Whitepaper

Het model-DSP als centraal verwerkingsregister

vhic bron van vernieuwing

Inleiding

Het begint bijna een magische datum te worden: 25 mei 2018. Er zijn websites waarop een klok het aantal dagen, uren en seconden tot deze dag aftelt. Niet eerder stond een datum waarop nieuwe wetgeving van kracht wordt zo massaal in de belangstelling als deze datum waarop de Algemene Verordening Gegevensbescherming (AVG) gaat gelden. Het besef dat er iets moet gebeuren is er bij de meeste organisaties wel, maar hoe dit proces aan te vliegen en waar te beginnen blijkt lastig.

De implementatie van de AVG vergt van organisaties een aantal organisatorische veranderingen. Afhankelijk van het type organisatie en de typen verwerkingen die plaatsvinden worden organisaties verplicht een intern gegevensbeschermingsbeleid (privacybeleid) vast te stellen, een functionaris voor gegevensbescherming (afgekort als FG[1]) 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[2] verplicht op het moment dat er veranderingen in diensten, producten, processen of informatiesystemen worden doorgevoerd (denk hierbij bijvoorbeeld aan het migreren van informatie naar de cloud, of het aanschaffen van een nieuw informatiesysteem). Ook dient centraal in de organisatie een verwerkingsregister te worden ingericht met allerlei informatie omtrent de verschillende verwerkingen die plaatsvinden.

Dit alles dus voor 25 mei 2018, want het niet naleven van de verordening vanaf deze datum kan een substantieel financieel risico opleveren. Boetes kunnen oplopen tot 20 miljoen euro of vier procent van de wereldwijde jaaromzet. Gezien deze mogelijke implicaties van de verordening is een goed doordachte implementatie noodzakelijk.

De verantwoordingsplicht

De grootste verandering tussen de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming is de verschuiving van ‘vertrouwen’ naar ‘bewijzen’. De AVG legt nadrukkelijk de verantwoordelijkheid om aan te tonen dat de organisatie aan de gestelde eisen voldoet bij de organisatie die de persoonsgegevens verwerkt. Dit komt expliciet terug in de verantwoordingsplicht[3] die is vastgelegd in artikel 5, lid 2 van de AVG waarin staat dat ‘de verwerkingsverantwoordelijke verantwoordelijk (is) voor de naleving (…) en deze kan aantonen’.

Om te voldoen aan de verantwoordingsplicht moet documentatie bij worden gehouden die kan dienen als bewijslast voor de juistheid van de verwerkingen. Immers deze verantwoordingsplicht introduceert ook een omgekeerde bewijslastverdeling. Wanneer een verwerkingsverantwoordelijke niet kan aantonen dat is voldaan aan het beginsel, dan is er sprake van een boetewaardige overtreding van de AVG.[4]

Het verwerkingsregister

Een groot deel van de documentatie om aan te tonen dat wordt voldaan aan de verantwoordingsplicht wordt vastgelegd in het centrale verwerkingsregister dat organisaties met meer dan 250 medewerkers[5] dienen bij te houden. Het register is vormvrij, wat inhoudt dat de AVG niet voorschrijft op welke wijze het register dient te worden bijgehouden (dit mag in papieren of in elektronische vorm, bijvoorbeeld in een speciale software tool, een Excel sheet, een Word bestand etc). Om dit verwerkingsregister goed op te zetten en in te vullen is een uitgebreide inventarisatie van de verwerkingen van persoonsgegevens die plaatsvinden noodzakelijk. Dit is een omvangrijke operatie waarbij alle werkprocessen van een organisatie moeten worden nagelopen en er moet worden bepaald of er al dan niet sprake is van verwerkingen van persoonsgegevens.

---

[1] ook bekend onder de Engelse benaming Data Protection Officer, afgekort als DPO
[2] of privacy impact assessment, afgekort als PIA
[3] ook wel accountability principe genoemd
[4] Engelfriet, Meij en Kager, ‘De Algemene Verordening Gegevensbescherming – artikelgewijs commentaar’ Editie 2017, ICT en Recht.
[5] De AVG bevat een uitzondering dat organisaties met minder dan 250 medewerkers geen verwerkingsregister hoeven bij te houden tenzij er op grote schaal persoonsgegevens worden verwerkt en/of bijzondere persoonsgegevens worden verwerkt.

