

# Periodieke Rapportage

Op weg naar voortdurende privacy compliance

Versie 1.01  
Maastricht, November 2019

# Inhoud

<b>1.</b>	<b>Inleiding</b>	<b>4</b>
1.1.	Algemeen	4
1.2.	Autoriteit Persoonsgegevens	5
1.3.	Functionaris voor Gegevensbescherming	5
1.4.	Werkzaamheden Functionaris voor Gegevensbescherming	5
1.5.	Periodieke rapportage Functionaris voor Gegevensbescherming	6
1.6.	Rapportage.	7
<b>2.</b>	<b>De Algemene Verordening Gegevensbescherming</b>	<b>8</b>
2.1.	Basisbegrippen	8
2.1.1.	Persoonsgegevens	8
2.1.2.	Verwerking	8
2.1.3.	De verwerkingsverantwoordelijke:	8
2.1.4.	De verwerker:	8
2.1.5.	De betrokkene:	9
2.1.6.	Bijzondere categorieën van persoonsgegevens:	9
2.1.7.	Wettelijke Identificatienummers:	9
2.2.	Rechtmatigheid van gegevensverwerking	9
2.2.1.	Beginnelsen bij de verwerking van persoonsgegevens	10
2.2.2.	De beginselen van proportionaliteit en subsidiariteit	11
2.2.3.	Rechtmatigheidsgronden	11
<b>3.</b>	<b>Normenkader</b>	<b>13</b>
3.1.	Doelstelling	13
3.2.	Privacy Baseline	13
3.3.	Volwassenheidsniveau	14
3.4.	Afbakening	15
3.5.	ISO/IEC 27701:2019	15
<b>4.</b>	<b>Privacy Baseline bevindingen en aanbevelingen</b>	<b>16</b>
4.1.	Het beleidsdomein	16
4.1.1.	B.01 Privacybeleid	17
4.1.2.	B.02 Organieke inbedding	19
4.1.3.	B.03 Risicomanagement, Privacy by Design en de GEB	22
4.1.4.	Resultaat gap-analyse beleidsdomein	25
4.2.	Het uitvoeringsdomein	26
4.2.1.	U.01 Doelbinding gegevensverwerking	26
4.2.2.	U.02 Register van verwerkingsactiviteiten	28
4.2.3.	U.03 Kwaliteitsmanagement	31
4.2.4.	U.04 Beveiligen van de verwerking van persoonsgegevens	32
4.2.5.	U.05 Informatieverstrekking betrokkene bij verzameling persoonsgegevens	34
4.2.6.	U.06 Bewaren van persoonsgegevens	36
4.2.7.	U.07 Doorgifte persoonsgegevens	37
4.2.8.	Resultaat gap-analyse uitvoeringsdomein	39
4.3.	Het Control- of Beheerdomein	40
4.3.1.	C.01 Intern toezicht	40
4.3.2.	C.02 Toegang gegevensverwerking voor betrokkenen	42
4.3.3.	C.03 Meldplicht Datalekken	43
4.3.4.	Resultaat gap-analyse Control- of Beheerdomein	45
4.4.	Resultaat Gap-analyse.	46

<b>5.</b>	<b>Vervolgstappen en prioritering</b>	<b>47</b>
5.1.	Focus Autoriteit Persoonsgegevens 2020 - 2023 en focusgebied Digitale Overheid.....	47
5.1.1.	Databeveiliging	47
5.1.2.	Smart cities	47
5.1.3.	Samenwerkingsverbanden / ongeoorloofd delen	48
5.1.4.	Verkiezingen en microtargeting	48
5.2.	Vervolgstappen en prioritering	49
<b>6.</b>	<b>In kort bestek</b>	<b>50</b>
<b>7.</b>	<b>Bijlagen</b>	<b>53</b>
7.1.	Bijlage A – Positionering Provinciaal Overleg Functionarissen voor Gegevensbescherming ....	53
7.2.	Bijlage B – Onderzoek Autoriteit Persoonsgegevens Haga Ziekenhuis	55
7.3.	Bijlage C – Lijst gebruikte afkortingen	58
7.4.	Bijlage D – Bronvermelding	59

# 1. Inleiding

## 1.1. Algemeen

In Nederland wordt privacy sinds 25 mei 2018 beschermd door de in heel Europa geldende Algemene Verordening Gegevensbescherming (AVG). Deze Europese wet is direct van toepassing in alle landen van de Europese Unie. Nationale privacywetten, zoals de Wet bescherming persoonsgegevens (Wbp) die in Nederland gold, zijn met de inwerkingtreding van die Europese verordening komen te vervallen. In het Engels wordt de AVG, General Data Protection Regulation (GDPR) genoemd.

De AVG verschilt op een aantal punten van de oude Wbp, en gaat strenger om met privacy. Zo worden de rechten van de personen over wiens privacy het gaat, versterkt en uitgebreid. De AVG is, anders dan de Wbp, van toepassing in heel Europa en op alle Europese burgers. Ook krijgen organisaties die persoonsgegevens gebruiken, meer verantwoordelijkheden en verplichtingen. Zo worden organisaties verplicht om bijvoorbeeld als ze toestemming hebben gekregen om persoonsgegevens te gebruiken, die toestemming te kunnen aantonen. De veranderingen zitten in de sfeer van accountability (aantoonbaar in control zijn) en handhaving (de boetebedragen zijn naar het niveau van commerciële wereldspelers getild).

De AVG is daarnaast meer uitgesproken en concreet gericht op verbetering van de rechtspositie van de “betrokkenen” (bijvoorbeeld burgers en medewerkers). Betrokkenen kunnen onder de AVG gemakkelijker controleren wat er met hun persoonsgegevens wordt gedaan en door wie ze verwerkt worden. De AVG brengt een uitbreiding van het inzage- en correctierecht en introduceert formeel het recht op vergetelheid. Het recht op vergetelheid is niet van toepassing bij verwerkingen op basis van een wettelijke taak.

Voor overheidsorganisaties is het vanuit een voorbeeldfunctie en uitstraling (het zijn van een betrouwbare overheid) van belang om zorgvuldig met de gegevens van personen om te gaan.

De AVG is een Europese verordening. Dit betekent dat decentrale overheden en betrokkenen rechtstreeks aan de regels gebonden zijn en zich ook direct op de bepalingen kunnen beroepen. De AVG biedt de lidstaten echter nog wel ruimte om bepaalde keuzes te maken. In Nederland zijn deze uitgewerkt in de Uitvoeringswet AVG (UAVG), waarmee ook de Wet bescherming persoonsgegevens is ingetrokken.

Al deze genoemde Europese en nationale wetgevingen kenmerken zich door het streven om het vertrouwen in de wijze waarop organisaties omgaan met persoonsgegevens te bevorderen en daarmee het vrije verkeer van goederen en diensten op Europees en internationale niveau te bevorderen.

De AVG is een omvangrijk stuk wetgeving met slechts een beperkte schriftelijke toelichting. Op veel punten is het daarom (nog) onduidelijk wat de precieze invulling is die gegeven moet worden aan begrippen en bepalingen. Verdere verduidelijking en invulling van deze Europese wet is aan de toezichthouder(s) en de (Europese) rechter.

## **1.2. Autoriteit Persoonsgegevens**

In de AVG staat dat elke lidstaat van de Europese Unie een privacyautoriteit heeft die onafhankelijk toezicht dient te houden op het gebruik van persoonsgegevens. In Nederland is dat de Autoriteit Persoonsgegevens (AP). De AP houdt onder andere toezicht op de naleving van de wettelijke regels voor de bescherming van persoonsgegevens, geeft advies omtrent nieuwe wetgeving, behandelt klachten, verschaft helderheid over de uitleg van wettelijke normen en heeft internationale taken.

Voor het uitvoeren van hun taken hebben de toezichthouders verschillende soorten bevoegdheden gekregen onder de AVG. Ze hebben de bevoegdheid om controles te verrichten en alle informatie te verkrijgen die voor het toezicht nodig is. Ze hebben de bevoegdheid gekregen tot het nemen van corrigerende maatregelen, het kunnen vorderen van inlichtingen en het betreden van plaatsen. De Autoriteit Persoonsgegevens heeft naast een boetebevoegdheid ook de mogelijkheid om een last onder bestuursdwang op te leggen.

De AP heeft de bevoegdheid om organisaties te gelasten om alle voor de uitvoering van haar taken vereiste informatie te verstrekken evenals de bevoegdheid om toegang te verkrijgen tot alle persoonsgegevens en de middelen die worden gebruikt voor de verwerking van persoonsgegevens. De AVG vereist daarnaast expliciet dat organisaties desgevraagd mee moeten werken met de toezichthouder bij het vervullen van haar taken. Wanneer de provincie een verzoek krijgt van de AP dient hieraan alle medewerking verleend te worden.

De AP heeft een uitgebreid onderzoek<sup>1</sup> uitgevoerd bij een Nederlands ziekenhuis. De volledige rapportage<sup>2 3</sup> van dit onderzoek geeft een goed beeld van de bevoegdheden van de van de AP en de mogelijkheid om een last onder bestuursdwang op te leggen.

## **1.3. Functionaris voor Gegevensbescherming**

Een andere belangrijke wijziging is dat organisaties intern hun privacy(beleid) beter moeten organiseren. Privacy dient (mede) een belangrijke plaats te krijgen en te houden in organisaties. Een maatregel om dat te bereiken is, volgens de AVG, het aanwijzen van een interne privacy toezichthouder. Die persoon wordt Functionaris voor Gegevensbescherming (FG) genoemd. Overheidsinstanties en publieke organisaties zijn altijd verplicht om een FG aan te stellen, ongeacht het type gegevens dat ze verwerken. Het kan gaan om de rijksoverheid, gemeenten en provincies. De provincie Limburg is verplicht<sup>4</sup> tot het hebben van een Functionaris voor Gegevensbescherming.

## **1.4. Werkzaamheden Functionaris voor Gegevensbescherming**

Onder de AVG is het aanstellen van een FG, een interne toezichthouder op de verwerking van persoonsgegevens, voor de provincie verplicht. De FG moet zonder instructies zijn werkzaamheden uit kunnen voeren en rapporteert rechtstreeks aan de algemeen directeur over zijn werkzaamheden. De FG heeft geen formele bevoegdheid om een bindend advies te geven, maar zijn oordeel is wel ‘zwaarwegend’. De FG moet zelfs controlebevoegdheden krijgen om ruimten te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen.

---

<sup>1</sup> <https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers>

<sup>2</sup> [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit\\_haga\\_-\\_ter\\_openbaarmaking.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf)

<sup>3</sup> [https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/haga\\_rapport\\_def.pdf](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/haga_rapport_def.pdf)

<sup>4</sup> AVG art. 37 lid 1a.

Voor de provincie zijn de taken van de FG als volgt vormgegeven waarbij uit is gegaan van de wettelijke vereisten met enkele aanvullingen:

- Toezien op de naleving van de AVG, andere relevante privacywetgeving en het provinciale privacybeleid, waaronder de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van betrokken personeel en betreffende audits;
- Adviseren over gegevensbeschermingseffectbeoordelingen (Data Protection Impact Assessments (DPIA's) en toezien op de uitvoering daarvan.
- Samenwerken met toezichthoudende autoriteiten (zoals de Autoriteit Persoonsgegevens) en optreden als provinciaal contactpunt voor toezichthoudende autoriteiten, waaronder met betrekking tot voorafgaande raadpleging en andere aangelegenheden.
- Helpen privacyklachten tot een goed einde te brengen (ombudsfunctie).
- Bij privacyincidenten adviseren over ernst en omvang.
- Toezien op het verwerkingsregister.
- Advieslid van de provinciale werkgroep privacy en informatiebeveiliging.
- Periodiek (minimaal halfjaarlijks) verslag uitbrengen van zijn/haar werkzaamheden aan de Algemeen directeur/secretaris.

### **1.5. Periodieke rapportage Functionaris voor Gegevensbescherming**

Dit is het tweede verslag van de Functionaris voor Gegevensbescherming (FG) van de provincie Limburg.

In eerste instantie is gekozen om vertrouwd te raken met de organisatie, cultuur en werkzaamheden van de medewerkers in relatie tot privacy.

Dit is gebeurd door middel van deskresearch en gesprekken met medewerkers van verschillende clusters. In de beginperiode is ook meegelopen met de privacy coördinator voor de creatie van bekendheid van de FG. Rondlopen en gesprekken voeren leidt er ook vaker toe dat er meteen van de situatie gebruikt wordt gemaakt om bepaalde topics dan maar meteen te bespreken.

Er is in deze fase voor gekozen om als teamlid van het Privacy en Informatiebeveiligingsteam prioriteiten in de uitvoering te adviseren en mede te bepalen omtrent een mogelijke aanpak waarbij de uitvoering door het privacyteam is opgepakt. In een latere fase, wanneer de organisatie opereert op een hoger volwassenheidsniveau zal meer de nadruk gaan liggen op auditing.

Deze eerste rapportage is ook opgezet vanuit de gedachte dat implementatie van privacy niet kan zonder framework, handvatten die de organisatie helpen om de implementatie volgens een bepaalde structuur te organiseren. Op dit framework wordt later uitgebreid ingegaan.

Voor vervolgrapportages zal bepaald worden wat een prettig format hiervoor is. Gedacht wordt aan een (veel) minder omvangrijke rapportage met een kortere tussenperiode gebaseerd op het framework.

Op het gebied van samenwerkingen met andere organisaties zijn er een aantal samenwerkingsverbanden waarbij de FG van de provincie Limburg is aangesloten:

- Het Provinciaal Overleg Functionarissen voor Gegevensbescherming (POFG) onder coördinatie van BIJ12.

Dit overleg vindt tweemaandelijks plaats en alle provincies nemen deel. Het overleg vindt plaats op locatie bij BIJ12. Een kwestie die hier speelt is de positionering van dit Provinciaal Overleg Functionarissen voor Gegevensbescherming in relatie tot het IPO. In Bijlage A is gemotiveerd waarom het IPO het POFG zou dienen te faciliteren. Dit schrijven wordt ondersteund door alle FG's van de provincies.

- Het Regionaal Privacy Overleg welke gecoördineerd wordt door de gemeente Kerkrade.

Dit overleg vindt maandelijks plaats bij de gemeente Kerkrade. De hoeveelheid deelnemers is wisselend. FG's en privacy coördinatoren van gemeenten en gemeenschappelijke regelingen in Limburg nemen hierin deel. In 2019 is de samenstelling van de groep sterk uitgebreid en de samenwerking verbeterd. Wel dient vermeld te worden dat de topics veelal van toepassing zijn op de gemeentelijke overheid.

#### **1.6. Rapportage.**

Deze rapportage kent de volgende opbouw:

In hoofdstuk 2 worden enkele AVG begrippen besproken omdat het van belang is om de betekenis te kennen van begrippen die in de AVG en in deze rapportage gebruikt worden.

In hoofdstuk 3 wordt kort uitleg gegeven over het gebruikte normenkader waarmee de provincie Limburg handvatten heeft voor verdere implementatie van de AVG binnen de organisatie en welke gebruikt kan worden om te bepalen in hoeverre de organisatie aan privacy wet- en regelgeving voldoet. Daarnaast helpt deze Privacy Baseline bij het maken van afwegingen omtrent zaken die nog opgepakt dan wel verbeterd dienen te worden.

Hoofdstuk 4 gaat in op de Privacy Baseline waarbij in de besproken domeinen en subdomeinen uitleg gegeven wordt omtrent de specifieke aspecten van de baseline, de risico's bij het niet voldoen en waarin bevindingen en adviezen zijn opgenomen.

Ieder hoofddomein wordt in dit hoofdstuk afgesloten met de resultaten van een uitgevoerde gap-analyse met als afsluiting een totaaloverzicht van de gap-analyse. Bij een vervolgmeting zouden verbeteringen duidelijk zichtbaar moeten zijn.

Hoofdstuk 5 gaat kort in op de focusgebieden van de AP, vervolgstappen en de prioritering hiervan.

In hoofdstuk 6 worden in heel kort bestek diverse topics aangehaald waar het afgelopen jaar aandacht aan is besteed.

## 2. De Algemene Verordening Gegevensbescherming

### 2.1. Basisbegrippen

In dit rapport worden een aantal begrippen gebruikt. De definitie van deze begrippen worden in artikel 4 van de AVG duidelijk omschreven. Het is van belang om de helderheid te onderkennen van de definitie die de AVG aan deze begrippen toekent. Dit geeft namelijk inzicht in de onderliggende rechten en plichten, de daarmee samenhangende aansprakelijkheid en de daarbij horende privacy documenten.

#### 2.1.1. Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals: een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon<sup>5</sup>.

#### 2.1.2. Verwerking

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens<sup>6</sup>.

Zodra er enige feitelijke macht over persoonsgegevens is, is de AVG van toepassing. Hiervoor hoeft niet altijd sprake te zijn van menselijke tussenkomst. Ook volledig geautomatiseerde vormen van verwerking vallen onder de wettelijke regeling van de AVG.

#### 2.1.3. De verwerkingsverantwoordelijke:

De verwerkingsverantwoordelijke is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt<sup>7</sup>. Het feitelijke beheer over de gegevensverwerking kan daarentegen toch aan een ander worden opgedragen.

#### 2.1.4. De verwerker:

De verwerker is een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt<sup>8</sup>. Dit doet de verwerker in overeenstemming met de instructies van de verwerkingsverantwoordelijke en onder diens (uitdrukkelijke) verantwoordelijkheid.

---

<sup>5</sup> AVG art. 4, lid 1.

<sup>6</sup> AVG art. 4, lid 2.

<sup>7</sup> AVG art. 4, lid 7.

<sup>8</sup> AVG art. 4, lid 8.



### **2.1.5. De betrokkene:**

Een natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

### **2.1.6. Bijzondere categorieën van persoonsgegevens:**

Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid<sup>9</sup>. Deze verwerkingen zijn verboden tenzij er een beroep gedaan kan worden op een specifieke wettelijke uitzondering en op 1 van de 6 grondslagen voor het verwerken van ‘gewone’ persoonsgegevens<sup>10</sup>.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekersapp worden verwerkt, ziekte en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media.

Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid<sup>11</sup>.

### **2.1.7. Wettelijke identificatienummers:**

In artikel 44 van de Uitvoeringswet Algemene verordening gegevensbescherming wordt het gebruik van een identificatienummer, zoals een BSN, genoemd. Artikel 44 van genoemde uitvoeringswet zegt hierover: “Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet”<sup>12</sup>.

Het mag duidelijk zijn dat een dergelijk uniek identificatienummer de koppeling van verschillende bestanden aanzienlijk vergemakkelijkt en daarmee een extra bedreiging voor de persoonlijke levenssfeer van betrokkenen vormen.

## **2.2. Rechtmatigheid van gegevensverwerking**

De bescherming van persoonsgegevens is een grondrecht. Persoonsgegevens mogen alleen worden verwerkt, indien de doeleinden hiervoor zijn vastgelegd. Daarbij geldt dat verwerking enkel mag gebeuren met toestemming van de betrokkene of wanneer sprake is van een gerechtvaardigde grondslag. De wet voorziet in de grondslagen voor de rechtmatige verwerking van persoonsgegevens.

In hoofdstuk II van de AVG wordt het toetsingskader voor de rechtmatige verwerking van persoonsgegevens uiteengezet. De artikelen in dit hoofdstuk beogen de eerlijke verwerking van gegevens en voorzien in de gerechtvaardigde grondslagen waarop verwerking gebaseerd kan worden.

---

<sup>9</sup> AVG art 9, lid 1.

<sup>10</sup> AVG art 9, lid 2, 3.

<sup>11</sup> Model Gegevenseffectbeschermingsbeoordeling Rijksdienst (PIA) v1.0 sept 2017 pagina 21

<sup>12</sup> Uitvoeringswet AVG art. 44.

### 2.2.1. Beginselen bij de verwerking van persoonsgegevens

Elke verwerking van persoonsgegevens moet in lijn zijn met de hieronder genoemde beginselen. Dit accountability-principe is, onder de naam “verantwoordingsplicht”, ook in de AVG terechtgekomen. Het komt erop neer dat de verwerkingsverantwoordelijke, de provincie, moet waarborgen dat de verwerking conform de AVG wordt uitgevoerd. Het gaat hier om maatregelen voorafgaand aan, tijdens en rondom de verwerking. Daarnaast dient de organisatie te kunnen aantonen dat deze *in control* is.

De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn (“rechtmatigheid, behoorlijkheid en transparantie”)

Uitgangspunt is dat persoonsgegevens alleen mogen worden verwerkt voor gerechtvaardigde doeleinden. Dit betekent dat de verwerking noodzakelijk moet zijn met het oog op het bereiken van specifiek in de verordening genoemde doelen, dan wel dat er toestemming is verkregen van degene wiens gegevens worden verwerkt. Wanneer het gerechtvaardigd is om persoonsgegevens te verwerken, dan moet de verwerking ervan vervolgens netjes en verantwoord gebeuren. Ten slotte moet duidelijk zijn voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt. Persoonsgegevens verwerken zonder dat ook maar iemand daarvan weet, is niet toegestaan.

De verwerking moet gebonden zijn aan specifieke verzameldoelen (“doelbinding”)

Persoonsgegevens mogen alleen worden verzameld en verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer de gegevens later voor een ander doel worden gebruikt, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel.

De gegevens moeten toereikend, ter zake dienend en beperkt tot het noodzakelijke zijn (“minimale gegevensverwerking”)

Wanneer persoonsgegevens worden verwerkt dan moeten zij voor het doel toereikend en ter zake dienend zijn. Verder mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk voor het doel. Met andere woorden, er mogen gelet op het doel, niet te veel, maar ook niet te weinig gegevens worden verwerkt voor het doel. Wanneer u namelijk te weinig gegevens verwerkt, dan kan er ten onrechte een onvolledig beeld ontstaan van de betrokkene.

De gegevens moeten juist zijn (“juistheid”)

De verwerkingsverantwoordelijke moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd.

De gegevens mogen niet langer worden bewaard dan nodig (“opslagbeperking”)

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Wanneer de gegevens niet langer noodzakelijk zijn, dan moeten zij worden vernietigd of gewist.

De gegevens moeten goed beveiligd zijn en vertrouwelijk blijven (“integriteit en vertrouwelijkheid”)

Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Voor al de bovenstaande beginselen geldt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving<sup>13</sup> en kan aantonen dat de gegevensverwerking in lijn is met de beginselen (de verantwoordingsplicht).

### **2.2.2. De beginselen van proportionaliteit en subsidiariteit**

Bij iedere verwerking van persoonsgegevens dient voldaan te worden aan de beginselen van proportionaliteit en subsidiariteit. Daarbij moet er een belangenafweging worden gemaakt, waarbij de belangen van de verwerkingsverantwoordelijke en die van de betrokkene tegen elkaar worden afgewogen. De gerechtvaardigde gronden van de verwerkingsverantwoordelijke moeten zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of moeten een rechtsoverweging betreffen. Is hier geen sprake van, dan is verwerking niet toegestaan. Met het proportionaliteitsbeginsel wordt bedoeld dat niet meer gegevens mogen worden verwerkt dan nodig is om het doel te bereiken.

Het subsidiariteitsbeginsel houdt in dat eerst gekeken moet worden of een minder ingrijpend middel voor de hand ligt om een doel te kunnen bereiken.

### **2.2.3. Rechtmatigheidsgronden**

Het verwerken van persoonsgegevens is alleen rechtmatig, indien de verwerking is gebaseerd op een van de rechtmatigheidsgronden van de AVG<sup>14</sup>. De verordening kent zes rechtmatigheidsgronden.

1. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.
2. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
4. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.

---

<sup>13</sup> Niet alleen aan de eisen uit de AVG maar ook naleving van de Uavg (en eventuele andere uitvoeringswetten).

<sup>14</sup> Artikel 6, lid 1, AVG

5. De verwerking is noodzakelijke voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.
6. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde. Hierbij geldt dat belangen, grondrechten of de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan die van de verwerkingsverantwoordelijke.

Deze lijst is limitatief. Voor een verwerking betekent dit dat er minimaal één van bovenstaande grondslagen van toepassing dient te zijn op de verwerking. Wel kan een verwerking onder meerdere grondslagen tegelijk vallen.

Indien de organisatie zich op grondslag 5 beroept dan dient het hierbij te gaan om taken die in de wet zijn vastgelegd en die relevant zijn voor de organisatie.

### 3. Normenkader

#### 3.1. Doelstelling

Artikel 24 van de AVG beschrijft de verantwoordelijkheid van de verwerkingsverantwoordelijke<sup>15</sup>. Het kan voor organisaties een uitdaging zijn om op een juiste manier met de persoonsgegevens om te gaan. Wat, waar, door wie en op welke wijze zaken geregeld moeten worden om de informatiele privacy op een juiste wijze te waarborgen is voor (medewerkers van) organisaties niet altijd duidelijk.

Het voldoen aan de wet- en regelgeving betekent het nemen van de juiste maatregelen binnen de organisatie en in de techniek. Een begrip dat hierbij gehanteerd wordt is “Privacy volwassenheid”. “Privacy volwassenheid” geeft aan hoe volwassen een organisatie omgaat met de borging van informatiele privacy (eerbiediging van de persoonlijke levenssfeer<sup>16</sup>). Bij het bepalen van de volwassenheid moeten organisaties nagaan in welke mate zij de correcte omgang met persoonsgegevens hebben geborgd binnen hun organisatie, hoe gestructureerd zij de privacy beschermt bij de verwerking van persoonsgegevens.

Daarom dient voldoen aan de AVG niet beschouwd te worden als het repareren van geconstateerde afwijkingen maar dient het een gestructureerde en planmatige aanpak te kennen.

#### 3.2. Privacy Baseline

Het zou eenvoudig zijn om een aantal aanbevelingen te geven om geconstateerde bevindingen te verhelpen. De vraag hierbij is dan of dit in deze fase de juiste werkwijze zou zijn en op welke wijze deze aanbevelingen opgepakt kunnen worden om te implementeren in de organisatie. In feite zouden deze aanbevelingen een vertaling van vigerende wetgeving zijn. Hierbij is het niet onbelangrijk om nieuwe kennis en/of nieuwe inzichten mee te kunnen nemen in een implementatietraject en daarna. Denk hierbij bijvoorbeeld aan nieuwe beleidsregels die door de Autoriteit Persoonsgegevens (AP) gepubliceerd worden.

Om op een juiste manier Privacy te kunnen implementeren in de organisatie is het zeer gewenst om gebruik te maken van een levend normenkader. Het uitgangspunt hierbij zou moeten zijn dat er door gebruik te maken van publiekelijk beschikbare, relevante informatie meer bereikt kan worden. De provincie Limburg heeft besloten om hiervoor het normenkader van het Centrum Informatiebeveiliging en Privacybescherming (CIP) te gebruiken.

Het CIP is een publiek-private netwerkorganisatie die bestaat uit Participanten en Kennispartners. Participanten zijn overheidsbedrijven waarvan medewerkers meedoen aan een of meer van de werkverbanden binnen de samenwerking. Kennispartners zijn marktpartijen die met een convenant verbonden zijn en een hoeveelheid uren hebben toegezegd in de samenwerking. Het CIP werkt op basis van “voor allen, door allen”.

Het CIP streeft ernaar om kennis ook in overdraagbare producten te vervatten om zo ook bij te dragen aan het bekijken daarvan en het daadwerkelijk toepassen in zowel overheidsorganisaties als bij marktpartijen die in de rol van leverancier of ketenpartner betrokken zijn bij de overheid.

---

<sup>15</sup> Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

<sup>16</sup> Grondwet art. 10.

Een van de producten van het CIP is de Privacy Baseline. In de Privacy Baseline zijn de eisen van de AVG vertaald naar concrete, hanteerbare normen die duidelijk maken wat organisaties moeten doen om in overeenstemming met de wet, de privacy van de betrokkenen te waarborgen.

Dit normenkader, de Privacy Baseline van de CIP, wordt gehanteerd om stapsgewijs de bescherming van persoonsgegevens verder te implementeren in de organisatie.

Hiertoe wordt ook – in eerste instantie – gebruik gemaakt van de tool “Gap-analyse Privacy”. Dit is een tool waarmee de organisatie getoetst wordt aan alle criteria van de Privacy Baseline.

In een latere fase zal overgestapt worden naar het Privacy Volwassenheidsmodel.

De producten van het CIP vallen onder een Creative Commons Naamsvermelding-GelijkDelen 4.0 Internationaal-licentie.

### **3.3. Volwassenheidsniveau**

Het kan voor organisaties een uitdaging zijn om op een juiste manier met de persoonsgegevens om te gaan. Wat, waar, door wie en op welke wijze zaken geregeld moeten worden om de informationele privacy op een juiste wijze te waarborgen is voor (medewerkers van) organisaties niet altijd duidelijk.

“Privacy volwassenheid” geeft aan hoe volwassen een organisatie omgaat met de borging van informationele privacy (eerbiediging van de persoonlijke levenssfeer). Bij het bepalen van de volwassenheid moeten organisaties nagaan in welke mate zij de correcte omgang met persoonsgegevens hebben geborgd binnen hun organisatie, hoe gestructureerd zij de privacy beschermt bij de verwerking van persoonsgegevens.

In het volwassenheidsmodel zijn 5 niveaus te onderkennen; 1 tot en met 5.

Het volwassenheidsniveau 0 is het niveau waarbij een organisatie zich niet druk maakt om privacy.

Wanneer privacy binnen een organisatie situationeel op verwerkingsniveau is ingericht, komt deze organisatie niet hoger dan niveau 1.

Op niveau 2 is grip op privacy gebaseerd op beslissingen die door meerdere personen gezamenlijk op een vastgelegde wijze worden genomen. Op dit niveau is er dan sprake van beheerste processen, maar is de aantoonbaarheid van hoe aan de wet- en regelgeving wordt voldaan nog beperkt.

Op niveau 3 werkt de organisatie organisatiebreed aan privacy en kan dit worden aangetoond. Niveau 3 kan aldus als een minimumniveau gezien worden om aan de wet- en regelgeving te voldoen. Simpelweg omdat de wet- en regelgeving de aantoonbaarheid vereist.

Door de volwassenheid van de organisatie op niveau 4 te brengen wordt niet alleen aan de wet- en regelgeving voldaan, maar kan er ook actief op wijzigingen worden geanticipeerd.

Op niveau 5 is privacy een speerpunt op alle niveaus binnen de organisatie geworden en krijgt het ook aandacht in communicatie uitingen naar publiek of klanten.

Het streven van de organisatie zou moeten zijn om binnen korte termijn voor een groot deel volwassenheidsniveau 3 bereikt te hebben conform de analyse van de Privacy Baseline en daardoor compliance aan de AVG te kunnen aantonen.

### 3.4. Afbakening

Randvoorwaarden voor implementatie zijn de AVG, de uitvoeringswet AVG, Memorie van Toelichting, sectorale wetgevingen, beleidsregels Autoriteit Persoonsgegevens en richtlijnen van de European Data Protection Board<sup>17</sup>/Article 29 Data Protection Working Party<sup>18</sup>. De EDPB onderschrijft de richtsnoeren van de WP29 conform de publicatie op de website van de EDPB<sup>19</sup>.

Het dient voor de organisatie ook volledig duidelijk te zijn aan welke overige wet- en regelgeving op het gebied van bescherming van persoonsgegevens zij zich dient te conformeren.

De Autoriteit Persoonsgegevens is een zelfstandig bestuursorgaan met als taken: toezicht, advisering, voorlichting, informatieverstrekking & verantwoording en internationale taken.

De taak van voorlichting en informatieverstrekking is hierbij interessant. De interpretatie van de wet kan in de praktijk soms lastig zijn. Daarom publiceert de AP over bepaalde onderwerpen beleidsregels (voorheen richtsnoeren genoemd). In deze thematische beleidsregels legt de AP de wettelijke normen uit. Hierdoor kan het voorkomen dat de uitleg anders is dan eerder geïnterpreteerd waardoor het normenkader aanpassing nodig heeft. Daarom is het nodig om gebruik te maken van een dynamisch Nederlands normenkader.

### 3.5. ISO/IEC 27701:2019

In aanvulling op de ISO/IEC 27001 en ISO/IEC 27002 is in augustus 2019 de ISO/IEC 27701 gepubliceerd. Dit nieuwe kader geeft de randvoorwaarden en richtlijnen voor het opzetten, implementeren, onderhouden en verbeteren van een Privacy Informatie Management Systeem (PIMS).

Hierbij dienen zich een aantal vragen aan.

- Hoe verhoudt deze ISO norm zich tot de door de provincie Limburg gehanteerde Privacy Baseline?
- Indien de provincie Limburg de ISO/IEC 27001 implementeert en zich hiervoor certificeert, dient dan afgestapt te worden van de Privacy Baseline en dient de provincie dan te opteren voor certificatie op basis van ISO/IEC 27701? Dit is dan mede afhankelijk van de 27001-scope.
- Hoe dient het traject van *continues improvement* zoals gehanteerd binnen een framework met continue verbeterproces gezien te worden in het licht van het boetebesluit van juli 2019 aangaande een ziekenhuis in Den Haag? In bijlage B is een samenvatting van de rapporten en een eigen interpretatie hiervan gegeven. Op eigen titel.

Tijdens de implementatie van de ISO/IEC 27001 zoals deze naar verwachting in 2020/2021 gaat plaatsvinden, zullen ook antwoorden op de hierboven gestelde vragen gegeven dienen te worden.

---

<sup>17</sup> [https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines\\_en](https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en)

<sup>18</sup> [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index\\_en.htm](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm)

<sup>19</sup> [https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb\\_en](https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en)

## 4. Privacy Baseline bevindingen en aanbevelingen

De Privacy Baseline kent de volgende 3 delen:

1. Het Privacy beleid van de organisatie, het beleidsdomein.
2. De eisen aan de uitvoering van de AVG, het uitvoeringsdomein.
3. Controle/beheer van het privacybeleid, het control- of beheerdomein.

Het beleidsdomein bestaat uit de volgende subdomeinen:

- B.01 – Privacybeleid
- B.02 – Organieke inbedding
- B.03 – Risicomanagement, Privacy by Design en de GEB

Het uitvoeringsdomein bestaat uit de volgende subdomeinen:

- U.01 – Doelbinding gegevensverwerking
- U.02 – Register van verwerkingsactiviteiten
- U.03 – Kwaliteitsmanagement
- U.04 – Beveiliging van de verwerking van persoonsgegevens
- U.05 – Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens
- U.06 – Bewaren van persoonsgegevens
- U.07 – Doorgifte persoonsgegevens

Het control- of beheerdomein bestaat uit de volgende subdomeinen:

- C.01 – Intern toezicht
- C.02 – Toegang gegevensverwerking voor betrokkenen
- C.03 – Meldplicht Datalekken

### 4.1. Het beleidsdomein

*Inleiding:*

Hierin zijn richtlijnen opgenomen voor het algemeen beleid rondom privacy. Met dit beleid geeft de organisatie zowel de eigen clusters als andere partijen duidelijkheid over de kaders waarbinnen de verwerkingen van persoonsgegevens plaatsvinden. Dit beleid beschrijft ook aan welke voorwaarden processen en systemen moeten voldoen en hoe dit beleid op naleving wordt gecontroleerd.

*Doelstelling:*

De doelstelling van het beleidsdomein is om ervoor te zorgen dat op strategisch niveau afdoende randvoorwaarden en condities aanwezig zijn om de persoonsgegevens verantwoord te verwerken en de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen.



#### 4.1.1. B.01 Privacybeleid

##### *Inhoud:*

Privacybeleid geeft op organisatie en strategisch niveau duidelijkheid en daarmee sturing aan de inrichting van privacy. Het privacybeleid geeft aan op welke wijze - door het treffen van maatregelen - voldaan wordt aan de van toepassing zijnde wet- en regelgeving. Omdat de wet- en regelgeving externe factoren zijn, is periodieke review nodig om vast te stellen of het beleid nog voldoet. Het volstaat dus niet om eenmalig beleid op te stellen en niet meer aan te passen. Maar ook interne factoren, zoals onvoldoende effectiviteit van het beleid en gewijzigde missie of visie kunnen bepalend zijn om te komen tot aanpassing van het beleid. Door het beleidsproces cyclisch in te richten wordt bereikt dat het beleid op de ontwikkelingen en de uitvoering is afgestemd.

