Roadmap voor de implementatie van de Algemene Verordening Gegevensbescherming

Tineke van Heijst - mei 2017

Managementsamenvatting

Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening vervangt de huidige Privacyrichtlijn die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). De AVG is van toepassing op publieke én private organisaties die persoonsgegevens verwerken. Dit vergt van die organisaties een aantal organisatorische veranderingen. In dit stappenplan zijn de eisen zoals gesteld in de AVG door VHIC vertaald naar tien concrete stappen die een organisatie kan nemen om te komen tot overeenstemming met de gestelde eisen. De stappen zijn genummerd, maar de volgorde is niet chronologisch. Het is dus niet noodzakelijk om de stappen in een bepaalde volgorde uit te voeren. De inventarisatie die de basis vormt van waaruit concrete vervolgstappen kunnen worden genomen zal wel als één van de eerste punten opgepakt moeten worden.

In het stappenplan van VHIC worden de volgende stappen beschreven:

Stap 1 – Stel een projectleider of een projectteam aan voor de implementatie

Voor organisaties is het van belang om zo spoedig mogelijk te starten met de implementatie om zodoende op 25 mei 2018 daadwerkelijk te voldoen aan de in de AVG gestelde eisen. Omdat de implementatie een omvangrijk proces kan vormen (zeker voor organisaties die nog niets hebben geregeld omtrent de bescherming van persoonsgegevens) is het raadzaam een speciaal projectteam samen te stellen en hier tijd en middelen voor vrij te maken.

Stap 2 – Stel een Functionaris Gegevensbescherming aan

Voor bepaalde organisaties wordt het verplicht gesteld een Functionaris Gegevensbescherming (FG) aan te stellen. Een FG heeft een vastgesteld takenpakket dat hij of zij naast eventuele andere taken binnen de organisatie kan uitvoeren. Aan de FG moeten alle middelen beschikbaar worden gesteld die hij of zij nodig heeft om zijn of haar taken naar behoren uit te kunnen voeren.

Stap 3 – Creëer bewustwording in de organisatie

Goed omgaan met persoonsgegevens start bij het bewust omgaan met persoonsgegevens. Het is daarom van belang om niet te wachten tot de implementatie van de AVG is voltooid om vervolgens pas de medewerkers van de organisatie te gaan informeren over de wijzigingen maar om de hele organisatie mee te nemen vanaf het begin in het proces.

Stap 4 – Inventariseer de verwerking van persoonsgegevens

Als één van de eerste stappen in de implementatie is het aan te bevelen om een inventarisatie te maken van persoonsgegevens en de verwerking hiervan in de organisatie. In de roadmap wordt gekeken naar informatiestromen binnen de werkprocessen van een organisatie. Per werkproces wordt gekeken:

- Of er persoonsgegevens worden verwerkt en zo ja.
- Welke persoonsgegevens worden verwerkt.
- Waar deze persoonsgegevens vandaan komen (bron).
- Aan welke verwerking(en) de gegevens worden onderworpen.
- Wat het doeleinde is per verwerking.
- Wat de grondslag is van de verwerking.
- In welke systemen de gegevens worden verwerkt.
- Door wie de gegevens worden verwerkt en met wie ze worden gedeeld (intern, extern en eventueel ook naar zogenaamde derde landen).
- Wat de bewaartermijn is van de gegevens en op welke wijze de gegevens worden vernietigd.

De AVG gaat uit van een documentatieplicht van zowel de verwerkingsverantwoordelijke als de verwerker en op diverse momenten moeten er gegevens over de verwerking worden gedocumenteerd of ter controle beschikbaar worden gesteld. De inventarisatie vormt de kapstok voor deze documentatieplicht en de basis voor iedere privacy compliancestrategie.

Stap 5 – Zorg voor passende beveiliging van de persoonsgegevens

Cruciaal binnen de verwerking van persoonsgegevens is te zorgen voor passende technische en organisatorische maatregelen om de gegevens te beveiligen. Op basis van de gemaakte inventarisatie kan worden gekeken hoe de persoonsgegevens beveiligd zijn.

In veel organisaties ligt de technische beveiliging van informatie die zich bevindt in systemen bij de ICT-afdeling en in de meeste organisaties is een Chief Information Security Officer (CISO) aangesteld die specifiek is belast met informatiebeveiliging. Het is belangrijk om ervoor te zorgen dat de CISO of in ieder geval ICT nauw wordt betrokken in het implementatieproces van de AVG. Verder is het van belang om naast de technische beveiliging van computersystemen ook in kaart te brengen welke andere informatiebeveiligingsmaatregelen zijn getroffen.

Een ander nieuw element binnen de AVG is dat gegevensbeschermingseffectbeoordelingen (privacy impact assessments) voor verwerkingen die waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen opleveren verplicht worden gesteld.

Stap 6 - Maak of controleer afspraken met de verwerkers

Wanneer er een overzicht is welke verwerkers namens de verwerkingsverantwoordelijke persoonsgegevens verwerken kan worden nagegaan of met iedere verwerker afspraken zijn gemaakt. De AVG stelt specifieke eisen aan de elementen die moeten worden opgenomen in een bewerkersovereenkomst.

Stap 7 – Zet een register van verwerkingsactiviteiten op

Na het afronden van de inventarisatie is het van belang om grip te houden op de verwerking van persoonsgegevens binnen de organisatie. Dit kan via een register van verwerkingsactiviteiten. Dit register is een verplichting onder de AVG voor zowel de verwerkingsverantwoordelijke als de verwerker en moet op verzoek beschikbaar worden gesteld aan de Autoriteit Persoonsgegevens.

Stap 8 – Ontwerp en stel een gegevensbeschermingsbeleid vast

Het is aan te bevelen om algemeen beleid te maken dat de naleving van de AVG op hoofdlijnen beschrijft. In feite komen in dit beleid de hoofdlijnen van dit stappenplan terug. Vaak zal het gegevensbeschermingsbeleid worden vertaald naar een privacyverklaring die aan de betrokkene wordt verstrekt. Het beleid dient regelmatig geëvalueerd en getest te worden en waar nodig te worden aangepast.

Stap 9 – Stel een procedure op voor de melding van een inbreuk in verband met persoonsgegevens

Er is sprake van een inbreuk in verband met persoonsgegevens wanneer persoonsgegevens zijn (1) vernietigd of verloren, (2) gewijzigd, (3) verstrekt of (4) toegankelijk zijn gemaakt op een manier die onrechtmatig is, oftewel die buiten de regels van de AVG plaatsvindt. Indien er sprake is van een inbreuk of datalek dient dit binnen 72 uur nadat de verwerkingsverantwoordelijke kennis heeft genomen van de inbreuk of het datalek te worden gemeld bij de Autoriteit Persoonsgegevens.

Stap 10 – Stel procedures op richting de betrokkenen

De verwerkingsverantwoordelijke heeft onder de AVG verschillende informatieverplichtingen richting de betrokkene. Ook heeft de betrokkene onder de AVG diverse rechten waar hij of zij beroep op kan doen zoals het recht op inzage, het recht op rectificatie, het recht op beperking van de verwerking, het recht op wissing van de gegevens, het recht op intrekken van toestemming en het recht op bezwaar. Hier moet een organisatie zich op voorbereiden door vast te stellen welke informatie op welk moment beschikbaar moet zijn om aan de betrokkene te verstrekken.

Organisaties hebben twee jaar de tijd gekregen (tot mei 2018) om de AVG te implementeren. Het niet naleven van de verordening kan een substantieel financieel risico opleveren. Boetes bij niet naleving kunnen oplopen tot 20 miljoen euro of vier procent van de wereldwijde jaaromzet.

Bij het verschijnen van dit stappenplan, in mei 2017, is nog een jaar de tijd om de nieuwe eisen van de AVG te implementeren. Hoogste tijd dus om aan de slag te gaan!

Inhoud

Inleiding

1.

Wie oplet ziet dat de implementatie van de Algemene Verordening Gegevensbescherming (AVG, ook wel bekend als de General Data Protection Regulation, afgekort GDPR) volop in het nieuws staat. In de meeste organisaties begint het besef te komen dat er iets moet gebeuren om straks de torenhoge boetes die kunnen worden uitgedeeld bij het niet naleven van de nieuwe wetgeving te voorkomen, maar waar te beginnen? Dit stappenplan van VHIC is een vertaling van de eisen en regels zoals vastgelegd in de AVG naar praktische stappen en concrete checklists en biedt als zodanig handvatten aan organisaties om in de praktijk aan de slag te gaan met de implementatie.

1.1 Aanleiding

Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG, ook wel bekend als de General Data Protection Regulation afgekort als GDPR) in werking getreden. Deze verordening vervangt de huidige Privacyrichtlijn die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp).

De belangrijkste redenen om de huidige wetgeving te herzien waren:

(1) de snelle technische ontwikkelingen en vergaande globalisering die ervoor zorgen dat er nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan.[1]

(2) de sterke toename van de hoeveelheid grensoverschrijdende stromen van persoonsgegevens.[2]

(3) de behoefte aan (verdere) harmonisatie van wet- en regelgeving op het gebied van privacy- wetgeving in de verschillende lidstaten. In de huidige situatie onder de Privacyrichtlijn gelden in de verschillende lidstaten uiteenlopende niveaus van bescherming van de rechten en vrijheden van natuurlijke personen op het gebied van de verwerking van persoonsgegevens.[3]

De AVG is van toepassing op publieke én private organisaties die persoonsgegevens verwerken. Dit vergt van organisaties een aantal organisatorische veranderingen. Afhankelijk van het type organisatie en het type verwerkingen die plaatsvinden worden organisaties verplicht een intern gegevensbeschermings-beleid (privacybeleid) vast te stellen, een functionaris voor gegevensbescherming (afgekort als FG ook bekend onder de Engelse benaming Data Protection Officer, afgekort als DPO) aan te stellen, privacy te integreren als vast onderwerp binnen de bedrijfsvoering en de werking ervan jaarlijks te controleren. Daarnaast wordt de toepassing van de gegevensbeschermingseffectbeoordeling (of privacy impact assessment afgekort als PIA) verplicht op het moment dat er veranderingen in diensten, producten, processen en informatiesystemen worden doorgevoerd (denk hierbij bijvoorbeeld aan het migreren van informatie naar de cloud, of het aanschaffen van een nieuw informatiesysteem).

Organisaties hebben twee jaar de tijd gekregen (tot mei 2018) om de AVG te implementeren. Het niet naleven van de verordening kan een substantieel financieel risico opleveren. Boetes bij niet naleving kunnen oplopen tot 20 miljoen euro of vier procent van de wereldwijde jaaromzet.[4] Gezien de mogelijke implicaties van deze verordening is een goede voorbereiding noodzakelijk.

1.2 Begrippenkader

Voordat wordt ingegaan op de stappen die moeten worden genomen om te komen tot implementatie van de AVG is het van belang om een duidelijk beeld te hebben van de belangrijkste begrippen die in de AVG worden gehanteerd. In bijlage 1 is een uitgebreide begrippenlijst opgenomen.

1.2.1 Persoonsgegevens

In de AVG worden persoonsgegevens als volgt gedefinieerd *'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 identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.*[5]

---

1 Verordening (EU) 2016/679 Van het Europees Parlement en de Raad, overweging 6, p.2 verschenen in het Publicatieblad van de Europese Unie, 4.5.2016
2 Verordening (EU) 2016/679 Van het Europees Parlement en de Raad, overweging 5, p.2 verschenen in het Publicatieblad van de Europese Unie, 4.5.2016
3 Verordening (EU) 2016/679 Van het Europees Parlement en de Raad, overweging 9 p.2 verschenen in het Publicatieblad van de Europese Unie, 4.5.2016
4 Artikel 83.4 en 83.5 van de AVG beschrijven de boeteclausules en welke inbreuken van de AVG leiden tot welke categorie boetes.
5 Zie art. 4 AVG.

Een meer vereenvoudigde definitie die vaak wordt gehanteerd is *'een gegeven aan de hand waarvan een persoon kan worden geïdentificeerd.*[6] De mogelijkheid tot het identificeren van een persoon is hierbij cruciaal. Wanneer een betrokkene niet identificeerbaar is, dan is het gegeven geen persoonsgegeven. Aan de hand van een persoonsgegeven kan men dus, zonder een bijzondere inspanning te leveren, de identiteit van een persoon vaststellen of achterhalen. Er moet dus een verband zijn tussen het gegeven en de persoon. Denk hierbij aan naam- en adresgegevens, geboortedata, e-mailadressen, telefoonnummers, en (pas)foto's. Maar ook gegevens zoals iemands IQ, een luchtfoto van een huis, het kenteken van een auto of de winst van een eenmanszaak kunnen worden geclassificeerd als persoonsgegevens. Ook online identificatoren zoals een IP-adres, cookie, RFID-tag of IMEI-nummer van een smartphone vallen onder persoonsgegevens.[7] Denk dus bij het vaststellen of iets een persoonsgegeven is of niet in de breedste zin of daarmee een persoon al dan niet identificeerbaar is.

1.2.2 Bijzondere persoonsgegevens

Een organisatie moet nog extra beveiligingsmaatregelen treffen indien de persoonsgegevens die worden verwerkt vallen onder de categorie bijzondere persoonsgegevens die in artikel 9 van de AVG worden gedefinieerd als *'persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken en de verwerking van genetische, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksuele gedrag of seksuele gerichtheid'*. Dit zijn gegevens die zo gevoelig zijn dat de verwerking ervan iemands privacy ernstig kan beïnvloeden. Ook het burgerservicenummer (BSN), irisscans, DNA en vingerafdrukken vallen onder deze categorie van persoonsgegevens.

1.2.3 Persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten

Een andere categorie persoonsgegevens die een bijzondere status hebben binnen de AVG en waarvan de verwerking aan specifieke eisen moet voldoen is de categorie persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten.

1.2.4 Verwerking

Een verwerking is *'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés.*[8] Onder verwerken vallen alle handelingen die een organisatie kan uitvoeren met persoonsgegevens van verzamelen tot en met het vernietigen. In de Wbp werden de volgende handelingen aangegeven die hieronder vallen: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.[9] Denk hierbij aan het uitbesteden van een salarisadministratie, maar ook de opslag van persoonsgegevens in bijvoorbeeld een CRM- systeem of een andere applicatie of in de cloud.

1.2.5 Verwerker

Een verwerker wordt in de AVG gedefinieerd als *'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.'*[10] De term verwerker is een nieuwe benaming voor wat men in de Wbp de bewerker noemde.

1.2.6 Betrokkene

De betrokkene is *'de identificeerbare of geïdentificeerde natuurlijke persoon'*[11]. Betrokkenen hebben rechten ten aanzien van de verwerking van hun persoonsgegevens, deze zullen nader worden toegelicht in deze Roadmap.

1.2.7 Verwerkingsverantwoordelijke

Een verwerkingsverantwoordelijke is *'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.*[12]*'*

---

6 Deze definitie wordt o.a. gebruikt op de website van Justitia http://www.justitia.nl/privacy/persoonsgegevens.html - geraadpleegd op 12 april 2017.
7 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 21'
8 Zie art. 4 lid 2 AVG.
9 Zie art. 1 lid b Wbp.
10 Zie art. 4 lid 8 AVG.
11 Zie art. 4 lid 1 AVG.
12 Zie art. 4 lid 7 AVG.