Tenzij een organisatie beschikt over het Model-DSP. Met de nieuwe uitbreiding van het Model-DSP kunt u het verwerkingsregister grotendeels al vullen op basis van door onze redactie aangeleverde standaard-content.

De AVG en het model-DSP

Het verwerkingsregister en het model-DSP

Het model-DSP is uitgebreid met AVG-gerelateerde metadata. Hiermee neemt het model-DSP een groot deel van de inventarisatie van persoonsgegevens uit handen. Naast het feit dat de toegevoegde AVG-metadata bij de inventarisatie veel tijd bespaart, is het ook zo dat in het geval van toekomstige wijzigingen in de werkprocessen de redactie van het model-DSP er zorg voor draagt dat de noodzakelijke wijzigingen ook in de AVG-metadata worden doorgevoerd. Daarmee bevat het model-DSP altijd een actueel verwerkingsregister.
Voor elk proces waarin het vanuit de aard van het proces nodig kan zijn om persoonsgegevens te verwerken zijn in het model-DSP de relevante AVG-gerelateerde metadata ingevuld. Deze metadata zijn opgesteld en ingevuld aan de hand van de stappen voor de inventarisatie van persoonsgegevens zoals beschreven in de “Roadmap voor de implementatie van de Algemene Verordening Gegevensbescherming”[6].
Hieronder zal per stap worden toegelicht op welke manier deze is opgenomen in het model-DSP.

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

Allereerst hebben wij bij deze stap per werkproces vastgesteld of er persoonsgegevens in verwerkt worden. Dit hebben we vastgelegd in het veld “Persoonsgegevens”. Van alle processen waarvan is vastgesteld dat er persoonsgegevens in verwerkt worden is vervolgens aangegeven om welk type persoonsgegevens het gaat. De volgende typen persoonsgegevens zijn opgenomen in het model-DSP:

- Basis persoonsgegevens (omvat naam, adres, geboortedatum, geboorteplaats, personeelsnummer)
- Burgerservicenummer
- Inkomensgegevens
- Ras of etnische afkomst
- Politieke opvattingen
- Religieuze of levensbeschouwelijke overtuiging
- Lidmaatschap van een vakbond
- Genetische of biometrische gegevens
- Gezondheid
- Seksuele geaardheid
- Strafblad en strafbare feiten
- Gegevens m.b.t. kind(eren)

Het tweede onderdeel van deze stap is het vastleggen van de bron van de persoonsgegevens die in het betreffende werkproces verwerkt worden. Hierin is onderscheid gemaakt tussen de volgende bronnen:

1. Afzender: De persoonsgegevens worden door de afzender van een ingekomen document zelf aangeleverd. Dit kunnen zowel persoonsgegevens van de afzender zelf zijn, als gegevens over een derde persoon, bijvoorbeeld in het geval van een klacht over een persoon.
2. Registratie: De persoonsgegevens worden opgehaald uit een registratie. Registraties zijn in het model-DSP opgenomen in de module ‘Registraties’ en gekoppeld aan de werkprocessen waarin ze gebruikt of gemuteerd worden. Op die manier kan altijd direct gezien worden welke registratie het betreft.

[6] Heijst, Tineke van, ‘Roadmap voor de implementatie van de Algemene Verordening Gegevensbescherming’, mei 2017, beschikbaar via https://vhic.nl/downloads

Onder registraties vallen de basisregistraties zoals de BRP (Basisregistratie personen) en de BAG (Basisregistratie Adressen en Gebouwen), maar ook bijvoorbeeld de registraties contracten, datalekken of honden.

3. Ketenpartner: De persoonsgegevens worden aangeleverd door een ketenpartner. Ketenpartners hebben wij eveneens in generieke vorm opgenomen in het model-DSP en gekoppeld aan de relevante werkprocessen. Enkele voorbeelden van in het model-DSP opgenomen ketenpartners zijn: provincie, waterschap, politie en belastingdienst.
4. Openbare bron: De persoonsgegevens komen uit een openbare bron, bijvoorbeeld een krant of sociale media.