##### *Doelstelling:*

De ontwikkeling van de organisatie tot een organisatie die aantoonbaar aan wet- en regelgeving voldoet (ofwel: “compliant” is aan wet- en regelgeving), vraagt om een cyclisch proces. Dit houdt in dat er sprake is van een terugkoppelmechanisme waarbij - door inzicht in de uitvoering - het beleid kan worden bijgestuurd en gecorrigeerd. Afspraken hoe dit cyclische proces vormgegeven wordt, maakt onderdeel uit van het beleid.

##### *Risico:*

Het ontbreken van of het hebben van een verouderd privacybeleid kan ertoe leiden dat de organisatie geen duidelijkheid heeft wat precies wordt verwacht en dat er geen verantwoording afgelegd kan worden aan de betrokken partijen over hoe zij privacy borgt.

##### *Bevindingen:*

Op het moment dat de AVG van toepassing was op 25 mei 2018 had de provincie Limburg nog geen vastgesteld privacybeleid. Wel was er een privacybeleid in voorbereiding en in concept aanwezig.

In de loop van de tweede helft van 2018 is dit beleid verder ontwikkeld en aangescherpt. Het Privacybeleid provincie Limburg 2018 is vastgesteld door het college van Gedeputeerde Staten op 30 oktober 2018 en gepubliceerd<sup>20</sup>.

De provincie Limburg heeft een privacybeleid waarin is vastgelegd en bekrachtigd op welke wijze persoonsgegevens in overeenstemming met de wet en behoorlijk en zorgvuldig worden verwerkt.

Diverse adviezen in relatie tot de evaluatie zullen met het Privacy en Informatiebeveiligingsteam gedeeld worden voor analyse en eventuele aanpassing.

In januari 2019 is het privacybeleid gepubliceerd op het (oude) intranet. Het privacybeleid is vindbaar binnen het (nieuwe) Social Intranet indien er actief naar gezocht wordt binnen de Selfservicedesk (Topdesk omgeving). Vanuit de hoofdpagina is het document niet te vinden. Het is bij medewerkers onduidelijk of er wel een privacybeleid binnen de organisatie aanwezig is. Uit de interactie met verschillende medewerkers blijkt dat de wettelijke kaders voor de verwerking van persoonsgegevens niet algemeen bekend zijn binnen de organisatie maar steeds bekender worden. Vanuit de organisatie komen ook steeds meer vragen of

---

<sup>20</sup> <https://zoek.officielebekendmakingen.nl/prb-2018-8377.html>

bepaalde zaken zonder meer mogen en bij twijfel en/of de behoefte om te weten dat men correct handelt, wordt eerder dan voorheen contact opgenomen met de Privacy coördinator (Zie Organieke inbedding).

In het collegeprogramma 2019-2023 is in hoofdstuk II, Uitgangspunten voor 2019 – 2023, tevens een punt met betrekking tot privacy opgenomen. Dit is een van de uitgangspunten die de basis vormen voor het programma. Punt 7 luidt: “Privacy is een groot goed. Wij respecteren de persoonlijke levenssfeer van de inwoners van Limburg. De provincie Limburg voert een privacybeleid dat voldoet aan de relevante, actuele wetgeving, jurisprudentie en ontwikkelingen.” Hier kan de vraag gesteld worden of de persoonlijke levenssfeer van alleen inwoners van Limburg gerespecteerd zullen worden.

Ontwikkelingen in relevante wet- en regelgeving wordt actief door de organisatie gevolgd zodat een eventuele impact hiervan en de benodigde middelen hiervoor tijdig bekend kunnen zijn. Echter in het beleid wordt beschreven dat sectorspecifieke privacywetgeving (hoofdstuk 2) in een separaat register wordt opgenomen. Deze is (nog) niet aanwezig dan wel niet compleet.

Er is binnen de organisatie aandacht besteed aan het vastgestelde privacybeleid van de provincie Limburg en zou ook algemeen bekend dienen te zijn. Aandacht aan het privacybeleid is gegeven door gesprekken met cluster managers, presentaties en workshops voor clusters, publicaties op het intranet. Verdere doorvertaling van het privacybeleid naar de clusters is een volgende stap.

#### *Aandachtspunten/advies:*

Met het opstellen van het privacybeleid wordt bereikt dat er op organisatie- en strategisch niveau duidelijkheid wordt gegeven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van gegevens op een rechtmatige wijze plaatsvindt. De vervolgstappen behelzen de uitvoering van dit beleid waardoor privacy aantoonbaar wordt geborgd in de organisatie.

Hierbij dient onder meer met de volgende aspecten rekening gehouden worden. Ook bij volgende revisies:

- Het beleid geeft duidelijkheid over hoe de verantwoordelijken hun verantwoordelijkheid voor de naleving van de beginselen en de rechtsgrondslagen invullen en dit kunnen aantonen ("verantwoordingsplicht")<sup>21</sup>.
- Het privacybeleid is tot stand gekomen langs een cyclisch proces.
- Het bestuur/management van de organisatie heeft het privacybeleid vastgesteld, bekrachtigd en gecommuniceerd binnen de organisatie.
- De organisatie heeft vastgesteld en vastgelegd welke wet- en regelgevingen gelden.
- In het beleid is vastgelegd en bekrachtigd op welke wijze invulling wordt gegeven aan de eisen van de sectorspecifieke wetgeving.

Eerder is gesteld dat het zinvol zou zijn als de provincie Limburg extra aandacht besteed aan het vastgestelde privacybeleid door bijvoorbeeld een bericht op intranet en door het informeren van de clustermanagers waarbij ze gewezen worden op het privacybeleid. Deze acties zijn uitgevoerd waarbij meermaals het bestaande beleid onder de aandacht is gebracht. Tevens is dit met de clusterambassadeurs privacy besproken.

---

<sup>21</sup> AVG art. 5 lid 2.

Een evaluatie van het beleid is geagendeerd voor het laatste kwartaal van 2019. Bewaking hiervan ligt bij het in het privacybeleid benoemde Privacy en Informatiebeveiligingsteam (PIT). Het is niet bekend op welke wijze vorm wordt gegeven aan het cyclische proces en wie hierbij de actoren zijn. Dit verdient verduidelijking.

De documenten op de website zoals de privacyverklaring en de proclamer dienen op elkaar afgestemd te worden zodat eenduidige informatie verstrekt wordt.

Er is geen cookieverklaring aanwezig dan wel opgenomen in de privacyverklaring terwijl het wel mogelijk is om de cookievoorkeur te wijzigen middels een knop op de pagina's. Het niet vragen voor toestemming voor het plaatsen van cookies en het gebruik hiervan is niet conform de Telecommunicatiewet. Hier is uitgebreider onderzoek naar gedaan waarvan een rapport beschikbaar is en deze zal gedeeld worden met het PIT.

Een register met sectorspecifieke privacywetgeving dient conform beleid opgesteld te worden.

#### *Voorgestelde planning:*

Communicatie omtrent het bestaan van het beleid heeft plaatsgevonden kw1/kw2-2019. Via berichten (ook inhakend op de actualiteit) is hier op Social Intranet melding van gemaakt.

Evaluatie en eventuele aanpassing privacybeleid kw4-2019.

Overige en nieuwe punten op te nemen in actiepuntenlijst PIT waaronder de eventuele toestemming voor en het gebruik van cookies op limburg.nl.

### **4.1.2. B.02 Organieke inbedding**

#### *Inhoud:*

Het waarborgen van de privacy ligt niet bij één persoon. Een veelheid van personen binnen een organisatie zo niet de gehele organisatie is betrokken om aan de vereisten van wet- en regelgeving te kunnen voldoen. Binnen de provincie Limburg is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten en verbale uitlatingen.

#### *Doelstelling:*

Door een juiste organieke inbedding van taken, bevoegdheden en verantwoordelijkheden, de benodigde middelen en vastgestelde rapportagelijnen zal een juiste invulling gegeven dienen te worden aan de eisen zoals deze verwoord worden in het beleid en in de AVG.

#### *Risico:*

Door het ontbreken van een duidelijk inzicht in de diverse taakgebieden binnen privacy en informatiebeveiliging, een goede en inzichtelijke taakverdeling en de daarvoor benodigde middelen en rapportagelijnen is niet altijd duidelijk wie wat moet doen, waardoor de eisen van de AVG, de sectorspecifieke wetgeving en het privacybeleid niet effectief worden ingevuld.

### *Bevindingen:*

De provincie heeft tijdig een Functionaris voor Gegevensbescherming (FG) aangesteld conform artikel 37, AVG. De Verordening heeft een belangrijke rol toegekend aan de FG. De FG houdt intern toezicht op en adviseert over de toepassing en naleving van de Verordening door een organisatie. Ook is de FG het aanspreekpunt voor de betrokkene. Het aanstellen van een FG is een verplichting voor de provincie Limburg.

Het contract met de huidige externe FG heeft een looptijd van 2 jaar. De provincie Limburg heeft de keuze gemaakt om als opvolgende FG een “eigen” medewerker aan te wijzen.

De AVG zegt hierover: “De functionaris voor gegevensbescherming wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen de in artikel 39 bedoelde taken te vervullen”.

En de vereiste expertise en vaardigheden van een FG omvatten volgens de Autoriteit Persoonsgegevens in ieder geval:

- kennis van nationale en Europese privacywet- en regelgeving over gegevensbescherming;
- begrip van de gegevensverwerkingen die de organisatie uitvoert;
- begrip van IT en informatiebeveiliging;
- kennis van de organisatie en de sector waarin die actief is;
- vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

Het is niet bekend of de provincie Limburg in het proces voor de keuze van de nieuwe FG de vereiste expertise en vaardigheden in voldoende mate onderdeel heeft laten uitmaken van het selectieproces.

In het beleid zijn de volgende functies/rollen en taken/verantwoordelijkheden beschreven in het privacybeleid:

<b>Functie/rol</b>	<b>Taken/verantwoordelijkheid</b>
<b>Gedeputeerde Staten</b>	Eindverantwoordelijk voor het privacybeleid en het waarborgen van de privacy van betrokkenen.
<b>Secretaris/algemeen directeur</b>	Verantwoordelijk voor kaderstelling en sturing met betrekking tot het privacybeleid.
<b>Cluster-/project/-programmamanagers</b>	Uitvoering en controle op naleving privacybeleid
<b>Functionaris Gegevensbescherming</b>	Controle op naleving en advies op het gebied van privacy.
<b>Het privacy- en informatiebeveiligingsteam (PIT)</b>	Ondersteuning en advisering bestuur, de clusterambassadeurs privacy en het management bij de op het terrein van bescherming van persoonsgegevens en uitvoering van het Provinciale privacybeleid.
<b>Privacy coördinator</b>	Advisering over en implementatie privacybeleid en -wetgeving. Actueel houden register van verwerkingsactiviteiten.
<b>Clusterambassadeurs privacy</b>	Informatieverstrekking, bewustwording en cluster specifieke privacy taken

De clustermanagers waren tijdens de gesprekken niet allen op de hoogte van het bestaan dan wel de inhoud van het privacybeleid. Onbekend is dan ook op welke wijze de verantwoordelijkheden op dit gebied vertaald worden naar de praktijk. Op het moment van versie 1.0 van dit schrijven zijn er met nagenoeg alle clustermanagers (kennismakings)gesprekken gevoerd waarin onder andere aandacht is gevraagd voor het nieuwe privacybeleid en de noodzaak en rol van de clusterambassadeur privacy. Het bekend worden van de

clusterambassadeurs privacy kende een langzame start maar inmiddels zijn van alle clusters de ambassadeurs bekend.

Er is een Privacy- en Informatiebeveiligingsteam (PIT) in het leven geroepen. Het PIT heeft concreet de volgende taken:

- advisering over uitvoering en actualisatie provinciaal privacybeleid;
- signaleren van privacyrisico's;
- ondersteuning management en bestuur bij privacyvraagstukken;
- implementeren (nieuwe) privacywetgeving;
- doen van aanbevelingen op het gebied van privacy en informatiebeveiliging;
- vertaling adviezen en bevindingen FG in concrete actiepunten.

De taken van dit team zijn duidelijk omschreven in het privacybeleid. In de praktijk wordt er invulling aan gegeven. Het PIT komt structureel tweewekelijks bij elkaar met agenda en een actiepuntenlijst welke bewaakt en opgevolgd wordt. Het PIT overleg is constructief en gericht op verbetering.

De provincie beschikt over een privacy coördinator en een (informeel) privacyteam die gestructureerd en ad-hoc zaken oppakken en in de organisatie wegzetten

De provincie beschikt over een standaard verwerkersovereenkomst (VWO). Deze overeenkomst wordt in principe gebruikt bij elke nieuwe uitvoering van een gegevensverwerking door een verwerker. Nu heeft de VNG c.q. de Informatiebeveiligingsdienst in november 2019 versie 2.1 van hun Standaard Verwerkersovereenkomst Gemeenten gepubliceerd<sup>22</sup>. Wellicht is het raadzaam om deze te beoordelen en te vergelijken met de standaard van de provincie.

#### *Aandachtspunten/advies:*

De provincie Limburg heeft in het beleid de verdeling van taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen op hoofdlijnen vastleggen. Verdere vertaling hiervan richting organisatie dient nog plaats te vinden. Het doel hiervan is om op een juiste wijze invulling te geven aan de eisen zoals verwoord in het beleid en in de AVG met gebruik van de Privacy Baseline van de CIP.

Aandachtspunten hierbij:

- Eindverantwoordelijkheid voor gegevensverwerking is duidelijk.
- Gekoppeld aan het privacybeleid voorziet de organisatie voldoende en aantoonbaar in de benodigde middelen voor de uitvoering ervan.

Een punt van aandacht is de verantwoordelijkheid van de leiding van de organisatie. In een recent boetebesluit waarbij een substantiële boete is toegekend voor een overtreding van de AVG heeft de AP de het basisbedrag voor de boete verhoogd omdat deze organisatie “elk geval bijzonder nalatig is geweest in het treffen van dergelijke<sup>23</sup> maatregelen”. In de zinssnede ervoor wordt melding gemaakt dat de directie op de hoogte was van de onrechtmatige verwerking. Een korte bewerking van het boetebesluit en onderzoek is toegevoegd als bijlage B.

---

<sup>22</sup> <https://www.informatiebeveiligingsdienst.nl/nieuws/nieuwe-versie-standaard-verwerkersovereenkomst-vwo-gepubliceerd/>

<sup>23</sup> Heeft betrekking op maatregelen die in het kader van het onderzoek geïmplementeerd hadden moeten zijn.

Waarschijnlijk zijn er niet voor alle verwerkingen met verwerkers verwerkersovereenkomsten afgesloten. Uit het register van verwerkingsactiviteiten zou moeten blijken waar nog hiaten zijn zodat deze kunnen worden verholpen. Op dit moment is het aannemelijk dat de RvV nog niet volledig is en dat hieruit geen conclusies getrokken kunnen worden omtrent het compleet zijn in relatie tot de wel of niet afgesloten verwerkersovereenkomsten.

Aandacht voor de Clusterambassadeurs privacy en opvolging geven aan de gemaakte afspraken.

#### *Planning:*

Als onderdeel van de evaluatie van het privacybeleid per kw4-2019.

Het uitbreiden en actueel houden van het register van verwerkingsactiviteiten samen met de overige registraties binnen dit register (zoals verwerker en overeenkomst verwerker) dient continue plaats te vinden.

Overige en nieuwe punten op te nemen in actiepuntenlijst PIT.

### **4.1.3. B.03 Risicomanagement, Privacy by Design en de GEB**

#### *Inhoud:*

Risicomanagement is een continu proces dat de privacyrisico's signaleert, beoordeelt en een passende behandeling daarvan bewaakt. Privacy-risicomanagement richt zich op het beheersen van privacyrisico's bij het verwerken, waaronder verzamelen, opslaan en doorgeven van persoonsgegevens. Door middel van privacy-risicomanagement worden, bij de ontwikkeling, de inrichting en de inzet van de gegevensverwerking de organisatie de privacyrisico's in lijn gebracht met het privacybeleid. Zo wordt voldaan aan de wet- en regelgeving en waarbij de belangen van de betrokkenen gewaarborgd worden.

#### *Doelstelling:*

Beoordeling van de privacyrisico's (de kans en hun potentiële omvang/impact) is nodig om te bepalen hoe deze, door het treffen van maatregelen, teruggebracht kunnen worden tot binnen grenzen die de organisatie acceptabel acht.

#### *Risico:*

Het niet op orde hebben van een gestructureerde risicomanagement systematiek kan ertoe leiden dat privacyrisico's niet of niet tijdig worden gesignaleerd. Hierdoor bestaat de kans dat de verwerking van persoonsgegevens niet aan de AVG voldoet en dat de organisatie de kans loopt op inbreuken op de beveiliging; dit kan leiden tot schade voor natuurlijke personen van wie de persoonsgegevens onrechtmatig worden verwerkt.

#### *Bevindingen:*

De provincie Limburg beschikt nog niet over een volledig ingericht risicomanagementproces op het gebied van privacybescherming en kan derhalve de risico's niet aantoonbaar maken en geen éénduidige inschatting maken van deze risico's.

Op basis van kennis van de organisatie is een inschatting gemaakt van privacyrisico's bij (de verwerkingen van) verschillende clusters. Hierbij zijn de clusters Personeel & Organisatie, Subsidies en het Kabinet



gekenmerkt als clusters met verwerkingen met een verhoogd risico. Met deze clusters zijn verschillende afspraken gemaakt om privacy te adresseren. Met P&O is vrij intensief samengewerkt tussen het privacyteam en de medewerkers om de verwerkingen duidelijk in kaart te brengen en conform AVG en interne eisen vast te leggen. Met de clusters subsidies, kabinet en sinds het laatste kwartaal van 2019 de overige clusters, zijn hernieuwd vervolgsafspraken gemaakt omtrent het privacybewustzijn binnen het cluster en verdere en/of verbeterde registratie van de verwerkingen.