1.3 Belangrijkste beginselen

De AVG kent een aantal beginselen die de rode lijn vormen door alle vereisten waaraan een organisatie moet voldoen te weten:[13]

- Rechtmatigheid – de verwerking van persoonsgegevens is rechtmatig.
- Eerlijkheid – de verwerking van persoonsgegevens is behoorlijk.
- Transparantie – de verwerking van persoonsgegevens is transparant.
- Doelbinding – de persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en vervolgens niet op onverenigbare wijze verwerkt.
- Dataminimalisatie – persoonsgegevens zijn adequaat en ter zake dienend en blijven beperkt tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt.
- Juistheid – de persoonsgegevens zijn juist en worden zo nodig geactualiseerd.
- Opslagbeperking – de persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden bewaard noodzakelijk is.
- Integriteit en vertrouwelijkheid – de persoonsgegevens worden door passende technische of organisatorische maatregelen op een dusdanige manier verwerkt dat een passende beveiliging gewaarborgd is.
- Verantwoordingsplicht – persoonsgegevens worden verwerkt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, die ervoor zorgt en kan aantonen dat de verwerking voldoet aan de bepalingen van de verordening.

Iedere maatregel die een organisatie moet treffen om te voldoen aan de eisen zoals geformuleerd in de AVG is terug te voeren op deze beginselen.

1.4 Uitgangspunten

Voor de leesbaarheid en om te voorkomen dat dit stappenplan te complex zou worden, zijn een aantal aspecten van de AVG buiten beschouwing gelaten.

1.4.1 AVG is van toepassing

Zo is er vanuit gegaan dat de AVG van toepassing is. Er zijn vier uitzonderingen voor de verwerking van persoonsgegevens waarbij de AVG niet van toepassing is. Het gaat dan om:

- verwerkingen die plaatsvinden in het kader van activiteiten die buiten de werkingssfeer van het unierecht vallen.
- een verwerking die plaatsvindt door de lidstaten bij de uitvoering van activiteiten binnen de werkingssfeer van de specifieke bepalingen betreffende het gemeenschappelijk buitenlands en veiligheidsbeleid (titel V, hoofdstuk 2, VEU).
- een verwerking die plaatsvindt door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.
- een verwerking die plaatsvindt door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van bescherming tegen en het voorkomen van gevaren voor de openbare orde.

Omdat deze uitzonderingen zo specifiek zijn, zijn ze alleen voor bepaalde organisaties van toepassing en is het dus niet voor iedere organisatie noodzakelijk om te toetsen op het al dan niet van toepassing zijn van de AVG.

1.4.2 Er is nog niets geregeld t.a.v. de verwerking van persoonsgegevens in de organisatie

De AVG vervangt de huidige Privacyrichtlijn die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). Om deze paper niet te complex te maken wordt er vanuit gegaan dat er nog niets is geregeld in de organisatie. Binnen organisaties waar de Wbp al is geïmplementeerd zullen delen van dit stappenplan sneller kunnen worden doorlopen (bijvoorbeeld wanneer al goed in kaart is gebracht waar in de organisatie zich persoonsgegevens bevinden en er al is vastgesteld welke doelen er zijn voor de verwerking van persoonsgegevens). Toch blijft het van belang om het stappenplan wel in zijn geheel door te nemen, om de eventuele wijzigingen t.o.v. de Wbp door te kunnen voeren. De AVG verschilt van de Wbp doordat er op verschillende aspecten veel explicietere eisen gesteld worden.

13 Deze beginselen liggen vast in artikel 5 van de AVG maar zijn ook heel duidelijk omschreven op de website van SURF https://wiki.surfnet.nl/display/privacy/De+privacyverordening+uitgewerkt#Deprivacyverordeninguitgewerkt-Rechtenvanbetrokkenen – geraadpleegd op 12 april 2017.

1.4.3 Verwerkingsverantwoordelijke is gevestigd in de EU

In de AVG worden ook regels gesteld voor organisaties die persoonsgegevens verwerken maar waarvan de gegevensverantwoordelijke niet in de EU gevestigd is. In dat geval kan de gegevensverantwoordelijke een vertegenwoordiger aanwijzen die wel in de EU gevestigd is. Ook hier gaat het om specifieke gevallen die alleen voor bepaalde organisaties van toepassing zijn en is dit scenario in het stappenplan buiten beschouwing gelaten.

1.4.4 Gedragscodes en certificeringen

In de AVG wordt gesproken over diverse gedragscodes en certificeringen. Dit onderdeel met name op het gebied van certificeringen is nog in ontwikkeling en is voornamelijk gebaseerd op de intentie om zaken goed te regelen en hier controle op uit te oefenen. Om deze reden en omdat de reikwijdte van dit onderzoek het niet toestaat uitgebreid onderzoek te doen naar de gedragscodes en certificeringen zijn deze in dit stappenplan buiten beschouwing gelaten.

1.4.5 Er is sprake van één verwerkingsverantwoordelijke

In sommige gevallen kunnen er twee of meer verwerkingsverantwoordelijken zijn die dan onderling een regeling dienen te treffen inzake de uitoefening van de rechten van de betrokkene en respectievelijke verplichtingen. In de regeling wordt dan één contactpunt aangewezen. In dit stappenplan wordt er vanuit gegaan dat er slechts één verwerkingsverantwoordelijke is.

1.4.6 De organisatie valt onder de Autoriteit Persoonsgegevens

Elke lidstaat bepaalt dat één of meer onafhankelijke overheidsinstanties verantwoordelijk zijn voor het toezicht op de toepassing van de AVG (artikel 51). In Nederland is de Autoriteit Persoonsgegevens de bevoegde instantie.
Wanneer een verwerking zich niet beperkt tot één lidstaat, kan de situatie ontstaan dat volgens artikel 55 van de AVG meerdere toezichthouders bevoegd zijn. In dat geval neemt één toezichthouder de leiding en kan deze zodoende over de gehele verwerking oordelen. De leidende toezichthouder is de toezichthouder die bevoegd is voor het land van de hoofdvestiging van de verwerkings-verantwoordelijke.[14] In dit stappenplan wordt er vanuit gegaan dat de Autoriteit Persoonsgegevens de (leidende) toezichthouder is (en niet een toezichthouder in een andere lidstaat van de EU). De rechten en plichten van de toezichthoudende autoriteit worden alleen genoemd wanneer deze rechtstreeks impact hebben op een van de te nemen stappen om te komen tot implementatie van de AVG.

1.4.7 Specifieke bewerkingen zijn niet opgenomen

In hoofdstuk 9 van de verordening wordt ingegaan op specifieke bewerkingen en de eisen die aan deze verwerkingen zijn gesteld. Deze specifieke bewerkingen zijn in dit stappenplan buiten beschouwing gelaten. Het gaat dan om de volgende verwerkingen:

- Verwerking en vrijheid van meningsuiting en van informatie (art. 85).
- Verwerking en recht van toegang van het publiek tot officiële documenten (art. 86).
- Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden (art. 89).

Er zijn twee andere verwerkingen die in hoofdstuk 9 Specifieke verwerkingen van de AVG worden behandeld, die in de praktijk veelvuldig aan de orde zijn. Deze twee verwerkingen komen wel terug in het stappenplan. Het gaat dan om de verwerking van het nationaal identificatienummer (art. 87) en de verwerking in het kader van de arbeidsverhouding (art. 88).

Rondom de verwerking van het nationaal identificatienummer (in Nederland het BSN nummer) zijn veel vragen. Lidstaten hebben onder de AVG de mogelijkheid om nadere regels te stellen over de verwerking van dit nummer. In de Uitvoeringswet (art. 44) is bepaald dat het BSN enkel mag worden verwerkt indien dit is gebaseerd op een wettelijke grondslag.

Voor de verwerking van een BSN door de overheid is de wettelijke grondslag neergelegd in art. 10 van de Wet algemene bepalingen burgerservicenummer (Wabb) waarin staat dat ‘overheidsorganen bij het verwerken van persoonsgegevens in het kader van de uitvoering van hun taak gebruik kunnen maken van het burgerservicenummer.’ Gebruik door overige instellingen moet zijn voorgeschreven in sectorale wetgeving. [15]

Verwerking in het kader van de arbeidsverhouding is een verwerking die in vrijwel iedere organisatie voorkomt. De AVG stelt in art. 88(1) dat lidstaten op hun grondgebied eigen regels kunnen stellen over de omgang met persoonsgegevens binnen de arbeidsverhouding. Deze nadere regels mogen afwijken van de AVG.

14 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 217
15 Idem, p. 293-294

Nederland heeft in de Memorie van Toelichting op de Uitvoeringswet Algemene Verordening Gegevensbescherming aangegeven dat er geen behoefte is om gebruik te maken van de ruimte die deze bepaling aan het lidstatelijk recht biedt.[16] Lidstaten hebben tot 25 mei 2018 de tijd om de regels over persoonsgegevens binnen de arbeidsverhouding te melden.[17]

1.5 Verschillen ten opzichte van het stappenplan van de Autoriteit Persoonsgegevens

Recent (13 april 2017) heeft de Autoriteit Persoonsgegevens een artikel gepubliceerd met de titel "In 10 stappen voorbereid op de AVG". Dit artikel zet de tien belangrijkste stappen op een rijtje. Deze stappen wijken af van de stappen die in dit stappenplan worden geïdentificeerd. De verschillen worden veroorzaakt doordat de Autoriteit Persoonsgegevens op een andere wijze de stappen heeft gegroepeerd. Zo worden bijvoorbeeld de privacy impact assessment, privacy by design en privacy by default apart als stappen genoemd, terwijl in het stappenplan van VHIC deze stappen zijn gecombineerd in de stap 'zorg voor een passende beveiliging van persoonsgegevens'. Binnen deze stap worden privacy impact assessments uitgevoerd om het juiste beveiligingsniveau te bepalen en wordt gekeken naar privacy by design en privacy by default.

De stappen die de Autoriteit Persoonsgegevens heeft gedefinieerd zijn als volgt:

1. Bewustwording: Deze stap komt terug in zowel stap 1 'stel een projectteam of projectleider aan voor de implementatie van de AVG' als in stap 3 'Creëer bewustwording in uw organisatie'. In beide stappen wordt het belang benadrukt om tijd en middelen vrij te maken in de organisatie om de implementatie van de AVG binnen uw organisatie te realiseren.
2. Rechten van betrokkenen: Deze stap vindt u terug in stap 10 'stel procedures op richting de betrokkenen'. In deze stap wordt uitgebreid ingegaan op de rechten van betrokkenen en hoe u zich op een beroep van een betrokkene op deze rechten moet voorbereiden.
3. Overzicht verwerkingen: In feite is de documentatieplicht van de AVG in het stappenplan van VHIC verdeeld over een aantal stappen te beginnen met stap 4 'Inventariseer de verwerking van persoonsgegevens' en stap 7 die voortbouwt op de inventarisatie door het 'opzetten van een register van verwerkingsactiviteiten'.
4. Privacy Impact Assessment: Deze stap is opgenomen onder stap 5 'Zorg voor passende beveiliging van per soonsgegevens'. De Privacy Impact Assessment die voor bepaalde verwerkingen verplicht moet worden uit gevoerd vormt de basis waarop de te nemen beveiligingsmaatregelen moeten zijn gebaseerd en is om die reden in deze stap ondergebracht.
5. Privacy by design & privacy by default: Net als de voorgaande stap is deze stap ondergebracht bij stap 5 'Zorg voor passende beveiliging van persoonsgegevens'. Een van de dingen waar een organisatie onder de AVG rekening mee moet houden is dat privacy by design altijd voorgaat op privacy by default. Dit wordt nader toe gelicht in stap 5.
6. Functionaris voor gegevensbescherming: Deze stap komt overeen met stap 2 in het VHIC stappenplan 'stel een functionaris gegevensbescherming aan'.
7. Meldplicht datalekken: Deze stap komt overeen met stap 9 'stel een procedure op voor de melding van een inbreuk in verband met persoonsgegevens'.
8. Bewerkersovereenkomsten: Deze stap komt overeen met stap 6 'Maak of controleer afspraken met verwerkers'.
9. Leidende toezichthouder: In het stappenplan van VHIC wordt uitgegaan van een toezichthouder – de Autoriteit Persoonsgegevens. De gevallen waarbij een organisatie vestigingen heeft in meerdere lidstaten of gegevensverwerkingen heeft die in meerdere lidstaten impact hebben dient de organisatie te bepalen onder welke privacytoezichthouder de organisatie valt. Hoe de organisatie dit bepaalt wordt in dit stappenplan niet nader uitgewerkt. Mocht u hier vragen over hebben, dan beantwoorden wij deze graag via info@vhic.nl.
10. Toestemming: Hierbij gaat het om het verkrijgen en vastleggen van toestemming van de betrokkene. Dit wordt nader toegelicht in stap 10 'Stel procedures op richting de betrokkenen'.

Naast de stappen uit de AP heeft VHIC nog een andere stap gedefinieerd die in het stappenplan van de AP niet terugkomt en dat is de stap die eigenlijk ten grondslag ligt aan de hele implementatie en naleving van de AVG: 'ontwerp en stel een gegevensbeschermingsbeleid vast'. Dit gegevensbeschermingsbeleid vormt het kader dat in hoofdlijnen beschrijft hoe u als organisatie op hoofdlijnen de naleving van de AVG vorm geeft.

16 Uitvoeringswet Algemene Verordening Gegevensbescherming, Memorie van toelichting – implementatietabel p. 70.
17 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 294-295

Tot slot is een groot verschil tussen de AP en de stappen als gedefinieerd door VHIC de mate van detail en uitwerking. In ons stappenplan hebben we geprobeerd een zo praktisch mogelijke vertaling te maken van de AVG zodat u een Roadmap hebt om de implementatie en in een later stadium de naleving vorm te geven.

Roadmap

2.

In dit hoofdstuk zijn de eisen zoals gesteld in de AVG vertaald naar concrete stappen die een organisatie kan nemen om te komen tot overeenstemming met de gestelde eisen. De stappen zijn genummerd, maar de volgorde ervan is niet chronologisch. Het is dus niet noodzakelijk om deze in een bepaalde volgorde uit te voeren. De inventarisatie die de basis vormt van waaruit concrete vervolgstappen kunnen worden genomen zal wel als één van de eerste punten opgepakt moeten worden.

De Roadmap is geschreven vanuit de ambitie om te voldoen aan de eisen die gesteld zijn in de AVG en niet om hier bovenuit te steken. Een organisatie kan het ambitieniveau zelf hoger leggen als de wil en mogelijkheid er is om meer tijd en energie vrij te maken en een voorbeeldrol te nemen richting andere organisaties op het gebied van privacy.

2.1 Stap 1 – Stel een projectleider of projectteam aan voor de implementatie

Vanaf het moment van inwerkingtreding van de AVG in mei 2016 is een periode van twee jaar voorzien voor organisaties om zich aan te passen aan de nieuwe regelgeving. Bij het verschijnen van dit stappenplan is er al een jaar van deze implementatieperiode voorbij. Organisaties die nog niets hebben gedaan aan de implementatie dienen dus zo spoedig mogelijk aan de slag te gaan om te zorgen dat ze op 25 mei 2018 ook daadwerkelijk voldoen aan de in de AVG gestelde eisen.

