter verduidelijking zijn de in deze paragraaf genoemde begrippen opgenomen in de begrippenlijst.
[17] Kranenborg & Verhey 2011, p. 81
[18] Rijkers 2002, p. 34
[19] Thole & Van der Jagt & Roerdink 2010, p. 40
[20] Sauerwein & Linnemann 2002, p. 27
[21] Kranenborg & Verhey 2011, p. 97

gegevensverwerkingen moet gebaseerd zijn op ten minste één van de weergegeven situaties.[22] De verschillende grondslagen zijn:

- De betrokkene heeft ondubbelzinnige toestemming gegeven voor de verwerking;
- De verwerking is noodzakelijk is voor de uitvoering van de overeenkomst;
- De verwerking is noodzakelijk om een wettelijke verplichting na te komen;
- De verwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;
- De verwerking is noodzakelijk voor de vervulling van een publiekrechtelijke taak;
- De verwerking dient een gerechtvaardigd belang van verantwoordelijke of van een derde aan wie de gegevens worden verstrekt.

Bij afwezigheid van één van de zes grondslagen is gegevensverwerking niet toegestaan.
Tenslotte verdient het de opmerking dat de Wbp moet worden uitgelegd met inachtneming van art. 8 EVRM, waarbij het verwerken van persoonsgegevens te allen tijde in overeenstemming moet zijn met de beginselen van proportionaliteit en subsidiariteit.[23]

§ 3.3 Verwerken van bijzondere persoonsgegevens

De wet maakt een onderscheid tussen algemene en bijzondere persoonsgegevens. Onder algemene persoonsgegevens worden verstaan de NAW-gegevens, geboortedatum, BSN-nummer, enzovoort verstaan. De bijzondere persoonsgegevens worden opgesomd in art. 16 Wbp. Bij bijzondere gegevens gaat het om gegevens betreffende iemands godsdienst, ras, politieke gezindheid, gezondheid, seksueel leven, het lidmaatschap van een vakvereniging en strafrechtelijke gegevens. Deze gegevens mogen niet worden verwerkt, tenzij er een uitzondering uit de artikelen 17 tot en met 22 Wbp van toepassing is. Is er sprake van een uitzondering dan zal de gegevensverwerking vervolgens ook getoetst moeten worden aan de algemene beginselen (zie paragraaf 3.2).[24] Het benoemen van de uitzonderingen zal worden beperkt tot hetgeen voor dit onderzoek het meest van belang is.

Godsdienst of levensovertuiging

Het verbod uit art. 16 Wbp betreffende de verwerking van gegevens over iemands godsdienst of levensovertuiging wordt in art. 17 Wbp niet van toepassing verklaard als de verwerking wordt verricht door kerkgenootschappen, zelfstandige onderdelen daarvan en andere genootschappen op geestelijke grondslag. Instellingen op godsdienstige of levensbeschouwelijke grondslag mogen alleen gegevens over iemands godsdienst verwerken als dit gelet op het doel van de instelling en voor de verwezenlijking van haar grondslag noodzakelijk is.[25] Overige instellingen mogen gegevens over iemand godsdienst verwerken voor zover dit noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene.[26]

Ras of etniciteit

Het begrip ‘ras’ wordt ruim opgevat en bevat onder andere iemands huidskleur, afkomst en nationale of etnische afstamming.[27] Art. 18 Wbp bepaalt dat verwerking alleen toegestaan is als het onvermijdelijk is met het oog op identificatie van de betrokkenen. Verder is verwerking toegestaan, onder voorwaarden, in het kader van een voorkeursbeleid voor bepaalde minderheidsgroepen.

Gezondheid

Gezondheidsgegevens bevatten alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen.[28] In art. 21 Wbp zijn de uitzonderingen omtrent de verwerking van gegevens betreffende de gezondheid opgesomd. Gezondheidsgegevens mogen worden verwerkt door: hulpverleners, instellingen voor gezondheidszorg of maatschappelijke

[22] Rijkers 2002, p. 33
[23] HR, 9 september 2011, ECLI:NL:HR:2011:BQ8097.
[24] Kamerstukken II 1997/98, 25892, nr. 3, p. 22 (MvT)
[25] Kamerstukken II 1997/98, 25892, nr. 3, p. 103-104 (MvT)
[26] Kranenborg & Verhey 2011, p. 105
[27] Kamerstukken II 1997/98, 25892, nr. 3, p. 104-105 (MvT)
[28] Thole & Van der Jagt & Roerdink 2010, p. 84

dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel voor het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is.[29] Alleen personen die een geheimhoudingsplicht hebben op grond van hun ambt, beroep, wettelijk voorschrift of een overeenkomst mogen gezondheidsgegevens verwerken. Daarnaast wordt in lid 3 beschreven dat ook andere categorieën gevoelige gegevens verwerkt mogen worden indien dit noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene.[30] Het verwerken van gezondheidsgegevens is tevens geregeld in andere wetgeving, zoals de Wet op de geneeskundige behandelingsovereenkomst (hierna WGBO) en de Wet bijzondere opneming in psychiatrische ziekenhuizen (hierna Wet Bopz).

§ 3.4 Verplichtingen van de verantwoordelijke

In deze paragraaf zullen de verplichtingen die de verantwoordelijke op grond van de Wbp heeft worden toegelicht.

Beveiliging

Op grond van art. 13 Wbp is de verantwoordelijke verplicht om passende technische en organisatorische maatregelen te nemen om het verlies van gegevens of onrechtmatige verwerking tegen te gaan. Deze verplichting strekt zich uit tot alle onderdelen van het proces van de gegevensverwerking.[31] Bij technische maatregelen kan gedacht worden aan het vastleggen van autorisatiestructuren in bepaalde programma's of het beveiligen van gegevens door middel van een wachtwoord. Onder organisatorische maatregelen vallen maatregelen voor de inrichting van de organisatie, zoals een verdeling van verantwoordelijkheden en bevoegdheden maar ook instructies, trainingen en calamiteitenplannen. Het begrip 'passend' wil zeggen dat er bij de keuze voor de methode van beveiliging de risico's van de verwerking en de aard van de te beschermen gegevens moet worden meegewogen. Bij passende maatregelen dient dus rekening gehouden te worden met het proportionaliteitsbeginsel. Hoe gevoeliger de gegevens, hoe zwaarder de toegepaste beveiliging moet zijn. Voor bepaalde elektronische systemen zijn in sommige gevallen nadere eisen gesteld. Zo is voor de zorgsector een code voor informatiebeveiliging opgesteld, ook wel de NEN 7510 genoemd, waarin normen en maatregelen die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging zijn neergelegd.[32] De NEN 7520 is vooralsnog niet verplicht gesteld. Tenslotte moeten de technische en organisatorische maatregelen er mede op gericht zijn onnodige verzameling of verdere verwerking te voorkomen. De personen die te maken hebben met gegevensverwering of toegang hebben tot gegevens, zijn op grond van art. 12 Wbp verplicht tot geheimhouding. De verantwoordelijke draagt zorg voor de naleving van de verplichtingen uit de Wbp.

Bewaartermijn

In art. 10 Wbp is bepaald dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor ze zijn verzameld. De Wbp geeft hier geen termijn voor. In het Vrijstellingsbesluit Wbp of in specifieke wetten zijn wel maximale bewaartermijnen opgenomen.[33] De bijzondere wetten WGBO en Wet Bopz hebben specifieke bewaartermijnen vastgesteld voor de persoonsgegevens in de zorgsector. Deze wetten hebben voorrang op algemene wetgeving, omdat het bijzondere wetten zijn.
De WGBO is van toepassing wanneer een betrokkene medische zorg van een deskundige krijgt en de Wet Bopz wanneer er sprake is van zorg aan mensen met een verstandelijke beperking of wanneer iemand tegen zijn wil mag worden opgenomen en behandeld in een psychiatrisch ziekenhuis. Voor de WGBO geldt een bewaartermijn van vijftien jaar en voor de Wet Bopz geldt een bewaartermijn van vijf jaar.

[29] Kranenborg & Verhey 2011, p. 109
[30] Berkvens & Prins 2007, p. 169
[31] Kranenborg & Verhey 2011, p. 99
[32] Gellearts & Jobse 2011, p. 60
[33] Thole & Van der Jagt & Roerdink 2010, p. 55

Meldingsplicht
Vaak is de verantwoordelijke verplicht geautomatiseerde gegevensverwerkingen te melden aan de AP. In het Vrijstellingsbesluit Wbp staan een aantal uitzonderingen genoemd.[34] De zorgsector is in art. 17 van dit besluit vrijgesteld van de meldingsplicht.

Informatieplicht
In art. 33 en 34 Wbp is de plicht tot informatieverstrekking neergelegd. Deze verplichting houdt in dat de verantwoordelijke steeds zijn identiteit en de doeleinden van de verwerking aan de betrokkene meedeelt en wel voorafgaand aan de gegevensverwerking.[35]

§ 3.5 Rechten van de betrokkene

Om transparantie te creëren ten aanzien van de gegevensverwerking en om te waarborgen dat persoonsgegevens behoorlijk en zorgvuldig worden verwerkt, kent de Wbp de burger een aantal rechten toe. Concreet heeft de betrokkene de volgende rechten:

Het recht op inzage
Een betrokkene kan zich wenden tot de verantwoordelijke met het verzoek aan hem mede te delen of er persoonsgegevens van hem worden verwerkt en zo ja welke. Als er gegevens van betrokkene worden verwerkt dan moet de verantwoordelijke een zo volledig mogelijk overzicht verschaffen van de verwerkte gegevens.[36] Daarnaast moet ook het doel van de verwerking vermeld worden en aan welke derde partijen de gegevens worden verstrekt.

Het recht van correctie
Indien uit het overzicht, dat door verantwoordelijke is verstrekt, blijkt dat bepaalde gegevens onjuist zijn, kan de betrokkene de verantwoordelijke verzoeken om de gegevens te corrigeren, aan te vullen, te verwijderen of af te schermen. [37]

Het recht van verzet
De betrokkene heeft onder bepaalde omstandigheden het recht om zich te verzetten tegen gegevensverwerking. Het recht van verzet kan alleen worden uitgeoefend indien de verantwoordelijke de gegevens verwerkt op de grondslagen van art. 8 onder e en f Wbp. Indien het recht op verzet terecht is dan moet de verantwoordelijke de gegevensverwerking beëindigen.

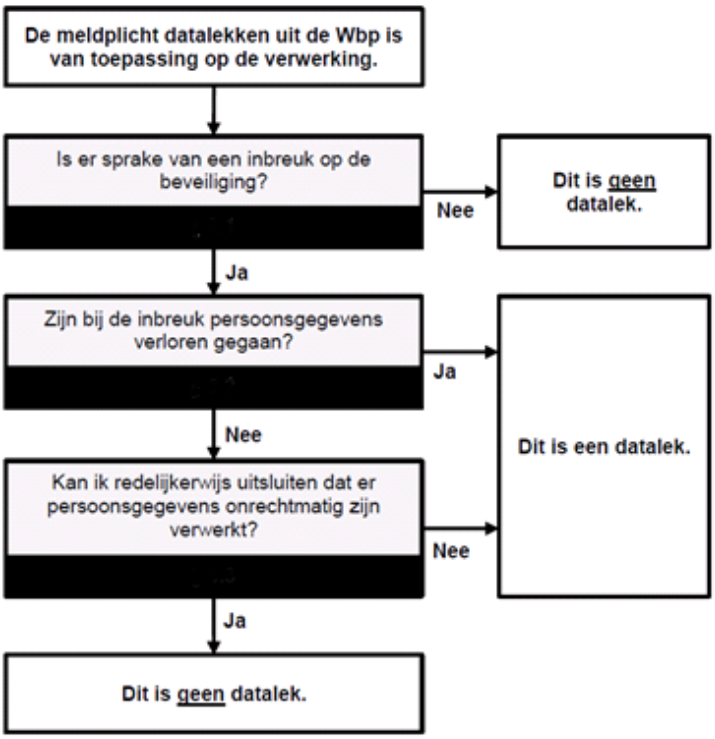
[34] Sauerwein & Linnmann 2002, p. 31
[35] Kranenborg & Verhey 2011, p. 125
[36] Thole & Van der Jagt & Roerdink 2010, p. 49
[37] Thole & Van der Jagt & Roerdink 2010, p. 50

4. Meldplicht datalekken en uitbreiding boetebevoegdheid

Eén van de wijzigingen die de AVG met zich meebrengt is de Meldplicht datalekken. Om daarop vooruit te lopen heeft de Tweede Kamer in 2013 een wetsvoorstel ingediend waarin de meldplicht wordt gepresenteerd in de Wbp. Het wetsvoorstel is uiteindelijk aangevuld met de uitbreiding van de bestuurlijke boetebevoegdheid.[38] Met de invoering van de meldplicht en de uitbreiding van de bestuurlijk boetebevoegdheid wil Nederland alvast inspringen op de nieuwe AVG. Het wetsvoorstel is aangenomen door de Tweede Kamer en op 1 januari 2016 in werking getreden. De Meldplicht datalekken is neergelegd in art. 34a Wbp en de boetebevoegdheid van de AP in art. 66 Wbp. Deze begrippen zullen in dit hoofdstuk nader worden toegelicht.

§ 4.1 Wat is een datalek?

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens en als deze gegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.[39] Het begrip 'datalek' komt niet voor in de Wbp. In plaats daarvan wordt er gesproken van ''een inbreuk op de beveiliging'', zoals bedoeld in art. 13 Wbp. Van een inbreuk op de beveiliging is sprake als de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Een datalek is het gevolg van een inbreuk op de beveiligingsmaatregelen. Het gaat niet alleen om het lekken van gegevens, maar het kan ook gaan om risico op verlies of wijziging van gegevens. Voorbeelden hiervan zijn: het kwijtraken van een usb-stick, de diefstal van een laptop, een inbraak in een computersysteem door een hacker of het slordig omgaan met het beheer van wachtwoorden.[40] Een datalek is een ruim begrip en kan variëren van een niet adequate vakkundig toegepaste beveiliging van de bestanden of gegevens tot menselijke fouten van ondergeschikten.[41]



Figuur 1: Wanneer is er sprake van een datalek?[42]

[38] Kamerstukken II 2012/13, 33662, nr. 3, p. 1 (MvT)
[39] Artikel 13 Wet bescherming persoonsgegevens
[40] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 5.
[41] Kamerstukken II 2012/13, 33662, nr. 3, p. 4 (MvT)
[42] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 16.