Indien als bron 'Ketenpartner' is aangegeven, wordt de betreffende ketenpartner aangegeven in het veld 'Bron ketenpartner'.

2. Stel vast welke verwerkingen van persoonsgegevens plaatsvinden en in welke systemen.

In het model-DSP is onderscheid gemaakt tussen drie brede verwerkingstypen:

- Raadplegen: persoonsgegevens worden enkel bekeken.
- Muteren: persoonsgegevens worden bewerkt: vastgelegd, gewijzigd, verwijderd, toegevoegd etc.
- Delen: persoonsgegevens worden gedeeld met derden.

De eerste twee verwerkingstypen zijn vastgelegd in het veld 'Verwerkingstype'. Indien de verwerking betrekking heeft op een registratie is dit ook vastgelegd in de relatie tussen het werkproces en de daaraan gekoppelde registratie. De opname van het derde verwerkingstype in het model-DSP wordt verder toegelicht in stap 6.
Deze tweede stap omvat ook het vaststellen in welke systemen persoonsgegevens verwerkt worden. Hierbij komt de module 'Informatiesystemen' in de i-Navigator van pas. Deze module is niet gevuld met model-content, aangezien informatiesystemen organisatie specifiek zijn. De i-Navigator biedt echter wel de mogelijkheid om de door een organisatie in gebruik zijnde informatiesystemen vast te leggen en te koppelen aan werkprocessen en registraties. Hiermee is dan ook gelijk de locatie van de gegevens vastgelegd. Voor gegevens die eventueel nog op papier worden vastgelegd is de module 'Archiefbestanden' beschikbaar.

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

Naast alle nieuwe velden die zijn toegevoegd, maak dit deel van de inventarisatie van de verwerking van persoonsgegevens al onderdeel uit van het model-DSP. Het doel van de verwerking van persoonsgegevens is namelijk vastgelegd in de naam van het werkproces. Het werkproces 'Bijzonder verlof' heeft bijvoorbeeld als doel om een aanvraag voor bijzonder verlof te kunnen beoordelen, dit wordt weergegeven in de naam van het werkproces, namelijk 'Het beoordelen van een aanvraag voor bijzonder verlof'.
Bij het definiëren van de persoonsgegevens die per werkproces worden verwerkt is rekening gehouden met het beginsel van dataminimalisatie. Alleen de minimaal noodzakelijke persoonsgegevens voor de uitvoer van het werkproces worden aangegeven.

4. Stel vast wat de grondslag van de verwerking is.

Per werkproces is aangegeven wat de grondslag is die het verwerken van persoonsgegevens binnen dat proces rechtvaardigt. Hierbij is gebruik gemaakt van de in de AVG genoemde voorwaarden voor verwerking van persoonsgegevens (AVG, artikel 6):

- Toestemming (bewijs is vastgelegd in het zaakdossier van het betreffende werkproces)
- Overeenkomst (bewijs is vastgelegd in het zaakdossier van het betreffende werkproces)
- Wettelijke grondslag (bewijs is vastgelegd in DSP, tabblad Behandeling)
- Publiekrechtelijke taak (bewijs is vastgelegd in DSP, tabblad Behandeling)
- Vitaal belang
- Gerechtvaardigd belang

Dit is overigens geen vereiste om vast te leggen in het verwerkingsregister maar het wordt wel aangeraden omdat in de communicatie naar de betrokkenen de grondslag een belangrijke rol speelt.

5. Stel vast wie de verwerkers zijn van de persoonsgegevens.

De vraag door wie de gegevens worden verwerkt is niet in detail op modelniveau vast te leggen, aangezien dit per organisatie en soms ook per zaak verschilt. In het model-DSP wordt echter wel het taakveld vastgelegd waarin een werkproces valt. Dit geeft in grote lijnen al wel aan door welk taakveld of afdeling het werkproces uitgevoerd wordt. Daarnaast bevat het model-DSP het veld ‘Proceseigenaar’, een veld om aan te kunnen geven wie (welke functie) verantwoordelijk is voor het proces. Dit veld dient altijd lokaal gevuld te worden.