Omdat implementatie een omvangrijk proces kan vormen (zeker voor organisaties die nog niets hebben geregeld omtrent de bescherming van persoonsgegevens) is het raadzaam een speciaal projectteam samen te stellen dat zich specifiek richt op de implementatie. Zorg ervoor dat dit projectteam geleid wordt door iemand met voldoende senioriteit en zeggenschap binnen de organisatie, zodat hij of zij zoveel mogelijk steun en medewerking krijgt vanuit sleutelfiguren in de organisatie.[18]

√ Stel ten minste een projectleider en bij voorkeur een projectteam aan dat verantwoordelijk is voor de implementatie van de AVG.

2.2 Stap 2 - Stel een Functionaris Gegevensbescherming aan

Onder de AVG wordt het voor bepaalde organisaties verplicht om een functionaris gegevensbescherming (FG of data protection officer) aan te wijzen. Dit geldt:[19]

1) voor overheidsinstanties of overheidsorganen (behalve in geval van gerechten bij de uitoefening van rechterlijke taken).
2) indien een verwerker of verwerkingsverantwoordelijke hoofdzakelijke is belast met verwerkingen die vanwege hun aard, omvang en/of doeleinden regelmatige en stelselmatige observatie op grote schaal van de betrokkenen vereisen.
3) indien een verwerker of verwerkingsverantwoordelijke hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens of strafrechtelijke gegevens.

Het is mogelijk om één FG aan te wijzen in geval van een concern of in geval van een overheidsinstantie of overheidsorgaan. Deze persoon vertegenwoordigt dan het concern of de verschillende instanties. Voorwaarde is wel dat de persoon vanuit iedere vestiging gemakkelijk te contacteren is.[20]

Een FG kan een personeelslid van een verwerkingsverantwoordelijke of een verwerker zijn of kan de taken op grond van een dienstverleningsovereenkomst verrichten.[21] Een FG kan andere taken en verplichtingen vervullen binnen dezelfde organisatie. De verwerkingsverantwoordelijke en de verwerker dienen ervoor te zorgen dat deze andere taken niet tot een belangenconflict leiden.[22]

18 Zie Louwers Advocaten, 'Stappenplan Algemene Verordening gegevensbescherming' op http://privacy-recht-louwersadvocaten.nl/stappenplan-avg/ - geraadpleegd op 12 april 2017.
19 Zie art. 37 lid 1 AVG.
20 Zie art. 37 lid 2 en 37 lid 3 AVG.
21 Zie art 37 lid 6 AVG.
22 Zie art 38 lid 6 AVG.

Een FG wordt aangewezen op grond van zijn of haar professionele kwaliteiten en deskundigheid op het gebied van wetgeving en de praktijk inzake gegevensbescherming en het vermogen deze volgende taken te vervullen:[23]

- Het informeren en adviseren van de verwerkingsverantwoordelijke, de verwerker of de werknemers over de verplichtingen zoals die zijn vastgelegd in de AVG.
- Het toezien op de naleving van de AVG en het beleid van de verwerkingsverantwoordelijke of de verwerker m.b.t. de bescherming, de toewijzing van verantwoordelijkheden, het bewust maken en de opleiding van bij de verwerking betrokken werknemers en de betreffende audits.
- Het verstrekken van adviezen m.b.t. de gegevensbeschermingseffect beoordeling en het toezien op de uitvoer ing hiervan.
- Het samenwerken met de Autoriteit Persoonsgegevens.
- Het optreden als contactpunt voor de Autoriteit Persoonsgegevens inclusief raadpleging en overleg.

De FG houdt bij uitvoering van de bovengenoemde taken naar behoren rekening met het aan verwerkingen verbonden risico en met de aard, omvang en context van verwerkingsdoeleinden.[24]

De contactgegevens van een FG worden gedeeld met de betrokkene, de verwerker, intern in de organisatie en met de Autoriteit Persoonsgegevens.[25] De betrokkenen kunnen contact opnemen met de FG over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van de rechten uit hoofde van de AVG.[26]

De FG heeft een aparte positie in de organisatie, zoals vastgelegd in artikel 38 van de AVG. Om de onafhankelijkheid van de FG te garanderen mag een FG geen instructies ontvangen van de verwerker of de verwerkingsverantwoordelijke m.b.t. de uitoefening van zijn of haar taken. Ook geniet de FG ontslagbescherming. Daarnaast dient de FG door de verwerker of verwerkingsverantwoordelijke tijdig te worden betrokken bij alle aangelegenheden die verband houden met de verwerking van persoonsgegevens. Ook dienen de verwerker en de verwerkingsverantwoordelijke de FG toegang te geven tot alle persoonsgegevens en verwerkingsactiviteiten en alle middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van deskundigheid. De FG is gehouden aan het recht tot geheimhouding of vertrouwelijkheid.

√ Stel indien van toepassing een FG met een bijbehorend takenpakket aan.
√ Stel alle middelen beschikbaar die de FG nodig heeft om zijn of haar taken naar behoren uit te kunnen voeren.
√ Deel de contactgegevens van de FG met de betrokkene, de verwerker, de Autoriteit persoonsgegevens en intern in de organisatie.

2.3 Stap 3 – Creëer bewustwording in de organisatie

Goed omgaan met persoonsgegevens start bij het bewust omgaan met persoonsgegevens. Het is daarom van belang om niet te wachten tot de implementatie van de AVG is voltooid om vervolgens pas de medewerkers van de organisatie te gaan informeren over de wijzigingen, maar om de hele organisatie vanaf het begin mee te nemen in het proces. Op die manier kunnen medewerkers meedenken in de inventarisatiefase en zal duidelijk worden dat persoonsgegevens zich op veel meer locaties bevinden en worden gebruikt dan vooraf was gedacht of dat meer mensen toegang hebben tot gegevens dan vooraf werd gedacht.

Bewustwording kan op verschillende manieren gebeuren. Zo kan een training worden aangeboden waarbij de medewerkers in de organisatie wordt verteld welke verplichtingen er gelden onder de nieuwe AVG en hoe de organisatie daar mee omgaat. Het is goed om met medewerkers hierover in gesprek te gaan.

Ook het ophangen van posters bijvoorbeeld in de kantine en bij de koffieautomaat kan ervoor zorgen dat medewerkers er steeds aan herinnerd worden dat ze bewust met persoonsgegevens moeten omgaan.

Daarnaast is het van belang dat er een open sfeer is in een organisatie waarin medewerkers elkaar durven aan te spreken op gedrag.

23 Zie art 38 lid 2 en art 39 AVG.
24 Zie art. 39 lid2 AVG.
25 Zie art. 37 lid 7 AVG.
26 Zie art. 38 lid 4 AVG.

Het is aan te raden om als er al een Functionaris Gegevensbescherming (zie paragraaf 2.2) is aangesteld deze persoon hier een rol in te laten spelen, zodat binnen de organisatie meteen duidelijk is wat zijn of haar rol is en welke taken en verantwoordelijkheden hierbij horen en hoe deze persoon intern bereikbaar is.

√ Betrek vanaf het begin de hele organisatie bij de implementatie van de AVG door actief alle medewerkers te informeren over de impact van de AVG en hun rol in het omgaan met persoonsgegevens.
√ Beschouw bewustwording als een continue proces en blijf hier steeds aandacht aan besteden.

2.4 Stap 4 – Inventariseer de verwerking van persoonsgegevens

Als één van de eerste stappen in de implementatie van de AVG is het aan te raden om een inventarisatie te maken van persoonsgegevens en de verwerking hiervan in de eigen organisatie. Hierbij wordt gekeken naar welke persoonsgegevens worden verzameld, welke gegevens worden verwerkt, waar deze gegevens vandaan komen en waar ze eventueel naartoe gaan. Deze inventarisatie is absoluut noodzakelijk voor iedere privacy-compliancestrategie.[27]

De AVG gaat uit van een documentatieplicht van zowel de verwerker als de verwerkings-verantwoordelijke en op diverse momenten moeten er gegevens over de verwerking worden gedocumenteerd of ter controle beschikbaar gesteld (of het nu is in de onderlinge samenwerking tussen verwerker en verwerkingsverantwoordelijke of tussen verwerkingsverantwoordelijke en betrokkene of zelfs tussen de verwerkingsverantwoordelijke of verwerker en de toezichthoudende autoriteit).

Een veelgebruikte benadering om een dergelijke inventarisatie aan te pakken is door te kijken naar de informatiestroom die wordt gevolgd via de data life cycle van creatie en initiële opslag tot het moment waarop de data niet meer nodig is en moet worden vernietigd. Dit wordt ook wel data flow mapping genoemd. In deze roadmap wordt ook gekeken naar een informatiestroom waarbij uitgegaan wordt van de werkprocessen in de organisatie. Per werkproces wordt gekeken:

- Of er persoonsgegevens worden verwerkt en zo ja.
- Welke persoonsgegevens worden verwerkt.
- Waar deze persoonsgegevens vandaan komen (bron).
- Aan welke verwerking(en) de gegevens worden onderworpen.
- Wat het doeleinde is per verwerking.
- Wat de grondslag is van de verwerking.
- In welke systemen de gegevens worden verwerkt.
- Door wie de gegevens worden verwerkt en met wie ze worden gedeeld (intern, extern en eventueel ook naar zogenaamde derde landen).
- Hoe de persoonsgegevens per verwerking worden beveiligd.
- Wat de bewaartermijn is van de gegevens en op welke wijze de persoonsgegevens worden vernietigd.

Deze tien stappen zijn gecomprimeerd tot 7 stappen in de inventarisatie:

1) Stel vast of en welke persoonsgegevens zich in de organisatie bevinden en waar ze vandaan komen.
2) Stel vast welke verwerkingen van persoonsgegevens plaatsvinden en in welke systemen.
3) Stel vast voor welke doeleinden de persoonsgegevens worden verwerkt (incl. dataminimalisatie).
4) Stel vast wat de grondslag van de verwerking is.
5) Stel vast wie de verwerkers zijn van de persoonsgegevens.
6) Stel vast of er sprake is van doorgifte van persoonsgegevens en bepalen van de ontvangers (incl. derde landen).
7) Stel vast hoe lang de persoonsgegevens bewaard worden en hoe zij moeten worden vernietigd.

Om het belang van de beveiliging van persoonsgegevens te onderstrepen is de stap in de inventarisatie om te kijken naar de beveiligingsmaatregelen die genomen zijn uit de inventarisatiefase gelicht en wordt deze besproken in paragraaf 2.5. Het is wel aan te bevelen deze stap in de inventarisatiefase mee te nemen, omdat dit een logisch moment is om de beveiliging in kaart te brengen.

27 Baker and McKenzie, 'Datamapping under the GDPR and beyond'. Geraadpleegd op 12 april 2017 van http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Data%20Mapping%20under%20the%20GDPR%20and%20Beyond.pdf en IT Governance, 'Getting started with the EU GDPR: Data mapping'. Geraadpleegd op 12 april 2017 van https://www.itgovernance.co.uk/blog/getting-started-with-the-eu-gdpr-data-mapping/

Naast het doorlopen van de werkprocessen op bovenstaande punten is het ook aan te raden met de verschillende afdelingen in gesprek te gaan over het omgaan met persoonsgegevens. Mogelijk worden er buiten de stappen in een bepaald werkproces wel meer persoonsgegevens verwerkt die anders buiten de inventarisatie zouden blijven.

2.4.1 Stel vast of en welke persoonsgegevens zich in de organisatie bevinden en waar ze vandaan komen

Het startpunt van de inventarisatie is te bekijken welke persoonsgegevens zich in een organisatie bevinden en waar deze persoonsgegevens vandaan komen. Vrijwel iedere organisatie verwerkt persoonsgegevens dus het zal niet snel voorkomen dat in deze fase wordt vastgesteld dat er geen persoonsgegevens worden verwerkt.

Bij het doorlopen van het werkproces kan worden aangegeven welke persoonsgegevens in dat werkproces worden verwerkt en waar deze persoonsgegevens vandaan komen (zijn deze bijvoorbeeld aangeleverd door de persoon zelf, zijn ze verkregen via een openbare bron of een derde partij etc.). Hierbij kan dan per werkproces worden aangegeven welke (categorieën) persoonsgegevens worden verwerkt, waar deze vandaan komen en of zij al dan niet onder de categorie bijzondere persoonsgegevens vallen.

- √ Stel aan de hand van de werkprocessen van de organisatie een inventarisatie op in welke werkprocessen persoonsgegevens worden verwerkt.
- √ Noteer per werkproces welke persoonsgegevens worden verwerkt (eventueel per categorie persoonsgegevens).
- √ Geef wanneer sprake is van de verwerking van bijzondere persoonsgegevens dit specifiek aan.
- √ Check wanneer sprake is van verwerking van het BSN nummer of er een wettelijke grondslag voor is (hetzij in art. 10 van de Wabb in het geval van overheidsorganisaties of in sectorale wetgeving). Is dit niet het geval dan mag het BSN nummer niet verwerkt worden.
- √ Noteer per (categorie van) persoonsgegeven(s) de bron waar de gegevens vandaan komen.
- √ Ga aan de hand van gesprekken met afdelingen na of er nog aanvullende persoonsgegevens worden verwerkt.

Voorbeeld:

Het wervingsproces van personeel binnen een organisatie ziet er als volgt uit: er wordt een vacature geplaatst, kandidaten reageren op de vacature per brief of email, de motivatiebrieven en de CV's worden opgeslagen op de netwerkschijf in het mapje werving onder personeelszaken. De manager die verantwoordelijk is voor de werving van een nieuwe kandidaat neemt samen met de officemanager die verantwoordelijk is voor personeelszaken de motivatiebrieven en de CV's door en maakt op basis van de sollicitaties een shortlist van kandidaten die worden uitgenodigd voor een sollicitatiegesprek.

De gegevens van de kandidaten die niet worden uitgenodigd worden gedurende de sollicitatieperiode bewaard omdat wanneer uit de gesprekken geen geschikte kandidaat volgt er teruggevallen kan worden op de overige kandidaten. Deze gegevens mogen maximaal vier weken na afsluiting van de sollicitatieprocedure worden bewaard, daarna moeten ze worden verwijderd. Tenzij een kandidaat toestemming heeft gegeven om gedurende een vastgestelde periode van maximaal een jaar zijn of haar gegevens in portefeuille te houden voor eventuele andere vacatures. De gegevens van de kandidaat die wordt aangenomen worden opgenomen in het personeelsdossier dat op dat moment wordt aangemaakt.

De organisatie in dit voorbeeld legt dan het volgende vast:

1. Welke persoonsgegevens worden verwerkt (in de genoemde motivatiebrieven en CV's bevinden zich persoonsgegevens– NAW gegevens, geboortedatum, geslacht, genoten opleiding, werkervaring, huwelijkse staat, wellicht een pasfoto etc) en hoe deze worden verwerkt (ontvangen, doorsturen, opslaan, selecteren (kandidaten die wel/niet worden uitgenodigd), vernietigen).

2. De bron waar de persoonsgegevens vandaan komen → in dit voorbeeld zijn de gegevens verstrekt door de betrokkene zelf of wanneer een kandidaat via een uitzendbureau wordt voorgedragen aangeleverd door een derde partij, te weten het uitzendbureau.