De wijze waarop een gegevensbeschermingseffectbeoordeling (GEB) wordt uitgevoerd is nog niet gestandaardiseerd. Op basis van het model van Norea (Privacy Impact Assessment) uit 2015 zijn GEB's uitgevoerd op de burgemeester applicatie en op de applicatie van vergunningen.

Onderkend werd dat dit model niet meer passend is in de huidige tijd en is er gezocht naar een nieuw toepasbaar model. De Informatiebeveiligingsdienst (onderdeel van de VNG) heeft in juli 2019 een aangepast model van de Franse DPA (het Franse equivalent van de Autoriteit Persoonsgegevens) beschikbaar gesteld<sup>24</sup> voor aangesloten leden. De provincie Limburg heeft besloten om dit model te gebruiken voor het uitvoeren van gegevensbeschermingseffectbeoordelingen.

De uitgevoerde GEB's op basis van het Norea model worden omgezet naar het nieuwe model te beginnen met de verwerkingen van burgemeestersbenoemingen.

Er wordt gebruik gemaakt van een uitgebreide mappenstructuur op de netwerkomgeving van de provincie Limburg zowel op cluster/projectenniveau als ook op individueel niveau. In het algemeen wordt dit gezien als een probleem in relatie tot welke gegevens hier bewaard worden. Het totaaloverzicht van deze gegevens waarbij persoonsgegevens aanwezig zijn ontbreekt. Tijdens de gesprekken is gebleken dat er onder meer een diversiteit aan persoonsgegevens langjarig in deze mappen opgeslagen wordt.

Documenten van gebruikers met persoonsgegevens komen naar verwachting voor in de persoonlijke mappen van de medewerkers. Dit worden ongestructureerde documenten genoemd en vormen een (privacy) risico.

De provincie Limburg ontwikkelt en implementeert een nieuw documentmanagementsysteem. Bij de ontwikkeling van een nieuw systeem is de toepassing van Privacy by Design<sup>25</sup> gewenst. Met Privacy by Design wordt het inbedden van de privacycriteria in de ontwerpen en het beheer (van delen) van informatiesystemen en het inbedden van de privacymaatregelen in de technologie bedoeld. Dit begint dus al bij de keuzes die gemaakt moeten worden, zodat privacy in een vroeg stadium wordt verankerd in de informatiebehoefte en het ontwerp. Want het aanpassen van functionaliteit van een applicatie is achteraf moeilijker en kostbaarder dan dit van het begin af aan inbouwen. Dat geldt derhalve ook voor het inbouwen van maatregelen en processen die privacy bewerkstellingen. De provincie Limburg heeft nog geen Privacy by Design toegepast. Dit wil niet zeggen dat er geen privacy beschermende maatregelen in de omgeving toegepast worden maar de vraag kan gesteld worden of het toepassen van dit soort maatregelen gestructureerd en op de juiste wijze plaatsvindt.

Het verder ontwikkelen en inpassen van deze nieuwe omgeving binnen de organisatie kan de problematiek van de (uitgebreide) mappenstructuur verder inperken.

---

<sup>24</sup> <https://www.informatiebeveiligingsdienst.nl/nieuws/dpia-tool-voor-gemeenten-online/>

<sup>25</sup> AVG art. 25.

Bij de lopende implementatie van de nieuwe VTH-applicatie is aan Privacy by Design meer aandacht besteed. Door het projectteam zijn onder andere privacy personen van de deelnemers aan dit traject uitgenodigd om input te geven. Weliswaar in een late fase maar sneller dan doorgaans gebruikelijk is bij de implementatie van nieuwe processen/verwerkingen in organisaties. Dit geeft hoop voor de toekomst.

#### *Aandachtspunten/Advies:*

De provincie zorgt voor de implementatie van een risicomanagement proces voor het beoordelen van de privacyrisico's, het treffen van passende maatregelen en het kunnen aantonen van het passend zijn van deze maatregelen. Een begin hiermee is gemaakt door het definiëren van de beheersmaatregelen uit de Privacy Baseline waarbij deze een risicowaardering hebben gekregen. Deze is in eerste concept aanwezig maar verdient nog uitgebreide aandacht.

Een eerste GEB's zijn uitgevoerd door ISO en privacy coördinator op basis van de Norea. Bij het beschikbaar komen van de tool van de Informatiebeveiligingsdienst zijn deze "vertaald" naar deze omgeving. Besloten dient te worden op welke (nieuwe) verwerkingen GEB'S uitgevoerd gaan worden en welk hulpmiddel hiervoor gebruikt gaat worden.

Er zijn verschillende methoden voor het uitvoeren van een GEB. De provincie dient een aantal alternatieven te analyseren en een keuze te maken voor een van deze methoden. Medio 2019 heeft de provincie een (voorlopige) keuze gemaakt voor het model van de Informatiebeveiligingsdienst (IBD). Een probleem hierbij is nog de opslag van de uitgevoerde GEB's. De opslag vindt binnen de browseromgeving plaats of de opslag vindt plaats op locatie van de IBD maar is hierbij toegankelijk voor alle gebruikers, dus ook voor gebruikers buiten de provincie. Geen van beide oplossingen is organiek bruikbaar. Hier dient een oplossing voor te komen die wellicht gevonden is in het [REDACTED]. Daarnaast is de IBD voornemens om een aangepaste versie van deze applicatie uit te brengen.

Aandachtspunten hierbij en nog te implementeren:

- Het beoordelen van de privacyrisico's
  - De uitvoering van een Gegevensbeschermingseffectbeoordeling<sup>26</sup> (GEB) voorafgaand aan een verwerking indien waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen bestaat.
  - Mogelijke hertoetsing.
- Het doorvoeren van passende technische en organisatie maatregelen door Privacy by Design en Privacy by Default en door het uitvoeren en evalueren van GEB's.
- Het beschikbaar zijn van een procesbeschrijving voor het uitvoeren van een GEB.
- Aantonbaar maken dat GEB's aanwezig zijn en maatregelen genomen zijn/worden.

#### *Planning:*

Evaluatie van het gebruik van de GEB van de informatiebeveiligingsdienst in kw3-2019.

Overige en nieuwe punten op te nemen in actiepuntenlijst PIT.

---

<sup>26</sup> Avg art. 35, lid1

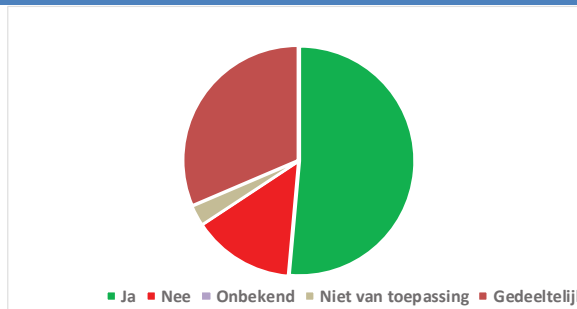


#### 4.1.4. Resultaat gap-analyse beleidsdomein

Er is een Gap-analyse uitgevoerd op de eisen vanuit de Privacy Baseline van de Cip tegenover de mate van implementatie hiervan binnen de provincie. Deze analyse is nog niet uitgevoerd op het niveau van het volwassenheidsniveau zoals in hoofdstuk 3 is besproken. Voor deze gap-analyse is beoordeeld of een bepaalde beheersmaatregel wel, niet of gedeeltelijk geïmplementeerd is dan wel of deze van toepassing is voor de organisatie. Voor de 35 beheersmaatregelen van het beleidsdomein geeft dit het volgende resultaat:

### B Beleidsdomein

Resultaat	Aantal
Ja	18
Nee	5
Onbekend	0
Niet van toepassing	1
Gedeeltelijk	11



## **4.2. Het uitvoeringsdomein**

### *Inleiding*

In dit hoofdstuk zijn de eisen opgenomen voor de uitvoering van de gegevensverwerking. Het beleid dat op de beleidslaag vanuit het management is ontwikkeld, is leidend voor de invulling van de specifieke aspecten van de gegevensverwerking.

### *Doelstelling*

In het uitvoeringsdomein worden persoonsgegevens verwerkt. De verantwoordelijke voor de verwerking moet hier de verwerking realiseren onder de condities en randvoorwaarden die in het beleidsdomein zijn gedefinieerd. Personen waarvan de persoonsgegevens worden verwerkt (betrokkenen) moeten de zekerheid kunnen krijgen dat de verwerking conform de wet- en regelgeving gebeurt.

### *Risico's*

Wanneer richtlijnen voor de specifieke aspecten van de gegevensverwerking ontbreken dan bestaat het risico dat onvoldoende sturing wordt gegeven aan de specifieke aspecten bij de verwerking van persoonlijke gegevens. Dit geeft onduidelijkheid bij de technische en organisatorische inrichting van de gegevensverwerkingen.

### **4.2.1. U.01 Doelbinding gegevensverwerking**

#### *Inhoud:*

Het uitgangspunt van doelbinding is, dat gegevens worden verwerkt en verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. “Welbepaald en uitdrukkelijk omschreven” houdt in dat men geen gegevens mag verzamelen zonder een precieze doelomschrijving. Het doel moet zijn bepaald alvorens men tot verzamelen overgaat.

“Welbepaald” houdt in dat deze doelomschrijving duidelijk moet zijn, niet zo vaag of ruim dat zij tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Het doel mag ook niet in de loop van het verzamelproces geformuleerd worden. “Uitdrukkelijk omschreven” houdt in dat de verantwoordelijke het doel waarvoor hij verwerkt, moet hebben omschreven.

#### *Doelstelling:*

Het doel hiervan is om te waarborgen dat persoonsgegevens alleen verzameld en (verder) worden verwerkt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden.

#### *Risico:*

Bij gegevensverwerkingen zonder een uitdrukkelijk omschreven en gerechtvaardigd welbepaald doel bestaat het risico van ongeoorloofd en onrechtmatig verzamelen en (verder) verwerken van persoonsgegevens.

#### *Bevindingen:*

Niet alle gegevensverwerkingen zijn omschreven en niet van alle gegevensverwerkingen is het doel welbepaald en uitdrukkelijk omschreven. Hierdoor bestaat het risico van ongeoorloofd en onrechtmatig verzamelen en verder verwerken van persoonsgegevens. Het doel dient van tevoren welbepaald en uitdrukkelijk omschreven te zijn. Indien dit correct gebeurt, wordt het voor verschillende verwerkingen

duidelijk of deze rechtmatig plaatsvinden of niet. Een voorbeeld hiervan zijn de schaduw personeelsdossiers van medewerkers waarvan gezegd wordt dat deze bij bepaalde clusters in gebruik zijn omdat dit handig is.

Ook komt het voor dat medewerkers in een ander cluster tewerkgesteld worden. Hierbij betreft het een vaste aanstelling bij het nieuwe cluster waarbij er geen verantwoordelijkheden meer bij het “oude” cluster bestaan. In de praktijk blijkt dat deze medewerkers nog rechten op hun oude omgeving hebben waarbij het mogelijk is dat persoonsgegevens nog onrechtmatig verwerkt kunnen worden. Het is hier niet belangrijk of deze medewerkers die verwerkingen ook uitvoeren maar de mogelijkheid is er. Dit betekent dat dit indruist tegen de organisatorische en technische beveiligingsmaatregelen.

Bij een beperkt onderzoek is gebleken dat deze rechten in stand zijn gebleven totdat de officiële wijziging van de functie een feit was. Bij het officiële traject via P&O zijn de mutaties van de rechten doorgevoerd. Dit kan in sommige gevallen enige tijd in beslag nemen. De vraag hierbij is of dit acceptabel is. Andere rechten dienen via de cluster manager te lopen. De mogelijkheid bestaat dat in de praktijk de wijzigingsinfo niet dan wel niet meteen dan wel nooit wordt doorgegeven ter mutatie.

Een *nice to have* kan nooit reden zijn om toegang te verlenen.

Onder dit subdomein valt ook de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Uit een uitgevoerde GEB blijkt dat deze persoonsgegevens ook binnen de provincie verwerkt worden waarin de GEB wordt aangegeven dat dit conform wetgeving is. Deze gegevens dienen conform GEB op de juiste manier in het RvV opgenomen te worden.

#### *Aandachtspunten/advies:*

Het doel van het voldoen aan de beheersmaatregelen uit dit subdomein is om te waarborgen dat persoonsgegevens alleen worden verzameld en (verder) verwerkt voor gerechtvaardigde doeleinden.

Aandachtspunten hierbij zijn:

- Het doel en de rechtmatigheid zijn welbepaald (kader scheppend) en uitdrukkelijk (nauwkeurig, specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden) omschreven.
- Minimale gegevensverwerking (Dataminimalisatie).
- Rechtmatigheid van de verwerking.
- Behoorlijke en transparante verwerking.
  - Juistheid
  - Passende beveiliging
  - Bewaartermijn
- De verdere verwerking van persoonsgegevens.
- De verwerking van bijzondere persoonsgegevens<sup>27</sup>.
- De verwerking van strafrechtelijke veroordelingen en strafbare feiten<sup>28</sup> en het BSN.
- De verwerking middels geautomatiseerde besluitvorming.

Het register van verwerkingsactiviteiten is een hulpmiddel om hier verder inzicht in te verkrijgen. Zie 4.2.2.

---

<sup>27</sup> AVG art. 9

<sup>28</sup> AVG art. 10

Het onrechtmatige gebruik van schaduwdoSSIers van medewerkers dient (door P&O) gecommuniceerd te worden zodat degenen die een schaduwdoSSIer onder beheer hebben, deze verwijderen.

#### *Planning:*

Dit wordt uitgevoerd samen met de verdere ontwikkeling en herziening van het register van verwerkingsactiviteiten in 2019/2020.

Bij nieuwe verwerkingen vóór aanvang van de gegevensverwerking.

Van een aantal normen is niet duidelijk hoe hier precies invulling aan gegeven wordt. Deze hebben de classificatie onbekend gekregen in de gap-analyse. Hier dient, afhankelijk van de prioritering, nader onderzoek plaats te vinden.

Continue. Hier ligt ook een taak voor de cluster ambassadeurs privacy.

### **4.2.2. U.02 Register van verwerkingsactiviteiten**

#### *Inhoud:*

Om de naleving van de AVG aan te kunnen tonen, dient de provincie Limburg een register bij te houden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden<sup>29</sup>. Het register van verwerkingsactiviteiten is een opsomming van de belangrijkste informatie over de verwerkingen van persoonsgegevens. Het register biedt een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens. Er is immers inzicht nodig in alle verwerkingen van persoonsgegevens met de vermelding voor welk doel deze verwerkingen gebeuren, waar deze gegevens vandaan komen en met wie we deze delen.

Het register dient in schriftelijke vorm waaronder begrepen in elektronische vorm, bijgehouden te worden. Er zijn geen andere vormvereisten. Het register mag dus worden opgesteld in een tekstverwerkingsbestand, een spreadsheet, speciaal daartoe bestemde software of elke andere schriftelijke vorm.

Het verwerkingsregister is overigens geen openbaar document.

#### *Doelstelling:*

Het doel van het register van verwerkingsactiviteiten (RvV) is om inzicht te verkrijgen in de verwerkingen en de gegevensstromen binnen de organisatie en bij de partijen die namens de organisatie zorgen voor de verwerking van persoonsgegevens. Hierbij is elke verwerkingsverantwoordelijke (en ook elke verwerker) ertoe verplicht medewerking te verlenen aan de toezichthoudende autoriteit en dit register desgevraagd te verstrekken met het oog op het gebruik daarvan voor het toezicht op de verwerkingsactiviteiten. De Autoriteit Persoonsgegevens beschouwt het hebben van een register van verwerkingsactiviteiten met de juiste informatie als een belangrijke eerste stap waarmee een organisatie laat zien dat zij de privacyregels serieus neemt.

---

<sup>29</sup> AVG overweging 82. AVG art. 30.

### *Risico:*

Het doel van een register van verwerkingsactiviteiten is inzicht te verstrekken in de verwerkingen en de gegevensstromen binnen de organisatie en bij de partijen die namens de organisatie zorgen voor de verwerking van persoonsgegevens. Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën van persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.

Bij het niet hebben van een actueel en volledig register van verwerkingsactiviteiten waarbij gegevensverwerkingen en de daarbij horende grondslagen, bewaartermijnen, e.d. niet inzichtelijk zijn, is de kans op onrechtmatige verwerking groot en kan de provincie Limburg niet in alle gevallen aantonen aan de wettelijke eisen te voldoen.

### *Bevindingen:*

Er is er een verplichting voor de provincie Limburg om een RvV bij te houden. De uitzonderingsgronden<sup>30</sup> voor het bijhouden van een RvV gelden niet voor de provincie.

Het RvV en de verantwoordelijkheid omtrent de beheersing hiervan is beschreven in het privacybeleid.

De provincie is ruim voor het van toepassing worden van de AVG begonnen met het in kaart brengen van de verwerkingen. Einde 2018, begin 2019 is een tweede ronde ingezet om een meer compleet beeld te krijgen van de verwerkingen binnen de organisatie en om de bestaande verwerkingen te herzien en te verbeteren waar nodig. Een derde ronde vindt op dit moment plaats. Het privacyteam ondersteunt waar nodig de clusters bij het vaststellen van de verwerkingen en het uitwerken hiervan voor het RvV.

Om het RvV een effectief instrument te laten zijn waarmee persoonsgegevens goed beschermd kunnen worden, dient het een beheersbaar register te zijn. Dat betekent een register dat volledig is, aansluit op processen en het juiste detailniveau heeft. De provincie heeft ervoor gekozen om dit register vast te leggen in afzonderlijke Word bestanden. Dit is toegestaan maar in de praktijk minder handig. Deze vastlegging is minder handig indien er deeloverzichten van specifieke informatie nodig is.

Momenteel wordt er gekeken of dit register niet ondergebracht kan worden in een [REDACTED] applicatie.