Er zijn twee verschillende soorten datalekken namelijk opzettelijke datalekken en onopzettelijke datalekken. Met opzettelijk wordt bedoelt dat ze bewust zijn veroorzaakt, bijvoorbeeld door externe hackers of door een medewerker. Voorbeelden zijn:

- het kopiëren, meenemen of aan andere verstrekken van vertrouwelijke gegevens door eigen medewerkers die voor hun werk toegang tot die gegevens hebben;
- het misbruiken van menselijke kwetsbaarheden door onder een valse naam. vertrouwelijke gegevens te bemachtigen, via e-mail of internet.[43]

Bij onopzettelijke datalekken wordt het datalek niet bewust veroorzaakt, maar gaat het om menselijke of technische fouten. Een voorbeeld hiervan is het verlies van niet beveiligde informatiebronnen, zoals een usb-stick of papieren dossiers of het verzenden van een e-mailbericht met vertrouwelijke gegevens aan de verkeerde ontvanger.[44]

§ 4.2 Wanneer moet een datalek gemeld worden?

Niet ieder datalek hoeft gemeld te worden bij de AP. Wanneer een datalek zich voordoet, moet worden beoordeeld of er sprake is van een inbreuk op de getroffen beveiligingsmaatregelen en of het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Een datalek valt, volgens art. 34a Wbp, pas onder de meldplicht als de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en de persoonsgegevens zijn blootgesteld aan een aanmerkelijke kans op verlies of onrechtmatige verwerking.[45] Of dit zo is moet naar feitelijke omstandigheden van het geval worden vastgesteld. Het is niet goed mogelijk aan te geven of het verlies van een usb-stick of laptop wel of geen aanleiding geeft om een melding te doen. Of die noodzaak aanwezig is, hangt af van de aard van de data die het betreft en het risico dat betrokkene en de verantwoordelijke lopen.[46] Om te kunnen beoordelen of een datalek gemeld moet worden, heeft de AP het volgende beslismodel opgesteld:

Figuur 2: moet het datalek gemeld worden?

Zoals uit bovenstaand schema blijkt, speelt bij de meldplicht de aard van de gelekte gegevens een grote rol. Bij persoonsgegevens van gevoelige aard is vaak een melding noodzakelijk. Gevoelige gegevens zijn onder andere: bijzondere persoonsgegevens, zoals bedoeld in art.

[43] Hutter & Katus & Terstegge & Versmissen, 2015, p. 19
[44] Hutter & Katus & Terstegge & Versmissen, 2015, p. 19
[45] Kamerstukken II 2012/2013, 33662, nr. 3, p. 5 (MvT)
[46] Kamerstukken II 2012/2013, 33662, nr. 3 p. 7 (MvT)

16 Wbp, gebruikersnamen, wachtwoorden of andere inloggegevens en gegevens die kunnen worden misbruikt voor identiteitsfraude. Wanneer er geen gevoelige gegevens gelekt zijn, kan het alsnog zo zijn dat het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de betrokkenen. Ook dan moet er een melding plaatsvinden. Personen die extra risico's lopen bij een datalek zijn hier een voorbeeld van. Denk aan mensen in een blijf-van-mijn-lijfhuis waarvan NAW-gegevens zijn gelekt.[47] De hoeveelheid van de gelekte gegevens kan ook aanleiding zijn om het datalek te melden.

§ 4.3 Hoe moet een datalek gemeld worden?

Op grond van art. 34a lid 1 Wbp moet het datalek ''onverwijld gemeld'' worden aan de AP. Wat het begrip 'onverwijld' precies inhoudt zal afhangen van de omstandigheden van het geval. Organisaties worden in ieder geval in de gelegenheid gesteld om na het ontdekken van het datalek enige tijd te nemen voor nader onderzoek. Zo worden onnodige meldingen voorkomen. In de beleidsregels meldplicht datalekken wordt gesproken over een meldingstermijn van 72 uur. Wanneer de melding aan de AP niet binnen 72 uur plaatsvindt, moet duidelijk worden gemotiveerd waarom de melding later is gedaan.

Op de website van de AP is een standaard meldingsformulier beschikbaar. Een melding omvat in ieder geval:[48]

- De aard van de melding;
- Algemene informatie en contactgegevens;
- Een beschrijving van de geconstateerde datalek en de vermoedelijke gevolgen;
- Informatie over inlichtingen aan eventuele betrokkenen;
- De maatregelen om negatieve gevolgen te beperken en verdere datalekken te voorkomen;
- Technische beschermingsmaatregelen.

Het verdient de opmerking dat de meldingstermijn in de AVG wordt verkort naar 24 uur. De inhoud en strekking van de melding blijft hetzelfde.

§ 4.4 Melden aan de betrokkene

Een datalek moet soms gemeld worden aan degene op wie het datalek betrekking heeft. Art. 34a lid 2 Wbp geeft aan dat een melding aan betrokkene moet plaatsvinden als het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer. Bij ongunstige gevolgen kan worden gedacht aan identiteitsfraude of aantasting in eer en goede naam.

Uit de beleidsregels blijkt dat bij de vraag of het datalek aan betrokkene moet worden gemeld de volgende drie vragen van belang zijn:[49]

1. Waren de gegevens goed versleuteld of geanonimiseerd?
   Als de gelekte persoonsgegevens op een passende technische wijze zijn beschermd waardoor de persoonsgegevens ontoegankelijk of onbegrijpelijk zijn voor een ander die geen recht heeft op kennisname van de gegevens dan hoeft er geen melding aan betrokkene plaats te vinden.[50]
2. Heeft het datalek waarschijnlijk nadelige gevolgen voor de betrokkene(n)?
   Bij het lekken van gevoelige gegevens zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de betrokkene. In alle andere gevallen zal er een afweging moeten worden gemaakt. In de beleidsregels wordt benadrukt dat de betrokkenen met name geïnformeerd moeten worden als dat ze in de gelegenheid stelt om eventuele maatregelen te nemen tegen (eventuele) ongunstige gevolgen. Hoe eerder de betrokkene dus wordt geïnformeerd, hoe sneller hij in actie kan komen.[51] Voor betrokkenen in kwetsbare groepen kan verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich meebrengen. Vooral

[47] Hutter & Katus & Terstegge & Versmissen, 2015, p. 75
[48] Artikel 34a lid 3 en 4 Wbp
[49] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 34.
[50] Kamerstukken II 2014/15, 33 662, nr. 11, p. 2
[51] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 6.

voor kinderen en volwassenen met een verstandelijke handicap kan het moeilijk zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk sneller ingaan op pogingen tot phishing of oplichting.[52]

3. Zijn er zwaarwegende redenen om het datalek (nog) niet te melden?
   Soms kunnen er zwaarwegende redenen zijn om het datalek niet te melden, bijvoorbeeld als er gegevens zijn gelekt over medische of psychische hulpvragen van kinderen of verstandelijk gehandicapten buiten medeweten van de wettelijk vertegenwoordigers. Door de melding zouden de vertegenwoordigers alsnog op de hoogte gesteld kunnen worden van de hulpvraag.[53] Wanneer zwaarwegende belangen later vervallen of minder zwaar gaan wegen dan moet het lek alsnog gemeld worden.

In de kennisgeving aan betrokkene wordt de aard van de inbreuk, de instantie waar de betrokkene meer informatie over de inbreuk kan krijgen en de maatregelen die de betrokkene worden aanbevolen om de negatieve gevolgen te beperken vermeld.[54] In tegenstelling tot de melding aan de AP wordt bij de melding aan betrokkene(n) geen meldingstermijn gehanteerd. In het geval dat betrokkenen zelf stappen kunnen ondernemen om de nadelige gevolgen van het datalek tegen te gaan, zal de melding zo snel mogelijk gedaan moeten worden.[55]

§ 4.5 De bewerker en de bewerkersovereenkomst

In sommige gevallen wordt de verwerking van persoonsgegevens geheel of gedeeltelijk uitbesteed aan een zogeheten bewerker. Een bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke, zonder dat hij aan het rechtstreeks gezag van de verantwoordelijke is onderworpen.[56] Wanneer er voor de verwerking een bewerker is ingeschakeld, moet de verantwoordelijke met een aantal dingen rekening houden in het kader van de meldplicht datalekken.

De verantwoordelijke moet ervoor zorgen dat de bewerker maatregelen treft, zodat de verantwoordelijke aan de meldplicht voldoet. Wanneer een datalek wordt geconstateerd moet de bewerker ervoor zorgen dat hij de verantwoordelijke zo snel mogelijk en adequaat informeert. De verantwoordelijke is namelijk aansprakelijk voor de melding bij de AP. Het is daarom van belang dat er goede afspraken worden gemaakt met de bewerker. Deze afspraken zijn noodzakelijk, omdat de verantwoordelijke anders geen weet heeft van het datalek en dus ook niet in staat is om deze te melden. Daarnaast heeft de bewerker zelf ook een aantal plichten ten aanzien van de meldplicht. Hij moet voldoende waarborgen bieden ten opzichte van de naleving van de meldplicht datalekken en hij dient de instructies van de verantwoordelijke op te volgen.[57]

Afspraken die worden gemaakt tussen de verantwoordelijke en de bewerker worden opgenomen in een schriftelijke bewerkersovereenkomst. De inhoud van de bewerkersovereenkomst is in de AVG ruimer beschreven dan in de Wbp. Het is in ieder geval belangrijk om duidelijke afspraken te maken over de meldplicht datalekken, zoals:

- Wie meldt het datalek?
- Op welke wijze wordt de verantwoordelijke op de hoogte gebracht?
- Welke consequenties zijn er voor de bewerker als hij de verantwoordelijke niet op tijd op de hoogte stelt?
- Etc.

[52] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 28.
[53] Hutter & Katus & Terstegge & Versmissen, 2015, p. 81
[54] Art. 34a lid 3 Wbp.
[55] Art. 34a lid 5 Wbp.
[56] Artikel 1 sub e Wbp.
[57] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 16.

Het is voor de verantwoordelijke belangrijk om toe te zien op de naleving van de regels door de bewerker. Afspraken rondom aansprakelijkheid en verantwoordelijkheid kunnen in de bewerkersovereenkomst worden opgenomen.

§ 4.6 Registreren datalek

In art. 34a lid 8 Wbp wordt de verplichting neergelegd om een overzicht bij te houden van alle inbreuken. Dat betreft ook de inbreuken die wel zijn geconstateerd, maar niet zijn gemeld. Het is belangrijk dat de verantwoordelijke een dergelijk overzicht opstelt en bijhoudt, omdat de verantwoordelijke zo op een adequate manier kan aantonen welke datalekken er zijn geconstateerd en welke maatregelen er zijn genomen.[58] Het overzicht moet in ieder geval de feiten en gegevens omtrent de aard van de inbreuk omvatten. Als het datalek ook aan de betrokkene is gemeld, moet het overzicht mede deze kennisgeving bevatten. Het overzicht wordt opgesteld voor de volgende doeleinden:

- Er kan lering worden getrokken uit het datalek;
- Het plaatsvinden van een evaluatie;
- Antwoord kunnen geven op vragen van betrokkenen en anderen;
- Eventueel alsnog melden van datalek aan berokkenen als de omstandigheden dit vereisen.[59]

De plicht om dit overzicht bij te houden is bedoeld voor de ondersteuning van het interne en externe toezicht op de gegevensverwerking. De AP kan aan de hand van het overzicht beoordelen of geconstateerde datalekken, die niet zijn gemeld, toch gemeld hadden moeten worden.

De wet schrijft overigens niet voor hoelang het overzicht bewaard moet blijven. In de beleidsregels Meldplicht datalekken wordt de bewaartermijn van minimaal één jaar voorgeschreven. In bepaalde gevallen kan het nodig zijn om een langere bewaartermijn te hanteren, bijvoorbeeld wanneer een datalek niet wordt gemeld aan betrokkene. Dan moet er een bewaartermijn worden gehanteerd van minimaal drie jaar.[60]

§ 4.7 Uitbreiding boetebevoegdheid

Naar aanleiding van de voorgestelde AVG heeft de wetgever besloten om de sanctiemogelijkheden van de AP te versterken om op die manier de naleving van de Wbp te bevorderen. De AP kon voorheen alleen een boete opleggen in geval van een overtreding van een administratieve verplichting. Die boete bedroeg maximaal € 4.500, maar werd niet vaak opgelegd. Door de uitbreiding van de boetebevoegdheid zijn de boetes verhoogd naar maximaal € 810.000 of 10% van de jaaromzet van een rechtspersoon. De verwachting is dat door de uitgebreide boetebevoegdheid organisaties worden gestimuleerd om aandacht te besteden aan de bepalingen uit de Wbp. De boetebevoegdheid van de AP is neergelegd in art. 66 Wbp. Aan de hand van dit art. heeft de AP beleidsregels opgesteld met betrekking tot het bepalen van de hoogte van de boetes. In dit hoofdstuk zal de uitbreiding van de boetebevoegdheid uiteen worden gezet.

Nieuwe boetestelsel

In de boetebeleidsregels worden drie boetemaxima onderscheiden. Voor ieder boetemaxima zijn een aantal categorieën met overtredingen vastgesteld waarbinnen een boetebandbreedte geldt. Ter verduidelijking is in onderstaande tabel per boetemaxima de boetebandbreedtes weergegeven:

[58] Kamerstukken II 2012/13, 33 662, nr. 3, p. 23
[59] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 47.
[60] Beleidsregels voor toepassing van artikel 34a Wbp, 2015, p. 46.

Boetemaxima	Categorieën	Boetebandbreedte (in euro's)
€ 820.000,-	I	0 - 200.000
	II	120.000 - 500.000
	III	350.000 – 820.000
€ 450.000,-	I	0 – 100.000
	II	60.000 – 300.000
	III	200.000 – 450.000
€ 20.500,-	I	0 – 12.500
	II	7.500 – 20.500

Per boetemaxima zijn er in de beleidsregels bijlagen opgenomen waarin één of meer categorieën worden toegewezen aan de overtreding van een art. en/of lid uit de Wbp.
Zo is bijvoorbeeld het niet melden van een datalek aan de AP strafbaar gesteld met een boete uit categorie II van boetemaxima € 820.000,-. Voor deze overtreding kan dus een boete worden opgelegd tussen de € 120.000,- en € 500.000,-.

De vraag rijst nu hoe het exacte boetebedrag wordt vastgesteld aangezien er aanzienlijke verschillen bestaan tussen de verschillende boetebandbreedtes. De vaststelling verloopt als volgt: indien de AP een overtreding heeft vastgesteld, bepaalt de AP eerst de 'basisboete' binnen een bandbreedte van de categorie waartoe de overtreding behoort. Deze basisboete kan vervolgens worden verhoogd of verlaagd (binnen het limiet van de bandbreedte) met het oog op de ernst van de overtreding.[61] Bij de beoordeling van de ernst van de overtreding houdt de AP rekening met de volgende factoren:
- De aard en omvang van de overtreding;
- De duur van de overtreding;
- De impact van de overtreding op de bescherming van persoonsgegevens voor de betrokkene en/of de maatschappij;
- De mate waarin de overtreding aan de overtreder kan worden verweten;
- De omstandigheden waaronder de overtreding is gepleegd;
- De financiële omstandigheden waarin de overtreder verkeert.[62]

Boeteverhogende en boeteverlagende omstandigheden
In de boetebeleidsregels worden een aantal boeteverhogende en boeteverlagende omstandigheden neergelegd. Gezien het verhogen van een boete heeft de AP de mogelijkheid om een boete op te leggen van maximaal 10% van de jaarlijkse netto-omzet als een boete van € 820.000,- (gezien de ernst van de overtreding) geen passende bestraffing met zich mee brengt. Daarnaast kan een hogere boete worden opgelegd als de overtreder al een keer eenzelfde of vergelijkbare overtreding heeft begaan of als de overtreder niet mee werkt aan het onderzoek van de AP.[63] Een boete kan verlaagd worden als de overtreder verdergaande medewerking aan de AP verleend dan waartoe hij wettelijk is gehouden, als de overtreder uit eigen beweging de overtreding beëindigd vóór bekendwording met het onderzoek van de AP of als de overtreder uit eigen beweging degenen die door de overtreding schade hebben gelden, schadeloos heeft gesteld.[64]

[61] Artikel 5 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[62] Artikel 6 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[63] Artikel 9 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.
[64] Artikel 10 Boetebeleidsregels Autoriteit Persoonsgegevens 2016.