2.4.2 Vaststellen welke verwerkingen er plaats vinden en in welke systemen

Gedurende het werkproces kunnen verschillende verwerkingen plaatsvinden. In de Wbp werden de volgende handelingen aangegeven die de basis kunnen vormen om de verwerkingen te identificeren. Gekeken wordt dan naar het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen. Kijk hierbij gelijk in welke systemen de verwerkingen plaatsvinden en waar de gegevens worden opgeslagen (verwerking in een CRM-applicatie, verzending per email, maar ook opslag in een fysieke kast etc.). Dit overzicht van de 'locaties' waar gegevens zich bevinden vormt weer de basis om afspraken te maken over de beveiliging van deze 'locaties' en om afspraken te maken met de verwerkers van de persoonsgegevens (de zogenaamde bewerkersovereenkomsten). Ook is het goed om te weten waar zich welke gegevens bevinden op het moment dat een betrokkene een aanvraag doet tot inzage, aanvulling, wijziging of wissing van gegevens. Vergeet hierbij vooral ook niet de gegevens die zich eventueel in mailboxen, op persoonlijke schijven of andere locaties buiten de eigen beheeromgeving om bevinden (e.g. Dropbox, een USB stick, externe harde schijf etc.) en beperk dit zoveel mogelijk. Denk ook aan back-ups die gemaakt worden van de verschillende systemen.

Voorbeeld:

Terug naar het voorbeeld van de binnengekomen sollicitaties (motivatiebrieven en CV). Het is van belang te kijken welke bewerkingen er plaatsvinden en waar deze persoonsgegevens zich bevinden. In dit geval worden de sollicitaties opgeslagen in een map op de netwerkschijf, maar worden ze ook vaak nog bijgehouden in een map in de inbox van personeelszaken. De sollicitaties worden gedeeld met de persoon die verantwoordelijk is voor de werving. Dit kan door deze persoon toegang te geven tot de map op de netwerkschijf, maar het gebeurt ook wel dat sollicitaties per mail of op papier worden doorgestuurd. Het is dus van groot belang al deze verschillende kanalen/locaties inzichtelijk te hebben en deze zo veel mogelijk te beperken om dubbele opslag te voorkomen zodat het eenvoudiger wordt om gegevens op het daartoe aangewezen moment te wissen en om gegevens op de juiste manier te beveiligen.

Bewerkingen en waar deze plaatsvinden: opslaan op netwerkschijf, opslaan in mailbox, mailen naar verantwoordelijke voor de werving, opslaan in mailboxverantwoordelijke, back up van de netwerkschijf en inboxen etc.

- √ Noteer welke verwerkingen er binnen het werkproces plaatsvinden.
- √ Geef per persoonsgegeven of per categorie persoonsgegevens aan op welke locatie (fysiek, digitaal en in de cloud) de persoonsgegevens zich bevinden.
- √ Maak een rationalisatie op het gebied van locaties waar persoonsgegevens zich bevinden – zijn alle locaties waar zich persoonsgegevens bevinden noodzakelijk?

2.4.3 Stel vast voor welke doeleinden persoonsgegevens worden verwerkt (incl. dataminimalisatie)

In de communicatie naar de betrokkene dient de verwerkingsverantwoordelijke steeds aan te geven voor welk doel de persoonsgegevens worden verwerkt. Ook in het verplichte verwerkingsregister dat dient te worden bijgehouden (zie ook paragraaf 2.7) moet aangegeven worden voor welke doeleinden de persoonsgegevens worden verwerkt. Het is voor een organisatie het meest overzichtelijk als op basis van de verwerkingen in de verschillende werkprocessen verwerkingsdoeleinden worden vastgesteld die voor de communicatie naar betrokkenen kunnen worden gebruikt. Deze verwerkingsdoeleinden dienen helder en duidelijk te worden geformuleerd zodat ze voor iedereen begrijpelijk zijn. Het is aan te raden centraal in de organisatie een lijst bij te houden (bijvoorbeeld door de functionaris gegevensbeheer) en deze ook constant te actualiseren.

Uitgangspunt bij de verwerking is het principe van doelbinding: persoonsgegevens mogen alleen worden verwerkt om het vooraf vastgestelde doel te bereiken. Gegevens die niet met dit doel in verband staan, mogen niet worden verwerkt.

Een verdere verwerking, oftewel een verwerking voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, moet apart gerechtvaardigd worden. De verwerkingsverantwoordelijke dient dan een extra afweging te maken of dit andere doel wel verenigbaar is.[28] Eventueel moet hiervoor aan de betrokkene toestemming worden gevraagd (zie ook paragraaf 2.10.1).

Hierbij wordt gekeken naar:

a) het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verwerking – hoe nauwer de doelen met elkaar verwant zijn, hoe eerder zij als verenigbaar worden aangemerkt.
b) het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen betrokkenen en de verwerkingsverantwoordelijke betreft.
c) de aard van de persoonsgegevens, met name of bijzondere categorieën persoonsgegevens worden verwerkt, overeenkomstig artikel 9 en of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt.
d) de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen – hoe kleiner de gevolgen zijn hoe eerder de verwerking als verenigbaar kan worden aangemerkt.
e) het bestaan van passende waarborgen, waaronder versleuteling of pseudonimisering – op deze manier worden de risico's van oneigenlijk gebruik beperkt.

Wanneer op basis van de bovenstaande afweging de verwerking verenigbaar is met het andere doel dient de betrokkene op de hoogte te worden gebracht dat de verwerkingsverantwoordelijke voornemens is om de persoonsgegevens verder te verwerken voor een ander doel dan waarvoor de gegevens zijn verzameld.

Wanneer de doeleinden per verwerking worden vastgesteld dient tegelijkertijd gekeken te worden of de hoeveelheid persoonsgegevens die wordt verzameld in relatie staat tot het doel (de zogenaamde doelbinding) waarvoor deze persoonsgegevens verzameld zijn. Het aantal persoonsgegevens dat wordt verzameld moet zo veel mogelijk beperkt worden. Er moet dus constant de vraag worden gesteld of met minder gegevens hetzelfde doel bereikt kan worden.

- √ Houdt centraal een lijst bij met de verschillende doeleinden waarvoor persoonsgegevens binnen de organisatie worden verwerkt.
- √ Voer bij iedere verwerking een check uit of er sprake is van doelbinding.
  - √ Geen doelbinding → Maak een extra afweging of het andere doel waarvoor de gegevens worden gebruikt wel verenigbaar is.
    - √ Is na extra afweging de verwerking verenigbaar? → Breng dan de betrokkene op de hoogte vóórdat de verwerking plaatsvindt.
  - √ Geen doelbinding én niet verenigbaar met een eventueel ander doel? → Stop de verwerking direct.
- √ Beperk het aantal persoonsgegevens dat wordt verwerkt voor een bepaald doel tot het minimum dat noodzakelijk is voor het verwezenlijken van dit doel.

Voorbeeld:

Terug naar het voorbeeld dat hiervoor genoemd werd van de persoonsgegevens binnen het wervingsproces. Deze persoonsgegevens worden verwerkt met als doel 'werven van personeel'.

Wanneer de persoonsgegevens van de kandidaten voor het doel 'werven van personeel' worden vastgelegd is het niet toegestaan om deze gegevens zonder meer te gebruiken om bijvoorbeeld een mailing toe te sturen met het opleidingsaanbod van de organisatie.

28 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 49

2.4.4 Stel vast wat de grondslag van de verwerking is

De AVG stelt in artikel 6 dat de verwerking alleen rechtmatig is indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

a) Toestemming: De betrokkene heeft toestemming gegeven (bijvoorbeeld het webformulier waarop betrokkene heeft aangegeven akkoord te gaan met de bewerking van zijn of haar gegevens).
b) Overeenkomst: De verwerking is noodzakelijk voor de uitvoer van een overeenkomst waarbij de betrokkene partij is.
c) Wettelijke grondslag: Wetgeving vereist dat de persoonsgegevens van een betrokkene worden verwerkt. Bij een werkprocesinventarisatie zou per werkproces kunnen worden aangegeven op welke juridische grond de uitvoer van het werkproces berust.
d) Publiekrechtelijke taak: De gegevensverwerking is noodzakelijk op basis van een opgedragen publiekrechtelijke taak.
e) Vitaal belang: De gegevensverwerking is noodzakelijk om een ernstige bedreiging van de gezondheid van de betrokkene te beperken/voorkomen.
f) Gerechtvaardigd belang: persoonsgegevens verzamelen is belangrijker dan het privacybelang van de betrokkene. Dit punt geldt overigens niet voor overheidsinstanties. Zij kunnen zich niet beroepen op een verwerking krachtens een eigen belang. Dit moet altijd terug te voeren zijn op een publiekrechtelijke taak.

Per verwerking wordt aangegeven welke gronden mogelijk zijn – toestemming, overeenkomst, wetgeving, publiekrechtelijke taak, vitaal belang (bescherming van de betrokkene), gerechtvaardigd belang. Uitsluitend de hier genoemde grondslagen bieden een rechtvaardiging om persoonsgegevens te mogen verwerken Wanneer er geen grondslag is voor de verwerking mogen de gegevens in principe NIET worden verwerkt.

Omdat onder de AVG steeds bewijs moet worden meegeleverd is het raadzaam om het bewijs voor de grondslag van de verwerking, met name waar het gaat om toestemming en verwerking op basis van een overeenkomst, duidelijk vast te leggen en een vaste locatie te bepalen waar dit bewijs kan worden gevonden. De AVG stelt ook striktere eisen op deze punten dan de Wbp, zie ook paragraaf 2.10.1.

√ Stel per verwerking vast op basis van welke grondslag de verwerking wordt uitgevoerd.
√ Zorg dat het bewijs voor de aanwezigheid van de grondslag is vastgelegd en dat het bewijs beschikbaar i

Voorbeeld:

Een organisatie stuurt maandelijks een nieuwsbrief. Hiervoor kunnen geïnteresseerden zich aanmelden via een webformulier. Dit formulier is het bewijs van toestemming dat deze persoon zijn of haar persoons-gegevens aan de organisatie afstaat om zodoende de nieuwsbrief te ontvangen.

2.4.5 Stel vast wie de verwerkers zijn van de persoonsgegevens

In de paragraaf waarin de belangrijkste begrippen uit de AVG worden behandeld valt te lezen dat het verwerken van gegevens alle handelingen omvat die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot vernietigen. In een werkproces kunnen dus verschillende verwerkingen en verwerkers naar voren komen (bijvoorbeeld degene die de gegevens bijwerkt, aanvult of opslaat kunnen twee of meerdere personen/partijen zijn). Kijk hierbij ook specifiek naar waar informatie opgeslagen wordt. Veel organisaties maken tegenwoordig gebruik van opslag in de cloud. In dat geval is de leverancier van de cloudoplossing de verwerker waarmee een verwerkersovereenkomst moet worden opgesteld (zie ook paragraaf 2.6 over de verwerkersovereenkomst).

√ Geef in het overzicht van de werkprocessen per verwerking aan wie de verwerker is of wie de verwerkers zijn binnen de verschillende stappen in het werkproces.
√ Houdt centraal een lijst bij van de verwerkers.

2.4.6 Stel vast of er sprake is van doorgifte van persoonsgegevens en het bepalen van de ontvangers van persoonsgegevens (incl. derde landen)

Bij het volgen van het werkproces kan direct in kaart worden gebracht of er op enig moment in het proces sprake is van doorgifte van persoonsgegevens aan derden. Noteer per verwerking aan welke derde partijen de persoonsgegevens worden doorgegeven. Wanneer blijkt dat je als organisatie bijvoorbeeld onnauwkeurige persoonsgegevens bijhoudt en deze gegevens zijn gedeeld met een derde partij ben je als organisatie verantwoordelijk om de derde partij in te lichten zodat deze partij de gegevens kan corrigeren.[29] Dit is ook van belang in het kader van het recht van de betrokkene tot het wissen van zijn of haar gegevens of in het kader van het recht tot de tijdelijke beperking van een bewerking. Ook kan de betrokkene in het kader van het recht op inzage verzoeken om een kopie of raadpleging van de persoonsgegevens die zijn doorgegeven aan een derde partij. Stel hierbij tevens vast of er sprake is van doorgifte aan derde landen. Bij het vaststellen of er sprake is van doorgifte aan derde landen of internationale organisaties dient met name extra aandacht te worden besteed aan cloudoplossingen. Dikwijls staan de fysieke servers in andere landen dan waar de afnemer van de cloudoplossing gevestigd is en kan het zijn dat de data binnen de cloudoplossing buiten de EU wordt opgeslagen. In dat geval is er sprake van doorgifte aan derde landen en moet rekening gehouden worden met de specifieke eisen die hieraan gesteld worden.

De aanvullende eisen met betrekking tot doorgifte aan derde landen komen voort uit de wens van de EU om ervoor te zorgen dat het hoge beschermingsniveau dat in de EU geldt niet aan kracht verliest wanneer persoonsgegevens door worden gegeven aan derde landen. Om die reden zijn voor het doorgeven of laten verwerken van persoonsgegevens buiten de rechtsmacht van de EU specifieke regels opgesteld.

Als algemeen beginsel kan worden gesteld dat doorgifte of verwerking door entiteiten buiten de EU slechts toegestaan is wanneer er:

1. *een adequaat en met de EU vergelijkbaar beschermingsniveau van kracht is* (art. 45 lid 1).

De Commissie kan besluiten dat er sprake is van een passend niveau. Wanneer dit het geval is zijn er geen nadere waarborgen vereist voor doorgifte naar dit land. Ook kan de Commissie dit besluit weer intrekken.[30] Wanneer een derde land door de Commissie is aangewezen als een land met een adequaat beschermingsniveau dan is er geen specifieke toestemming nodig voor doorgifte naar een entiteit in dat land.

2. *passende waarborgen genomen zijn en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.*

Passende waarborgen kunnen worden geboden door de instrumenten genoemd in art. 46 lid 2. [31]

3. bindende bedrijfsregels zijn vastgesteld.

Binnen een concern of groep van ondernemingen is het mogelijk bindende bedrijfsregels vast te stellen. Dit zijn beleidsregels over doorgifte(n) van persoonsgegevens aan concernonderdelen in derde landen. Deze beleidsregels moeten voldoen aan de algemene eisen die worden genoemd en dienen ten minste de elementen te bevatten die in art. 47 worden genoemd. De bedrijfsregels moeten worden goedgekeurd door de toezichthouder.[32]

4. *uitdrukkelijke toestemming van de betrokkene of een andere grondslag zoals beschreven in artikel 49.*

In dit artikel worden acht mogelijkheden beschreven waarbij doorgifte naar derde landen wel kan worden toegestaan. De belangrijkste om hier te noemen is de uitdrukkelijke toestemming van de betrokkene waarbij de betrokkene apart dient te worden geïnformeerd over de risico's die deze doorgifte met zich mee brengt.

---

29 Commissie voor de bescherming van de persoonlijke levenssfeer, 'Algemene verordening gegevensbescherming: bereid je voor in 13 stappen', https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf -geraadpleegd op 12 april 2017.

30 Engelfried, Meij en Kager noemen op pagina 187 een lijst van landen die op het moment van het schrijven van het Handboek Algemene Verordening Gegevensbescherming te boek staan als landen waarvoor de Commissie heeft besloten dat er een passend beschermingsniveau geldt. Het gaat dan om Andorra, Argentinië, Canada (alleen voor de commerciële sector en alleen in gebieden waar de Canadian Personal Information Protection and Electronic Documents Act van toepassing is), de Faeröer Eilanden, Guernsey, Israël, het Isle of Man, Jersey, Nieuw-Zeeland, Uruguay, de Verenigde Staten (alleen indien de betrokken Amerikaanse partij bij Privacy Shield is aangesloten) en Zwitserland. Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 187.