Einde 2018 is er een WOB verzoek ontvangen van de Open State Foundation (OSF) die, in het kader van een onderzoek naar dergelijke registers bij overheden, het register van de provincie hebben opgevraagd. Dit verzoek is niet alleen aan de provincie Limburg gedaan maar aan alle provincies en gemeenten. OSF heeft na het onderzoek de bevindingen gepubliceerd<sup>31</sup> in juni 2019. Het onderzoek naar de staat van de onderzochte registers heeft geleid tot een samenwerking met onder andere de Informatiebeveiligingsdienst van de VNG en diverse gemeenten. Hier is een standaardtemplate<sup>32</sup> uit voortgekomen.

Eén van de moeilijkheden waarmee men bij het samenstellen van de standaardtemplate mee kampte, was het gewenste dan wel benodigde detailniveau van de verwerkingen. Dit speelt bij meerdere organisaties. Ook bij de Autoriteit Persoonsgegevens (AP). Wanneer het Register van de Autoriteit Persoonsgegevens nader bekeken wordt, kan men zien dat dit probleem ook bij de AP is opgetreden en dat verschillende afdelingen binnen de AP hier verschillend invulling aan hebben gegeven.

---

<sup>30</sup> AVG art.30 lid 5

<sup>31</sup> <https://openstate.eu/wp-content/uploads/sites/14/2019/06/Onderzoek-OSF-naar-registers-van-verwerkingen.pdf>

<sup>32</sup> <https://www.informatiebeveiligingsdienst.nl/product/leeg-verwerkingsregister-gemeenten/>

Ook doet de Autoriteit Persoonsgegevens onderzoek naar de registers bij organisaties waarbij deze opgevraagd zijn. Als resultante van dit onderzoek heeft de AP 5 concrete aanbevelingen<sup>33</sup> gedaan in relatie tot dit register. Van deze lijst heeft de provincie 3 aanbevelingen opgenomen in het RvV.

Het leek er medio 2019 op dat de verdere ontwikkeling en herziening van het RvV in een dip terecht was gekomen. De afdelingen zelf hebben de verantwoordelijkheid om te zorgen dat het RvV voor de eigen clusters juist is maar dit lijkt in deze fase nog moeilijk te zijn. Er wordt nu hernieuwd vanuit het privacy team met de clusters actief “getrokken” aan de verdere uitbouw van het register. Dit is mede mogelijk door de grotere capaciteit van het privacy team. Middels interviews bij de clusters door het privacy team worden de ontbrekende verwerkingen achterhaald en verder uitgewerkt.

De provincie treedt ook op als verwerker. Bijvoorbeeld voor de RUD-ZL. Ook verwerkingen die uitgevoerd worden als verwerker dienen in het RvV bijgehouden te worden.

Het niet hebben van een overzicht van verwerkingen leidt tot een incompleet beeld van de verwerkte categorieën van persoonsgegevens en getroffen maatregelen voor de relevante verwerkingen, processen en technische systemen.

#### *Aandachtspunten/advies:*

De provincie Limburg zal de gegevens over de gegevensverwerkingen herzien en uitbreiden in het bestaande register en indien van toepassing in het register in een nieuwe omgeving. Hierbij wordt er voor gezorgd dat het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens biedt. De provincie Limburg zal dit tevens opleggen aan de verwerkers.

De AP heeft de volgende concrete aanbevelingen gedaan met betrekking tot het RvV:

1. Benoem hoe lang en met welk doel je persoonsgegevens wil bewaren. Onder de Europese privacywetgeving is het niet toegestaan persoonsgegevens langer te bewaren dan noodzakelijk is voor het doel waarmee ze verzameld zijn. Ook moeten organisaties kunnen motiveren waarom ze deze gegevens verzamelen.
2. Neem de contactgegevens van de verwerkingsverantwoordelijke op in het register.
3. Zorg voor een overzichtelijk bestand van alle verwerkingen van persoonsgegevens waarin gebruikers eenvoudig kunnen navigeren.
4. Geef duidelijk aan op welke locatie of in welk bestand persoonsgegevens bewaard worden en neem deze locaties of bestanden op in het register. Deze informatie is relevant als mensen een verzoek om inzage of verwijdering indienen.
5. Maak duidelijk welk doel bij welke verwerking hoort. Alleen een opsomming van de verwerkingen per afdeling in combinatie met een opsomming van de diverse doeleinden van de verwerkingen is niet voldoende.

Bij verdere verbetering en uitbreiding van het RvV dienen de verwerkingen die de provincie Limburg uitvoert als verwerker, opgenomen te worden in het RvV.

Clusters blijvend informeren omtrent noodzaak van het register van verwerkingsactiviteiten en de correctheid hiervan. Hier ligt ook een taak voor de clusterambassadeurs privacy.

---

<sup>33</sup> <https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-doet-aanbevelingen-voor-registers-van-verwerkingen>

Vanaf oktober 2019 is een hernieuwde ronde ingezet ter verdere verbetering en vervolmaking van het RvV waarbij de clusters actiever benaderd worden en desgewenst meer ondersteuning krijgen. Als resultaat hiervan zijn zo'n 40 nieuwe verwerkingen geregistreerd.

#### *Planning:*

Kwartaal 4-2019 is een hernieuwde impuls gegeven aan het verbeteren en uitbreiden van het RvV, geïnitieerd door het privacyteam. De verwachting is dat einde kwartaal 1-2020 significante stappen zijn gemaakt in kwaliteit en kwantiteit van de verwerkingen. Momenteel zijn er circa 150 verwerkingen opgenomen in het register.

Hierbij worden tevens de verwerkingen meegenomen waarvoor provincie Limburg optreedt als verwerker

### **4.2.3. U.03 Kwaliteitsmanagement**

#### *Inhoud:*

Kwaliteitsmanagement zorgt voor de processen die de verwerking, juistheid en nauwkeurigheid van de persoonsgegevens bewaken en die, bij onjuistheid en onnauwkeurigheid van de gegevens of bij ongewenste verwerking, de gegevens te rectificeren, te vervolledigen, te wissen, de verwerking te beperken en toestemming tot verwerking in te trekken.

#### *Doelstelling:*

Kwaliteitsmanagement in relatie tot de bescherming van persoonsgegevens dient ervoor te zorgen dat een gegevensverwerking correct en in overeenstemming met wetgeving en met de wens van de betrokkene is.

#### *Risico:*

Wanneer de gegevens onjuist en onnauwkeurig zijn ingevoerd of gecorrumpeerd raken, kunnen verkeerde conclusies over de betrokkene getrokken worden met negatieve consequenties tot gevolg of naar het oordeel van de betrokkene ongewenste verwerking van zijn of haar gegevens.

#### *Bevindingen:*

Tijdens gesprekken is een van de opmerkingen die enkele keren gemaakt werden of bepaalde medewerkers toegang hebben tot te veel gegevens. Er werd dan gerefereerd naar medewerkers die voorheen bij een ander cluster behoorden maar bij het nieuwe cluster nog de "oude" rechten hebben behouden.

Er is een opmerking gemaakt dat er dubbele dossiers (papier en digitaal) op na worden gehouden. Wordt hierbij voldaan aan de kwaliteitseisen van de gegevens? Wordt wel voldaan aan de interne afspraken hieromtrent?

De historische persoonsgegevens in de mailboxen verdwijnen daarnaast ook niet vanzelf.

#### *Uitvoering:*

De provincie Limburg heeft en zal verder kwaliteitsmanagement inrichten ten behoeve van de bewaking van de juistheid en nauwkeurigheid van persoonsgegevens. De verwerking is zo ingericht dat de persoonsgegevens kunnen worden gecorrigeerd, gestaakt of overgedragen. Indien dit op verzoek van betrokkene gebeurt, wordt deze over de status van de afhandeling geïnformeerd.

Hierdoor wordt bereikt dat een gegevensverwerking correct en indien van toepassing in overeenstemming met de wens van betrokkenen is.

Aandachtspunten hierbij:

- Het treffen van de nodige maatregelen om de juistheid en nauwkeurigheid van persoonsgegevens te waarborgen en de bijbehorende controle en rapportage.
- De mogelijkheid tot correctie van persoonsgegevens.
- De mogelijkheid tot het wissen van persoonsgegevens<sup>34</sup> in bepaalde gevallen.
- De mogelijkheid tot staking van de verwerking<sup>35</sup>.
- De overdracht van persoonsgegevens.
- Afhankelijkheid van software aanbieders voor standaardapplicatie.

#### *Planning:*

Het betreft hier mede uitgebreidere rechten van de betrokkenen waar onder andere ook de gebruikte software voor aangepast dient te worden. Gaandeweg tijdens het traject zal dit mede geïmplementeerd en gepland worden.

Er is een “Protocol rechten betrokkene” in een afrondende fase waarin een aantal van bovengenoemde aandachtspunten worden behandeld. Dit protocol zal einde 2019 gereed zijn en in 2020 geïmplementeerd worden in de organisatie.

Continue.

#### **4.2.4. U.04 Beveiligen van de verwerking van persoonsgegevens**

##### *Inhoud:*

Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen, alsmede procedures en processen om eventuele gevolgen van beveiligingsincidenten tot een acceptabel (passend), vooraf bepaald niveau te beperken. De maatregelen zijn gebaseerd op een risicoanalyse en wettelijke verplichtingen (waaronder de AVG).

---

<sup>34</sup> AVG art 17, lid 1.

<sup>35</sup> AVG art. 21, lid 1.



### *Doelstelling:*

Beveiliging van persoonsgegevens is om persoonsgegevens te beschermen tegen verlies, het niet beschikbaar zijn, het corrupt raken en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.

### *Risico:*

Indien niet adequaat aan de aspecten van technische en organisatorische maatregelen invulling gegeven wordt, bestaat het risico van ongewenst openbaar worden, manipulatie, misbruik en het niet beschikbaar zijn van gegevens.

### *Bevindingen:*

Omtrent de fysieke beveiliging is door de Zuidelijke Rekenkamer eerder al gerapporteerd waarbij ongeautoriseerd toegang is verkregen. [REDACTED]

[REDACTED] n 2019 is dit niet geconstateerd.

Binnen (een gedeelte van) de organisatie is er behoefte aan veilig mailen. Men ziet dat externe relaties wel de mogelijkheid hebben om gevoelige informatie via mail beveiligd aan te leveren maar zelf heeft men geen vergelijkbare mogelijkheden om op een veilige manier mail met gevoelige gegevens te versturen.

Tevens worden er onbeveiligd e-mails verstuurd met strafrechtelijke en medische gegevens. Dat dit anno 2019 niet meer kan, moge duidelijk zijn.

Dit is ook onderkend door de organisatie. Er was eerder sprake van dat in 2019 een keuze gemaakt zou worden voor een 'veilig mailen' oplossing. Door prioritering binnen het verantwoordelijke cluster is dit naar achter geschoven. Wellicht dat in 2020 een oplossing wordt geboden.

Implementatie en gebruik van Veilig Mailen door de organisatie kan beter vandaag dan morgen plaatsvinden.

In niet alle gevallen is de verwerker vermeldt in het RvV dan wel de aanwezigheid van een verwerkersovereenkomst. Dit manco zal verholpen dienen te worden omdat ook van verwerkers een passend niveau van beveiliging gevraagd dient te worden.

### *Aandachtspunten/advies:*

De provincie Limburg dient de benodigde technische en organisatorische maatregelen te treffen om een verwerking van persoonsgegevens op een passend niveau te beveiligen<sup>36</sup>. De provincie Limburg dient dit tevens op te leggen aan de verwerkers waar dit nog niet gebeurd is. Het doel hiervan is om persoonsgegevens te beschermen tegen het ongewenst openbaar worden, het niet beschikbaar zijn, data corruptie en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.

---

<sup>36</sup> AVG art. 32.

Aandachtpunten hierbij:

- Technische en organisatorische maatregelen.
  - Correct autorisatiebeheer
  - Fysieke beveiliging
  - Beveiligingsplan
  - Passend beveiligingsniveau waaronder
    - Pseudonimisering en versleuteling
    - Herstelcapaciteit van systemen
    - Testen, beoordelen en evalueren van de doeltreffendheid van de maatregelen
- Een passend niveau van beveiligingsmaatregelen.
  - Aantoonbaar en passend.
  - Gebaseerd op een risicoanalyse
  - Gebaseerd op NEN-ISO/IEC27001:2017 dan wel Baseline Informatiebeveiliging Overheid.

*Planning:*

Omgeving voor Veilig Mailen. Implementatieperiode onbekend.

Protocol Veilig Mailen. Beslisboom Veilig Mailen.

Gereed voor certificatie NEN-ISO/IEC27001:2017 in 2021?

#### **4.2.5. U.05 Informatieverstrekking betrokkene bij verzameling persoonsgegevens**

*Inhoud:*

Een individu die persoonsgegevens verstrekt aan een organisatie heeft het recht te weten waarvoor, op welke wijze en door wie deze gegevens worden gebruikt. De organisatie heeft hiertoe een informatieplicht. Deze informatieplicht geldt ook wanneer persoonsgegevens van anderen worden ontvangen.

*Doelstelling:*

Het doel hiervan is om transparantie aan betrokkenen te garanderen over de gegevensverzameling en de verwerkingen met het doel om de betrokkene de mogelijkheid te bieden zijn rechten uit te oefenen overeenkomstig de beginselen van behoorlijke en transparante verwerking.

*Risico:*

De organisatie is niet transparant, waardoor de organisatie niet kan verantwoorden dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking.

*Bevindingen:*

Wanneer burgers op zoek zijn naar informatie over hoe de provincie met ‘privacy’ omgaat, gaan ze meestal naar de privacyverklaring op de website. De provincie heeft een privacyverklaring opgenomen op de website. De verklaring is eenvoudig te vinden en de tekst is goed leesbaar en duidelijk. In de vernieuwde privacyverklaring is onder andere de gegevensverwerking in relatie tot Social Media Management

meegenomen. Echter wordt in de privacyverklaring alleen verwezen naar verwerking van persoonsgegevens voor de nieuwsbrief. Daarnaast is het ook mogelijk om een contactformulier voor een klacht, een storing of een vraag in te vullen en is er een doorverwijzing naar een ander formulier voor het melden van een milieuklacht. In deze gevallen worden er ook persoonsgegevens verwerkt. Tevens is er een proclamer gepubliceerd op de site. Hierin staat dat persoonsgegevens alleen worden gebruikt voor de afhandeling van een subsidieverzoek. De privacyverklaring dient conform de feitelijke situatie aangepast te worden.

#### *Aandachtpunten/advies:*

De provincie Limburg zal bij elke verzameling van persoonsgegevens, tijdig en op een vastgelegde en vastgestelde wijze, informatie aan de betrokkene beschikbaar stellen, zodat de betrokkene, tenzij een uitzondering (waaronder verwerking berustend op een wettelijke bepaling) geldt, toestemming kan geven voor de verwerking<sup>37</sup>.

Het doel hiervan is om transparantie aan betrokkene te garanderen over de gegevensverzameling en de verwerking<sup>38</sup>, zodat de betrokkene zijn rechten kan uitoefenen in overeenstemming met de beginselen van behoorlijke en transparante verwerking<sup>39</sup>.

#### *Aandachtpunten hierbij:*

- Tijdigheid van toestemmingsverkrijging van en informatieverstrekking aan betrokkene.
- Duidelijk omschreven toestemmingsverzoek.
- Juiste informatieverstrekking aan betrokkene<sup>40</sup>.
- De uitzonderingen die van toepassing zijn
  - Betrokkene beschikt al over de informatie
  - Onevenredige inspanning van informatieverstrekking
  - de verwezenlijking van de doeleinden van de verwerking onmogelijk dreigt te worden of ernstig in het gedrang dreigt te brengen
  - Uitdrukkelijk wettelijk voorgeschreven
  - Geheimhoudingsplicht/beroepsgeheim
  - In het kader van de Archiefwet

#### *Planning:*

Kw1-2020.

---

<sup>37</sup> AVG art. 13, AVG art. 14, AVG art. 6 lid 1 f

<sup>38</sup> Overweging 60.en AVG art. 12.

<sup>39</sup> AVG overweging 60

<sup>40</sup> AVG art. 13, AVG art. 14

#### 4.2.6. U.06 Bewaren van persoonsgegevens

##### *Inhoud:*

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld of niet langer dan de bewaartermijn die (sectorspecifieke) wetgeving stelt.

De bewaartermijn kan worden beëindigd door actieve verwijdering van de gegevens of door anonimisering van de persoonsgegevens. Bij een passende anonimisering zijn de gegevens niet meer herleidbaar tot de betrokkene.

##### *Doelstelling:*

Het doel is om te borgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het te bereiken doel dan wel conform wetgeving.

##### *Risico:*

Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen.

##### *Bevindingen:*

Tijdens gesprekken is gebleken dat er rekening gehouden wordt met diverse geldende bewaartermijnen en dat gegevens periodiek vernietigd worden. Ook is gezegd dat dit waarschijnlijk niet met alle gegevens zal gebeuren. Het is waarschijnlijk dat op de netwerkomgeving veel gegevens aanwezig zullen zijn waarvan de bewaartermijn is verstreken. Ook zullen persoonsgegevens onder de radar vertoeven. Denk hierbij aan de gegevens in persoonlijke mappen en – *last but not least* – de Outlook database.

Alhoewel er ook medewerkers zijn die zeggen maar in beperkte mate mails met persoonsgegevens te bewaren zal het in het algemeen niet zo rooskleurig zijn. De praktijk leert dat de Outlook database een vergaarbak is van diverse ‘gewone’ en bijzondere persoonsgegevens die doorgaans bewaard blijven zolang men voor een organisatie werkt en zelfs daarna. Dit geldt ook voor de mappenstructuur. De redenering die meestal gehanteerd wordt is dat de gegevens wel eens handig kunnen zijn voor toekomstig gebruik.

Hierbij een voorbeeld: Bij een onderzoek naar een cluster bleek dat op de ████████ van dit cluster 440.000 bestanden aanwezig waren; circa 9.000 bestanden per medewerker. Vooruitlopend op een aangekondigd onderzoek van de FG zijn de medewerkers van het cluster gevraagd om hun bewaarde gegevens op te schonen. Na deze actie is het aantal bestanden met 60.000 afgenomen. In vervolg op de opschoonactie is een vervolgonderzoek naar mogelijke onrechtmatige verwerkingen binnen dit cluster gepland. Dit zal einde 2019 plaatsvinden waarover afzonderlijk gerapporteerd wordt.