Bindende aanwijzing
De bevoegdheid van de AP om boetes op te leggen wordt beperkt doordat de AP in de meeste gevallen als eerst een 'bindende aanwijzing' moet geven.[65] Een bindende aanwijzing wordt gezien als een soort waarschuwing. In de aanwijzing zal de AP aangeven welke wettelijke bepaling is overtreden en de overtreder opdragen om de overtreding binnen een bepaalde termijn te herstellen. Indien de aanwijzing niet wordt opgevolgd kan de AP alsnog een boete opleggen. Indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid, wordt er direct een boete opgelegd.[66]

[65] Art. 66 lid 3 Wbp
[66] Art. 66 lid 4 Wbp.

5. Algemene verordening gegevensbescherming

In 2012 heeft de Europese Commissie een voorstel voor een verordening ingediend met betrekking tot de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. De reden hiervoor is dat door de snelle en technologische ontwikkelingen nieuwe uitdagingen voor de bescherming van persoonsgegevens zijn ontstaan. Daarnaast moet de verordening de privacy van burgers versterken en de verschillen in de privacyregelgeving in de Europese unie tegengaan. De verordening stelt meer specifieke eisen aan de verwerking van persoonsgegevens. Met deze hervorming wordt de huidige privacyregelgeving grondig herzien. Tegelijkertijd brengt de AVG een aantal verruimingen van begrippen en veranderingen met zich mee.

Op 14 april 2016 heeft het Europees Parlement ingestemd met de AVG. De wetgeving is nog niet gepubliceerd in het EU publicatieblad en is dus nog niet in werking getreden. De AVG zal, eenmaal gepubliceerd, twintig dagen na de publicatie in werking treden. Na de inwerkingtreding hebben de Europese lidstaten nog twee jaar de tijd om de verordening te implementeren. Met de AVG worden de privacyregels in alle lidstaten gelijk. De Wbp is dan niet meer leidend in Nederland en vervalt.

De AVG is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens alsmede op de niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen. Wat de AVG precies inhoudt en welke veranderingen in de AVG voor SOVAK van belang zijn, worden in deze paragraaf besproken.

§ 5.1 Begrippen

De AVG introduceert nieuwe begrippen en wijzigt er een aantal. Voorbeelden hiervan zijn: ‘de bewerker’ wordt in de AVG ‘de verwerker’ genoemd en het begrip ‘ondubbelzinnig toestemming’ wijzigt naar ‘uitdrukkelijke toestemming’.[67] Voorbeelden van nieuwe begrippen zijn: ‘’genetische gegevens’’, ‘’biometrische gegevens’’ en ‘’kind’’. De meeste begrippen zijn hetzelfde gebleven, niet letterlijk maar wel qua strekking. Hierna zal alleen het begrip ‘’uitdrukkelijke toestemming’’ nader omschreven, omdat deze het meest relevant is voor dit onderzoeksrapport.

Uitdrukkelijke toestemming

De definitie toestemming is in de Wbp omschreven als: ‘’*elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegeven worden verwerkt’.* De Wbp voegt hier het criterium ‘’ondubbelzinnig’’ aan toe. Ondubbelzinnig betekent dat er geen twijfel mag bestaan over het feit dat betrokkene zijn toestemming heeft gegeven. In de Wbp is ondubbelzinnig toestemming vereist voor de verwerking van persoonsgegevens en uitdrukkelijke toestemming voor de verwerking van bijzondere persoonsgegevens. In de AVG wordt het criterium ‘’ondubbelzinnig’’ vervangen door ‘’uitdrukkelijk’’. Er is dus nog maar één manier van toestemming mogelijk en dat is de uitdrukkelijke toestemming. Met de wijziging van dit criterium is een aanscherping bedoeld ten opzichte van de toestemming van betrokkene. Een stilzwijgende of impliciete toestemming is niet meer genoeg. De betrokkene moet voortaan middels een verklaring of een andere handeling kenbaar maken dat hij toestemming verleend. Daarnaast wordt met deze wijziging ook beoogd dat betrokkene zich ervan bewust is waarvoor hij toestemming geeft. [68]

De verantwoordelijke moet aan kunnen tonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.[69] De verantwoordelijke draagt dus de

[67] In dit rapport zal de term bewerker worden gebruikt.
[68] COM(2012)11 final, p. 8.
[69] Artikel 7 lid 1 AVG.

bewijslast op dit gebied. Daarnaast heeft de betrokkene te allen tijde het recht om zijn toestemming in te trekken. [70]

§ 5.2 Verplichtingen van de verantwoordelijke

In de AVG wordt de algemene documentatie verplichting geïntroduceerd en de informatieplicht wordt sterk uitgebreid. Deze twee verplichtingen van de verantwoordelijke worden hieronder uiteengezet.

In art. 28 AVG is de algemene documentatieverplichting neergelegd. Deze verplichting komt in plaats van de verplichting om gegevensverwerking te melden bij de AP. Dit art. verplicht verantwoordelijken om alle documenten inzake de verwerking van persoonsgegevens te bewaren. De introductie en uitbreiding van de algemene documentatieverplichting ziet toe op een aansporing aan verantwoordelijken om de organisatie zo in te richten dat zij voldoen aan de verplichtingen uit de AVG. In lid 2 is opgenomen welke gegevens de documenten moeten bevatten:[71]

- Naam en contactgegevens van de verantwoordelijke;
- Naam en contactgegevens van de FG;
- De doeleinden van de verwerking;
- Persoonsgegevens betrokkenen;
- Ontvangers van persoonsgegevens (bijvoorbeeld overheidsdiensten);
- Beschrijving van de werkwijzen die er voor moeten zorgen dat de persoonsgegevens in overeenstemming met de verordening worden verwerkt.

De informatieplicht is neergelegd in art. 14 AVG. De verantwoordelijke moet op grond van de Wbp het doel van de gegevensverwerking en haar identiteit doorgeven aan de betrokkene. De verantwoordelijke zal de betrokkene nu ook moeten informeren over:[72]

- De vertegenwoordiger van de verantwoordelijke;
- De FG;
- De bewaartermijn van de persoonsgegevens;
- Het bestaan van de rechten van betrokkenen;
- Het recht om een klacht in te dienen bij de AP;
- De ontvangers van zijn/haar persoonsgegevens.

Het is mogelijk dat de Europese commissie standaardformulieren vaststelt voor het verstrekken van de verplichte informatie aan betrokkenen.[73]

§ 5.3 Rechten van betrokkenen

De rechten, die de betrokkene al had op basis van de Wbp, blijven gelden met de komst van de AVG. In de AVG worden daarentegen een aantal nieuwe rechten toegekend aan betrokkenen. Deze zullen hierna worden besproken.

Recht om vergeten te worden

Het recht om vergeten te worden is neergelegd in art. 17 AVG. Betrokkenen dienen het recht te hebben dat hun persoonsgegevens worden uitgewist en niet verder mogen worden verwerkt wanneer gegevens, gelet op het doel waarvoor ze worden verwerkt, niet langer meer nodig zijn, de gegevens onrechtmatig zijn verwerkt of wanneer de betrokkene zijn toestemming intrekt.

De verantwoordelijke dient te allen tijde gehoor te geven aan het verzoek van de betrokkene. Een uitzondering is dat de verantwoordelijke persoonsgegevens niet hoeft te wissen als deze bewaard worden voor: de uitoefening van het recht op vrijheid van meningsuiting, om redenen van algemeen belang van de volksgezondheid of ter voldoening van een wettelijke

[70] Artikel 7 lid 3 AVG.
[71] Artikel 28 lid 2 AVG.
[72] Artikel 14 AVG.
[73] Artikel 14 lid 8 AVG.

verplichting.[74] Indien gegevens zijn verstrekt aan derden, dient de verantwoordelijke deze in te lichten en te vragen de gegevens te wissen.

Recht op dataportabiliteit
De toegang tot gegevens voor betrokkenen wordt in de AVG versoepeld. De betrokkene heeft namelijk het recht alle persoonsgegevens op te vragen die hij aan de verantwoordelijke verstrekt heeft.[75] De verantwoordelijke moet dan alle gegevens aanleveren in een gestructureerd bestand. Dit wordt vaak gedaan, zodat een betrokkene de gegevens mee kan nemen naar een andere dienstverlener.

Procedures
In de AVG wordt gesproken over het inrichten van procedures die betrekking hebben op de uitoefening van de rechten van betrokkenen. Hiermee wordt bedoeld dat er elektronische indiening van verzoeken door betrokkenen mogelijk moet zijn en dat er werkinstructies moeten worden opgesteld over de termijn van beantwoording van dergelijke verzoeken.[76] Daarnaast is de verantwoordelijke verplicht om verzoeken, die geweigerd worden, te motiveren.

§ 5.4 Privacy by Design en Privacy by Default

De verantwoordelijke moet op grond van de Wbp passende technische en organisatorische beveiligingsmaatregelen nemen. De AVG voegt aan deze verplichting de twee beginselen Privacy by Design en Privacy by Default toe.[77] De verantwoordelijke dient ervoor te zorgen dat is voldaan aan deze beginselen, zowel bij het ontwerpen als bij de uitvoering van passende technische en organisatorische maatregelen.

Privacy by Design houdt in dat er tijdens de ontwikkelingen van bepaalde producten en diensten aandacht wordt besteedt aan privacyverhogende maatregelen. Door van te voren na te denken over de beveiliging van persoonsgegevens en deze beveiliging bij het ontwikkelen van systemen in te bouwen, is de kans op succes het grootst. Het doel bij Privacy by Design is de beveiliging van persoonsgegevens optimaliseren. Ook moet er rekening gehouden worden met dataminimalisatie. Dit wil zeggen dat er zo min mogelijk persoonsgegevens mogen worden verwerkt. Op deze manier wordt een zorgvuldige en verantwoorde omgang met persoonsgegevens gewaarborgd.[78] Privacy by Design is van groot belang in een organisatie. Als Privacy by Design niet juist wordt toegepast worden de privacyrisico's niet in een vroegtijdig stadium herkent. De kans is dan groot dat de noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn.[79]

Privacy by Default betekent dat door middel van systeeminstellingen maximale privacy van een betrokkene wordt gewaarborgd. De verantwoordelijke moet hiervoor technische en organisatorische maatregelen treffen. Onderdeel van Privacy by Default is het opstellen van een privacybeleid, het aanstellen van een FG en het integreren van privacy als vast onderwerp binnen de bedrijfsvoering. Voorbeelden van het ontbreken van Privacy by Default zijn:
- In algemene voorwaarden opnemen dat gegevens met derden worden gedeeld;
- Vragen om gegevens terwijl deze niet relevant zijn voor het te behalen resultaat.

Ook bij Privacy by Default moet het minimaliseren van gegevens en het beperken van de doeleinden in acht worden genomen.

[74] Artikel 17 lid 3 AVG.
[75] Artikel 18 AVG.
[76] A.W. Duthler, A.J. Biesheuvel RA RE, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.
[77] Artikel 23 AVG.
[78] A.W. Duthler, A.J. Biesheuvel RA RE, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.
[79] https://autoriteitpersoonsgegevens.nl/ (zoek op: *Privacy by Design).*

§ 5.5 Privacy Impact Assessment

Een Privacy Impact Assessment (hierna PIA) is een instrument om de risico's met betrekking tot privacy zichtbaar te maken. Wanneer verwerkingen gezien hun aard, reikwijdte of doeleinden bijzondere risico's inhouden voor de rechten en vrijheden van betrokkenen, voert de verantwoordelijke een beoordeling uit van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens.[80] In bepaalde omstandigheden wordt een PIA verplicht gesteld. Een PIA moeten worden uitgevoerd wanneer er sprake is van bijzondere risico's. Er is sprake van bijzondere risico's in geval van:

- Een systematische en uitgebreide beoordeling van de persoonlijkheidsaspecten van een natuurlijk persoon, die is gebaseerd op een geautomatiseerde verwerking;
- De verwerking van gegevens over het seksuele leven, de gezondheid, het ras of de etnische afkomst, voor het bieden van gezondheidszorg of voor onderzoek naar geestes- of besmettelijke ziekten, wanneer de gegevens op grote schaal worden verwerkt voor het nemen van maatregelen of besluiten met betrekking tot specifieke personen;
- De verwerking van grote bestanden van persoonsgegeven inzake kinderen en van genetische of biometrische gegevens;
- Andere verwerkingen die gezien hun aard, omvang en doel waarschijnlijk specifieke risico's voor de rechten en vrijheden van betrokkenen met zich meebrengen en waarvoor de AP op grond van art. 34 lid 2 AVG moet worden geraadpleegd.[81]

In een PIA moet onder andere een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de risico's, de maatregelen om de risico's te beperken en de waarborgen en beveiligingsmaatregelen die de bescherming van persoonsgegevens verzekeren, worden opgenomen.

§ 5.6 Functionaris voor de gegevensbescherming

De mogelijkheid om een Functionaris voor de gegevensbescherming (hierna FG) aan te stellen is opgenomen in de Wbp. In de AVG worden de positie en taken van de FG echter versterkt en uitgebreider omschreven. Daarnaast wordt de FG in veel gevallen verplicht gesteld.

Taken FG

Op grond van art. 35 AVG is elke verantwoordelijke voortaan verplicht een FG aan te wijzen indien het verwerken van persoonsgegevens wordt uitgevoerd door een overheidsinstantie, door een onderneming met minimaal 250 werknemers of indien de verantwoordelijke hoofdzakelijk is belast met verwerkingen die vanwege hun aard, omvang en doel regelmatige observatie van betrokkenen vereisen. De taken van de FG zijn: [82]

- Het informeren en adviseren van de verantwoordelijke (en de verwerker) over de verplichtingen die zij heeft op grond van de AVG;
- Toezien op de uitvoering en toepassing van het privacybeleid;
- Toezien op de uitvoering en toepassing van de AVG, met name ten aanzien van Privacy by Design, Privacy by Default, de gegevensbeveiliging, de informatieplicht
- Behandelen van vragen en klachten omtrent privacy van personeelsleden, klanten, patiënten;
- Toezien op de documentatieverplichting;
- Toezien op het naleven van de meldplicht datalekken;
- Toezien op de uitvoering van de PIA;
- Optreden als contactpersoon voor de AP en het verlenen van medewerking aan de AP.