31 Om de omvang van dit stappenplan enigszins te beperken wordt hier voor meer details over de instrumenten die gelden als passende waarborgen verwezen naar art. 46 lid 2.

32 Ook hier is om de omvang van het stappenplan te beperken de keuze gemaakt alleen een verwijzing op te nemen naar de eisen die gesteld worden aan bindende bedrijfsvoorschriften.

√ Leg per verwerking vast of er sprake is van doorgifte van persoonsgegevens aan derden en aan wie de persoonsgegevens worden doorgegeven (de zogenaamde ontvangers of categorieën van ontvangers). Kijk hier specifiek ook naar doorgifte aan derde landen.
√ Controleer indien sprake is van doorgifte aan derde landen of de gegevens mogen worden doorgegeven of welke eisen aan doorgifte worden gesteld:
  √ Valt het land onder de lijst van landen met een adequaat beschermingsniveau – zo ja dan hoeft er geen toestemming gevraagd te worden voor doorgifte.
  √ Zijn er instrumenten beschikbaar die passende waarborgen bieden?
  √ Zijn er bindende bedrijfsregels vastgesteld?
  √ Is er sprake van uitdrukkelijke toestemming of een andere grondslag als beschreven in art. 49?
√ Leg vast waar betrokkene een kopie kan verkrijgen of waar persoonsgegevens kunnen worden geraadpleegd in geval van doorgifte.

Voorbeeld:

In het voorbeeld van de sollicitaties komen deze binnen bij personeelszaken die de sollicitaties vervolgens doorzet aan de verantwoordelijke voor het wervingsproces. Wanneer in het wervingsproces de eerste selectie zou zijn uitbesteed aan een wervings- en selectiebureau zou het kunnen zijn dat er sollicitaties zowel direct binnenkomen bij het bureau als bij de eigen organisatie en dat vervolgens de sollicitaties vanuit de eigen organisatie worden doorgezonden aan het W&S bureau. Wanneer een kandidaat zich zou terugtrekken uit het sollicitatieproces is het van belang dat dit ook aan het W&S bureau wordt doorgegeven.

2.4.7 Stel vast hoe lang de persoonsgegevens bewaard worden en hoe zij moeten worden vernietigd

In veel (overheids)organisaties is een selectielijst beschikbaar waarop is aangegeven welke informatie gedurende welke periode moet worden bewaard en wanneer informatie moet worden vernietigd. Deze lijst kan helpen met het bepalen van de vernietigingstermijn voor persoonsgegevens. Wanneer een organisatie nog niet over een dergelijke lijst beschikt is het raadzaam om een centrale lijst te maken met daarin per verwerking de termijn waarop de persoonsgegevens moeten worden vernietigd. Deze lijst kan dan ook worden gebruikt om betrokkenen actief te informeren over de periode waarin hun persoonsgegevens worden verwerkt.

√ Stel per verwerking vast hoe lang de persoonsgegevens bewaard worden.
√ Informeer betrokkene over de duur van de verwerking.
√ Zorg voor een goede procedure voor het vernietigen van persoonsgegevens – houdt hierbij ook rekening met eventueel aanwezige kopieën (intern of bij derden).

Voorbeeld:

De persoonsgegevens uit het voorbeeld van de sollicitatieperiode dienen maximaal vier weken na het sluiten van de sollicitatieperiode verwijderd te worden, tenzij een kandidaat heeft aangegeven dat hij of zij voor een vooraf vastgestelde periode van maximaal een jaar in portefeuille wil worden gehouden zodat contact kan worden gezocht op het moment dat er zich een nieuwe vacature voordoet.

2.5 Stap 5 – Zorg voor passende beveiliging van de persoonsgegevens

Wanneer de inventarisatie is gemaakt kan op basis van de inventarisatie worden gekeken hoe de persoonsgegevens die worden verwerkt beveiligd zijn. Er kan ook gekozen worden om deze stap mee te nemen in de inventarisatiefase. Echter om het belang van informatiebeveiliging in dit stappenplan te benadrukken is ervoor gekozen deze stap als aparte stap uit te lichten.

Artikel 32 stelt dat *'rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. (..)*[33]

Wanneer gesproken wordt over informatiebeveiliging gaat het om het geheel van maatregelen, procedures en processen die erop zijn gericht de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen een organisatie te garanderen, met als doel de continuïteit van informatie en informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten te beperken tot een acceptabel vooraf bepaald niveau.[34] Betrouwbaarheid, als zijnde de mate waarin een organisatie voor de informatievoorziening kan rekenen op een informatiesysteem, staat hierbij centraal. De betrouwbaarheid van een systeem is de verzamelterm voor drie aspecten van beveiliging die algemeen zijn geaccepteerd te weten:

(1) beschikbaarheid – dit betreft de waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (toegang tot informatiesystemen waarbij rekening gehouden wordt met bijvoorbeeld uitvalstijden, storingen en incidenten).

(2) integriteit – dit betreft de waarborgen dat informatie actueel en correct is. Kenmerken hierbij zijn juistheid, volledigheid en geautoriseerdheid van transacties.

(3) vertrouwelijkheid – dit betreft de waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd en dat informatie niet kan uitlekken.

Met name dit laatste begrip staat centraal binnen de AVG omdat dit een grote rol speelt in privacyvraagstukken. Toch zijn de andere twee begrippen minstens zo belangrijk en worden juistheid en integriteit ook specifiek genoemd in de beginselen van de AVG.

De AVG geeft een aantal voorbeelden van hoe de beveiliging van persoonsgegevens kan worden gerealiseerd. Zo wordt gesproken over:

- Pseudonimisering: het zodanig aanpassen van persoonsgegevens dat zij niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder aanvullende gegevens.[35]
- Versleuteling: langs wiskundige weg (algoritmes) omzetten van gegevens tot een brij zodanig dat zonder de sleutel de gegevens niet hersteld kunnen worden.[36]
- Privacy by design: dit houdt in dat al bij de start van het ontwerp en gedurende de hele levenscyclus van een informatiesysteem rekening gehouden wordt met de bescherming van persoonsgegevens. Het doel hierbij is de beveiliging van persoonsgegevens te optimaliseren.[37]
- Privacy by default: dit houdt in dat de instellingen van een programma, app, website of dienst zodanig zijn dat de maximale bescherming van persoonsgegevens wordt betracht. Hierbij moet de waarschuwing worden gegeven dat het gaat om de maximale mogelijkheden binnen het systeem wat niet hoeft te betekenen dat dit ook echt de maximale bescherming is. [38]

33 Zie art. 32 AVG.
34 Deze definitie is gebaseerd op de definitie van informatiebeveiliging op Wikipedia (geraadpleegd op 12 april 2017 van https://nl.wikipedia.org/wiki/Informatiebeveiliging), de definitie die wordt gegeven in de CBP richtsnoeren voor de beveiliging van persoonsgegevens (geraadpleegd op 12 april 2017 van https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf) en de definitie die wordt gegeven op EAR online in het overzicht van de Baseline Informatiebeveiliging Rijksdienst (geraadpleegd op 12 april 2017 van http://www.earonline.nl/index.php/Overzicht_Baseline_Informatiebeveiliging_Rijksdienst_(BIR_2012)).
35 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 139
36 Idem.
37 Justitia, 'Wat is privacy by design?', http://justitia.nl/privacy/privacy-by-design.html -geraadpleegd op 12 april 2017.
38 Justitia, 'Wat is privacy by default?', http://justititia.nl/privacy/privacy-by-default.html - geraadpleegd op 10 april 2017.

Het is goed om in dit kader ook het begrip anonimisering te noemen. Bij anonimisering worden alle gegevens onomkeerbaar ontdaan van persoonlijke kenmerken, dit kan bijvoorbeeld door de identificeerbare gegevens te verwijderen of helemaal niet op te slaan of door gegevens van meerdere personen samen te voegen. Wanneer er sprake is van anonimisering zijn de gegevens niet langer herleidbaar naar een natuurlijke persoon en is er geen sprake meer van persoonsgegevens. De opslag van dit soort gegevens valt hiermee buiten de AVG.

In veel organisaties ligt de technische beveiliging van informatie bij de ICT-afdeling en in de meeste organisaties is een Chief Information Security Officer (CISO) aangesteld die specifiek is belast met informatiebeveiliging. Het is belangrijk om ervoor te zorgen dat de CISO of in ieder geval ICT nauw wordt betrokken in het implementatieproces van de AVG. Verder is het van belang om naast de technische beveiliging van computersystemen ook in kaart te brengen welke andere informatiebeveiligingsmaatregelen zijn getroffen (bijvoorbeeld wanneer personeelsdossiers zich in papieren vorm in een kast op de personeelsafdeling bevinden, zoek dan uit wie toegang heeft tot deze kast en waar de sleutel van deze kast zich bevindt).

De verwerkingsverantwoordelijke dient steeds een analyse te maken van het risico waarbij rekening wordt gehouden met de kans op mogelijke nadelige gevolgen en de impact die dit heeft op de betrokkene (denk hierbij zowel aan vernietiging en verlies van data maar ook het aanpassen van en de toegang tot gegevens). Op basis hiervan kan dan een passende maatregel worden genomen. Het is dus niet nodig om steeds de zwaarste maatregelen te nemen, maar algemeen geldt wel: hoe gevoeliger de persoonsgegevens, hoe zwaarder de beveiligingsmaatregelen moeten zijn.[39] De beweegredenen om voor een bepaalde beveiligingsmaatregel te kiezen worden toegelicht in het gegevensbeschermingsbeleid (zie paragraaf 2.8).

Bepaal als eerste welke beveiliging nu aanwezig is en waar de beveiliging (nog) niet geregeld is. Dit kan vervolgens als direct actiepunt worden opgenomen. In een vervolgstap kan worden gekeken of de beveiliging verder kan worden geoptimaliseerd.

2.5.1 Gegevensbeschermingseffectbeoordeling

Een nieuwe verplichting onder de AVG die onderdeel uitmaakt van informatiebeveiliging is het uitvoeren van een gegevensbeschermingseffectbeoordeling (of privacy impact assessment, afgekort tot PIA) voor verwerkingen die waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen opleveren. Engelfriet, Meij en Kager beschrijven de gegevensbeschermingseffectbeoordeling als 'een drietrapsraket. Bij iedere verwerking moet een eerste beoordeling gemaakt worden van de risico's die daarbij kunnen bestaan. Volgt daaruit dat er waarschijnlijk een hoog risico kleeft aan een verwerking, dan moet daarop een uitgebreide gegevensbeschermingseffectbeoordeling worden uitgevoerd. Als daar vervolgens uit blijkt dat het hoge risico niet kan worden beperkt met redelijke middelen dan moet de toezichthouder eerst worden geraadpleegd.'[40] De AVG definieert drie gevallen waarin een PIA vereist is:

- De geautomatiseerde beoordeling van personen.
- De grootschalige verwerking van bijzondere persoonsgegevens.
- Het grootschalig monitoren van openbare ruimtes.

Naast deze drie gevallen zal de Autoriteit Persoonsgegevens een lijst opstellen van het soort verwerkingen waarvoor een PIA verplicht is. Hetzelfde geldt voor een lijst van verwerkingen waarvoor een PIA niet is vereist. Deze lijsten zijn op het moment van schrijven van dit stappenplan nog niet beschikbaar.

Een goed voorbeeld van een PIA is verschenen via SURF (de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland) te vinden op: https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2015/201412--model-privacy-impact-assessment.pdf.

Checklist beveiliging algemeen

√ Stel (samen met ICT/de CISO) per verwerking vast hoe de beveiliging van de verwerking is gegarandeerd.
√ Neem direct maatregelen wanneer wordt geconstateerd dat er geen beveiliging is bij een verwerking.
√ Neem direct maatregelen wanneer wordt geconstateerd dat er onvoldoende beveiliging is wanneer het gaat om de verwerking van bijzondere persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

39 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 116.
40 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 148

√ Maak in een later stadium van de implementatie per verwerking een impactanalyse om de kans en de impact in kaart te brengen om zo de beveiligingsmaatregelen te optimaliseren.

Checklist gegevensbeschermingseffectbeoordeling

√ Stel een procedure op voor de uitvoer van een gegevensbeschermingseffectbeoordeling (PIA).
√ Beoordeel per verwerking de risico's van de verwerking.
√ Is er sprake van een hoog risico voer dan een gegevensbeschermingseffectbeoordeling (PIA) uit.
√ Is er sprake van (1) geautomatiseerde beoordeling van personen, of (2) grootschalige verwerking van bijzondere persoonsgegevens of (3) het grootschalig monitoren van openbare ruimtes? – voer dan altijd een gegevensbeschermingseffectbeoordeling uit.
√ Win bij het uitvoeren van een PIA altijd het advies van de functionaris gegevensbescherming in.
√ Komt uit de PIA dat het hoge risico niet kan worden gedekt met redelijke middelen raadpleeg dan eerst de Autoriteit Persoonsgegevens.

2.6 Stap 6 – Maak of controleer afspraken met de verwerkers

Wanneer er een overzicht is welke verwerkers er namens de verwerkingsverantwoordelijke persoonsgegevens verwerken, moet worden gekeken of met deze verwerkers ook een verwerkersovereenkomst is vastgesteld. Indien dit niet het geval is dient dit alsnog te gebeuren. Voor toekomstige verwerkingen dienen voorafgaand aan de verwerking verwerkersovereenkomsten te worden gesloten.

Naast een verwerkingsovereenkomst dient een verwerkingsverantwoordelijke ook een schriftelijke instructie op te stellen voor de verwerker over hoe de persoonsgegevens verwerkt dienen te worden. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verwerkingsverantwoordelijke.[41]

√ Stel per verwerker vast of er een verwerkersovereenkomst is en of deze voldoet aan de nieuwe vereisten onder de AVG.
√ Loop per verwerkersovereenkomst de onderstaande checklist na.
√ Stel bij iedere toekomstige verwerking een verwerkersovereenkomst aan de hand van de checklist op.
√ Zorg dat er een schriftelijke instructie is voor de verwerker inzake de gegevensverwerking.

Checklist verwerkersovereenkomst[42]

De verwerkersovereenkomst beschrijft in ieder geval het volgende ten aanzien van de verwerking:

√ Het onderwerp.
√ De duur.
√ De aard van de verwerking (gaat het om het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens? Of een combinatie van deze verwerkingen?)
√ Het doel (afkomstig uit de centraal beschikbare lijst van doeleinden).
√ De omgang met data bij beëindiging.
√ Het soort persoonsgegevens.
√ De categorieën van betrokkenen.
√ De rechten en plichten van de verwerkingsverantwoordelijke.
√ De mogelijkheid voor de verwerkingsverantwoordelijke om te kunnen controleren of de verwerker zich houdt aan de gemaakte afspraken, bijvoorbeeld door het uitvoeren van audits.

41 IBD, 'Factsheet verwerkersovereenkomsten'. Geraadpleegd op 12 april 2017 van https://www.ibdgemeenten.nl/wp-content/uploads/2017/03/20170314-factsheet-verwerkersovereenkomsten-v1.00-1.pdf.pagespeed.ce.6xf726bJFt.pdf

42 Deze checklist is samengesteld op basis van de elementen zoals genoemd in artikel 28 van de AVG en de elementen die worden genoemd in bijlage 1 – inhoud verwerkersovereenkomst die onderdeel is van de factsheet verwerkersovereenkomsten van de IBD: https://www.ibdgemeenten.nl/wp-content/uploads/2017/03/20170314-factsheet-verwerkersovereenkomsten-v1.00-1.pdf.pagespeed.ce.6xf726bJFt.pdf - geraadpleegd op 12 april 2017.