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

In het model-DSP zijn de derde partijen die betrokken (kunnen) zijn bij een werkproces gedefinieerd als ketenpartners. Uitgangspunt bij deze stap is dat wanneer gegevens worden gedeeld met derden, dit altijd met een ketenpartner is. De betreffende ketenpartners zijn vastgelegd in het veld ‘Naar ketenpartners’.

Daarnaast is het van belang om te weten of gegevens al dan niet gedeeld worden met het buitenland. Hiervoor hebben wij het veld ‘Doorgifte buitenland’ opgenomen en de mogelijkheid om dit nader toe te lichten. Indien persoonsgegevens worden bewaard in een cloud-oplossing kan het zijn dat de locatie van de cloud-opslag zich in het buitenland bevindt, waarmee er ook sprake is van doorgifte van persoonsgegevens naar het buitenland. Dit kan lokaal worden vastgelegd bij de gegevens over het betreffende informatiesysteem in de module ‘Informatiesystemen’.

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

Het laatste onderdeel van de inventarisatie is de bewaartermijn van de persoonsgegevens en de wijze waarop de gegevens worden vernietigd. Voor wat betreft de bewaartermijn van de persoonsgegevens is dit in het model-DSP afgedekt door de waardering van de resultaattypen van het betreffende zaaktype. Voor het omgaan met persoonsgegevens in registraties zal een handreiking worden opgesteld; in sommige gevallen zijn hiervoor namelijk termijnen vastgelegd in de Selectielijst en in andere gevallen geldt een termijn van 2 jaar na afhandeling op basis van de Wbp.

De manier waarop persoonsgegevens vernietigd moeten worden, is geen informatie die geschikt is om opgenomen te worden in het model-DSP, aangezien dit o.a. afhankelijk is van de vorm van de persoonsgegevens. Hoe persoonsgegevens vernietigd moeten worden zal per organisatie in bijvoorbeeld een beleidsdocument opgenomen moeten worden.

Het in gebruik nemen van het verwerkingsregister in het Model-DSP

Hoewel het toevoegen van de AVG-velden aan het model-DSP organisaties veel werk uit handen neemt, vergt het model nog wel enige aandacht van de organisatie voordat dit daadwerkelijk compleet en inzetbaar is. Om zoveel mogelijk profijt te hebben van de toegevoegde velden zijn de volgende punten van belang:

Controle op de verwerkingen van persoonsgegevens

Het model-DSP is een standaard beschrijving van de werkprocessen. De werkelijkheid is weerbarstiger. Het is daarom raadzaam om de verwerkingen die plaatsvinden in de eigen organisatie na te lopen om te kijken waar deze verwerkingen afwijken van de verwerkingen zoals beschreven in het model-DSP. Voor de standaard invulling van de AVG-velden is uitgegaan van dataminimalisatie – alleen die persoonsgegevens die daadwerkelijk nodig zijn voor het ten uitvoer brengen van het werkproces zijn aangevinkt. Echter kan het best zo zijn dat bij navraag in de organisatie blijkt dat er aanvullende persoonsgegevens worden verwerkt. Hiervan dient dan te worden bepaald of deze persoonsgegevens echt noodzakelijk zijn voor de verwerking en dient er een bewuste keuze te worden gemaakt deze gegevens wel of niet te blijven verwerken.

Lokale aanvulling op de AVG-velden

De AVG-velden zijn modelvelden die niet door organisaties zelf te wijzigen zijn, ze worden namelijk continue bijgehouden door de redactie van het model-DSP. Wanneer een organisatie toch zelf informatie wil toevoegen kan dit door kenmerken toe te voegen in de i-Navigator.

Informatiesystemen (en archiefbestanden) op orde krijgen

In stap 2 van de inventarisatie dient te worden vastgelegd in welke systemen de verwerking van persoonsgegevens plaatsvindt. Hiervoor is het van belang om als organisatie de module ‘Informatiesystemen’ te vullen met alle relevante informatiesystemen en bijbehorende kenmerken. Vervolgens zullen de informatiesystemen (en eventuele archiefbestanden) zowel aan werkprocessen als aan registraties gekoppeld moeten worden, waarmee veel sneller inzichtelijk gemaakt kan worden waar informatie zich in de organisatie bevind.