Eisen aan FG

Het is belangrijk dat de FG wordt aangewezen op grond van zijn professionele kwaliteiten en op basis van zijn kennis op het gebied van de wetgeving en de praktijk inzake

[80] Artikel 33 lid 1 AVG.
[81] Artikel 33 lid 2 AVG.
[82] Artikel 37 AVG.

gegevensbescherming. De FG dient niet alleen te beschikken over juridische deskundigheid, maar hij dient ook kennis te hebben van ICT en informatiebeveiliging. De FG ziet toe op de (nieuwe) privacywet- en regelgeving binnen een organisatie. Aan de hand van bovengenoemde taken wordt de FG gezien als adviseur en toezichthouder. Tot slot moet de FG betrouwbaar zijn, wat zich onder meer kan uiten in een geheimhoudingsverklaring. [83]

Positie en bevoegdheden FG
In art. 36 AVG wordt de positie van de FG omschreven. De FG moet door de verantwoordelijke tijdig worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast moet hij zijn plichten en taken onafhankelijk kunnen uitvoeren. Hij behoort dus geen instructies te krijgen over het uitoefenen van zijn functie. De FG heeft geen formele sanctiebevoegdheden maar de organisatie moet hem wel controlebevoegdheden geven. Hieronder valt bijvoorbeeld de bevoegdheid om ruimtes te betreden, zaken te onderzoeken maar ook het vragen van inlichtingen en inzage. Een FG wordt voor twee jaar aangewezen en kan vervolgens worden herbenoemd. Hij geniet dezelfde ontslagbescherming als de leden van de ondernemingsraad. Hij kan dus pas ontslagen worden na toestemming van de kantonrechter.[84] De wet laat het vrij om iemand intern of extern aan te stellen als FG. Een externe FG verricht zijn taken op basis van een dienstverleningscontract.

§ 5.7 Sanctiebevoegdheden
De sanctiebevoegdheden van de AP zijn in de AVG behoorlijk uitgebreid, ook ten opzichte van de wetswijziging in de Wbp (zie paragraaf 4.7). De reden hiervoor is dat de Europese Commissie vindt dat afschrikkende en doeltreffende sancties van groot belang zijn om de handhaving van de wet te garanderen. [85]

In de AVG krijgt de AP de bevoegdheid om boetes op te leggen die variëren van € 250.000,- tot € 1.000.000,- en van 0,5% tot 2% van de wereldwijze jaaromzet. Er kunnen boetes worden opgelegd als er in strijd wordt gehandeld met de AVG. Enkele redenen voor het opleggen van een boete zijn:
- Het verwerken van persoonsgegevens verwerking zonder rechtmatige grondslag;
- Het ontbreken van een intern privacybeleid;
- Het niet melden van een datalek aan de AP.

Ook is er in de AVG een bepaling opgenomen waarin staat dat bij niet-opzettelijke niet-naleving van de verordening als eerst een waarschuwing kan worden gegeven. Meerdere redenen voor het opleggen van een boete staan vermeld in art. 79 AVG.

De hoogte van de boete wordt vastgesteld op grond van de aard, de ernst en de duur van de inbreuk. Daarnaast wordt gekeken naar het feit of de inbreuk opzettelijk of uit nalatigheid is gepleegd. Tenslotte spelen de genomen technische en organisatorische maatregelen en procedures een rol bij de bepaling van de hoogte van de boete. [86]

§ 5.8 Meldplicht Datalekken
In de AVG krijgt de verantwoordelijke de plicht om datalekken te melden. Deze verplichting is neergelegd in de art.en 31 en 32 AVG. De meldplicht datalekken is per 1 januari 2016 al in werking getreden. In de AVG is deze verplichting ook neergelegd en verschilt in een paar opzichten van de meldplicht datalekken zoals neergelegd in de Wbp. Deze verschillen zullen hieronder nader worden besproken.

[83] A.W. Duthler, A.J. Biesheuvel RA RE, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.
[84] https://autoriteitpersoonsgegevens.nl/ (zoek op: *Functionaris voor de gegevensbescherming)*
[85] A.W. Duthler, A.J. Biesheuvel RA RE, *Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.
[86] Artikel 79 lid 2 AVG.

Op grond van art. 31 lid 1 AVG dient de verantwoordelijke binnen 24 uur, nadat hij kennis heeft genomen van een datalek, een melding te maken bij de AP. Dit is het eerste verschil ten opzichte van de meldplicht datalekken in de Wbp, aangezien hier de termijn van 72 uur wordt bepaald.

De inhoud van de melding wordt omschreven in art. 31 lid 3 AVG. Ten opzichte van de meldplicht datalekken in de Wbp wordt er een extra eis gesteld aan de inhoud van de melding. De verantwoordelijke moet namelijk in de omschrijving van de aard van de inbreuk ook vermelden welke betrokken categorieën en het aantallen betrokkenen bij het datalek betrokken zijn.

De overige eisen die worden gesteld aan de melding van een datalek zijn gelijk aan de eisen zoals vermeld in hoofdstuk 4.

§ 5.9 Privacybeleid

De verantwoordelijke moet een privacybeleid hanteren en handhaven om te voldoen aan de eisen die voortvloeien uit de AVG. Daarnaast moest de verantwoordelijke passende maatregelen uitvoeren om ervoor te zorgen dat de verwerkingen in overeenstemming met de verordening worden uitgevoerd. Het opstellen van een privacybeleid is een verplichting die voortvloeit uit de art. 22 lid 1 AVG. Dit art. luidt als volgt: ‘’*De voor de verwerking verantwoordelijke stelt beleid vast en voert passende maatregelen uit om ervoor te zorgen en te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met deze verordening worden uitgevoerd”.*

Het nut van een privacybeleid is dat aantoonbaar kan worden gemaakt dat de eisen uit de privacyverordening worden nageleefd. Hierbij spelen de interne regelingen en werkwijzen een belangrijke rol.

6. Privacy binnen SOVAK getoetst aan de Wbp

In dit hoofdstuk wordt het beleid en de handelswijze van SOVAK omtrent het verwerken van persoonsgegevens beschreven en getoetst aan de bepalingen uit de Wbp die na inwerkingtreding van de AVG in grote lijnen hetzelfde blijven. SOVAK hanteert bij de verwerking van persoonsgegevens het reglement 'bescherming van cliëntgegevens'.[87] Dit reglement is omgezet in een werkinstructie ''privacy cliëntgegevens'', zodat het reglement ook voor medewerkers van woningen en dagactiviteitencentra leesbaar is.[88] Om de handelswijze van SOVAK goed in kaart te kunnen brengen, zijn het beleid en de werkinstructies geanalyseerd en zijn er interviews afgenomen met verschillende afdelingen. Wanneer informatie voortkomt uit een intern document of interview, wordt dit in de tekst of in een voetnoot aangegeven. Interne documenten en de uitwerkingen van interviews zijn tevens opgenomen in de bijlage. In de paragrafen 6.1 en 6.2 wordt allereerst geïnventariseerd welke gegevens er binnen SOVAK worden verwerkt en door middel van welke systemen dit gebeurd.

§ 6.1 Welke gegevens worden er verwerkt?

Een cliënt kan zich bij SOVAK aanmelden door middel van het aanmeldformulier.[89] Op het aanmeldformulier worden de persoonlijke gegevens van cliënt, de NAW-gegevens van de contactpersoon (vaak familie) en de NAW-gegevens van de wettelijk vertegenwoordiger ingevuld. Om de aanvraag in behandeling te kunnen nemen moeten er ook een aantal andere gegevens worden opgestuurd. Een aantal voorbeelden zijn:

- Geldig indicatiebewijs;
- Kopie identiteitsbewijs;
- Meest recent psychologisch onderzoek/diagnostische gegevens;
- IQ bepaling van vóór het 18e levensjaar;
- Beschrijving van eventuele bijkomende problematiek.

Wanneer overeenstemming is bereikt over de te leveren zorg, wordt een overeenkomst 'zorg en dienstverlening' opgemaakt en ondertekent door de cliënt en door de Raad van Bestuur. Vanaf dat moment is cliënt in zorg bij SOVAK. Er wordt een fysiek en digitaal dossier aangemaakt, waar alle gegevens in worden opgeslagen.

	Algemeen	**Bijzonder**	**Gevoelig**
NAW-gegevens	X		
Geboortedatum	X		
Nationaliteit	X		
Geslacht	X		
BSN-nummer	X		X
Burgerlijke staat	X		
Verzekeringsgegevens	X		
Rekeningnummer			X
Uitkering/PGB			X
Medische gegevens		X	X
Indicatie gegevens		X	X
Overige gezondheidsinformatie		X	X
IQ-score			X
Godsdienst		X	X
Kopie ID		X	X

Bovenstaande tabel is een overzicht van de gegevens die binnen SOVAK worden verwerkt. In deze tabel is weergegeven of de gegevens algemeen, bijzonder en/of gevoelig zijn. De

[87] Zie bijlage I.
[88] Zie bijlage II.
[89] Zie bijlage III.

rechtmatigheid van het verwerken van bijzondere gegevens komt aan de orde in paragraaf 6.6. Persoonsgegevens van gevoelige aard zijn het meest kwetsbaar. Er zijn dan ook passende beveiligingsmaatregelen nodig om dit soort gegevens te beschermen. Daarnaast moet bij een datalek van gevoelige gegevens een melding aan de AP worden gedaan. De beveiliging van gevoelige gegevens komt aan bod in paragraaf 6.7.

In het beleid wordt niet aangegeven welk soort gegevens er worden verzameld ten behoeve van de digitale registratie en het vormen van dossiers. In art. 5.1 van het privacyreglement wordt verwezen naar een bijlage waarin de verschillende soorten gegevens zouden zijn opgenomen. Deze bijlage is daarentegen nog niet samengesteld.

§ 6.2 Hoe worden deze gegevens verwerkt?

SOVAK verwerkt gegevens van cliënten door middel van een geautomatiseerd systeem, genaamd CURA en papieren dossiers. In deze paragraaf komen de hiervoor genoemde verwerkingen aan de orde.

Elektronisch cliëntdossier CURA[90]

SOVAK maakt voor het verwerken van cliëntgegevens sinds 1 maart 2016 gebruik van het elektronisch cliëntdossier (hierna ECD), genaamd CURA. Voorheen werd er gebruik gemaakt van een Persoonlijk Ondersteuningsplan (hierna POS). Doordat POS een inhoudelijk ingewikkeld systeem was is er de afgelopen jaren nagedacht over een nieuw ECD. Het nieuwe ECD CURA is eenvoudiger in het gebruik en minder tijdrovend. Wanneer een cliënt in zorg wordt genomen, wordt een dossier aangemaakt in CURA. In CURA staan alle gegevens die in bovenstaande tabel zijn weergegeven. Daarnaast bevat CURA ook het persoonlijk ondersteuningsplan. Het persoonlijk ondersteuningsplan van een cliënt is een bundeling van historische gegevens, recente verslaglegging en actuele observaties.

De toegang tot CURA wordt geregeld door middel van authenticaties. Dit houdt in dat iedere medeweker zijn/haar eigen inlognaam en wachtwoord heeft. De medewerkers van de woongroepen en activiteitencentra kunnen inloggen op CURA door middel van een webversie. Wat iemand binnen CURA wel of niet mag, wordt geregeld door middel van autorisaties. De afspraken over de toekenning van autorisaties is vastgesteld in het protocol ‘toegang tot cliëntgegevens’.[91] Dit protocol is opgesteld conform het privacyreglement cliëntgegevens. Tot de gegevens in CURA hebben verschillende functionarissen toegang. Het uitgangspunt is dat er alleen toegang tot de gegevens wordt verschaft aan degene die de gegevens daadwerkelijk nodig heeft bij de uitvoering van zijn/haar werkzaamheden. De functionaris kan aan de hand van de toegekende autorisaties in CURA niet méér inzien, toevoegen, wijzigen, verwijderen en/of printen dan waarvoor hij toegang heeft. Voor wat betreft de persoonlijke ondersteuningsplannen hebben alleen de functionarissen die rechtstreeks betrokken zijn bij de uitvoering van het ondersteuningsplan recht op inzage van de gegevens. Zo hebben bijvoorbeeld begeleiders alleen toegang tot dossiers betreffende de locatie waar zij werkzaam zijn. De rechten die begeleiders hebben zijn het schrijfrecht, leesrecht en printrecht. Een assistent begeleider heeft, in tegenstelling tot een begeleider, alleen het leesrecht en het recht om een rapportage te schrijven. De medewerkers van de zorgadministratie hebben wel lees-, schrijf- en printrechten met uitzondering van het persoonlijk ondersteuningsplan, omdat zij met het persoonlijk ondersteuningsplan niets van doen hebben.

De afdeling cliëntservice werkt nog niet optimaal met CURA. Stukken die binnenkomen via de post worden gescand en komen dan in de individuele map van de cliënt te staan. Deze mappen staan onder ‘mijn documenten’. Het streven is wel dat in de toekomst alleen met CURA wordt gewerkt.

[90] Informatie over CURA vloeit voort uit gesprekken met de afdeling cliëntservice en Dennis Koreman, systeembeheerder.
[91] Zie bijlage IV.

Cliëntdossiers[92]
Binnen SOVAK zijn er, naast de gegevens in CURA, ook fysieke dossiers beschikbaar. Deze dossiers bevinden zich in dossierkasten op de woningen, activiteitencentra en op de afdeling cliëntservice. De dossiers zijn aangelegd ten behoeve van specifiek onderzoek, specialistische behandeling of gerichte hulpverlening.

In de dossiers op de woongroepen bevinden zich verschillende gegevens, zoals: algemene gegevens, medicatiegegevens, cliëntgebonden wensen bv. niet-reanimeren, voedsel, activiteiten en bepaalde rapportages over cliënt. Wanneer bepaalde informatie nodig is, kan elke begeleider per cliëntdossier informatie inzien en wanneer nodig toevoegen.

De afdeling cliëntservice maakt ook nog gebruik van fysieke dossiers. De gegevens uit deze dossiers zijn ook terug te vinden in CURA en worden gebruikt als er bijvoorbeeld een evaluatie of intakegesprek met een cliënt plaatsvindt.