Daarnaast bevat de verwerkersovereenkomst in ieder geval dat:

- √ Persoonsgegevens uitsluitend worden verwerkt op basis van een schriftelijke instructie van de gegevensverantwoordelijke.
- √ Er wordt gewaarborgd dat de tot het verwerken van persoonsgegevens gemachtigde personen vertrouwelijkheid in acht nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.
- √ De verwerker alle passende technische en organisatorische maatregelen neemt om een op het risico afgestemd beveiligingsniveau te waarborgen.
- √ De verwerker bijstand dient te verlenen als de betrokkene een van zijn rechten uitoefent.
- √ Na afloop van de verwerking alle persoonsgegevens worden gewist en/of aan de verwerkingsverantwoordelijke worden terugbezorgt en dat bestaande kopieën worden verwijderd.

Andere onderwerpen die worden aangeraden op te nemen in de verwerkersovereenkomst:

- √ Beschrijving van de beveiligingsmaatregelen.
- √ Rapportages over de beveiliging.
- √ Hoe om te gaan en rapporteren over beveiligingsincidenten en datalekken.
- √ Doorgifte van persoonsgegevens buiten Nederland/de Europese Unie.
- √ Locatie van de data.
- √ Verstrekking van persoonsgegevens aan derden.
- √ Geheimhouding.
- √ Verzoeken van betrokkenen (waaronder recht op inzage, recht op rectificatie, recht op wissing van gegevens).
- √ Aansprakelijkheid.
- √ Bewaar, back-up en vernietigingsprocessen.

Verschillende sectoren hebben model-verwerkersovereenkomsten opgesteld die een organisatie op weg kunnen helpen bij het maken van de afspraken met de verwerkers. Een voorbeeld hiervan is de model inhoud verwerkersovereenkomst die is opgesteld door de Informatie Beveiligings Dienst (IBD) in samenwerking met KING en de Vereniging van Nederlandse Gemeenten (VNG). Deze is te vinden op https://www.ibdgemeenten.nl/wp-content/uploads/2017/03/20170314-factsheet-verwerkersovereenkomsten-v1.00-2.pdf.pagespeed.ce.smCsSEPlWq.pdf. Een ander meer specifiek voorbeeld is de Modelbewerkerovereenkomst die beschikbaar is gesteld via de PO-Raad of de VO-Raad voor onderwijsinstellingen om afspraken te maken met uitgevers. Deze is nog gebaseerd op de Wbp en is beschikbaar via https://www.poraad.nl/nieuws-en-achtergronden/onderwijs-en-uitgeverijen-maken-afspraken-over-beschermen-leerlinggegevens.

2.7 Stap 7 - Zet een register op van verwerkingsactiviteiten

Na het afronden van de inventarisatie is het van belang om grip te houden op de verwerking van persoonsgegevens binnen de organisatie. Dit kan via een register van verwerkingsactiviteiten. Verwerkingsverantwoordelijke en verwerkers zijn onder de AVG verplicht een schriftelijke (of elektronische) administratie (register) bij te houden, waarin alle activiteiten worden omschreven waarbij persoonsgegevens worden verwerkt. Deze registers worden op verzoek ter beschikking gesteld aan de Autoriteit Persoonsgegevens (bijvoorbeeld in geval van een datalek). Veel van de zaken die tijdens de inventarisatie in kaart zijn gebracht vormen de basis van dit register.

De AVG stelt dat het bijhouden van een register niet verplicht is voor organisaties onder de 250 medewerkers tenzij de verwerking(en) die zij verrichten een dusdanig risico vormt voor de rechten en plichten van de betrokkenen, de verwerking niet incidenteel is of het gaat om een verwerking van de bijzondere categorieën persoonsgegevens of gegevens inzake strafrechtelijke veroordelingen of strafbare feiten.

Checklist register verwerkingsactiviteiten verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke houdt een register van verwerkingsactiviteiten bij met daarin de volgende gegevens:

- √ Naam en contactgegevens van de verwerkingsverantwoordelijke (of indien van toepassing de gezamenlijke verwerkingsverantwoordelijke of de vertegenwoordiger van de verwerkingsverantwoordelijke) en van de functionaris gegevensbescherming.
- √ De verwerkingsdoeleinden.

√ Een beschrijving van de categorieën van betrokkenen.
√ De categorieën van persoonsgegevens.
√ De categorieën van ontvangers.
√ Indien van toepassing – doorgiften naar derde landen of internationale organisaties en de passende waarborgen die zijn getroffen.
√ Beoogde termijnen waarop gegevens worden gewist.
√ Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Checklist register verwerkingsverantwoordelijkheden verwerker
De verwerkingsverantwoordelijke houdt een register van verwerkingsactiviteiten bij met daarin de volgende gegevens:
√ Naam en contactgegevens van de verwerkers en van de verwerkingsverantwoordelijke voor rekening waarvan de verwerker handelt (en waar nodig ook van de vertegenwoordiger van de verwerkingsverantwoordelijke) en van de functionaris gegevensbescherming.
√ De categorieën van verwerkingen die voor de verwerkingsverantwoordelijke zijn uitgevoerd.
√ *Indien van toepassing* – doorgiften naar derde landen of internationale organisaties en de passende waarborgen die zijn getroffen.
√ Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

2.8 Stap 8 – Ontwerp en stel een gegevensbeschermingsbeleid vast

Als belangrijkste verantwoordelijkheid van de verwerkingsverantwoordelijke wordt in artikel 24 van de AVG vastgelegd dat *'de verwerkingsverantwoordelijke 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 plichten van natuurlijke personen, passende technische en organisatorische maatregelen dient te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Deze maatregelen dienen te worden geëvalueerd en indien nodig te worden geactualiseerd.'*

Aan de basis van de documentatieplicht van de verwerkingsverantwoordelijke ligt dus een solide beleid op het gebied van gegevensbescherming ten grondslag.[43] Het gegevensbeschermingsbeleid (of data security policy) documenteert hoe een organisatie omgaat met gegevensbescherming, zowel organisatorisch als technisch. In de uitgave 'De algemene verordening gegevensbescherming – artikelgewijs commentaar van Engelfriet, Meij en Kager' wordt verder gesteld dat 'het aan te bevelen is om algemeen beleid te maken dat naleving van de AVG op hoofdlijnen beschrijft (van de doelen waarvoor wordt verwerkt en de stappen ter beveiliging daarvan tot de wijze waarop betrokkenen hun rechten kunnen uitoefenen), gevolgd door specifieke aanvullingen op verschillende gebieden.[44] In feite komen in dit beleid dus de hoofdlijnen van dit stappenplan terug. Vaak zal het gegevensbeschermings-beleid worden vertaald naar een privacyverklaring die aan de betrokkene wordt verstrekt.[45] De functionaris gegevensbescherming moet worden betrokken bij het opstellen en uitvoeren van het beleid.

Bij heel eenvoudige verwerkingen hoeft niet perse beleid te worden vastgesteld en uitgevoerd, maar het is wel een manier om als organisatie aan te tonen dat voldaan wordt aan de AVG.[46]

De bescherming van persoonsgegevens vormt een onderdeel van het bredere informatiebeveiligingsbeleid. Het is hier dan ook noodzakelijk om ICT en de eventueel aanwezige Chief Information Security Officer in te schakelen die verantwoordelijk zijn voor de bredere informatiebeveiliging.

Bescherming van persoonsgegevens is een continue proces. Wat nu goed geregeld lijkt, kan door de voortschrijdende techniek (of kennis van hackers) over een aantal maanden al weer achterhaald zijn. Het is daarom van belang dat de organisatie het gegevensbeschermingsbeleid regelmatig evalueert/test en waar nodig aanpast. De AVG beschrijft een aantal aspecten die in dit kader moeten zijn geregeld en die moeten worden opgenomen in het beleid.

43 Zie art. 24 lid 1 AVG.
44 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 117.
45 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 117.
46 Idem, p. 117

√ Stel een gegevensbeschermingsbeleid op wat de naleving van de AVG op hoofdlijnen beschrijft en waarin de passende technische en organisatorische maatregelen worden vastgelegd.

Uitgangspunten binnen het beleid zouden moeten zijn:

- √ Streef ernaar om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen.[47]
- √ Herstel bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot gegevens tijdig.[48]
- √ Stel een procedure op om op gezette tijdstippen de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging te testen, te beoordelen en te evalueren.[49]
- √ Vertaal het gegevensbeschermingsbeleid naar een privacyverklaring voor betrokkenen.

2.9 Stap 9 – Stel een procedure op voor melding van een inbreuk in verband met persoonsgegevens

Er is sprake van een inbreuk in verband met persoonsgegevens of een zogenaamd datalek wanneer persoonsgegevens zijn (1) vernietigd of verloren, (2) gewijzigd, (3) verstrekt of (4) toegankelijk zijn gemaakt op een manier die onrechtmatig is oftewel die buiten de regels van de AVG plaatsvindt. In alle vier de gevallen komen persoonsgegevens ergens waar zij niet behoren te zijn.[50] Maar ook het verlies van gegevens door bijvoorbeeld brand en het ontbreken van een back up kan worden gekenmerkt als een datalek.

Indien er sprake is van een inbreuk of datalek dient dit binnen 72 uur nadat de verwerkingsverantwoordelijke kennis heeft genomen van de inbreuk of het datalek te worden gemeld aan de toezichthoudende autoriteit,[51] in dit stappenplan de Autoriteit Persoonsgegevens. De verwerkingsverantwoordelijke dient hiertoe een procedure op te stellen om te bepalen of er melding moet worden gedaan en hoe deze melding wordt gedaan.[52] Wanneer een melding niet binnen 72 uur na het ontdekken wordt gedaan moet de melding bij de Autoriteit Persoonsgegevens vergezeld gaan met een motivering voor vertraging.[53] Wanneer het niet mogelijk is om bij melding alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt.[54]

Er hoeft geen melding te worden gedaan als het niet waarschijnlijk is dat de inbreuk of het datalek redelijkerwijs een risico heeft gevormd voor de betrokkenen. Deze datalekken moeten wel worden gedocumenteerd.

Stel een procedure op om een inbreuk in verband met persoonsgegevens te melden bij de Autoriteit persoonsgegevens. Hierin moeten de volgende elementen worden opgenomen:

- √ Wanneer een datalek redelijkerwijs een risico heeft gevormd voor de betrokkenen dient binnen 72 uur na het ontdekken ervan een melding te worden gedaan bij de Autoriteit Persoonsgegevens. Bij een melding dienen de volgende gegevens verstrekt te worden:
  - √ Aard van de inbreuk, waar mogelijk onder vermelding van de categorieën betrokkenen en het verwerkingsregisters, en bij benadering het aantal betrokkenen.
  - √ De maatregelen die genomen zijn, die men neemt of die men zal nemen
  - √ De naam en contactgegevens van de functionaris gegevensbescherming of ander contactpunt waar meer informatie kan worden verkregen.
  - √ De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens.
  - √ Wanneer de melding na 72 uur wordt gedaan wordt een motivering voor vertraging toegevoegd.
- √ De melding dient te worden gedaan door de Functionaris Gegevensbescherming (als een organisatie die heeft).
- √ Wanneer er sprake is van een datalek met een hoog risico moeten betrokkenen worden geïnformeerd.
- √ Wanneer een melding niet hoeft te worden gemeld bij de Autoriteit persoonsgegevens dient deze wel opgenomen te worden in een overzicht van datalekken.
- √ Maak afspraken met de verwerker dat deze zonder redelijke vertraging de organisatie in kennis stelt van een datalek.

47 Zie art. 32 lid 1a AVG.
48 Zie art. 32 lid 1b AVG.
49 Zie art. 32 lid 1c AVG.
50 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 142.
51 Zie art. 33 AVG.
52 Zie art. 33 lid 3 a t/m d AVG
53 Zie art. 33 AVG.
54 Zie art. 33 lid 4 AVG.

2.10 Stap 10 – Stel procedures op richting de betrokkenen

De verwerkingsverantwoordelijke heeft onder de AVG verschillende informatieverplichtingen richting de betrokkene. Ook heeft de betrokkene onder de AVG diverse rechten waar hij of zij een beroep op kan doen. Hier moet een organisatie zich op voorbereiden door vast te stellen welke informatie op welk moment beschikbaar moet zijn om aan de betrokkene te verstrekken. Veel informatie die beschikbaar moet worden gesteld is al beschikbaar uit de inventarisatie en kan op die manier worden gebruikt (bijvoorbeeld de categorieën van persoonsgegevens die worden verwerkt, de doeleinden voor verwerking, de grondslagen van de verwerking, de bewaartermijn van de gegevens, de categorieën van ontvangers van de persoonsgegevens (doorgifte aan derden), hoe de organisatie de persoonsgegevens heeft verkregen (de bron).

Iedere communicatie naar de betrokkene moet in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in eenvoudige taal plaatsvinden (helemaal wanneer de informatie voor een kind bestemd is).
Verder is het raadzaam om in iedere communicatieuiting de betrokkene te wijzen op zijn of haar rechten.
Het gaat hierbij specifiek om:

- Recht op inzage
- Recht op rectificatie
- Recht op beperking van de verwerking
- Recht op wissing van de gegevens
- Recht op intrekken van toestemming
- Recht op bezwaar

√ Alle communicatie van de gegevensverantwoordelijke aan de betrokkene voldoet aan de daaraan gestelde eisen:
- √ Beknopt, transparant en begrijpelijke communicatie.
- √ In een duidelijke en eenvoudige taal (met name bij kinderen).
- √ De communicatie vind plaats in een gemakkelijk toegankelijke vorm – elektronisch of schriftelijk. Wanneer betrokkene elektronisch communiceert dient de verwerkingsverantwoordelijke ook elektronisch te antwoorden tenzij betrokkene anders verzoekt.
- √ In iedere communicatie moeten de rechten van de betrokkene worden opgenomen – het gaat daarbij specifiek om het recht op inzage, het recht op rectificatie, het recht op de beperking van de verwerking, het recht op het intrekken van toestemming en het recht op het indienen van een klacht. Stel hier standaardteksten voor op.

2.10.1 Procedure voor het verkrijgen van toestemming

Een betrokkene moet toestemming geven voor de verwerking van zijn of haar persoonsgegevens. Een toestemmingsverklaring moet aan vastgestelde eisen voldoen.[55] De organisatie dient een procedure in te richten om deze toestemming te krijgen en vervolgens vast te leggen als bewijs dat toestemming is verleend.

√ De organisatie heeft een procedure voor het vragen van toestemming, hierbij zijn de voorwaarden waaraan het verzoek moet voldoen in acht genomen.
- √ Toestemming is aantoonbaar.
- √ Het is voor betrokkene helder voor welke verwerking hij of zij toestemming heeft gegeven.
- √ Het verzoek om toestemming en de uitleg zijn geformuleerd in duidelijke heldere taal.
- √ Er is duidelijk aangegeven dat betrokkene het recht heeft zijn of haar toestemming in te trekken.
- √ Het moet heel eenvoudig zijn om toestemming in te trekken.
- √ Bij verwerking van persoonsgegevens van een kind heeft de persoon die de ouderlijke verantwoordelijkheid draagt toestemming gegeven en dit is gecontroleerd door de beschikbare technologie.