##### *Aandachtpunten/advies:*

De provincie Limburg zal de nodige maatregelen treffen waardoor de organisatie voor persoonsgegevens een bewaartermijn hanteert die niet wordt overschreden. Hierdoor wordt bereikt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk voor het te bereiken doel.

Met betrekking tot anonimisering lijkt een anonimiseringprotocol gewenst.

Aandachtspunten hierbij:

- Bij het verlopen van de bewaartermijn het verwijderen, vernietigen of anonimiseren van de persoonsgegevens.
- Het vaststellen van de bewaartermijn van alle persoonsgegevens.
- Als in (sectorspecifieke) wetgeving een bewaartermijn is vastgelegd voor specifieke persoonsgegevens, dan geldt die bewaartermijn.
- Archivering, wetenschappelijk of historisch onderzoek of statistische doeleinden<sup>41</sup>.

*Planning:*

Continue.

#### **4.2.7. U.07 Doorgifte persoonsgegevens**

*Inhoud:*

Doorgifte kan plaatsvinden aan verwerker(s) en aan andere verwerkingsverantwoordelijke(n). Een verwerker verricht de verwerking namens een verwerkingsverantwoordelijke<sup>42</sup> <sup>43</sup>. Waar sprake is van meerdere verwerkingsverantwoordelijken, bepalen zij gezamenlijk de doelstellingen en middelen voor de verwerking en zijn zij gezamenlijke verwerkingsverantwoordelijken<sup>44</sup>.

Bij de doorgifte wordt onderscheid gemaakt tussen doorgifte binnen de EU, waar de AVG geldt, en doorgifte naar buiten de EU. Als doorgifte naar buiten de EU plaatsvindt, dan spreekt de AVG van doorgifte aan derde landen en internationale organisaties.

*Doelstelling:*

Het doel hiervan is om te waarborgen dat de persoonsgegevens op een rechtmatige manier worden doorgegeven aan andere verwerkers dan wel mede-verwerkingsverantwoordelijken, deze op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid goed geregeld blijft.

*Risico:*

Als een organisatie niet voldoet aan dit criterium is het niet duidelijk voor de organisatie wat exact wordt verwacht bij het doorgeven van persoonsgegevens waardoor de kans bestaat dat persoonsgegevens onrechtmatig worden doorgegeven en onrechtmatig verder worden verwerkt en gebrek is aan het nemen van verantwoordelijkheid en controle.

---

<sup>41</sup> AVG art. 89 lid 1.

<sup>42</sup> AVG art. 28 lid 1.

<sup>43</sup> AVG art. 28 lid 10: Indien een verwerker in strijd met de AVG handelt, wordt die verwerker als verwerkingsverantwoordelijke beschouwd.

<sup>44</sup> AVG art. 44.

### *Bevindingen:*

Afspraken met een verwerker omtrent de verwerking van persoonsgegevens worden doorgaans vastgelegd in een zogenaamde verwerkersovereenkomst. Een totaaloverzicht van deze overeenkomsten is nog niet volledig evenmin een overzicht van de externe partijen, de onderlinge verhoudingen en de noodzakelijkheid van afspraken omtrent de verwerking van persoonsgegevens.

Bij de provincie Limburg zijn enkele verwerkersovereenkomsten ontvangen. De kwaliteit van deze verwerkersovereenkomsten is variabel en de kans bij accepteren van deze externe overeenkomsten is dat niet afdoende de rechtmatige manier van verwerken van persoonsgegevens is vastgelegd. De provincie Limburg heeft als verwerkingsverantwoordelijke een eigen verwerkersovereenkomst en sluit deze in principe af met de verwerkers. Indien de beschikbare overeenkomst van de verwerker passend is, kan in voorkomende gevallen overwogen worden om deze te gebruiken.

Het is niet in alle gevallen binnen de organisatie duidelijk of er een overeenkomst afgesloten dient te worden. Op dit moment is er zelfs sprake van de verwerkersovereenkomsten meegestuurd worden terwijl er geen sprake is van een verwerker.

### *Aandachtpunten/advies:*

De provincie Limburg zorgt ervoor dat bij de doorgifte van persoonsgegevens aan een andere verwerkingsverantwoordelijke de onderlinge verantwoordelijkheden duidelijk zijn en bij de doorgifte aan een verwerker afdoende garanties zijn. Het doel hiervan is om te waarborgen dat persoonsgegevens op een rechtmatige manier worden doorgegeven, op een juiste manier worden gebruikt en dat de verantwoordelijkheid voor deze rechtmatigheid en juistheid ingeregeld blijft.

De verstrekkingen dienen duidelijk in het RvV gedocumenteerd te zijn.

Er ontbreekt een totaaloverzicht van verwerkende partijen en de mogelijk afgesloten verwerkersovereenkomsten. In een totaaloverzicht dient duidelijk te zijn wie de verwerkers zijn voor bepaalde verwerkingen en dat er een overeenkomst is afgesloten en waar deze te vinden is.

De provincie Limburg zorgt er in principe voor dat er geen doorgifte plaatsvindt buiten de EU maar dit is niet altijd mogelijk. Een item dat recentelijk speelde is de [REDACTED] en [REDACTED] en de opslag hiervan binnen de [REDACTED] in de US. Hier is afzonderlijk advies over afgegeven door het PIT.

Het ongeoorloofd delen van persoonsgegevens is een van de aandachtsgebieden van de AP voor 2020-2023.

### *Aandachtpunten hierbij:*

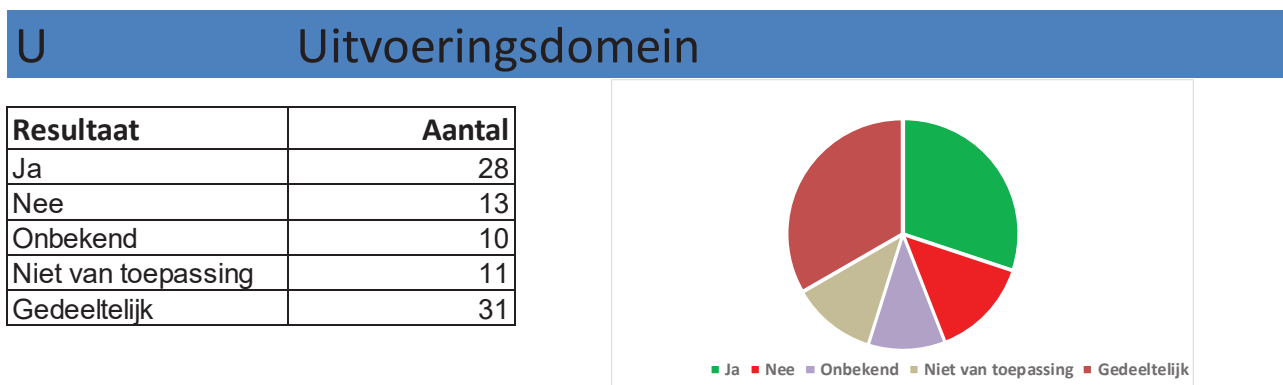
- De onderlinge verantwoordelijkheden bij gedeelde verantwoordelijkheid en de rechten van de betrokkene in deze.
- Afdoende garanties met betrekking tot verwerking door een verwerker in een overeenkomst of andere rechtshandeling.
- Uitzonderingsgronden voor doorgifte of verdere verwerking.
- Afwijkingen voor een bepaalde situatie waardoor doorgifte van persoonsgegevens mag plaatsvinden.
- Beschermingsniveau dient passend te zijn voor het soort gegevens dat verwerkt wordt.
- 100% Inzicht in verwerker en afgesloten overeenkomst.

*Planning:*

Continue aandacht hiervoor.

#### 4.2.8. Resultaat gap-analyse uitvoeringsdomein

Er is een Gap-analyse uitgevoerd op de eisen vanuit de Privacy Baseline van de Cip tegenover de mate van implementatie hiervan binnen de provincie. Deze analyse is nog niet uitgevoerd op het niveau van het volwassenheidsniveau zoals in hoofdstuk 3 is besproken. Voor deze gap-analyse is beoordeeld of een bepaalde beheersmaatregel wel, niet of gedeeltelijk geïmplementeerd is dan wel of deze van toepassing is voor de organisatie. Voor de 93 beheersmaatregelen van het uitvoeringsdomein geeft dit het volgende resultaat:



### 4.3. Het Control- of Beheerdomein

#### *Inleiding*

In dit gedeelte zijn richtlijnen opgenomen voor de specifieke beheeraspecten van de gegevensverwerking; dit houdt onder meer in dat een adequate technische- en organisatorische maatregelen moeten zijn ingericht, om de beheerprocessen vorm te geven.

#### *Doelstelling*

De doelstelling van de laag algemene control (beheersing) is ervoor te zorgen en/of vast te stellen dat maatregelen ter waarborging van de privacy afdoende zijn ingericht.

#### 4.3.1. C.01 Intern toezicht

##### *Inhoud:*

Binnen de organisatie wordt toezicht gehouden op de rechtmatigheid van de gegevensverwerking. Een gegevensverwerking is rechtmatig als deze voldoet aan de eisen die de AVG, sectorspecifieke wetgeving en/of een (eventuele) gedragscode stelt.

##### *Doelstelling:*

Het doel van 'Intern toezicht' is het garanderen van een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens, het garanderen van naleving van de AVG en van andere wet- en regelgeving betreffende de gegevensbescherming, en het garanderen en aantoonbaar maken van naleving van het beleid van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens.

##### *Risico:*

Als de verwerking van persoonsgegevens niet voldoet aan de AVG, dan zijn de risico's tweeledig: de betrokkene loopt persoonlijke privacyrisico's en de verwerkingsverantwoordelijke wordt geconfronteerd met politiek-bestuurlijke en/of juridische maatregelen, verlies van vertrouwen en beschadiging van imago als gevolg van communicatieve of handhavende maatregelen van betrokkenen, derden en/of de toezichthoudende autoriteiten.

##### *Bevindingen:*

De provincie Limburg beschikt over een Functionaris voor Gegevensbescherming<sup>45</sup> (FG). Een FG mag in dienst zijn van de organisatie, maar de functie mag ook ingevuld worden op grond van een dienstverleningsovereenkomst. De organisatie dient de FG te ondersteunen bij de uitvoering van de taken conform art. 39, AVG. Deze taken moet de FG onafhankelijk kunnen uitvoeren zonder instructies te krijgen over de uitvoering van de taken. Het rapporteren over de taken doet de FG rechtstreeks aan de directie van de organisatie. Daarnaast is de FG in overeenstemming met EU en nationaal recht verplicht tot geheimhouding/vertrouwelijkheid.

---

<sup>45</sup> Art. 37-39 AVG.



Door het onvolledig zijn van het register van verwerkingsactiviteiten is de organisatie niet eenduidig in staat om de rechtmatigheid van de gegevensverwerkingen aan te tonen.

Interne afspraken, gedragsregels, procedures en beleid zijn er om nageleefd te worden. In de praktijk blijkt dat hier niet altijd gevolg aan gegeven wordt. Door het intern toezicht blijft hier continue aandacht voor binnen de organisatie en dat niet alleen voor privacy.

#### *Aandachtpunten/advies:*

Door de provincie Limburg vindt evaluatie plaats van de gegevensverwerkingen door middel van een register van verwerkingsactiviteiten en is de ook de rechtmatigheid hierin aangetoond. Het doel hiervan is het garanderen van een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens, het garanderen van naleving van de AVG en van andere wet- en regelgeving betreffende de gegevensbescherming, en het garanderen en aantoonbaar maken van naleving van het beleid van de provincie Limburg met betrekking tot de bescherming van persoonsgegevens.

#### *Aandachtpunten hierbij:*

- Controle of gegevensverwerkingen voldoen aan de wettelijke verplichtingen door middel van periodieke compliance assessments en rapportage hierover.
- Aantonen van de rechtmatigheid van de verwerking van persoonsgegevens
  - Doelbinding (U.01)
  - Minimale gegevensverwerking (U.01)
  - Rechtmatigheid (U.01)
  - Verwerkersovereenkomsten (U.07)
  - Technische en organisatorische maatregelen (U.04)
  - Juistheid van de persoonsgegevens (U.03)
  - Behoorlijkheid van verwerken (B.03)
  - Transparantie richting betrokkene (U.05)
  - Verantwoordingsplicht verwerkingsverantwoordelijke (AVG art.5 lid 2)
  - Verwerkingenregister (U.02).

Het Register van verwerkingsactiviteiten bevindt zich in een volgende fase van uitbreiding en doorvoeren van verbeteringen. Op dit moment (einde 2019) is er bijvoorbeeld een intensieve samenwerking met nagenoeg alle clusters met een vermoeden van een achterstand en het privacy team om de juiste verwerkingen op de juiste manier te registreren.

#### *Planning:*

Continue. Te zijner tijd worden de activiteiten in het kader van het beoordelen van de compliance vastgesteld.

### 4.3.2. C.02 Toegang gegevensverwerking voor betrokkenen

#### *Inhoud:*

Iedere betrokkene heeft (binnen grenzen van redelijkheid) het recht te weten of, door wie, waarvoor en op welke wijze zijn persoonsgegevens worden verwerkt. De verwerkingsverantwoordelijke moet deze transparantie kunnen bieden.

#### *Doelstelling:*

Deze transparantie is nodig om de betrokkene of diens wettelijke vertegenwoordiger in staat te stellen - indien nodig - zonder onevenredige kosten en/of moeite zijn gegevens te laten corrigeren of de verantwoordelijke aan te spreken bij onrechtmatigheid van een gegevensverwerking zodat deze onrechtmatigheid beëindigd kan worden.

#### *Risico:*

Het risico ligt hierin dat als de organisatie in deze niet op de juiste manier transparant is, waardoor het inzicht in de rechtmatigheid van verwerkingen ontbreekt, het vertrouwen in de organisatie verloren kan gaan.

#### *Bevindingen:*

Op dit moment krijgt de betrokkene op verzoek uitsluitel over het al dan niet verwerken van persoonsgegevens betreffende deze betrokkene. De wijze waarop is nog niet geformaliseerd.

#### *Aandachtpunten/advies:*

De provincie Limburg biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit tijdig en in een passende vorm, zodat de betrokkene zijn rechten kan uitoefenen<sup>46</sup>, tenzij er een specifieke uitzonderingsgrond geldt.

Het doel hiervan is om zo nodig transparantie te bieden over de gegevensverwerking, zodat de betrokkene zijn rechten kan uitoefenen en zo de verantwoordelijke kan aanspreken bij onrechtmatigheid van een gegevensverwerking zodat deze onrechtmatigheid beëindigd kan worden.

#### Aandachtpunten hierbij:

- De betrokkene kan op verzoek uitsluitel krijgen omtrent verwerking van persoonsgegevens.
- De tijdigheid hieromtrent.
- Een passende vorm van de communicatie (beknopt, transparant, begrijpelijk).
- Wettelijke bepalingen waarbij een specifieke uitzondering geldt<sup>47 48</sup>.

---

<sup>46</sup> AVG art. 12.

<sup>47</sup> AVG art. 23.

<sup>48</sup> Memorie van Toelichting uitvoeringswet AVG, § 2.4

Planning:

Er is een “protocol rechten betrokkene” in een afrondende fase. Dit protocol zal begin 2020 gereed zijn en geïmplementeerd worden in de organisatie.

#### **4.3.3. C.03 Meldplicht Datalekken**

*Inhoud:*

Het bieden van inzicht in een datalek<sup>49</sup> en de mogelijke gevolgen ervan, kan mogelijk (negatieve) consequenties voor de betrokkenen beperken<sup>50</sup>. Een datalek is een "inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

*Doelstelling:*

Het doel van deze meldplicht is om de negatieve consequenties van een datalek te beperken en waar mogelijk te voorkomen.

*Risico:*

Gevolgen van een datalek kunnen de negatieve consequenties zijn voor de persoonlijke levenssfeer van de betrokkenen maar ook indien het een extern datalek betreft, negatieve consequenties voor het imago van de provincie Limburg.

*Bevindingen:*

De provincie Limburg heeft een protocol datalekken. Deze dateert van januari 2017 en is beschikbaar via intranet. Tevens refereert dit protocol aan de vervallen Wet Bescherming Persoonsgegevens.

Er is sinds het derde kwartaal 2019 een nieuw protocol datalekken in ontwikkeling. Dit protocol refereert naar de AVG in plaats van de Wet Bescherming Persoonsgegevens en naar de “Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, oftewel WP250 rev 1(NL). Dit nieuwe protocol dat waarschijnlijk eind 2019 gereed zal zijn, biedt ook handvatten om de ernst van een datalek te kunnen beoordelen om zodoende objectiever te kunnen bepalen of een datalek meldingsplichtig is.

Uit de gesprekken is gebleken dat het niet bij iedereen binnen de organisaties geheel duidelijk is wat een datalek is, dat er een protocol datalekken is en wat dient te gebeuren als een medewerker een datalek ontdekt dan wel vermoedt.

---

<sup>49</sup> AVG: „inbreuk in verband met persoonsgegevens”

<sup>50</sup> AVG art. 33 en 34.

#### *Aandachtpunten/Advies:*

Het verdient aanbeveling om het huidige protocol datalekken te herzien, hetgeen nu in behandeling is. Hierbij dient deze overeen te stemmen met de AVG en tevens de beleidsregels van de EDPB/ WP29. Een moeilijk punt hierbij is de mogelijke melding aan de AP wanneer een datalek waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een uitbreiding van het protocol is mogelijk met een objectieve methode voor de bepaling van de ernst van het lek. Hiertoe kan gebruik worden gemaakt van “*Recommendations for a methodology of the assessment of severity of personal data breaches*”<sup>51</sup> van de Enisa. Binnen het PIT is een aangepaste en verbeterde versie van deze methodiek in ontwikkeling om de ernst van een datalek meer objectief te kunnen bepalen.

De provincie Limburg zal het nieuwe protocol formaliseren en implementeren in de organisatie. Het doel van de procedure is om negatieve consequenties van een datalek te beperken en waar mogelijk te voorkomen.