§ 6.3 Toepasselijkheid Wbp
De Wbp is van toepassing als er sprake is van het geautomatiseerd verwerken van persoonsgegevens. De software CURA is een voorbeeld van een geautomatiseerd systeem. In CURA worden persoonsgegevens verwerkt. De Wbp is dus van toepassing op de verwerkingen in CURA. De fysieke cliëntdossiers, die worden bewaard op de afdeling cliëntservice, woongroepen en activiteitencentra, zijn een voorbeeld van een niet-geautomatiseerde verwerking van persoonsgegevens, die in een bestand zijn opgenomen. De dossiers zijn ingedeeld op naam van de cliënt. Dit betekent dat er sprake is van een bestand, omdat de dossiers volgens enige systematiek worden opgeborgen en het betrekking heeft op personen. Ook de fysieke cliëntdossiers vallen dus onder de reikwijdte van de Wbp. SOVAK bepaalt het doel en de middelen van de verwerking. Dit wil zeggen dat SOVAK kan worden aangemerkt als de verantwoordelijke. SOVAK is, als het gaat om de verwerking van persoonsgegevens, gebonden aan de wettelijke regels van de Wbp. Wat betreft het geautomatiseerde systeem CURA is er ook sprake van een bewerker. Unit 4 is de leverancier van het programma CURA. Zij kunnen in het systeem aangezien zij de ontwikkelaar van het programma is en tevens als helpdesk fungeert. Met Unit4 is een bewerkersovereenkomst gesloten.

§ 6.4 Doeleinden
De doeleinden voor de verwerkingen zijn opgenomen in art. 3 van het privacyreglement. Art. 3 privacyreglement maakt onderscheid tussen twee soorten gegevensverzameling, namelijk de geautomatiseerde persoonsregistratie in CURA en dossiervorming. Het hoofddoel van beide gegevensverwerkingen is dat persoonsgegevens uitsluitend worden verwerkt met het oog op het verwezenlijken van de zorg- en dienstverlening aan de cliënt.
Voor de geautomatiseerde persoonsregistratie in CURA geldt het specifieke doel dat gegevens van cliënten worden geregistreerd, verzameld en bewerkt ten behoeve van het administratief en financieel afhandelen van de zorg- en dienstverlening. Voor de dossiervorming zijn ook nog een aantal specifieke doelen omschreven, namelijk dat gegevens alleen worden verwerkt ten behoeve van de ondersteuning van de uitvoering van het primaire proces, voor het controleren en toetsbaar maken van de kwaliteit van de zorg- en dienstverlening, voor verantwoording ten opzichte van de cliënt en voor het afstemmen van aspecten van de verzorging en behandeling.

De verwerkingen zijn getoetst aan de hiervoor genoemde doeleinden en komen hiermee overeen. De doelen voor de gegevensverwerking zijn volledig en voldoende duidelijk beschreven. Er zijn geen verwerkingen geconstateerd die niet verenigbaar zijn met de doelen. Daarnaast is in art. 10.2 van het privacyreglement opgenomen dat de betrokkene wordt

[92] Informatie over cliëntdossiers vloeit voort uit interviews met de afdeling cliëntservice en de woongroepen.

geïnformeerd als de gegevensverwerking voor een ander doel dan beschreven wordt gebruikt. Op basis van het beleid en de praktijk voldoet SOVAK aan de eisen die art. 7 Wbp stelt.

§ 6.5 Grondslag voor de verwerking

De grondslagen voor gegevensverwerking worden genoemd in art. 8 Wbp. Het verwerken van persoonsgegevens is alleen toegestaan indien er een rechtmatige grondslag aanwezig is. Cliënten die bij SOVAK in zorg komen ondertekenen een zorg- en dienstverleningsovereenkomst. Door middel van het ondertekenen van deze overeenkomst gaan zij ook akkoord met de algemene voorwaarden.[93] In de algemene voorwaarden wordt de gegevensverwerking onder de aandacht gebracht. Op deze manier geeft de cliënt dus ondubbelzinnige toestemming voor de gegevensverwerking. Met de komst van de AVG wordt het begrip ondubbelzinnige toestemming aangescherpt. Enkel het verwijzen naar de algemene voorwaarden is dan niet meer voldoende. Doordat dit begrip verandert met de komst van de AVG, wordt de rechtmatigheid van deze grondslag verder besproken in paragraaf 7.1.

Op grond van art. 8 lid 1 sub b mogen gegevens verwerkt worden, indien dit noodzakelijk is voor de uitvoering van de overeenkomst met cliënt. Wanneer cliënt of vertegenwoordiger geen toestemming zou geven voor de verwerking van persoonsgegevens, is het voor SOVAK onmogelijk om uitvoering te geven aan de overeenkomst. Op basis van deze grondslag mag SOVAK rechtmatig gegevens verwerken. Tenslotte is ook de grondslag van art. 8 lid 1 sub c, het verwerken van gegevens op basis van een wettelijke verplichting, van toepassing. De zorgaanbieder heeft namelijk op grond van de WGBO de plicht om dossiers aan te maken. De noodzakelijkheidseis is hierbij van belang. SOVAK kan namelijk haar wettelijke verplichting niet uitvoeren als zij geen gegevens van cliënten mag verwerken. SOVAK mag dus ook gegevens verwerken middels cliëntdossiers.

De conclusie is dat SOVAK op basis van art. 8 lid 1 sub b en c Wbp gerechtvaardigde gronden heeft voor de verwerking van persoonsgegevens.

§ 6.6 Bijzondere persoonsgegevens

Bijzondere gegevens zijn gegevens die extra risico met zich meebrengen. Deze gegevens mogen niet worden verwerkt, tenzij er een uitzondering bestaat. SOVAK verwerkt de volgende bijzondere gegevens:

- Gezondheidsgegevens;
- Godsdienst;
- Ras.

SOVAK verwerkt gezondheidsgegevens die betrekking hebben op de lichamelijke en geestelijke gesteldheid van cliënten. Deze gegevens worden zowel verwerkt in CURA als in de fysieke cliëntdossiers. Op basis van art. 21 lid 1 sub a Wbp mogen gezondheidsgegevens worden verwerkt door hulpverleners en instellingen voor de gezondheidszorg of maatschappelijke dienstverlening voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk, noodzakelijk is. SOVAK is een organisatie die mensen met een verstandelijke beperking ondersteunt op verschillende gebieden, zoals werken, wonen en vrijetijd. Het is dus noodzakelijk om gezondheidsgegevens te verwerken gezien de goede behandeling en verzorging van cliënten. Het verwerken van gezondheidsgegevens is toegestaan, aangezien SOVAK zich kan beroepen op de uitzondering uit art. 21 lid 1 sub A Wbp.

Gegevens omtrent godsdienst of levensovertuiging van een cliënt wordt geregistreerd in CURA. Het verwerken van persoonsgegevens betreffende iemands godsdienst of levensovertuiging is op grond van art. 17 lid 1 sub c Wbp toegestaan als de verwerking noodzakelijk is met het oog op de geestelijke verzorging van een betrokkene. SOVAK heeft

[93] Zie bijlage XIII.

twee geestelijk verzorgers in dienst. Zij bieden begeleiding aan cliënten bij levens- en geloofsvragen, bij ziekte, bij het rouwproces, bij ethische vraagstukken en zij verzorgen de kerkdiensten en speciale vieringen. Met het oog op de geestelijke verzorging van cliënten mag SOVAK gegevens omtrent godsdienst verwerken. Daarnaast zou een beroep kunnen worden gedaan op art. 21 lid 3 Wbp. Hierin wordt bepaald dat bijzondere persoonsgegevens ook mogen verwerkt voor zover dit noodzakelijk is in aanvulling op de verwerking van persoonsgegevens betreffende iemands gezondheid met het oog op een goede behandeling of verzorging van betrokkene. Wel dient rekening te worden gehouden met het feit dat niet iedere cliënt gebruik maakt van geestelijke verzorging. Dit betekent dat SOVAK voor deze cliënten geen gegevens omtrent godsdienst of levensovertuiging mag verwerken, tenzij die cliënt hier toestemming voor heeft gegeven. Het is gezien het voorgaande raadzaam om in een toestemmingsformulier uitdrukkelijk op te nemen dat er gegevens omtrent godsdienst of levensovertuiging worden verwerkt.

In CURA wordt van elke cliënt een kopie van het identiteitsbewijs opgeslagen. Onder ras wordt verstaan iemands huidskleur, afkomst en nationale of etnische afstamming.[94] Van de foto van het identiteitsbewijs kunnen deze eigenschappen worden afgeleid. Voor SOVAK is het noodzakelijk om een kopie van het identiteitsbewijs te maken om zo de cliënt te kunnen identificeren. SOVAK mag dus op grond van art. 18 sub A Wbp alleen gegevens van ras of etniciteit verwerken met het oog op identificatie van betrokkene en voor zover dit voor dit doel onvermijdelijk is.

§ 6.7 Verstrekken van gegevens

Gegevens mogen alleen worden verstrekt aan derden als dit verenigbaar is met de doeleinden en als er een rechtmatige grond voor bestaat. Om de zorg- en dienstverlening aan een cliënt zo goed mogelijk te kunnen uitvoeren, is het noodzakelijk dat SOVAK met instanties gegevens uitwisselt over cliënten, zoals bijvoorbeeld het zorgkantoor. SOVAK vraagt vóór het verstrekken van gegevens aan derden altijd toestemming aan de cliënt door middel van een toestemmingsformulier. In art. 12 van het privacybeleid wordt aandacht besteed aan het verstrekken van gegevens aan derden. Hierin komt naar voren dat in beginsel altijd toestemming aan de cliënt wordt gevraagd, tenzij voor zover voor de taakuitoefening noodzakelijk, degenen aan wie de gegevens worden verstrekt rechtstreeks zijn betrokken bij de actuele zorg- en dienstverlening aan de cliënt op basis van het uitvoeren van de overeenkomst of aan ziekenfonds en particuliere ziektekostenverzekeraars. SOVAK verstrekt deze gegevens in overeenstemming met de wet.

§ 6.8 Beveiliging

De verantwoordelijke moet zorg dragen voor passende technische en organisatorische maatregelen voor de beveiliging van persoonsgegevens. Een slechte beveiliging kan immers leiden tot een datalek. Om datalekken te voorkomen zijn organisaties verplicht om de persoonsgegevens die zij gebruiken te beveiligen. Daarbij geldt hoe gevoeliger de gegevens hoe beter het beveiligingsniveau moet zijn. In deze paragraaf zullen allereerst de technische beveiligingsmaatregelen en daarna de organisatorische beveiligingsmaatregelen binnen SOVAK aan de orde komen.

Technische beveiligingsmaatregelen [95]

In het kader van de meldplicht datalekken moeten organisaties voortaan zorg dragen voor moderne technieken om persoonsgegevens te beveiligen. Binnen SOVAK zijn een aantal beveiligingselementen aanwezig om persoonsgegevens technisch te beveiligen. Als eerst de systeembeveiliging. SOVAK maakt gebruik van een netwerk. Dit netwerk wordt beveiligd door middel van verschillende manieren van systeembeveiliging namelijk firewall, proxyservers en

[94] Kamerstukken II 1997/98, 25892, nr. 3, p. 104-105 (MvT).

[95] Informatie over dit onderdeel vloeit voort uit gesprekken met Dennis Koreman, systeembeheerder bij SOVAK.

virusscanners. Een firewall is een systeem dat de middelen van een netwerk kan beschermen tegen misbruik van buiten af en scant binnenkomend netwerkverkeer om ervoor te zorgen dat het geen schadelijke gegevens binnenhaalt. Een proxyserver is een aparte server tussen de computer, de gebruiker en de firewall. Door middel van een poort 'relay' wordt de beveiliging van het internetverkeer verhoogd. Daarnaast zijn er specifieke regels in het systeem ingebouwd die er voor zorgen dat er geen programma's gedownload of geïnstalleerd kunnen worden door gebruikers en dat bepaalde websites ontoegankelijk zijn als deze kwaadaardige software bevatten. Op de proxyserver zit ook een virusscanner. Dit is een andere virusscanner dan het standaard viruspakket.

Om binnen SOVAK programma's (applicaties) te beveiligen wordt er gebruik gemaakt van zogenaamde applicatiebeveiliging. Applicatiebeveiliging is het gebruik van software en procedures om applicaties te beschermen tegen externe bedreigingen. CURA is een voorbeeld van een programma waarin cliëntgegevens worden verwerkt. Voor deze applicatie moeten dus passende beveiligingsmaatregelen worden genomen, aangezien hier veel (gevoelige) gegevens in staan. Alhoewel de systeembeveiliging al een groot deel beveiligd, moeten applicaties zoals CURA extra beveiligd worden. Dit gebeurd door middel van een persoonlijke inlognaam met wachtwoord en door middel van de rechten die binnen de applicatie worden toegekend.

Om de beveiliging van het systeem van SOVAK te testen heeft er vorig jaar een security- audit plaatsgevonden door Secwatch. Dit is een onafhankelijk bedrijf dat gespecialiseerd is in beveiliging van systemen. De security experts die de audit uitvoeren zijn getraind en gecertificeerd op het gebied van databeveiliging, cybercrime, internet-technologieën en onderzoeksmethodieken.[96] In een security-audit worden verschillende aspecten van het systeem grondig onderzocht op veiligheid. Door middel van deze audit wordt getoetst of er bepaalde kwetsbaarheden in het systeem aanwezig zijn waardoor er makkelijk in het systeem kan worden ingebroken. Naar aanleiding van deze audit is de beveiliging van het systeem op verschillende punten aangescherpt.

Tenslotte zijn er voor elektronische systemen in de zorgsector nadere beveiligingseisen gesteld. Zoals al eerder in dit onderzoek naar voren is gekomen, is er voor de zorgsector een code voor informatiebeveiliging opgesteld, ook wel de NEN 7510 genoemd. De NEN 7510 biedt zorginstellingen een leidraad voor het formuleren, vastleggen en controleren van de interne informatiebeveiliging. SOVAK bewaakt de status van informatiebeveiliging met behulp van de NEN 7510. Er is een checklist beschikbaar die bestaat uit 145 vragen. Door het invullen van deze checklist is duidelijk geworden waar de risico's op het gebied van informatiebeveiliging liggen. In het intern document 'procedure NEN 7510' wordt aangegeven dat de checklist jaarlijks wordt geëvalueerd.[97] SOVAK heeft de checklist voor het laatst ingevuld in 2012. Het is dus aan te raden om de checklist (met het oog op de nieuwe privacywetgeving) binnen een kort tijdsbestek te evalueren. In de wetgeving wordt namelijk benadrukt dat de beveiliging van persoonsgegevens binnen een organisatie een blijvend punt van aandacht moet zijn om zo eventuele datalekken te voorkomen. De NEN 7510 is overigens niet verplicht gesteld.

Organisatorische beveiligingsmaatregelen[98]

Onder organisatorische beveiligingsmaatregelen wordt verstaan: ''maatregelen voor de inrichting van de organisatie''. Hieronder vallen de maatregelen die worden genomen om cliëntgegevens op de woongroepen, activiteitencentra en het hoofdkantoor te beveiligen.

[96] <www.secwatch.nl>
[97] Zie bijlage V.
[98] Informatie over dit onderdeel vloeit voort uit interviews met de afdeling cliëntservice, de woongroepen en het activiteitencentra. Zie bijlage IX tot en met XII.