2.10.2 Procedure voor het afhandelen van verzoeken om informatie

De betrokkene kan een verzoek om informatie indienen bij de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke dient op dit verzoek te reageren, ook wanneer er geen gevolg zal worden gegeven aan het verzoek. De reactie is aan termijnen gebonden (zie hieronder) die in interne procedures dienen te worden opgenomen.

55 Zie art. 7 AVG.

In principe zijn aan de verzoeken, de communicatie hierover en de te treffen maatregelen geen kosten verbonden voor de betrokkene, tenzij de verwerkingsverantwoordelijke kan aantonen dat het verzoek ongegrond is of buitensporig. In die gevallen kunnen administratiekosten in rekening worden gebracht of kan de verwerkingsverantwoordelijke besluiten geen gevolg te geven aan dit verzoek. De verwerkingsverantwoordelijke mag aanvullende informatie opvragen bij de betrokkene om zodoende de identiteit van de betrokkene te kunnen vaststellen.[56]

De organisatie heeft een procedure ingericht voor het behandelen van verzoeken waarin ten minste is opgenomen:

- √ Reactietermijn – binnen een maand na ontvangst van het verzoek moet informatie worden verschaft over het gevolg dat aan het verzoek is gegeven.
- √ De reactietermijn kan met nog eens twee maanden worden verlengd – dit moet wel binnen de reactietermijn van een maand worden gecommuniceerd naar betrokkene.
- √ Verzoek elektronisch = reactie elektronisch tenzij betrokkene anders verzoekt.
- √ Indien nodig kan aanvullende informatie worden opgevraagd om de identiteit van de betrokkene die het verzoek indient vast te stellen.
- √ Informatieverzoeken zijn kosteloos voor de betrokkene tenzij de verwerkingsverantwoordelijke kan aantonen dat:
  - √ het verzoek ongegrond is
  - √ het verzoek buitensporig is

  In die twee gevallen kunnen óf administratiekosten in rekening worden gebracht of besloten worden geen gevolg te geven aan het verzoek.
  - √ Geen gevolg aan het verzoek?
  - √ Informeer betrokkene hier binnen één maand na ontvangst van het verzoek
  - √ Geef hierbij de mogelijkheid een klacht in te dienen bij de Autoriteit Persoonsgegevens en een beroep bij de rechter in te stellen.

2.10.3 Recht op inzage van de betrokkene

Er dient een procedure te worden ingericht om een betrokkene inzicht te geven in zijn of haar persoonsgegevens. Wanneer een organisatie in potentie veel verzoeken kan krijgen tot inzage kan dit recht een aanzienlijke impact hebben. Op termijn kan het zelfs kostenbesparend zijn om het systeem of de systemen zo te ontwikkelen dat de betrokkene in staat is om de gegevens zelf online te raadplegen.[57]

De organisatie heeft de volgende informatie direct beschikbaar om aan verschillende informatieverplichtingen te voldoen:

- √ Identiteit en contactgegevens van de verwerkingsverantwoordelijke en in voorkomende gevallen de vertegenwoordiger van de verwerkingsverantwoordelijke.
- √ Contactgegevens van de functionaris voor gegevensbescherming.
- √ Verwerkingsdoeleinden waarvoor persoonsgegevens zijn bestemd en de rechtsgrond voor de verwerking- wanneer het gaat om een gerechtvaardigd belang dient dit specifiek te worden toegelicht.
- √ De betrokken (categorieën van) persoonsgegevens.
- √ *Indien van toepassing* - De ontvangers of categorieën van ontvangers.
- √ *Indien van toepassing* - Waar een kopie kan worden verkregen of waar persoonsgegevens kunnen worden geraadpleegd ingeval van doorgifte.
- √ De periode gedurende welke de persoonsgegevens zullen worden opgeslagen of indien dat niet mogelijk is de criteria ter bepaling van die termijn.
- √ De bron waar persoonsgegevens vandaan komen en in voorkomend geval of zij afkomstig zijn van openbare bronnen.
- √ Informatie over de onderliggende logica alsmede het belang en de verwachte gevolgen van de verwerking voor de betrokkene.
- √ *Indien van toepassing* – bij doorgifte aan derde landen de organisatie waaraan gegevens worden doorgegeven en de passende waarborgen.

56 Zie art 12 lid 3 t/m lid 7 van de AVG.

57 Commissie voor de bescherming van de persoonlijke levenssfeer, 'Algemene verordening gegevensbescherming: bereid je voor in 13 stappen', https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf – geraadpleegd op 12 april 2017

2.10.4 Procedure voor het recht op rectificatie

Er dient een procedure te worden opgesteld voor het recht op rectificatie. De AVG stelt in artikel 16 dat de betrokkene het recht heeft op onverwijlde rectificatie betreffende onjuiste gegevens. Dit houdt in dat wanneer de persoonsgegevens onjuist of onvolledig zijn, de betrokkene het recht heeft deze te corrigeren of aan te vullen.[58] Zorg dus dat dit mogelijk is en dat kan worden aangetoond dat 'onverwijld' aan dit verzoek is voldaan. Wanneer de correctie of aanvulling niet evident is kan het langer dan "onverwijld" duren voordat de correctie of aanvulling wordt doorgevoerd omdat eerst onderzoek moet worden gedaan. Gedurende de tijd van het onderzoek kan de betrokkene verzoeken dat de verwerking gedurende die tijd wordt beperkt (zie ook recht op beperking van de verwerking).[59]

- √ Zorg voor een procedure om onverwijld de correctie of aanvulling van persoonsgegevens door te kunnen voeren.
- √ Zorg er ook voor dat als er sprake is van doorgifte aan derden, deze ontvangers ook op de hoogte worden gesteld van de correctie of aanvulling.
- √ Informeer de betrokkene dat de correctie of aanvulling van zijn of haar persoonsgegevens heeft plaats gevonden.

2.10.5 Procedure voor het recht op gegevenswissing – 'recht op vergetelheid'

Artikel 18 van de AVG legt vijf gevallen vast waarin de betrokkene het recht heeft op wissing van zijn of haar persoonsgegevens zonder onredelijke vertraging. Het gaat hierbij om:

- Persoonsgegevens die niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld.
- Gevallen waarin betrokkene zijn of haar toestemming intrekt en er geen andere rechtsgrond voor verwerking is.
- Persoonsgegevens die onrechtmatig zijn verwerkt.
- Persoonsgegevens die gewist moeten worden om te voldoen aan een Unie- of lidstatelijk recht.
- Persoonsgegevens die verzameld zijn in verband met een aanbod van diensten aan een kind.

De verwerkingsverantwoordelijke is verplicht om afspraken te maken met verwerkers over hoe de gegevenswissing technisch wordt gerealiseerd (de zogenaamde kennisgevingsplicht uit artikel 19 van de AVG). Het gaat hierbij om alle gegevens alsmede iedere koppeling naar deze persoonsgegevens en iedere reproductie (denk bijvoorbeeld aan back-ups) van deze gegevens. Er wordt aangeraden om het verzoek tot wissing via een technisch protocol door te geven aan derden die de persoonsgegevens hebben ontvangen. Ook hier is het dus weer van belang terug te kunnen vallen op een goede inventarisatie en een goed bijgehouden register van verwerkingsactiviteiten waarin wordt bijgehouden welke persoonsgegevens, waar worden bijgehouden en aan wie deze persoonsgegevens eventueel zijn doorgegeven.

In de AVG zijn wel vijf uitzonderingsgevallen vastgelegd aangaande het recht op gegevenswissing. Indien verwerking nodig is:[60]

- voor het uitoefenen van het recht op de vrijheid van meningsuiting en informatie (dit kan op gespannen voet staan met het recht op privacy).
- voor het nakomen van een wettelijke verwerkingsverplichting voor het vervullen van een taak van algemeen belang.
- op basis van redenen van algemeen belang op het gebied van de volksgezondheid.
- met het oog op archivering in het algemeen belang.
- voor instelling, uitoefening of onderbouwing van rechtsvordering.

- √ Zorg dat alle gegevens (dus ook koppelingen naar de gegevens en reproducties van de gegevens) definitief worden verwijderd, zowel intern als bij externe verwerkers.
- √ Zorg dat in de bewerkersovereenkomst ook duidelijke afspraken worden gemaakt omtrent de praktische realisatie van het recht op gegevenswissing.
- √ Informeer de betrokkene dat de persoonsgegevens zijn gewist.

58 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 89
59 Idem, p.90
60 Zie art. 17 lid 3 AVG.

2.10.6 Procedure voor het recht op beperking van de verwerking

Artikel 18.1 legt het recht op de beperking van de verwerking van persoonsgegevens vast. Betrokkene heeft dit recht indien:

- De juistheid van gegevens wordt betwist – in dit geval geldt de beperking gedurende de periode die de gegevensverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren.
- De verwerking onrechtmatig is en de betrokkene verzoekt om beperking in plaats van wissing.
- De verwerkingsverantwoordelijke de gegevens niet meer nodig heeft maar betrokkene ze nodig heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
- De betrokkene bezwaar gemaakt heeft tegen verwerking en in afwachting is van het antwoord.

Wanneer de betrokkene inderdaad recht heeft op beperking van de verwerking mag de gegevensverantwoordelijke de gegevens slechts verwerken met toestemming van de betrokkene tenzij:[61]

- er sprake is van een instelling, uitoefening of onderbouwing van een rechtsvordering.
- dit is ter bescherming van de rechten van een natuurlijke persoon of rechtspersoon.
- er gewichtige redenen zijn van algemeen belang voor de Unie of de lidstaat.

Wanneer na verloop van tijd de beperking van de verwerking wordt opgeheven (bijvoorbeeld na afronden van een onderzoek naar onjuiste gegevens) stelt de verwerkingsverantwoordelijke de betrokkene op de hoogte vóórdat beperking van de verwerking daadwerkelijk wordt opgeheven. [62]

√ Zorg dat er een procedure is vastgesteld die tijdelijk de verwerking van persoonsgegevens stop kan zetten.
√ Zorg dat in de bewerkersovereenkomst duidelijke afspraken worden gemaakt omtrent de praktische realisatie van het recht op beperking van de verwerking.
√ Informeer de betrokkene dat de verwerking van zijn of haar persoonsgegevens tijdelijk is stilgelegd.
√ Informeer de betrokkene voorafgaand aan het opheffen van de beperking van de verwerking.

2.10.7 Procedure voor het recht op overdraagbaarheid van gegevens (dataportabiliteit)

Een nieuw recht voor de betrokkene in de AVG is het recht op overdraagbaarheid van gegevens oftewel dataportabiliteit. Dit is een verbeterde vorm van toegang waarbij de betrokkene het recht heeft de persoonsgegevens die op hem van toepassing zijn in een gestructureerde, gangbare en elektronische vorm te verkrijgen en deze aan een andere verwerkingsverantwoordelijke over te dragen.[63] Net als bij verzoeken op basis van het recht op inzage kan het ook voor het faciliteren van dataportabiliteit handig zijn om op termijn een systeem te ontwikkelen wat de betrokkene in staat stelt de gegevens zelf in te zien en te downloaden.[64]

√ Zorg ervoor dat het technisch mogelijk is om de persoonsgegevens van een betrokkene in een gestructureerde, gangbare en elektronische vorm aan de betrokkene beschikbaar te stellen.
√ Zorg ervoor dat er een procedure is om dit recht op overdraagbaarheid uit te voeren ook naar een andere verwerkingsverantwoordelijke.

2.10.8 Procedure voor het indienen van een bezwaar en het uitvoeren van het bezwaar

De betrokkene heeft op basis van artikel 21 het recht van bezwaar tegen de verwerking van zijn of haar betreffende persoonsgegevens. Wanneer een betrokkene bezwaar indient dient de verwerkingsverantwoordelijke direct de verwerking van persoonsgegevens van deze betrokkene te staken (tenzij er dwingende rechtmatige gronden zijn voor verwerking zoals in verband met de instelling, uitoefening of onderbouwing van een rechtsvordering).

Het recht op bezwaar moet actief worden gedeeld met de betrokkene vanaf het eerste contact met de betrokkene.[65]

61 Zie art. 18 lid 2 AVG.
62 Zie art. 18 lid 3 AVG.
63 Commissie voor de bescherming van de persoonlijke levenssfeer, 'Algemene verordening gegevensbescherming: bereid je voor in 13 stappen', https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf – geraadpleegd op 12 april 2017.
64 Autoriteit Persoonsgegevens, 'Hoe kan ik mijn organisatie voorbereiden op dataportabiliteit?', https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/recht-op-dataportabiliteit - geraadpleegd op 12 april 2017.
65 Zie art. 21 lid 4 AVG.

√ Zorg dat er een procedure is vastgesteld voor het indienen van bezwaar met daarin tevens de stappen die in het bezwaarproces worden doorlopen.
√ Wijs betrokkene vanaf het eerste contact actief op het recht van bezwaar.
√ Indien een betrokkene bezwaar indient tegen de verwerking wordt de verwerking onmiddellijk gestaakt.
√ Informeer de verwerkers van het stopzetten van de verwerking in geval van bezwaar tegen de verwerking.

2.10.9 Recht van betrokkene om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering

Steeds meer besluitvorming vindt vandaag de dag geautomatiseerd plaats (zonder tussenkomst van personen), waarbij de uitkomst van deze computeranalyse ook steeds zwaarwegender is in die besluitvorming. In deze analyses worden vaak ook persoonsgegevens betrokken. Dit individualiseert de besluitvorming met mogelijk negatieve effecten voor de betrokkene.[66] Artikel 22 stelt dat een betrokkene het recht heeft niet aan deze geautomatiseerde individuele besluitvorming, waaronder profiling te worden onderworpen. Op dit recht zijn echter drie uitzonderingen:

- De verwerking is noodzakelijk voor de totstandkoming of uitvoering van een overeenkomst.
- De verwerking op deze wijze is Unierechtelijk of lidstaatrechtelijk toegestaan.
- De verwerking heeft de uitdrukkelijke toestemming van de betrokkene.

Om dit recht te faciliteren dient de verwerkingsverantwoordelijke passende maatregelen ter bescherming van de betrokkene te treffen waaronder ten minste het recht op menselijke tussenkomst[67] en het recht van betrokkene om zijn of haar standpunt kenbaar te maken en het besluit dat is gebaseerd op uitsluitend geautomatiseerde verwerking aan te vechten.

√ Voorkom zo veel mogelijk uitsluitend op geautomatiseerde verwerking gebaseerde besluitvorming, voeg hier altijd een menselijke schakel in.
√ Zorg dat betrokkene op de hoogte is hoe hij of zij bezwaar kan maken tegen op geautomatiseerde verwerking gebaseerde besluitvorming en stel hem of haar in staat de verwerking aan te vechten.

2.10.10 Procedure voor melding inbreuk aan betrokkene

Wanneer zich een inbreuk in verband met persoonsgegevens of een zogenaamd datalek zich voordoet moet door de verwerkingsverantwoordelijke worden ingeschat of deze inbreuk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. Wanneer dit het geval is wordt de betrokkene hierover zo snel als mogelijk in een duidelijke en eenvoudige taal ingelicht.[68]

Er is geen melding richting de betrokkene vereist in geval van een inbreuk in verband met persoonsgegevens wanneer:[69]

- De gegevens versleuteld waren.
- Wanneer achteraf maatregelen zijn genomen om de gevolgen van het hoge risico voor de rechten en plichten van de betrokkene te voorkomen.
- Het inlichten van de betrokkene over de inbreuk onevenredige inspanningen zou vergen. In dit geval wordt volstaan met een openbare mededeling.