AVG-processen in het model-DSP

Naar aanleiding van de AVG is er aan het model-DSP niet alleen nieuwe metadata toegevoegd. Er zijn ook een aantal werkprocessen toegevoegd. Het model-DSP bevat daarmee de volgende AVG-gerelateerde werkprocessen:

- Datalek melding
- Persoonsgegevens verwerking melding
- Persoonsgegevens verwerking melding intrekking
- Persoonsgegevens verwerking melding wijziging
- Persoonsgegevens verwerking toestemming betrokkene
- Persoonsgegevens inzageverzoek
- Persoonsgegevens verwijderingsverzoek
- Persoonsgegevens bewerkersovereenkomst (beschikbaar per update 24 van het model-DSP voor gemeenten)
- Dataportabiliteit persoonsgegevens verzoek (dit werkproces zal begin 2018 toegevoegd worden)

Verdere aandachtspunten voor de implementatie van de AVG

Naast de genoemde punten rondom het DSP, zijn er nog twee andere punten die we graag onder uw aandacht brengen wanneer u aan de slag gaat met het invoeren van de AVG in uw organisatie:

Privacy bewustzijn onder medewerkers (blijven) promoten

Het bijhouden van de verwerkingen in het centrale verwerkingsregister om ervoor te zorgen dat de organisatie kan voldoen aan de verantwoordingsplicht is één ding. Het binnen de organisatie naleven van de regels rondom verwerkingen van persoonsgegevens is een tweede en behoeft minstens zoveel continue aandacht. Bij gebrek aan bewustzijn binnen de organisatie is het immers dweilen met de kraan open en zullen zich steeds opnieuw datalekken voordoen door menselijke fouten. Het blijft dus zaak om medewerkers in de organisatie te blijven trainen in het omgaan met persoonsgegevens. Blijf hier dus consequent aandacht aan besteden.

Veranker de bescherming van persoonsgegevens in uw informatieveiligheidssystematiek

De CISO van uw organisatie heeft de taak te zorgen voor een samenhangend pakket van maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen uw organisatie te waarborgen[7]. De bescherming van persoonsgegevens is hier een onderdeel van. Het is dan ook niet meer dan logisch dat u bij de implementatie van de AVG waar mogelijk aansluit bij de systematiek die gehanteerd wordt door de CISO. Om deze aansluiting te ondersteunen hebben wij het Privacy en Informatieveiligheid (PIV) Framework ontwikkeld: een set van SMART controls waarin normenkaders voor informatieveiligheid (ENSIA, BIG, BIR, ...) en privacy (de Privacy Baseline) zijn gebundeld tot een overzichtelijke set van maatregelen die direct gekoppeld kunnen worden aan de processen in het model-DSP. Informatieveiligheid en bescherming van persoonsgegevens worden op deze wijze ingebed in de ‘normale’ werkprocessen van uw organisatie, waardoor het vervullen van de documentatieplicht neerkomt op ‘normale’ dossiervorming. Door het op deze wijze in te richten wordt voorkomen dat informatieveiligheid een aparte kolom in uw organisatie wordt en wordt het juist ingebed in de lopende processen van de organisatie.

Conclusie

Met de verweving van de AVG in het model-DSP heeft uw organisatie een goede basis om verwerkingen van persoonsgegevens conform de AVG vast te leggen. Er zijn echter zoals hierboven omschreven nog wel de nodige stappen door de organisatie zelf te nemen. Wanneer u gedurende het invoeren van de AVG aan de hand van het model-DSP vragen of opmerkingen heeft kunt u hiervoor altijd onze model-DSP helpdesk benaderen. Ook zal er binnenkort een nieuwe i-NO cursus gepubliceerd worden die nog dieper in gaat op de toevoeging van de AVG-content aan het model-DSP. Houdt u tenslotte ook onze opleidingen in de gaten, binnenkort start de voorinschrijving voor een leergang op het gebied van informatieveiligheid en privacy waarin onder andere het gebruik van het model-DSP en de AVG behandeld zal worden.

---

7 Handreiking IB-functieprofiel Chief Information Security Officer (CISO), https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0218-Handreiking-CISO-functieprofiel-v1.0.pdf