Binnen het hoofdkantoor worden een aantal maatregelen genomen om cliëntgegevens te beschermen. Ten eerste is toegang tot kantoren en het archief alleen mogelijk door middel van een toegangsdruppel. Elk personeelslid heeft een toegangsdruppel en kan met deze druppel alleen de ruimtes in waarvoor hij/zij toegang nodig heeft. Binnen SOVAK geldt het beleid dat alle ruimtes bij vertrek worden afgesloten. Ten tweede geldt de regel dat alle computers worden vergrendeld wanneer de medewerker even niet op zijn/haar kantoor aanwezig is, zodat er geen onbevoegde personen bij verschillende gegevens kunnen. Op de afdeling cliëntservice staan kasten met fysieke cliëntdossiers. Er is geconstateerd dat deze aan het einde van de dag worden afgesloten.

Op de woongroepen worden de cliëntdossiers opgeborgen in een kast op het kantoor van de begeleiders. Bij het verlaten van deze ruimte wordt de kast op slot gedaan. Alleen de begeleiders hebben toegang tot het kantoor. Het is dan ook uitgesloten dat een onbevoegd persoon toegang kan krijgen tot het kantoor aangezien er altijd een begeleider op de woning aanwezig is. Persoonlijke eigendommen van cliënten, zoals bank- en identiteitspassen worden bewaard in een kluis. De code van deze kluis is alleen bekend bij de begeleiders van de woning. Als cliënten een dagje uit gaan of als er een ziekenhuis bezoek plaatsvindt worden de benodigde pasjes met daarop persoonsgegevens meegenomen. De begeleider die op dat moment zorg draagt voor de cliënt(en) zorgt ook voor de benodigde pasjes.
Er is echter geen controlesysteem (bijvoorbeeld een aftekenlijst) waar duidelijk op te zien is wie de pasjes uit de kluis heeft gehaald en of ze ook weer terug zijn gelegd.

Op het activiteitencentrum worden de fysieke dossiers bewaard in een kast op elke activiteitengroep. Elke groep heeft dus haar eigen kast waar de dossiers van de desbetreffende cliënten van die groep in worden opgeborgen. De kasten worden aan het einde van de dag op slot gedaan. Uit interviews is gebleken dat dossiers soms mee naar huis worden genomen, omdat er vaak door werkdruk geen tijd is om in het dossier een rapportage te maken. Wanneer cliëntdossiers mee naar huis worden genomen, is er geen optimale beveiliging. Medewerkers geven ook aan niet goed te weten wat de regels omtrent dit onderwerp zijn. Er zijn op dit punt niet voldoende waarborgen om de beveiliging van persoonsgegevens te garanderen.

Verder is uit verschillende interviews gebleken dat op woongroepen en activiteitencentra foto's van cliënten gemaakt worden met privéapparatuur, zoals telefoons. Uit één interview is zelfs naar voren gekomen dat er onder de medewerkers van een bepaalde woongroep een ''whatsapp groep'' bestaat waarin foto's en video's van cliënten worden gedeeld. De medewerkers zijn van mening dat dit is toegestaan aangezien er bij de aanmeldingsprocedure toestemming wordt gevraagd voor het maken en delen van foto's. Deze toestemming is er echter alleen op gericht foto's te plaatsen op onder andere de SOVAK facebookpagina, op de SOVAK website of in nieuwsbrieven. Hieruit blijkt dat medewerkers zich onvoldoende bewust zijn van de veiligheidsrisico's van dergelijk gedrag. Doordat zij de risico's onderschatten, ontstaat er een gevaar voor de privacy van cliënten (een kwetsbare doelgroep). Al met al blijkt uit de interviews dat medewerkers van woongroepen en activiteitencentra zich niet bewust zijn van de privacy risico's voor cliënten. Medewerkers zijn niet op de hoogte van het privacyreglement of de werkinstructies noch de nieuwe regels omtrent privacy zoals datalekken. Tevens verdient het de opmerking dat het beleid geen aandacht besteed aan verschillende beveiligingsaspecten in de organisatie en op welke manier deze worden gewaarborgd.

SOVAK dient zorg te dragen voor een optimaal beveiligingsniveau. Op dit moment zijn er op organisatorisch vlak binnen onvoldoende waarborgen om een passend beveiligingsniveau te garanderen. Er worden binnen SOVAK veel bijzondere en gevoelige persoonsgegevens verwerkt. De kans op onjuiste of onrechtmatige verwerking is groot en brengt veel risico's met zich mee, zoals manipulatie, discriminatie, risico op fraude etc. Er zal in de organisatie meer

bewustwording moeten worden gecreëerd en er moeten voor verschillende aspecten protocollen en werkinstructies worden opgesteld.

§ 6.9 Verplichtingen verantwoordelijke

Bewaartermijn

De wettelijke bewaartermijnen zijn in paragraaf 2.4 besproken. SOVAK heeft te maken met een bewaartermijn van vijftien jaar op grond van de WGBO. Voor dossiers van cliënten die onvrijwillig zijn opgenomen geldt een bewaartermijn van vijf jaar op grond van de Wet Bopz. In art. 9.1 privacyreglement staan de juiste bewaartermijnen genoemd. SOVAK heeft naast het beleid een document opgesteld waarin de bewaartermijnen voor cliëntgerichte documenten zijn neergelegd en wie voor de bewaartermijnen verantwoordelijk is.[99]

Een klein deel van het archief bevat cliëntdossiers. Uit eigen waarneming is gebleken dat SOVAK de bewaartermijnen goed in kaart heeft gebracht aangezien op elke archiefmap wordt aangegeven wanneer de gegevens -met inachtneming van de juiste bewaartermijn- moeten worden vernietigd. Daarentegen wordt deze vernietigingsdatum niet gehandhaafd aangezien er is geconstateerd dat er in het archief dossiers aanwezig zijn die in 2014 en 2015 vernietigd hadden moeten worden. Er kan dus worden geconcludeerd dat persoonsgegevens te lang worden bewaard, hetgeen in strijd is met de artikelen uit de Wgbo en Wet Bopz en het kwaliteitsbeginsel neergelegd in art. 11 Wbp en art. 5.3 privacyreglement.

Informatieplicht

Indien persoonsgegevens bij de cliënt (of vertegenwoordiger) worden verkregen is SOVAK verplicht om vooraf informatie aan de cliënt te verschaffen betreffende de verwerking van persoonsgegevens. Onder deze informatie wordt in ieder geval verstaan: de identiteit van de verantwoordelijke en de doeleinden waarvoor de gegevens worden verwerkt.
Wanneer een cliënt in zorg wordt genomen wordt de brochure ‘welkom bij SOVAK’ verstrekt.[100] In deze brochure komen een aantal aspecten op het gebied van privacy naar voren. Er wordt onder andere beschreven dat het reglement ‘’bescherming cliëntgegevens’’ van toepassing is, dat daarin de rechten van cliënt staan beschreven en dat er bepaalde bewaartermijnen voor dossiers gelden. Ook wordt er aangegeven dat er toestemming van de cliënt nodig is als dossier aan instanties buiten SOVAK worden verstrekt. Het privacyreglement wordt daarentegen op geen enkele manier aan cliënt ter beschikking gesteld. In art. 10.1 van het privacyreglement staat wel vermeld dat de cliënt op de hoogte wordt gesteld van het bestaan van de gegevensverwerking en het beleid. Alleen uit het interview met de afdeling cliëntservice blijkt dat hier geen uitvoering aan wordt gegeven. Aan cliënt wordt dus niet duidelijk gemaakt wie de verantwoordelijke is en voor welke doeleinden de persoonsgegevens worden verwerkt, omdat er geen inzicht wordt verworven in het privacyreglement. Cliënten dienen geïnformeerd te worden over de verwerking van persoonsgegevens in CURA en de fysieke cliëntdossiers. SOVAK voldoet dus niet aan de wettelijke informatieplicht.

Bovendien valt op te merken dat de informatieplicht in de AVG sterk is uitgebreid zoals besproken in paragraaf 5.2. Dit zal in hoofdstuk 7 verder aan bod komen.

§ 6.10 Meldplicht datalekken en uitbreiding boetebevoegdheid AP

Meldplicht datalekken

De meldplicht datalekken brengt voor SOVAK een aantal verplichtingen met zich mee. Mocht er een datalek optreden met kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens dan moet SOVAK deze binnen 72 uur melden aan de AP. Dit kan door middel van het webformulier op de website van de AP.[101] Bij twijfel of het datalek gemeld moet worden kan figuur 2 uit paragraaf 4.2 geraadpleegd worden. Daarnaast bestaat er ook de kans

[99] Zie bijlage VI.
[100] Zie bijlage VII.
[101] <https://datalekken.autoriteitpersoonsgegevens.nl>

dat SOVAK het datalek moet melden aan de betrokkene, zie hiervoor paragraaf 4.4. SOVAK moet een document opstellen waarin alle voorgekomen datalekken in worden opgenomen. Dit geldt ook voor de datalekken die niet zijn gemeld bij de AP. Tenslotte moeten afspraken omtrent datalekken en eventuele aansprakelijkheid voldoende gewaarborgd worden in een bewerkersovereenkomst. Het is belangrijk dat SOVAK de bewerkersovereenkomsten goed controleert en waar nodig in overleg met de bewerker aanpast. SOVAK houdt immers de verplichting om de meldplicht na te komen.

Om de AP binnen 72 uur te kunnen informeren moet er een goed beleid zijn. Het is onmogelijk om dit ad hoc te regelen. Een voorbereiding op een datalek is dus vereist. Zo wordt er snel en juist gehandeld en kan de schade voor SOVAK en de betrokkene beperkt blijven. Om dit te kunnen waarborgen moet er een datalekbeleid worden opgesteld waarin in ieder geval de volgende aspecten naar voren komen:

- Degene die de organisatie van een datalek op zich neemt, zijn/haar bereikbaarheid en bevoegdheden;
- Meldprotocollen voor de belangrijkste systemen, zoals plannen hoe er gemeld gaan worden aan de AP en betrokkene;
- Herstelprotocollen voor de belangrijkste datalekken, zoals hoe wordt er nazorg geleverd aan betrokkenen;
- Een registratiesysteem/document voor datalekken;
- Hoe medewerkers worden getraind en hoe systemen getest worden.

De meldplicht datalekken maakt per 1 januari 2016 onderdeel uit van de Wbp en komt ook terug in de AVG. Het is dus raadzaam om de voornoemde acties zo snel mogelijk te bewerkstelligen.

Uitbreiding boetebevoegdheid
Zoals aan de orde is gekomen in paragraaf 4.7, kan de AP hoge boetes opleggen wanneer SOVAK zich niet houdt aan de verplichtingen uit de Wbp. In de tabel op de volgende pagina is geïnventariseerd aan welke wettelijke vereisten van de Wbp SOVAK nog niet optimaal voldoet en welke boetes hieraan verbonden zijn. Ook de boetes omtrent het niet nakomen van de eisen verbonden aan de meldplicht datalekken zijn vermeld.

Overtreding	**Boetebedrag tussen**
Art. 10 Wbp Overschrijden van de bewaartermijn	€ 120.000 – € 500.000
Art. 13 Wbp Ontoereikende beveiligingsmaatregelen	€ 120.000 – € 500.000
Art. 16 Wbp Verwerken van bijzondere persoonsgegevens terwijl dit niet is toegestaan	€ 350.000 – € 820.000
Art. 33 Wbp Niet nakomen van de informatieverplichting	€ 120.000 – € 500.000
Art. 34a lid 1 Wbp Niet nakomen van de meldplicht datalekken aan de AP	€ 120.000 – € 500.000
Art. 34a lid 2 Wbp Niet nakomen van de meldplicht aan betrokkene	€ 120.000 – € 500.000
Art. 34a lid 4 Wbp Ondeugdelijke melding aan de AP	€ 0 – € 200.000
Art. 34a lid 8 Wbp Niet bijhouden van een logboek datalekken	€ 120.000 – € 500.000

Zoals al eerder aan bod is gekomen worden de boetes met in werking treden van de AVG verhoogd. Wat de precieze boetebedragen worden per overtreding staat in de verordening niet expliciet aangegeven. De bovenstaande tabel is een indicatie van de boetes die de AP op kan leggen op grond van de Wbp.

§ 6.11 Rechten van betrokkene

In art. 13 en 14 van het privacyreglement worden cliënten in de gelegenheid gesteld om het recht op inzage en het recht op correctie uit te oefenen.

Ten aanzien van het recht op inzage wordt in het beleid neergelegd dat betrokkenen schriftelijk of mondeling hun verzoek kenbaar kunnen maken. Binnen vier weken wordt op het verzoek gereageerd. In de praktijk wordt hier ook op deze manier uitvoering aan gegeven. In de algemene voorwaarden is het recht op inzage ook neergelegd. Het verdient de opmerking dat in het beleid wordt vermeld dat het recht op inzage kosteloos is, terwijl in de algemene voorwaarden een kleine vergoeding wordt gevraagd.

Ten aanzien van het recht op correctie staat in het beleid vermeld dat betrokkenen een verzoek kunnen indienen. De verantwoordelijke zorgt dat een dergelijk verzoek zo spoedig mogelijk wordt uitgevoerd. Binnen twee maanden zal de verantwoordelijke de betrokkene op de hoogte stellen of aan het verzoek is voldaan.

7. Privacy binnen SOVAK getoetst aan de AVG

In dit hoofdstuk wordt de AVG toegepast op het beleid en de werkwijze van SOVAK. Er zal naar voren komen wat de invoering van de AVG voor SOVAK betekent en op welke punten SOVAK actie moet ondernemen.

§ 7.1 Uitdrukkelijke toestemming

Aan de orde is gekomen dat het begrip ‘’ondubbelzinnige’’ toestemming voor de gegevensverwerking wijzigt in het begrip ‘’uitdrukkelijke’’ toestemming. Deze begrippen zijn eerder aan de orde gekomen in paragraaf 5.1 en paragraaf 6.5.

SOVAK moet aan kunnen tonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn of haar persoonsgegevens. Nu wordt er toestemming gegeven door het ondertekenen van de zorg- en dienstverleningsovereenkomst waar de algemene voorwaarden op van toepassing zijn. Met komst van de AVG geldt dat de betrokkene zijn of haar toestemming afzonderlijk van bepaalde documenten moet geven. Er mag dus niet meer impliciet toestemming worden gegeven. Het geven van toestemming door middel van het ondertekenen van de zorg- en dienstverleningsovereenkomst is niet meer toereikend om te voldoen aan het (nieuwe) toestemmingscriterium. Dit betekent dat de algemene voorwaarden apart ondertekent moeten worden. Een andere manier is om in de zorg- en dienstverleningsovereenkomst een passage toe te voegen waarin de verwerking van persoonsgegevens expliciet aan de orde komt.