De Autoriteit Persoonsgegevens heeft tevens de bevoegdheid om indien de verwerkingsverantwoordelijke de inbreuk niet heeft ingeschat als hoog risico en de betrokkene hierover niet heeft geïnformeerd, dit alsnog te eisen.

---

66 Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 105
67 Engelfried, Meij en Kager gaan in hun toelichting meer expliciet in op menselijke tussenkomst en geven hierbij aan dat 'dit niet betekent dat het besluit niet automatisch genomen mag worden, of dat een conceptbesluit altijd eerst gezien moet worden door een mens, maar wel dat betrokkene een mens aan de mouw moet kunnen trekken om te reageren op het besluit'. Engelfried, A, Meij, L. & Kager, P., (2017) Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017), Amsterdam: ICT en Recht, p. 107-108
68 Zie art. 34 lid 1 AVG.
69 Zie art. 34 lid 3 AVG.

√ Is er sprake van een datalek met een hoog risico voor de rechten en vrijheden van de betrokkene, licht de betrokkene dan zo snel mogelijk in.

√ Een melding van inbreuk aan de betrokkene bevat in ieder geval:

- √ De aard van de inbreuk.
- √ De naam en contactgegevens van de functionaris gegevensbescherming of ander contactpunt waar meer informatie kan worden verkregen.
- √ De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens.

Conclusies

3.

Met dit stappenplan worden mogelijke stappen doorlopen om te komen tot een implementatie van de Algemene Verordening Gegevensbescherming. Het moge duidelijk zijn dat implementatie niet over een nacht ijs gaat en dat het werk niet klaar is op het moment dat de AVG is geïmplementeerd.

De basis: Documenteren, documenteren, documenteren

De implementatie en in een later stadium de compliance met de Algemene Verordening Gegevensbescherming gaat samen met het voortdurend documenteren van allerhande informatie die betrekking heeft op de verwerking van persoonsgegevens in opdracht van de verwerkingsverantwoordelijke. Na het lezen van dit stappenplan lijkt het een enorme lijst aan informatie die moet worden bijgehouden, maar wie nauwkeurig leest zal zien dat veel informatie op verschillende momenten in een andere context wordt gedeeld. Wanneer dus aan de basis de juiste informatie over de verwerkingen wordt gedocumenteerd en dit in de toekomst consequent wordt bijgehouden kan daaruit relatief eenvoudig informatie worden hergebruikt.

Relatie tot de betrokkenen

Met de uitbreiding van de rechten van de betrokkene zal de relatie van de betrokkene binnen het gegevensbeschermingsbeleid een centrale rol in nemen. Het is aan te raden te inventariseren of het mogelijk is om zo veel mogelijk autonomie aan de betrokkene te geven waarbij via een webportal ten alle tijden de eigen persoonsgegevens kunnen worden ingezien, gewijzigd, aangevuld, beperkt, gecontroleerd en geëxporteerd (om door te geven aan een andere partij). Ook kan via de webportal worden geregeld dat de betrokkene de gegeven toestemming op eenvoudige wijze weer intrekt en dat bijvoorbeeld met een eenvoudig formulier een bezwaar kan worden ingediend tegen een verwerking. Wanneer dit wordt ingericht moet de identificatie wel zorgvuldig geregeld worden. Ook moet duidelijk zijn dat niet ieder verzoek tot correctie of verwijdering kan of hoeft gehonoreerd te worden.

Echter vaak gaat achter een verwerking van persoonsgegevens een brij aan systemen schuil. Denk aan emails, excellijsten, databases, documenten op netwerkschijven, gegevens in back-ups, dus eenvoudig zal het zeker niet zijn om dit inzichtelijk te maken en te ontsluiten richting betrokkene. Er ligt dus nog een grote uitdaging op rationalisatie van systemen bij de verwerkingsverantwoordelijken. Besteedt hier aandacht aan in je beleid en de uitvoering daarvan.

Bewustwording in de organisatie staat centraal

Je kunt nog zo een goed gegevensbeschermingsbeleid op papier hebben met alle checks en bewijsstukken, als er in de organisatie niet voldoende bewustwording is ten aanzien van het omgaan met persoonsgegevens is het dweilen met de kraan open en zullen zich steeds opnieuw datalekken voordoen door menselijke fouten. Het blijft dus zaak om medewerkers in de organisatie van zowel de verwerkingsverantwoordelijke als de verwerker te blijven trainen in het omgaan met persoonsgegevens. Blijf hier dus consequent aandacht aan besteden.

Bescherming van persoonsgegevens is een continue proces

Het is van belang om binnen je gegevensbeschermingsbeleid een duidelijke kwaliteitscirkel in te bouwen (zoals de bekende Deming Circle) waarbij je voortdurend de stappen plan – do –check – act uitvoert. Beleid ontwikkelen, beleid uitvoeren, beleid evalueren en beleid aanpassen. De wereld blijft in beweging en zeker ontwikkelingen op het gebied van techniek gaan razendsnel. Een beveiliging die vandaag voldoende is kan volgende week al weer achterhaald zijn en een ernstig risico vormen voor je bedrijfsvoering. Blijf dus constant je beleid aanpassen en voer regelmatig risicoanalyses uit waarbij je kijkt naar de kans dat een gebeurtenis zich voordoet en de impact die het heeft om zo je prioriteiten te bepalen en beveiliging aan te scherpen waar nodig.

De functionaris gegevensbescherming ambassadeur van gegevensbescherming

Benoem een functionaris gegevensbescherming met voldoende autoriteit en draagvlak binnen de organisatie die een actieve houding heeft en die als ambassadeur kan optreden in de organisatie. Dit zal het bewustzijn van medewerkers stimuleren en de weg naar de FG in geval zich een probleem voordoet vereenvoudigen.

Non-compliance kan leiden tot serieuze financiële risico's

Het niet voldoen aan de voorschriften uit de AVG kan leiden tot serieuze financiële risico's. In het stappenplan wordt niet ingegaan op de hoogtes van de administratieve geldboetes maar deze kunnen substantieel zijn. In de AVG zijn twee categorieën van geldboetes gedefinieerd[70]:

a. Een boete van € 10.000.000 of tot 2% van de wereldwijde jaaromzet voor een overtreding van administratieve bepalingen; en
b. Een boete van € 20.000.000 of tot 4% van de wereldwijde omzet voor meer fundamentele overtredingen of het niet opvolgen van bevelen van de toezichthoudende autoriteit.

70 Zie art. 83 lid 4 en 83 lid 5 AVG.

Om deze boetes te voorkomen is implementatie en het continue in overeenstemming blijven met de verplichtingen van de AVG essentieel.

De tijd dringt..
Bij het verschijnen van dit stappenplan, in mei 2017 is krap een jaar de tijd om de nieuwe eisen van de AVG te implementeren. Hoogste tijd dus om aan de slag te gaan!

Nawoord

De implementatie van de Algemene Verordening Gegevensbescherming is een behoorlijke uitdaging voor alle organisaties die eraan moeten voldoen. Met deze Roadmap voor de implementatie van de AVG bieden we inzicht in de stappen die hiervoor genomen moeten worden. Wij hebben dit stappenplan gratis beschikbaar gesteld om organisaties op weg te helpen. Graag horen wij van u hoe er binnen uw organisatie wordt gewerkt aan de implementatie van de AVG en wanneer deze van kracht is ook hoe u de verwerking van persoonsgegevens binnen uw organisatie in lijn houdt met de AVG. Ook horen we graag ervaringen van organisaties die dit stappenplan in de praktijk brengen.

Wanneer u vragen heeft over dit stappenplan, de implementatie in uw organisatie of wanneer u tips voor de implementatie heeft of goede aanvullingen op dit stappenplan dan horen wij dit graag via info@vhic.nl. Via onze gratis digitale adviseur Zaalberg zullen we binnengekomen vragen beantwoorden en op onze site en in onze nieuwsbrief Sited (geanonimiseerd) publiceren.

Wij wensen u veel succes met de implementatie!

Met vriendelijke groet,

Tineke van Heijst
Directeur VHIC

Literatuurlijst

Algemene Verordening Gegevensbescherming. Geraadpleegd op 12 april 2017 van Autoriteit Persoonsgegevens, *'Richtlijnen voor functionarissen voor de gegevensbescherming'*. Geraadpleegd op 12 april 2017 van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_fg.pdf

Autoriteit Persoonsgegevens, *'Richtlijnen voor het recht op dataportabiliteit'*. Geraadpleegd op 12 april 2017 van https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtlijnen_dataportabiliteit.pdf

Baker and McKenzie, *'Datamapping under the GDPR and beyond'*. Geraadpleegd op 12 april 2017 van http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Data%20Mapping%20under%20the%20GDPR%20and%20Beyond.pdf

Clements, Tim, *'GDPR data flow mapping – an approach'*. Geraadpleegd op 12 april 2017 van https://www.linkedin.com/pulse/gdpr-data-flow-mapping-approach-tim

Commissie voor de bescherming van de persoonlijke levenssfeer, *'Algemene Verordening Gegevensbescherming – Bereid je voor in 13 stappen'*. Geraadpleegd op 12 april 2017 van https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20NL%20-%20V2.pdf

Concept Uitvoeringswet Algemene Verordening Gegevensbescherming. Geraadpleegd op 13 april 2017 van https://www.internetconsultatie.nl/uitvoeringswetavg

Engelfried, A, Meij, L. & Kager, P., (2017) *Handboek Algemene Verordening Gegevensbescherming – artikelsgewijs commentaar (editie 2017)*, Amsterdam: ICT en Recht.

Informatie Beveiligings Dienst, *'Factsheet Verwerkersovereenkomsten'*. Geraadpleegd op 12 april 2017 van https://www.ibdgemeenten.nl/wp-content/uploads/2017/03/20170314-factsheet-verwerkersovereenkomsten-v1.00-1.pdf.pagespeed.ce.6xf726bJFt.pdf

IT Governance, *'Getting started with the EU GDPR: Data mapping'*. Geraadpleegd op 12 april 2017 van https://www.itgovernance.co.uk/blog/getting-started-with-the-eu-gdpr-data-mapping/

Justitia, *'Wat is privacy by Default?'*. Geraadpleegd op 12 april 2017 van http://www.justitia.nl/privacy/privacy-by-default.html

Justitia, *'Wat is privacy by Design?'*. Geraadpleegd op 12 april 2017 van http://www.justitia.nl/privacy/privacy-by-design.html

Kennisnet, *'Privacy in tien stappen – een praktische handleiding voor privacy op school'*. Geraadpleegd op 12 april 2017 van https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Privacy_in_10_stappen.pdf

Kennisnet, *'Deze zeven dingen moet je weten over de nieuwe Europese Privacywet'*. Geraadpleegd op 12 april 2017 van https://www.kennisnet.nl/artikel/deze-7-dingen-moet-je-weten-over-de-nieuwe-europese-privacywet/

Louwers advocaten, *'Stappenplan Algemene Verordening Gegevensbescherming'*. Geraadpleegd op 12 april 2017 van http://privacy-recht.louwersadvocaten.nl/stappenplan-avg/

Ross, Adrian, *'Data Flow Mapping and the EU GDPR'*. Presentatie gehouden op 29 september 2016. Geraadpleegd op 12 april 2017 van https://www.itgovernance.co.uk/download/Data-Flow-Mapping-and-the-EU-GDPR-September-2016.pdf

SURF, *'Privacy impact assessment (PIA)'*. Geraadpleegd op 12 april 2017 van https://www.surf.nl/themas/beveiliging/beleidsondersteuning-privacy/implementatie-algemene-verordening-gegevensbescherming-avg/privacy-impact-assessment-pia/index.html

SURF, *'Model Privacy Impact Assessment – toelichting en invulinstructie bij gebruik van het PIA risico formulier'*. Geraadpleegd op 12 april 2017 van https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2015/201412---model-privacy-impact-assessment.pdf

Zwenne, prof. Mr. G. en Mommers L., *'De tien belangrijkste veranderingen die de Algemene Verordening Gegevensbescherming gaat brengen'*, Tijdschrift voor Compliance, augustus 2016, p. 182 – 189. Geraadpleegd op 12 april 2017 van https://zwenneblog.weblog.leidenuniv.nl/files/2016/09/2016.08.02_AVGB_TijdschriftCompliance.pdf

Bijlagen

Lijst van definities

Anonimisering	Alle gegevens worden onomkeerbaar ontdaan van persoonlijke kenmerken, dit kan bijvoorbeeld door de identificeerbare gegevens te verwijderen of helemaal niet op te slaan of door gegevens van meerdere personen samen te voegen.
Beperken van de verwerking	Het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken.
Beschikbaarheid (in het kader van informatiebeveiliging)	De waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen (toegang tot informatiesystemen waarbij rekening gehouden wordt met bijvoorbeeld uitvaltijden, storingen en incidenten).
Bestand	Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.
Betrokkene	De identificeerbare of geïdentificeerde natuurlijke persoon op wie de persoonsgegevens betrekking hebben.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken en de verwerking van genetische, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksuele gedrag of seksuele gerichtheid.
Bindende bedrijfsvoorschriften	Beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen.
Biometrische gegevens	Persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.
Concern	Een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de persoon die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.
Derde land	Alle landen buiten de Europese Economische Ruimte (de EU plus Liechtenstein, Noorwegen, en IJsland). Zwitserland is geen lid van de EER en wordt daardoor gecategoriseerd als een derde land.
Gegevens over gezondheid	Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
Genetische gegevens	Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.

Hoofdvestiging	Met betrekking tot een verwerkings-verantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten.
Inbreuk in verband met persoons-gegevens	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.
Informatiebeveiliging	Het geheel van maatregelen, procedures en processen die erop zijn gericht de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen een organisatie te garanderen, met als doel de continuïteit van informatie en informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten te beperken tot een acceptabel vooraf bepaald niveau.
Integriteit (in het kader van informatiebeveiliging)	Dit betreft de waarborgen dat informatie actueel en correct is. Kenmerken hierbij zijn juistheid, volledigheid en geautoriseerdheid van transacties.
Onderneming	Een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoons-vennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen.
Ontvanger	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoons-gegevens worden verstrekt.
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 identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Privacy by default	De instellingen van een programma, app, website of dienst zodanig zijn dat de maximale bescherming van persoonsgegevens wordt betracht.
Privacy by design	Al bij de start van het ontwerp en gedurende de hele levenscyclus van een informatiesysteem rekening gehouden wordt met de bescherming van persoonsgegevens. Het doel hierbij is de beveiliging van persoonsgegevens te optimaliseren.
Profilering	Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroeps-prestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Pseudonimisering	Het zodanig aanpassen van persoonsgegevens dat zij niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder aanvullende gegevens.
Toestemming van de betrokkene	Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.
Toezichthoudende autoriteit	In door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie.
Versleuteling	Langs wiskundige weg (algoritmes) omzetten van gegevens tot een brij zodanig dat zonder de sleutel de gegevens niet hersteld kunnen worden.
Vertegenwoordiger	In de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening.
Vertrouwelijkheid (in het kader van informatiebeveiliging)	Dit betreft de waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd en dat informatie niet kan uitlekken.
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
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.
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of met anderen, het doel van en middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.