De AP heeft een naar aanleiding van een onderzoek van incidentregistraties van ook overheden een aantal tips opgesteld<sup>52</sup> waaraan een incident/datalekregistratie dient te voldoen. Deze tips dienen verwerkt te worden in de betreffende registratie.

De incidenten/datalekken dienen regelmatig op het juiste niveau binnen de organisatie als onderdeel van een plan-do-check-learn-act cyclus besproken te worden. Het juiste niveau en de vorm van rapportage dienen bepaald te worden. Informatiebeveiliging en Privacy zou periodiek een agendapunt bij het DT en/of MT dienen te zijn.

#### *Aandachtpunten hierbij:*

- Mogelijke melding aan de AP, de vorm waarin en de gestelde termijn.
- Mogelijke melding aan de betrokkene, de vorm waarin en de gestelde termijn.
- De documentatie omtrent de “inbreuk in verband met persoonsgegevens”.
- De uitzonderingen omtrent een mogelijk melding aan de AP en betrokkene.
- Het incidentenregister minimaal conform aanbevelingen Autoriteit Persoonsgegevens.
- Rapportages in de juiste vorm voor verschillende niveaus binnen de organisatie.

#### *Planning:*

Kw1-2020 voor het gereviseerde protocol datalekken en de incidenten/datalekkenregistratie.

---

<sup>51</sup> <https://www.enisa.europa.eu/publications/dbn-severity>

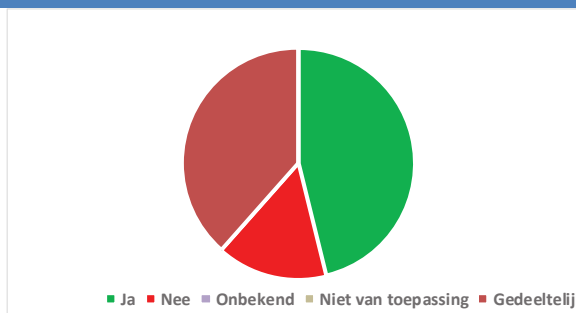
<sup>52</sup> <https://autoriteitpersoonsgegevens.nl/nl/nieuws/kwaliteit-datalekregister-bij-overheidsorganisaties-loopt-nog-uiteen>

#### 4.3.4. Resultaat gap-analyse Control- of Beheerdomein

Er is een Gap-analyse uitgevoerd op de eisen vanuit de Privacy Baseline van de Cip tegenover de mate van implementatie hiervan binnen de provincie. Deze analyse is nog niet uitgevoerd op het niveau van het volwassenheidsniveau zoals in hoofdstuk 3 is besproken. Voor deze gap-analyse is beoordeeld of een bepaalde beheersmaatregel wel, niet of gedeeltelijk geïmplementeerd is dan wel of deze van toepassing is voor de organisatie. Voor de 39 beheersmaatregelen van het Control- of Beheerdomein geeft dit het volgende resultaat:

### C Controledomein

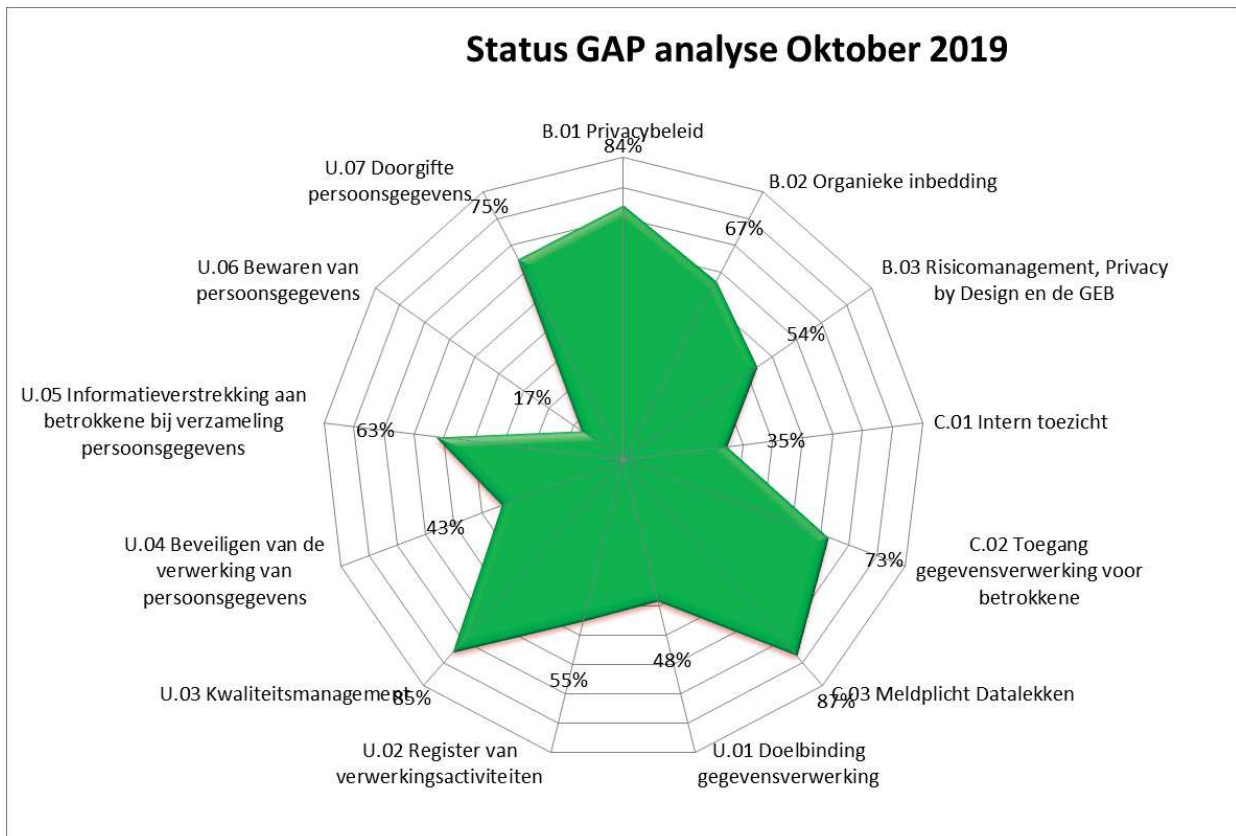
Resultaat	Aantal
Ja	18
Nee	6
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	15



#### 4.4. Resultaat Gap-analyse.

In deze fase zijn alle beheersmaatregelen beoordeeld. Gezien het karakter van de beheersmaatregelen, sommige op subjectieve basis. Ook is het niet uit te sluiten dat sommige beheersmaatregelen die op dit moment de status “Niet van toepassing” hebben, toekomstig opnieuw beoordeeld dienen te worden.

Onderstaande grafiek geeft de situatie weer van oktober 2019.



## 5. Vervolgstappen en prioritering

In het vorige hoofdstuk is – samen met bevindingen – aangegeven welke stappen genomen dienen te worden om een adequaat volwassenheidsniveau te verkrijgen om aan de AVG te kunnen voldoen. Het mag duidelijk zijn dat een en ander niet binnen korte termijn verder gerealiseerd zal kunnen worden. Hiertoe dient overwogen te worden welke werkzaamheden prioriteit krijgen en mogelijk parallel met andere activiteiten uitgevoerd kunnen worden.

Bij het gebruik van het framework van de CIP zal er gewerkt worden met zo'n 165 beheersmaatregelen.

### 5.1. Focus Autoriteit Persoonsgegevens 2020 - 2023 en focusgebied Digitale Overheid

De Autoriteit Persoonsgegevens legt de komende jaren (2020-2023) in het toezichtwerk extra nadruk op drie focusgebieden: datahandel, digitale overheid en artificiële intelligentie en algoritmes. De AP vindt dat extra nadruk op deze thema's nodig is om de bescherming van persoonsgegevens in Nederland te borgen. Hierbij geven tot en met 2023 deze focusgebieden onder meer richting aan de uitvoering van de wettelijke taken van de AP. De AP houdt hierbij risicogestuurd toezicht. Dat betekent dat de AP is gespist op onderwerpen met een groot risico voor burgers. Daarbij weegt de AP af om hoeveel data het gaat en hoe gevoelig die data zijn. Op basis daarvan gebruikt de AP een of meerdere toezichtsinstrumenten, zoals normuitleg, wetgevingsadvies, voorlichting of handhaving.

De Autoriteit zal de focusgebieden programmatisch aanpakken. De belangrijkste aandachtsgebieden binnen Digitale overheid zijn:

- Databeveiliging
- Smart cities
- Samenwerkingsverbanden / ongeoorloofd delen
- Verkiezingen en microtargeting

Voor deze focus- en aandachtsgebieden geldt dat de provincie hieraan een passende invulling dient te geven waar van toepassing. Het aandachtsgebied databeveiliging is besproken in 4.2.4. De aandachtsgebieden zullen meegenomen worden in toekomstig toezicht en onderzoek.

#### 5.1.1. Databeveiliging

De AP verwacht van overheidsorganisaties dat zij structureel en op toereikende wijze investeren in hun informatiebeveiliging. De komende jaren wil de AP overheidsorganisaties controleren op hun beveiligingsniveau en hen stimuleren om werk te maken van een sterke IT- en datahuishouding. De AP wil bevorderen dat overheidsorganisaties behendig worden in privacyrisicomanagement en hun IT-systemen laten auditen als onderdeel van hun databoekhouding.

#### 5.1.2. Smart cities

Steden, stedelijke gebieden en gemeenten zijn steeds vaker op zoek naar slimme oplossingen voor vraagstukken op het gebied van mobiliteit, energie, veiligheid en huisvesting. Deze slimme oplossingen vinden zij in sensoren en data. Ondersteund door technologieën zoals machine learning proberen steden data te verzamelen of slim data te combineren over bijvoorbeeld afvalstromen, energiegebruik of stromen van mensen. Slim gebruik van de data kunnen bewoners 'verleiden' tot betere keuzes en het gebruik van de

openbare ruimte optimaliseren. Hiermee raken steden en gemeenten aan de grenzen tussen het openbaar belang en de privacy van bewoners.

De AP vindt het belangrijk dat overheidsorganisaties vroegtijdig in hun processen stilstaan bij de grondrechten en keuzevrijheden van mensen. De AP spreekt overheidsorganisaties erop aan dat zij hun processen zodanig inrichten dat zij zo min mogelijk persoonsgegevens verzamelen (privacy by design). De AP zal de ontwikkelingen op dit terrein volgen en in kaart brengen. Waar nodig treedt de AP handhavend op.

#### **5.1.3. Samenwerkingsverbanden / ongeoorloofd delen**

Steeds vaker deelt en koppelt de overheid bestanden; van centraal tot lokaal, al dan niet in Europees verband. Dit gebeurt zowel tussen overheidsorganisaties onderling als tussen de overheid en de private sector. Hoewel de intenties vaak goed zijn, kan het delen en koppelen van bestanden een schending zijn van het wettelijke beginsel van doelbinding. De overheid moet daarom voorzichtig zijn met bestanden aan elkaar koppelen, zelfs als dat kostentechnisch voor de hand ligt.

Het is aan overheidsbestuurders en aan de wetgever om een goede afweging te maken over het nut en de noodzaak van het gebruik van data en nieuwe verwerkingen. De AP spreekt bestuurders hierop aan. Schending van het beginsel van doelbinding pakt de AP zo nodig aan. Dit betekent ook dat de wetgever het beginsel van doelbinding in acht moet houden bij het opstellen van nieuwe wetgeving, zowel op nationaal als op Europees niveau.

#### **5.1.4. Verkiezingen en microtargeting**

Politieke partijen verwerken en gebruiken steeds vaker persoonsgegevens, met als doel zo gericht mogelijk hun leden te bereiken. Ook maken zij gebruik van externe partijen om dit werk voor hen te doen. De Europese wetgever heeft aangegeven dat dit op grond van een algemeen belang is toegestaan, maar dat er wel waarborgen worden vastgesteld. Een rechtmatige, behoorlijke en transparante verwerking is belangrijk om vrije verkiezingen in een open samenleving te waarborgen.

De AP houdt toezicht op de naleving van de AVG door politieke partijen. Dit doet de AP door verkennend onderzoek te doen, nadere normen te formuleren, zelfregulering te stimuleren en eventueel te handhaven. De AP hecht hierbij veel waarde aan samenwerking met de Europese collega's.



## **5.2. Vervolgstappen en prioritering**

### **Beoordeling van het huidige privacybeleid en correlerende documenten.**

Een goed privacybeleid toont aan dat een organisatie zelf nadenkt over de gegevens die zij verwerkt en daarover transparant communiceert. Het huidige beleid is 1 jaar geleden vastgesteld en dient periodiek geëvolueerd te worden.

### **Toezicht op de uitbreiding en verbetering van het register van verwerkingsactiviteiten.**

Het register van verwerkingsactiviteiten met de juiste informatie is een eerste stap waarmee een organisatie laat zien dat zij de privacyregels serieus neemt. Het correct zijn van dit register is een must.

### **Toezicht op de herziene protocol datalekken inclusief een rekenmethodiek voor het bepalen van de ernst van een datalek.**

Hierbij is het belangrijk dat aan het hele proces aandacht is besteed. Het begint immers bij de initiële melding (de eigen medewerkers hebben hier ook een rol) tot en met de implementatie van verbeteringen.

### **Toezicht op de herziene registratie van datalekken.**

De documentatie omtrent datalekken dient minimaal conform aanbevelingen AP te zijn.

### **Toetsing bewustwording binnen de organisatie op het vlak van privacy (en informatiebeveiliging).**

Het continue bewust zijn is een must voor iedere organisatie.

### **Toetsingsmodel opzetten en inrichten naar toetsing conform volwassenheidsniveau en toetsen conform.**

Het streven van de provincie is om volwassenheidsniveau 3 aantoonbaar te behalen.

### **Warme overdracht naar de nieuwe Functionaris voor Gegevensbescherming.**

Spreekt voor zich.

## 6. In kort bestek

Puntsgewijs zaken die het afgelopen jaar de revue zijn gepasseerd zonder uitputtend te zijn.

- De organisatie is zich ervan bewust dat het nog stappen dient te maken op het gebied van privacy en informatiebeveiliging en dat dit niet vanzelf gaat.
- Het privacybeleid is in een aantal sessies besproken in het Privacy en Informatiebeveiligingsteam (PIT), verder ontwikkeld en aangescherpt. Het privacybeleid is vastgesteld en staat geagendeerd voor review conform vastgesteld beleid.
- Als uitvloeisel van het privacybeleid is er nu voor ieder cluster een clusterambassadeur privacy.
- Er was een eerste bijeenkomst gepland met de clusterambassadeurs privacy in april 2019. Naast opleiding op het gebied van privacy zal de rol van de ambassadeur besproken worden.
- Het PIT (ook benoemd in het beleid) komt structureel bij elkaar met agenda en activiteitenlijst en geeft opvolging aan de punten uit de activiteiten lijst. Bij specifieke vragen hebben de leden een flexibele instelling als de situatie daarom vraagt.
- Enkele actiepunten van het PIT van de afgelopen tijd zonder hierbij uitputtend te zijn:
  - Privacybeleid. Extern en intern
  - Aanvullingen RvV borgen
  - Voorlichting handelswijze datalek
  - Onderzoek, advies en opvolging bij datalekken
  - Gap-analyse en GEB-analyse
  - Verwerkersovereenkomsten
  - DDI
  - Themalunch Privacy
  - Social Media Management Systeem waaronder Monitoring
  - Privacyverklaring Social Media
  - Veilig mailen
  - Wob verzoek datalekken
  - ██████████
  - Gevoelige verwerkingen bij Kabinet
  - Clusters hernieuwd ondersteunen bij de registratie van de verwerkingen
  - Verwerkingen vertrouwenspersoon

- Prioriteitenlijst van de Autoriteit Persoonsgegevens bij onderzoek
  - De nieuwe ISO 27701 als Privacy Information Management System
- 
- Er is een eerste volledige gap-analyse gemaakt in relatie tot de 165 beheersmaatregelen van de CIP. Deze zal verder uitgewerkt dienen te worden.
  - Er is een FAQ beschikbaar via Intranet met veel gestelde vragen omtrent de AVG.
  - Een handleiding betrokkenen is nagenoeg afgerond.
  - Er is een standaardverwerkersovereenkomst en deze wordt ook gebruikt. Misschien ook in die gevallen waar het niet van toepassing is.
  - Risicomanagementproces met privacy is nog niet ingericht.
  - GEB is gestandaardiseerd maar nog niet beschreven.
  - Er is een GEB uitgevoerd op de applicatie van burgemeestersbenoemingen en bij subsidies.
  - Er loopt nu een derde ronde ter uitbreiding en verbetering van het register van verwerkingsactiviteiten.
  - Verwerkingen die de provincie Limburg uitvoert als verwerker, dienen opgenomen te worden in het RvV.
  - ☞ Sommige medewerkers kunnen te veel autorisaties hebben vooral wanneer ze van cluster zijn gewijzigd en geen bemoeienissen meer hebben met het “oude” cluster. Deze dienen herzien te worden.
  - ☞ Schaduw P&O dossiers zijn ongewenst. Hier dient toch een activiteit op plaats te vinden.
  - Implementatie van een mogelijkheid van Veilig Mailen liever vandaag dan morgen. Hier hoort een protocol met beslisboom bij om te bepalen wanneer een medewerker veilig dient te mailen.
  - Bewaartermijnen van gegevens zal altijd een moeilijk punt blijven. Maar met de uitbreiding van het RvV en het bewustzijn bij de medewerkers zijn er stappen mogelijk.
  - Clusters die aangeduid zijn met een verhoogd risico in relatie tot de verwerking van persoonsgegevens zijn Personeel & Organisatie, Subsidies en Kabinet. Met VTH zijn nog afspraken gepland. Wellicht dat Subsidies hieruit verdwijnt. Naar de verwerkingen van de vertrouwenspersoon wordt nader onderzoek gedaan.
  - De datalekken welke zich hebben voorgedaan zijn energiek opgepakt en afgehandeld.
  - Protocol datalekken verdiende aanpassing en is nagenoeg afgerond.
  - Veel medewerkers zijn zich bewust van de gevoeligheid van de gegevens en gaan hier over het algemeen bewust mee om.