Het is belangrijk dat de wijze waarop toestemming wordt verkregen er toe lijdt dat de betrokkene zich voldoende bewust is van het feit dat hij toestemming voor geeft en waar hij precies toestemming voor geeft. Dit moet SOVAK kunnen aantonen.

§ 7.2 Algemene documentatieverplichting

De algemene documentatieverplichting is een nieuwe verplichting die de AVG met zich meebrengt. SOVAK moet passende maatregelen nemen om aan te kunnen tonen dat de verwerken van persoonsgegevens in overeenstemming met de AVG. Onder passende maatregelen wordt ook de algemene documentatieverplichting verstaan.

Organisaties die voorheen de gegevensverwerking moesten melden aan de AP hebben waarschijnlijk al een basisdocument met daarin alle gegevensverwerkingen. Aangezien SOVAK op basis van het vrijstellingsbesluit vrijgesteld was van deze meldplicht is er binnen SOVAK nog geen document voorhanden inzake alle gegevensverwerkingen. Deze documentatie moet geordend en duidelijk zijn, zodat deze op het verzoek van de AP direct overhandigd kan worden. In paragraaf 5.2 werd toegelicht welke gegevens in de documentatie opgenomen moeten worden. Daaruit blijkt dat ook werkinstructies omtrent het verwerken van persoonsgegevens onderdeel uitmaken van de documentatieverplichting. Zoals is gebleken uit hoofdstuk 6 heeft SOVAK één werkinstructie omtrent het omgaan met cliëntgegevens. Deze werkinstructie is te beknopt en niet volledig aangezien er, zoals uit het vorige hoofdstuk is gebleken, een aantal aspecten omtrent privacy ontbreken. SOVAK zal een basisdocument moeten opstellen en de werkinstructie moet worden uitgebreid.

§ 7.3 Informatieverplichting

Zoals gebleken uit paragraaf 5.2 wordt met de invoering van de AVG de informatieplicht van de verantwoordelijke uitgebreid. In paragraaf 6.8 is naar voren gekomen dat SOVAK niet voldoet aan de huidige informatieverplichting op grond van de Wbp. Er zijn dus geen procedures of mechanismen vastgelegd om aan de verplichting om informatie aan betrokkenen over gegevensverwerking te verstrekken te voldoen.

Het is raadzaam om zo snel mogelijk een procedure in te richten om elke betrokkene te informeren over de gegevensverwerking en de overige aspecten van de informatieplicht.

SOVAK zou bijvoorbeeld alle gegevens die zij moet informeren aan betrokkene op kunnen nemen in het privacybeleid. Er moeten dan wel procedures worden ingericht om aan deze verplichting te voldoen, zoals het bijvoegen van het privacybeleid bij het aanmeldingsformulier of de zorg- en dienstverleningsovereenkomst.

In de AVG wordt vermeld dat de Europese Commissie standaardformulieren kan opstellen voor het verstrekken van de verplichte informatie. Deze formulieren zijn vooralsnog niet opgesteld. SOVAK kan dus eigen formulieren opstellen.

§ 7.4 Functionaris voor de gegevensbescherming

Het aanstellen van een FG wordt met de invoering van de AVG verplicht gesteld wanneer er meer dan 250 medewerkers werkzaam zijn binnen een organisatie. SOVAK heeft meer dan 250 medewerkers in dienst. Het aanstellen van een FG is dus verplicht voor SOVAK.[102] De taken en de positie van de FG zijn in paragraaf 5.6 aan de orde gekomen.

De FG kan helpen bij het opstellen van een compleet privacybeleid en het inrichten van bepaalde procedures en mechanismen. Ook is de FG nauw betrokken bij de toepassing van de verplichtingen tot privacy by design en privacy by default en het uitvoeren van een PIA. Een FG zou dus veel taken omtrent privacy voor SOVAK uit handen kunnen nemen. Vooral als het draait om het inrichten van procedures, het uitvoeren van PIA's en het proces rondom de meldplicht datalekken.[103] SOVAK moet wel rekening houden met de eisen die aan een FG worden gesteld. Een medewerker kan niet zomaar worden aangesteld als FG omdat deze niet onafhankelijk en onvoldoende deskundig is op het gebied van de wetgeving en de praktijk inzake gegevensbescherming. Een externe FG is hiervoor de oplossing. Een externe FG wordt aangesteld voor een periode van vier jaar op basis van een dienstverleningscontract en geniet ontslagbescherming. In de AVG staat dat de FG alleen kan worden ontslagen als hij niet langer voldoet aan de voorwaarden voor de uitvoering van zijn taken. De uiteindelijke verantwoordelijkheid blijft te allen tijde bij de verantwoordelijke van de organisatie.

§ 7.5 Privacy by Design & Privacy by Default

Nieuw in de AVG zijn de twee begrippen privacy by design en privacy by default. In paragraaf 5.4 zijn deze begrippen toegelicht. SOVAK dient tijdens het verwerken van persoonsgegeven rekening te houden met alle privacyaspecten. Ook zal SOVAK continu de beveiligingsmaatregelen moeten optimaliseren.

Ten aanzien van privacy by design moet bij het ontwerpen van een bepaald informatiesysteem die privacy van cliënten optimaal beschermd worden. Binnen de organisatie moet worden onderzocht welke technische en organisatorische maatregelen de bescherming van persoonsgegevens waarborgen. Privacy by design hangt samen met de beveiliging van persoonsgegevens en daarmee ook met het voorkomen van datalekken. Bij het maken van een systeem ter voorkoming van datalekken zal dus goed nagedacht moet worden welke maatregelen, zowel organisatorisch als technisch, er genomen gaan worden om gegevens optimaal te beschermen. Dit kan door middel van gegevensminimalisatie, afschermen van de identiteit van cliënt, transparantie over het gebruik van gegevens en het implementeren van sterke privacyregels in de organisatie.

Ten aanzien van privacy by default moet de privacy van cliënten gewaarborgd worden door middel van het beschermen van het (computer)systeem. Zoals gebleken uit paragraaf 6.7 maakt SOVAK gebruik van verschillende manieren om het systeem optimaal te beveiligen zoals firewall, proxyservers en virusscanners. SOVAK

SOVAK zal moeten inventariseren wat de organisatie nu al doet of heeft gedaan aan deze twee begrippen en of dit voldoet aan de eisen uit de AVG. Er moeten worden bekeken welke ICT-projecten of ICT-systemen er zijn en of er rekening is gehouden met de twee begrippen. Ook is het van belang om te inventariseren of in de bewerkersovereenkomst met Unit4 de

[102] Artikel 35 AVG.
[103] Artikel 36 AVG.

verantwoordelijkheden omtrent privacy by design en default en aansprakelijkheden voldoende zijn beschreven. Een PIA kan bijdragen aan het inventariseren van de huidige beschermingsmaatregelen en het in kaart brengen van de nog te treffen beschermingsmaatregelen. Meer over de PIA is te lezen in de volgende paragraaf.

§ 7.6 Privacy Impact Assessment

De PIA is in paragraaf 5.5 naar voren gekomen. Door het uitvoeren van een PIA wordt de verwerking van persoonsgegevens onderzocht en beoordeelt. Dit draagt bij aan het vermijden van privacyrisico's. Voor SOVAK is het uitvoeren van een PIA verplicht, omdat er gegevens worden verwerkt over het seksuele leven, de gezondheid en het ras van cliënten in het kader van het bieden van gezondheidszorg. Dit zijn gegevens van gevoelige aard en daarom is het essentieel dat privacyrisico's vroegtijdig in kaart worden gebracht. De resultaten van een PIA worden gebruikt om betere beveiligingsmaatregelen te treffen. Om een PIA goed te kunnen uitvoeren moet SOVAK vooraf een aantal stappen doorlopen:[104]

- Bepalen wie de PIA uitvoert;
- Verzamelen van relevantie informatie;
- Het invullen van de PIA;
- Beoordelen van de impact van bepaalde aspecten waar nog niet voldoende privacy maatregelen voor zijn;
- Het nemen van maatregelen;
- Het vermijden en verminderen van risico's;
- Opstellen van een PIA rapport.

Zoals al eerder aan de orde is gekomen heeft SOVAK de checklist van de NEN 7510 uitgevoerd. De NEN7510 is een leidraad om de informatiebeveiliging in de zorgsector te waarborgen en gaat over de gehele informatiebeveiliging binnen een organisatie. Een PIA richt zich alleen op de verwerking van bepaalde persoonsgegevens. De NEN 7510 is in tegenstelling tot een PIA niet verplicht.

NOREA (Nederlandse Orde van Register EDP-Auditors) heeft een handreiking voor het PIA-proces opgesteld. In deze handreiking is ook een PIA-vragenlijst opgenomen die SOVAK kan gebruiken bij het uitvoeren van de PIA. Het is aan te raden om deze vragenlijst in te vullen om zo inzicht te krijgen in mogelijke risico's van de gegevensverwerking. Bij het niet uitvoeren van een PIA kan door de AP een boete worden opgelegd.

§ 7.7 Rechten van betrokkenen

Het recht om vergeten te worden loopt gelijk met de naleving van de wettelijke bewaartermijnen. Er is geconstateerd dat de wettelijke bewaartermijnen niet consequent worden nageleefd. Dit betekent dat het recht om vergeten te worden niet wordt geeffectueerd.

Het recht op dataportabiliteit hangt samen met het overdragen van persoonsgegevens aan een andere dienstverlener zonder hier door de verantwoordelijke te worden weerhouden. In het beleid van SOVAK wordt het overdragen van persoonsgegevens neergelegd in art. 15. Hierin staat dat de verantwoordelijke kan weigeren het verzoek in te willigen om de in art. 15.1 genoemde redenen. Dit is in strijd met de AVG aangezien het recht op dataportabiliteit de betrokkene meer controle moet geven over zijn data. De betrokkene moet voortaan zelf kunnen bepalen wat er gebeurt met de data en bij welke dienstverlener hij deze onder wil brengen.

Aangezien deze rechten beide nieuw zijn zal SOVAK deze moeten opnemen in het privacyreglement. Tevens verplicht de AVG om procedures in te stellen die betrekking hebben op de uitoefening van de rechten van betrokkene. SOVAK zal dus zorg moeten dragen voor middelen die (elektronische) indiening van een hier bovengenoemd verzoek mogelijk maken.

[104] NOREA, *Privacy Impact Assessment: introductie, handleiding en vragenlijst.* www.norea.nl.

8. Conclusies en aanbevelingen

Gedurende dit onderzoek heeft de volgende vraag centraal gestaan: ‘*’Welke aanpassingen zijn nodig in het beleid en de werkwijze van SOVAK als gevolg van de invoering van de AVG en de meldplicht datalekken en uitbreiding boetebevoegdheid, ten aanzien van de verwerking van persoonsgegevens van cliënten?”.* In dit hoofdstuk zullen de belangrijkste conclusies aan de orde komen. Tot slot zullen er aanbevelingen worden gegeven.

§ 8.1 Conclusies

Binnen SOVAK zijn enorm veel persoonsgegevens van cliënten beschikbaar waar elke dag bewust, maar ook onbewust mee wordt gewerkt. De verwerking van persoonsgegevens gebeurt door middel van het elektronisch cliëntdossier CURA en door middel van fysieke cliëntdossiers die zich bevinden op de woongroepen en activiteitencentra. Het waarborgen van de privacy van cliënten is belangrijk aangezien SOVAK te maken heeft met een kwetsbare doelgroep. Om de privacy van cliënten te waarborgen is SOVAK gehouden aan de privacywetgeving, namelijk de huidige Wbp en de aankomende AVG. De AVG is tijdens dit onderzoek aangenomen door de Europese Commissie. Dit betekent dat elke organisatie in 2018 volledig aan de nieuwe privacywetgeving moet voldoen. De meldplicht datalekken en de uitbreiding boetebevoegdheid maken tevens onderdeel uit van de AVG, maar zijn per 1 januari 2016 al van kracht geworden in de huidige Wbp. De AVG zal de Wbp geheel gaan vervangen. De algemene strekking van de Wbp is in de AVG overgenomen en blijft dus hetzelfde. De algemene elementen van de Wbp zijn daarom alsnog getoetst, aangezien niet geheel duidelijk was of SOVAK hieraan voldeed. Aan de hand van de uitwerkingen van de deelvragen is gebleken dat de handelswijze en het privacybeleid van SOVAK nog niet geheel voldoen aan de privacywetgeving. Hierna worden de geanalyseerde resultaten besproken.

§ 8.1.1 Resultaten op basis van de eisen uit de huidige privacywetgeving

- *Bewaartermijn*
  Een van de verplichtingen uit de Wbp is de bewaartermijn. SOVAK valt onder de bijzondere wet WGBO waarin een bewaartermijn is neergelegd van vijftien jaar. De cliëntdossiers bevatten verschillende gegevens zoals personalia, indicatiestelling, de zorg- en dienstverleningsovereenkomst en kopie ID. Op dit moment handelt SOVAK in strijd met de bewaartermijn, omdat in het archief cliëntdossiers zijn aangetroffen die langer dan vijftien jaar worden bewaard.

- *Gegevens over godsdienst*
  SOVAK verwerkt van alle cliënten gegevens omtrent godsdienst. Godsdienst is een bijzonder persoonsgegeven en mag alleen worden verwerkt indien hier een uitzonderingsgrond voor bestaat. SOVAK kan zich beroepen op de uitzonderingsgrond dat het verwerken van gegevens over iemands godsdienst noodzakelijk is met het oog op de geestelijke verzorging van een cliënt. Binnen SOVAK zijn er geestelijke verzorgers werkzaam die geestelijke verzorging bieden aan cliënten. Alleen van cliënten die gebruik maken van geestelijke verzorging of hier behoefte aan hebben mogen de gegevens over godsdienst worden verwerkt. Van alle overige cliënten is uitdrukkelijke toestemming nodig. Zonder deze toestemming mogen deze gegevens niet worden verwerkt. SOVAK vraagt alleen toestemming voor de verwerking van persoonsgegevens, maar nog niet specifiek voor het verwerken van gegevens omtrent godsdienst.

- *Beveiligingsmaatregelen*
  SOVAK is verplicht om passende technische en organisatorische beveiligingsmaatregelen te treffen. Geconcludeerd kan worden dat SOVAK op technisch gebied veel waarborgen biedt voor de beveiliging van persoonsgegevens.
  Op organisatorisch gebied zijn de beveiligingsmaatregelen echter ontoereikend. Onder organisatorische maatregelen vallen maatregelen over de inrichting van de organisatie, instructies, protocollen en trainingen. Op het gebied van privacybescherming is er maar

één werkinstructie beschikbaar waarin aspecten over organisatorische beveiligingsmaatregelen onbesproken blijven. Er zijn dus vrijwel geen instructies waarin wordt aangegeven hoe er met verschillende soort gegevens van cliënten moet worden omgegaan. Op de woongroepen en dagactiviteitencentra zijn geen instructies hoe om te gaan met bepaalde gegevens en foto's van cliënten. Tevens zijn de medewerkers van de woongroepen en dagactiviteitencentra zich onvoldoende bewust van de privacyrisico's die er kunnen ontstaan. Dit komt voornamelijk omdat hier geen organisatorische maatregelen voor worden getroffen. Een kans op een inbreuk op de beveiliging van persoonsgegevens is dus groot. Dit brengt kansen op datalekken met zich mee. Om een optimaal beveiligingsniveau op organisatorisch gebied te garanderen zal SOVAK moeten beginnen met het creëren van privacybewustzijn bij de medewerkers. Dit kan door het opstellen van instructies en het geven van voorlichtingen over de privacywetgeving en mogelijke privacyrisico's.

- *Meldplicht datalekken*
  Er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot deze gegevens horen te hebben. Een datalek is het gevolg van het ontbreken van passende technische of organisatorische maatregelen. Alleen de inbreuken waarvan redelijkerwijs kan worden aangenomen dat er een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens moeten door SOVAK worden gemeld. Soms moet een datalek ook worden gemeld aan de betrokkene. Daarnaast bestaat de verplichting om een logboek bij te houden met daarin alle voorgekomen datalekken. De meldplicht datalekken speelt een belangrijke rol in een organisatie zoals SOVAK. Om te voldoen aan de verplichtingen die de meldplicht datalek met zich meebrengt zal SOVAK een datalekbeleid op moeten stellen. Het is ook belangrijk om in bewerkersovereenkomsten afspraken te maken omtrent datalekken. Komt SOVAK één van de verplichtingen uit de meldplicht datalekken niet na, dan kan de AP een forse boete opleggen.

- *Uitbreiding boetebevoegdheid*
  In de Wbp zijn per 1 januari 2016 ook nieuwe regels omtrent het opleggen van boetes neergelegd. De boetes zijn fors omhoog gegaan en kunnen worden opgelegd wanneer SOVAK zich niet houdt aan de regels uit de Wbp. Uit de boetebeleidsregels, die het AP heeft gepubliceerd, blijkt dat boetes kunnen oplopen tot wel € 820.000,-.
  Zoals eerder naar voren is gekomen anticipeert deze nieuwe regelgeving zich op de AVG. In de AVG worden de boetes verhoogd tot wel € 1.000.000,- en van 0,5% tot 2% van de wereldwijze jaaromzet. Vaak wordt er als eerst een bindende aanwijzing gegeven. Dit is een kans om de overtreding ongedaan te maken of enigszins te herstellen. De kans dat een boete wordt opgelegd wordt hierdoor een stuk kleiner voor SOVAK. De hoogte van de boete wordt vastgesteld op grond van de aard, de ernst en de duur van de inbreuk. Ook wordt gekeken of het feit of de inbreuk opzettelijk of uit nalatigheid is gepleegd. Tenslotte spelen de genomen technische en organisatorische maatregelen en procedures een rol bij de bepaling van de hoogte van de boete. In de tabel op paragraaf 6.8 is naar voren gekomen welke boetes SOVAK riskeert op het moment dat zij de genoemde wettelijke verplichtingen niet nakomt

§ 8.1.2 Resultaten op basis van de eisen uit de AVG

- *Algemene documentatie- en informatieplicht*
  Op basis van de Wbp bestaat de informatieverplichting. In de AVG wordt deze aangescherpt. In art. 14 AVG is opgenomen wat SOVAK dient op te stellen ten aanzien van de informatie die de verantwoordelijke moet verstrekken aan de betrokkene. SOVAK informeert de cliënten over de gegevensverwerking door middel van een pagina uit de welkomstbrochure. Dit is echter onvoldoende, omdat hier niet alle elementen uit de informatieplicht in terug komen. De algemene documentatieverplichting uit art. 28 AVG is een nieuwe verplichting. SOVAK dient alle

documenten inzake de gegevensverwerking te bewaren. De inhoud van de documentatieverplichting komt terug in art. 28 AVG.

- *Uitdrukkelijke toestemming*
  Het toestemmingscriteria wordt met ingang van de AVG verscherpt. De verantwoordelijke moet kunnen aantonen dat de betrokkene expliciet toestemming heeft gegeven voor de verwerking van persoonsgegevens. Binnen SOVAK tekenen cliënten de zorg- en dienstverleningsovereenkomst waarop de algemene voorwaarden van toepassing zijn. In de algemene voorwaarden komt de toestemming van de verwerking van persoonsgegevens aan bod. Gezien het begrip uitdrukkelijke toestemming zal SOVAK er voor moeten zorgen dat de betrokkene expliciet toestemming geeft voor de verwerking van persoonsgegevens. Is er geen toestemming verleend door de betrokkene dan is de gegevensverwerking onrechtmatig.

- *De functionaris voor de gegevensbescherming*
  Met het inwerkingtreden van de AVG zal voor sommige organisaties het aanstellen van een FG verplicht worden. De criteria voor het verplicht aanstellen is dat er minimaal 250 medewerkers in dienst moeten zijn. SOVAK voldoet aan dit criterium en moet (intern of extern) een FG aanstellen.

- *Privacy Impact Assessment*
  SOVAK is voortaan verplicht om PIA's uit te voeren, omdat zij bijzondere gegevens verwerkt. Door het uitvoeren van een PIA worden mogelijke bedreigingen en risico's bij het verwerken van persoonsgegevens in kaart gebracht. Door middel van het uitvoeren van de NEN 7510 heeft SOVAK de risico's omtrent informatiebeveiliging in kaart gebracht. Een PIA haalt echter specifiek de risico's bij het verwerken van persoonsgegevens naar voren.

- *Nieuwe rechten betrokkene*
  De AVG introduceert nieuwe rechten voor de betrokkene, namelijk het recht om vergeten te worden en het recht op dataportabiliteit. Het recht om vergeten te worden wil zeggen dat de betrokkene het recht heeft dat zijn of haar persoonsgegeven worden gewist en niet verder worden verwerkt indien dit gelet op het doel niet langer meer nodig is. Het recht op dataportabiliteit houdt in dat de betrokkene het recht heeft om alle persoonsgegevens op te vragen die de verantwoordelijke onder zich heeft.

- *Privacybeleid*
  Een privacybeleid wordt in de AVG verplicht gesteld voor elke organisatie die persoonsgegevens verwerkt. SOVAK maakt gebruik van het 'Reglement bescherming van cliëntgegevens' en voldoet daarmee aan deze verplichting. Om een goed intern beleid te kunnen voeren is het nodig om de organisatie door middel van werkinstructies, protocollen en procedures zodanig in te richten dat het beleid daarmee kan worden uitgevoerd. Van belang is dat SOVAK kan aantonen dat aan de eisen uit de AVG wordt voldaan. Op dit moment kan geconcludeerd worden dat SOVAK de uit de wet voortvloeiende privacy eisen goed in kaart heeft gebracht en deze in het beleid heeft uitgedrukt. Daarentegen ontbreekt het aan werkinstructies, protocollen en procedures waarmee een effectief beleid kan worden gevoerd. Bovendien valt op te merken dat de verplichting tot het nemen van passende technische en organisatorische beveiligingsmaatregelen niet is opgenomen in het beleid. Met het oog op nieuwe verplichtingen uit de AVG zal het beleid op een aantal punten moeten worden aangevuld.

§ 8.2 Aanbevelingen

Om ervoor te zorgen dat het beleid en de handelswijze van SOVAK voldoet aan de nieuwe privacywetgeving worden de volgende aanbevelingen gedaan.

Aanbevelingen met betrekking tot de huidige privacyregelgeving

- *Privacybewustzijn creëren*
  De medewerkers zijn niet bekend met de verplichtingen die voortvloeien uit de (nieuwe) privacywetgeving. Door middel van voorlichtingen en werkinstructies moet dit onder de aandacht worden gebracht. Ook zal SOVAK procedures moeten instellen om te kunnen toetsen dat de verwerking van persoonsgegevens in overeenstemming met de geldende wet- en regelgeving en het beleid gebeurt. Deze toetsing kan bijvoorbeeld gebeuren door middel van interne of externe controleurs. Door dit te bewerkstelligen wordt bovendien het beveiligingsniveau op organisatorisch gebied gewaarborgd. Werkinstructies, voorlichtingen en procedures spelen een belangrijke rol bij het uitvoeren van het beleid maar vooral bij het creëren van privacybewustzijn.

- *Vernietigen van dossiers in het archief conform bewaartermijn*
  In het archief zijn dossiers geconstateerd waarvan de bewaartermijn is verstreken. SOVAK handelt op dit punt in strijd met de Wbp. Deze gegevens moeten zo snel mogelijk vernietigd worden.

- *Opstellen datalekbeleid inclusief logboek*
  Het is voor een organisatie, zoals SOVAK, noodzakelijk om een protocol te hebben waarin actiepunten staan vermeld die moeten worden ondernomen op het moment dat er sprake is van een datalek. Dit zorgt ervoor dat SOVAK sneller kan handelen op het moment dat er daadwerkelijk een datalek voordoet. Elk datalek, gemeld of niet gemeld, moet worden opgenomen in een document. Het is aan te bevelen dat een logboek wordt opgesteld waarin alle datalekken worden geregistreerd.

- *Opstellen datalekprotocol*
  Het lekken van persoonsgegevens moet zoveel mogelijk worden beperkt. Het is daarom raadzaam om een datalekprotocol te hanteren. In een datalekprotocol kunnen gedragsregels en richtlijnen worden neergelegd ten aanzien van het verantwoord en onverantwoord gebruik van ICT-voorzieningen, foto's en video's. Een datalekprotocol kan helpen om menselijke fouten zoveel mogelijk te voorkomen en eventuele schade te beperken. Een werkinstructie voor de medewerkers van de woongroepen en activiteitencentra kan een deel uit maken van het datalekprotocol. In deze instructie komt naar voren wat een datalek is, hoe een datalek wordt voorkomen en wat er moet gebeuren als er een datalek wordt geconstateerd. De werkinstructie draagt bij aan het beperken van datalekken en tevens aan het creëren van privacybewustzijn in de organisatie.

Aanbevelingen met betrekking tot de AVG

- *Aanstellen FG*
  SOVAK wordt verplicht om een FG aan te stellen. De FG kan SOVAK helpen bij het opstellen van een datalekbeleid en het uitvoeren van PIA's. Ook ziet een FG toe op de naleving van het datalekprotocol. De aanbeveling is om extern een FG aan te stellen aangezien een FG deskundig moet zijn op het gebied van privacy. Door de vele kwaliteiten die de FG moet bezitten, het uitgebreide takenpakket en de eis van onafhankelijkheid is het niet aan te raden om een FG intern aan stellen. Een externe FG wordt benoemd voor de periode van twee jaar.

- *Aanvullingen in het beleid*
  Het reglement bescherming van cliëntgegevens moet, naar aanleiding van de AVG, op verschillende punten worden aangevuld. Aan het reglement moeten de volgende

elementen worden toegevoegd: nieuwe rechten van betrokkenen, informatie over de FG en welke taken en bevoegdheden deze heeft, passages omtrent de meldplicht datalekken waarin wordt verwezen naar het datalekbeleid en passages omtrent de verschillende beveiligingsmaatregelen.

- *Inrichten procedures rechten betrokkenen*
  De AVG is verplicht om procedures in te stellen, zodat betrokkenen hun rechten kunnen uitoefenen. SOVAK zal zorg moeten dragen voor middelen en procedures die – elektronische- indiening van verzoeken door cliënten of wettelijk vertegenwoordigers mogelijk maakt.

- *Voldoen aan algemene documentatie- en informatieplicht*
  Om te voldoen aan de algemene documentatieplicht zal SOVAK een algemeen document moeten opstellen waarin alle informatie omtrent de verwerking van persoonsgegevens is neergelegd. Om te voldoen aan de informatieplicht moet SOVAK de betrokkene voorafgaand aan de verwerking op de hoogte stellen van haar identiteit, de gegevensverwerking, de doeleinden, de bewaartermijnen, de FG en de rechten van betrokkene. SOVAK moet zorgen dat deze gegevens worden opgenomen in het beleid. Aan elke cliënt die in zorg komt, wordt het beleid, eventueel in een simpele versie, meegegeven. Een andere optie is om de pagina over privacy in de welkomstfolder aan te vullen.

- *Vragen om uitdrukkelijke toestemming*
  SOVAK zal uitdrukkelijke toestemming aan betrokkenen moeten vragen voor het verwerken van zijn of haar persoonsgegevens. Dit kunnen zij het beste bewerkstelligen door een passage toe te voegen aan de zorg- en dienstverleningsovereenkomst. Er kan ook een apart toestemmingsformulier, inzake de gegevensverwerking, worden opgesteld die elke cliënt, naast de zorg- en dienstverleningsovereenkomst, ondertekent.

Bronnenlijst

Literatuur

Fennell, Kroes & Koppejan 2015
S. Fennell, R. Kroes & F. Koppejan, *Privacy wetgeving inclusief voorgestelde meldplichten, boetes en concept algemene verordening gegevensbescherming,* Oisterwijk: Wolf Legal Publishers 2015.

Gellaerts & Jobse 2011
S. Gellaerts & C. Jobse, *Inleiding ICT & Recht,* Deventer: Kluwer 2011.

Hooghiemstra & Nouwt 2014
T.F.M. Hooghiemstra & S. Nouwt, *Sdu Commentaar Wet bescherming persoonsgegevens,* Den Haag: Sdu Uitgevers 2014.

Hutter, Katus, Terstegge & Versmissen 2015
J. Hutter, S. Katus, J. Terstegggе & K. Versmissen, *Grip op datalekken,* Deventer: Kluwer 2015.

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

Sauerwein & Linnemann 2002
L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002.

Thole, Van der Jagt & Roerdink 2010
E. Thole, F van der Jagt & H. Roerdink, *50 vragen over privacy,* Deventer: Kluwer 2010.

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

De Vries & Rutgers 2012
H.H. de Vries & D.J. Rutgers, *Actualiteiten sociaal recht: Wet bescherming persoonsgegevens,* Deventer: Kluwer 2012.

Handleidingen

College bescherming persoonsgegevens, *CBP Richtsnoeren beveiliging van persoonsgegevens,* 2013.

A.W. Duthler en A.J. Biesheuvel RA RE, *Het Europees privacyrecht in beweging, een overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors*, februari 2013.

L.B. Sauerwein en Mr. J.J. Linnemann Ministerie van Justitie, *Handleiding wet bescherming persoonsgegevens*, Den Haag: april 2002.

NOREA – de beroepsorganisatie van IT-auditors, Privacy Impact Assessment: introductie handleiding en vragenlijst, 2013.

Parlementaire stukken

Kamerstukken II 1997/98, 25 892, nr. 3.
Memorie van toelichting: Wet bescherming persoonsgegevens

Kamerstukken II 2012/13 33 662, nr 3.
Memorie van toelichting: Wet meldplicht datalekken.

Kamerstukken II 2014/15, 33 662, nr 11.
Nota naar aanleiding van het nader verslag.