- De *awareness* games zullen mede een bijdrage leveren om de medewerkers bewust te maken. Dit is inmiddels in uitvoering en draagt ertoe bij om risico's te mitigeren.
- Een analyse tool van de CIP zal later in gebruik genomen worden om het globale volwassenheidsniveau van de implementatie periodiek te kunnen meten.
- Ontwikkeling protocol cameratoezicht. Wordt er ook gebruik gemaakt van heimelijk cameratoezicht? Gebruik van mobiele apparatuur? Hier dient onderzoek plaats te vinden.
- Informatiebeveiliging en Privacy bescherming dienen aandachtspunten te zijn en te blijven voor iedere medewerker in de organisatie.

## 7. Bijlagen

### 7.1. Bijlage A – Positionering Provinciaal Overleg Functionarissen voor Gegevensbescherming

*Alle provincies hebben een interne toezichthouder op het gebied van privacy en gegevensbescherming: de Functionaris voor Gegevensbescherming. Het aanwijzen van een dergelijke functionaris is namelijk verplicht voor publieke organisaties op grond van de Algemene Verordening Gegevensbescherming. De 12 Functionarissen voor Gegevensbescherming van de Nederlandse provincies zoeken een manier om samen te werken. Dit stuk is bedoeld om (1) de uitgangspunten voor samenwerking onder elkaar te zetten en (2) een formele plek te vinden voor het bijbehorende overleg.*

#### (1) Uitgangspunten voor de samenwerking

##### I. Kennisuitwisseling staat voorop

Het POFG komt bij elkaar om **kennis te delen**. Deze samenwerking met andere provincies verbetert de kwaliteit van de individuele Functionarissen voor Gegevensbescherming (hierna: FG). Het uitwisselen van *best practices* bespaart bovendien kosten: niet elke provincie hoeft het wiel opnieuw uit te vinden. Zo kunnen FG's samen (beleids)instrumenten ontwikkelen of gezamenlijk diensten inkopen. Door deze samenwerking vindt efficiënte kennisuitwisseling plaats.

##### II. Samenwerken onder eigen verantwoordelijkheid

De FG is een interne toezichthouder en opereert **onafhankelijk**. De werkgever van een FG mag geen instructies geven over de uitvoering van zijn taken. Het POFG mag dit evenmin en moet dit nimmer willen. Dat betekent dat elke FG die deelneemt aan het overleg, eigen verantwoordelijkheid draagt voor zijn interne toezicht. Samenwerking mag er dus nooit toe leiden dat de onafhankelijkheid van de FG in het geding komt.

##### III. Collectief waar mogelijk, individueel waar dat moet

Het POFG **adviseert** en **vertegenwoordigt** de belangen van de provinciale functionarissen voor gegevensbescherming. Om de individuele onafhankelijkheid te waarborgen gelden daarbij de volgende condities:

- minderheidsmeningen worden altijd gerespecteerd, afwijkende meningen zijn mogelijk<sup>53</sup>;
- advisering gebeurt op strategisch niveau: géén punten en komma's maar hoofdlijnen;
- externe advisering gebeurt alleen vrijwillig en niet op afroep. Zonder draagvlak geen advies.

##### IV. Inhoudelijke samenwerking boven formele overlegstructuur

Op dit moment is het POFG een provinciaal overleg zonder formele status. Het overleg zoekt een formele plek in het provinciale landschap, al dan niet gekoppeld aan financiële ondersteuning voor het realiseren van de doelstellingen. Bij deze zoektocht is de **inhoudelijke samenwerking** belangrijker dan de formele overlegstructuur. Dit moet ertoe leiden dat het POFG wordt gepositioneerd op een plek die strookt met het wettelijk statuut van de FG.

---

<sup>53</sup> Dit kan praktisch ingevuld worden door gebruik te maken van *concurring* en *dissenting opinions* zoals in internationale context gebeurt bij rechterlijke uitspraken. De *dissenting opinion* bevat een van de meerderheid afwijkende conclusie, terwijl de *concurring opinion* de conclusie van de meerderheid bijvalt, maar die conclusie baseert op een andere juridische redenering.

## (2) Positie overleg

Op dit moment vinden de overleggen van het POFG plaats op informele basis. Daarbij wordt gebruik gemaakt van het vergadercentrum van BIJ12, dat speciaal bestemd is voor medewerkers van provincies en het IPO. Het POFG zoekt een formele positie in het provinciale landschap.

Met een formele inbedding kan het POFG kennisuitwisseling borgen en meerwaarde leveren aan provincies. Het ligt voor de hand om daarbij naar de vereniging van provincies te kijken: het Interprovinciaal Overleg (IPO). Op de website van het IPO worden twee taken genoemd<sup>54</sup>:

- Belangenbehartiging
- Innovatie & kennisuitwisseling

In de eerste taak van het IPO heeft het POFG geen rol: het POFG kan namelijk wel de belangen van de functionarissen voor gegevensbescherming behartigen, maar niet die van de provincies.

De tweede taak van het IPO past wel binnen de plannen van het POFG: *“Het IPO biedt tevens een platform aan de provincies voor het stimuleren van innovatie en de uitwisseling van kennis. Op deze wijze kunnen provincies ‘best practices’ uitwisselen en vernieuwingen in het provinciaal beleid entameren. Doel daarbij is een bijdrage leveren aan de kwaliteit, effectiviteit en efficiency van het openbaar bestuur.”*

Het POFG zal met het IPO in gesprek gaan om te onderzoeken of een formele ophanging daar mogelijk is. De hierboven geformuleerde uitgangspunten voor samenwerking zijn daarbij leidend.

Idealiter verzorgt het IPO een **secretaris** en een **vergaderlocatie**. Deze ondersteuning aan het POFG levert kostenbesparing op. Elke provincie is namelijk verplicht een FG aan te wijzen. Tegelijkertijd moet elke provincie *“alle benodigde middelen ter beschikking stellen”* zodat de FG zijn taken uit kan voeren en zijn deskundigheid in stand kan houden.<sup>55</sup> Zo kan het POFG gezamenlijk trainingen of kennis inkopen en hoeven de leden niet het wiel zelf uit te vinden.

Het POFG draagt bij aan deze wettelijke verplichting en maakt dat de deskundigheid van FG's op efficiënte wijze onderhouden kan worden. Het IPO kan dit vanuit de verenigingsdoelen faciliteren.

---

<sup>54</sup> <https://ipo.nl/over-het-ipo>

<sup>55</sup> Artikel 38 lid 2 Algemene Verordening Gegevensbescherming

## 7.2. Bijlage B – Onderzoek Autoriteit Persoonsgegevens Haga Ziekenhuis

De Autoriteit Persoonsgegevens (AP) had het al vermeld in het jaarverslag over 2018:

*“In 2019 gaan wij aan de slag om onze werkprocessen verder te verbeteren, onze risico gestuurde aanpak door te ontwikkelen en de focus van ons toezicht te verbreden van voornamelijk voorlichting naar meer handhaving”<sup>56</sup>.*

Dat dit niet zo maar een loze kreet was, blijkt wel uit de eerste grote boete die de AP uitgedeeld heeft à € 460.000,-- en een last onder dwangsom van € 300.000,--.

### Wat was er gebeurd?

In het Haga ziekenhuis was het patiëntendossier van een bekende Nederlander onrechtmatig ingekeken door medewerkers. Een klokkenluider heeft dit gemeld via Publeaks<sup>57</sup>. Het Haga ziekenhuis heeft dit incident op 4 april 2018 (ten tijde van de Wet Bescherming Persoonsgegevens!) gemeld als een datalek bij de AP.

### Waarom een datalek?

Omdat deze medewerkers van het Haga ziekenhuis niet direct betrokken waren bij de behandeling van deze patiënt maar gewoon nieuwsgierig waren.

### Wat was de onderzoeksvraag van de AP?

Het procesverloop is beschreven in het boetebesluit. De AP heeft de volgende onderzoeksvragen geformuleerd:

Zijn de maatregelen die het Haga Ziekenhuis heeft getroffen, teneinde te waarborgen dat persoonsgegevens in het digitale patiëntdossier niet worden ingezien door onbevoegde medewerkers, ‘passend’ als bedoeld in artikel 32 van de AVG? De AP heeft in dit kader de volgende aspecten onderzocht: authenticatie, autorisaties, logging, controle van de logging en de bewustwording van medewerkers.

Voorts heeft de AP onderzoek gedaan naar de procedures rondom het melden van datalekken (artikel 33, eerste lid, en artikel 34, eerste lid, van de AVG).

### Wat deed het ziekenhuis goed binnen het onderzochte kader?

Binnen het onderzochte kader heeft de AP van de volgende zaken geconcludeerd dat deze op orde waren hetgeen in de media meestal onderbelicht blijft:

- Toegangscontrolebeleid: context-gebonden, zorgvuldig opgesteld, beleid wordt uitgevoerd.
- Logging: alle toegang wordt gelogd; mogelijk om achteraf misbruik vast te stellen.
- Bewustwording medewerkers: introductieprogramma's, werkoverleg, intranet, workshops, landelijke campagne informatieveiligheid.
- Melden datalekken: Passende procedure en intern datalekkenregister.

### Wat is naar het oordeel van de AP niet correct binnen de onderzochte context?

In het boetebesluit wordt snel geschakeld naar artikel 32 AVG. Hierin wordt in ruime bewoordingen gesteld dat er passende technische en organisatorische maatregelen dienen te zijn om een op het risico afgestemd beveiligingsniveau te waarborgen.

---

<sup>56</sup> [https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap\\_jaarverslag\\_2018.pdf](https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2018.pdf)

<sup>57</sup> <https://www.publeaks.nl/>

De “Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg” wordt erbij gehaald in relatie tot het “Besluit elektronische gegevensverwerking door zorgaanbieders” als Algemene maatregel van Bestuur waarnaar de eerstgenoemde wet verwijst. Hierin is ook een verwijzing naar onder andere de NEN7510 en NEN7513.

Zorginstellingen moeten bij elektronische patiëntendossiers door middel van tweefactor-authenticatie de identiteit van de gebruiker vaststellen. De AP constateert dat authenticatie van de identiteit van de medewerker in het Haga ziekenhuis op twee manieren mogelijk is:

Ten eerste kunnen gebruikers inloggen op de virtuele werkplek (VDI) door de personeelspas voor een paslezer te houden. Vervolgens voert de gebruiker zijn gebruikersnaam, het wachtwoord en een viercijferige (door de gebruiker opgegeven vaste) pincode in. Er is sprake van een “single -sign-on” functionaliteit, waardoor eenmaal ingelogd op de VDI ook toegang mogelijk is tot het ziekenhuisinformatiesysteem. De gebruiker kan daarna vier uren op een willekeurig werkstation met de pas af- en aanmelden zonder invoer van gebruikersnaam, wachtwoord en/of pincode.

Ten tweede kan de gebruiker zonder personeelspas inloggen op de VDI en het ziekenhuisinformatiesysteem met een gebruikersnaam en wachtwoord, bijvoorbeeld als de medewerker de personeelspas is vergeten.

#### **De AP concludeert dat hiermee niet is voldaan aan de NEN7510 norm 9.4.1.**

De AP constateert in relatie tot de controle op de logging van toegang tot de dossiers in het Haga ziekenhuis het volgende:

Logbestanden hebben systematische, consequente controle nodig. Het beleid voor controle van de logging van het Haga ziekenhuis regelt dat controle op de rechtmatigheid van toegang tot de patiëntdossiers plaatsvindt via de logging van een aselechte steekproef van jaarlijks zes patiëntdossiers, waarbij wordt gelet op mislukte toegangspoging en alsmede gerealiseerde toegang tot het digitaal dossier buiten de behandelrelatie en gerealiseerd via de noodknopprocedure.

Indien een geselecteerd dossier hoort tot een van de vijf ‘gevoelige’ groepen, dient de logging van dat dossier volledig te worden gecontroleerd. Echter, met een controle van de logging van een aselechte steekproef van jaarlijks zes patiëntdossiers, heeft het Haga ziekenhuis geen beleid ten aanzien van systematische, risicogerichte c.q. intelligente controle van de logging.

Ook in de praktijk heeft geen systematische controle van de logging plaatsgevonden, want de controles die de afgelopen periode wel hebben plaatsgevonden waren naar aanleiding van enkele klachten en verzoeken maar niet risicogericht en voorts in omvang onvoldoende, gelet op de schaal van de verwerking van het ziekenhuis.

#### **De AP concludeert dat niet is voldaan aan de NEN 7510 norm 12.4.1.**

#### **Wat gaat het kosten?**

De melding van het datalek was ten tijde van Wbp (4 april 2018) maar het onderzoek heeft plaatsgevonden naar de situatie van oktober 2018 dus ruimschoots na het van toepassing zijn van de AVG.

In het rapport van de AP wordt gesteld dat geldboeten in elke zaak **doeltreffend, evenredig en afschrikkend** dienen te zijn.

Deze boete is opgelegd omdat het ziekenhuis in de periode van januari 2018 tot ten tijde van het onderzoek niet heeft voldaan aan:



- Het vereiste van tweefactor authenticatie en
- Het regelmatig en op de juiste wijze beoordelen van logbestanden.

Artikel 32 AVG valt onder een categorie II boete. De bandbreedte hiervan ligt tussen € 120.000 en € 500.000. De basisboete is € 310.000 welke naar het maximum of het minimum bijgesteld kan worden afhankelijk van de bevindingen van de AP. De AP houdt bij de hoogte van de boete ook rekening met de financiële situatie van de overtreder.

Het basisbedrag van de boete is € 310.000. Hierop is een verhoging toegepast van € 75.000 in verband met de aard, ernst en duur van de overtreding.

Tevens is er een verhoging toegepast van € 75.000 in verband met de opzettelijke of nalatige aard van de inbreuk. De directie was als deelnemend lid van de datalekcommissie namelijk op de hoogte van deze datalekken en heeft hierop niet adequaat gehandeld. Wat de totale boete voor het Haga ziekenhuis brengt tot € 460.000,--.

Verder dient het Haga ziekenhuis binnen vijftien weken na dagtekeningen maatregelen te nemen die ertoe leiden dat:

1. deze toegang uitsluitend mogelijk is met toepassing van twee factor authenticatie;
2. de logbestanden regelmatig worden gecontroleerd op onrechtmatige toegang of onrechtmatig gebruik van patiëntgegevens.

Indien het Haga ziekenhuis niet uiterlijk binnen vijftien weken na datum van het besluit van de AP de maatregelen heeft uitgevoerd om (geheel) aan de last te voldoen, verbeurt het Haga ziekenhuis een dwangsom van €100.000,-- voor iedere twee weken na afloop van de begunstigingstermijn, tot een maximumbedrag van in totaal € 300.000,--.

De vordering van de boete loopt via het Centraal Justitieel Incassobureau (CJIB).

### **Lessons to be learned!**

- De Autoriteit Persoonsgegevens blaft niet meer alleen maar bijt ook. (Zij het vooralsnog in beperkte mate).
- In mijn optiek heeft de AP voor de scope van het onderzoek (zeer) behoorlijk werk geleverd.
- In het onderzoek wordt niet alleen uitgegaan van privacy en sectorale wetgeving maar ook hieraan gerelateerde normen.
- De verantwoordelijkheid van de directie is meegewogen en heeft wellicht mede geleid tot een verzwaring van de boete.
- Geen sprake van PDCA of een continue verbeter proces. Het is goed of het is niet goed. Dus geen sprake van ernstige afwijkingen/non-conformiteit met de mogelijkheid van reparatie. Het dient op orde te zijn!
- Nu een onderzoek naar een zorginstelling. Wanneer is een overheidsorgaan aan de beurt?
- Controle op logging op een beperkt aantal dossiers omdat de controle erg tijdsintensief is. Geen tijd en geld voor de juiste authenticatie en om de controle van de logging juist te doen. Maar naderhand wel juridische kosten maken, de boete moeten ophoesten en dan alsnog de tijd en het geld in de juiste werkwijze moeten steken.
- Een onderzoek uitgevoerd op deze manier zal bij veel organisatie leiden tot non-conformiteit of beter gezegd overtredingen van de wet. Dus niet voldoen aan de gestelde eisen. Hoe gaat de AP hiermee om...

### 7.3. Bijlage C – Lijst gebruikte afkortingen

AAD	Azure Active Directory
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BSN	Burgerservicenummer
CIP	Centrum Informatiebeveiliging en Privacybescherming
CISO	Chief/Corporate Information Security Officer
DPIA	Data Protection Impact Assessment (GEB)
EDPB	European Data Protection Board
FG	Functionaris voor de Gegevensbescherming
GDPR	General Data Protection Regulation
GEB	Gegevensbeschermingseffectbeoordeling (DPIA)
IB	Informatiebeveiliging
IBD	Informatiebeveiligingsdienst
ISO	Information Security Officer
MFA	Multi Factor Authentication
OSF	Open State Foundation
PIA	Privacy Impact Assessment
PIT	Het Privacy- en Informatiebeveiligingsteam
RvV	Register van Verwerkingsactiviteiten
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
VNG	Vereniging Nederlandse Gemeenten
VWO	Verwerkersovereenkomst
Wbp	Wet Bescherming Persoonsgegevens

#### **7.4. Bijlage D – Bronvermelding**

- VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming)
- Uitvoeringswet Algemene verordening gegevensbescherming
- Memorie van toelichting uitvoeringswet Algemene verordening gegevensbescherming
- Centrum Informatiebeveiliging en Privacybescherming – De Privacy Baseline
- Centrum Informatiebeveiliging en Privacybescherming – Privacy volwassenheidsmodel
- Centrum Informatiebeveiliging en Privacybescherming – Grip op Secure System Development
- Ministerie van Justitie en Veiligheid – Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming
- Autoriteit Persoonsgegevens – Boetebesluit HagaZiekenhuis openbare versie
- Autoriteit Persoonsgegevens – Onderzoek toegang digitale patiëntendossiers Hagaziekenhuis.
- Autoriteit Persoonsgegevens – Focus AP 2020 – 2023