Data Protection Impact Assessment

Versie: 3

Datum: maart 2020

Auteurs: ir. Hugo Leisink CIPP/E
mr. ir. Frans Dondorp CIPP/E CIPT

Versie	Datum	Wijzigingen
1	oktober 2018	Eerste publicatie.
2	april 2019	Indeling in thema-secties en geschikt gemaakt voor online versie.
3	maart 2020	Aanvullende juridische toelichting en aanscherping van enkele vragen.

Over dit Data Protection Impact Assessment model

Persoonsgegevens worden op vele manieren en op vele plekken verwerkt. Onze maatschappij is daar voor een belangrijk deel van afhankelijk. Echter, het verwerken daarvan neemt ook risico's voor de betrokkenen met zich mee. Een goede manier om deze risico's inzichtelijk te maken, is door het uitvoeren van een Data Protection Impact Assessment (DPIA).

Een DPIA is een aanpak waarin door middel van kritische vragen wordt nagegaan of u op een goede en respectvolle wijze omgaat met de gegevens van de betrokkenen. Een DPIA helpt u bij het leren inrichten van verwerkingen volgens het privacy by design principe. Het resultaat van privacy by design is een verwerking waarbij de inbreuk op de privacy van de betrokkenen minimaal is en de rechten van de betrokkenen worden nageleefd. Dit levert u tegelijkertijd een voordeel op. Iedere overbodige verwerking die geschrapt wordt, scheelt namelijk tijd, geld en moeite voor de bescherming van die gegevens. En gegevens die u niet in huis heeft, kunt u ook niet lekken.

Of het resultaat van een DPIA nuttig zal zijn, hangt vooral af van hoe u deze hanteert. Gebruik een DPIA niet om enkel en alleen uw (geplande) verwerking te rechtvaardigen of om de risico's vanuit de AVG voor uw organisatie in kaart te brengen. Een DPIA is namelijk in de eerste plaats bedoeld ter bescherming van de privacy van de betrokkenen. Hanteer deze daarom ook als zodanig.

Wij realiseren ons dat ook andere DPIA modellen beschikbaar zijn. De meest bekende is het Model Gegevensbeschermingseffectbeoordeling Rijksdienst. Echter, waar dat model geschikt is voor organisaties die beschikken over de benodigde juridische kennis, richt dit DPIA model zich op organisaties die daar niet over beschikken. Dit model is daarom anders van opzet; meer sturend. Bij het opstellen van dit model hebben we zorgvuldig gekeken naar wat artikel 35 en 36 van de AVG daarover zegt.

Dit DPIA model is verkrijgbaar via de Privacy Friendly website [1] en is uitgegeven onder de CC BY-ND 4.0 licentie. Dit betekent dat u dit model vrij mag gebruiken en, mits ongewijzigd, vrij mag verspreiden. We zijn van plan om ons model te blijven verbeteren. Geef ons dus vooral uw reactie en commentaar. Dit kunt u sturen naar info@privacy-friendly.nl.

Wij wensen u veel succes bij het uitvoeren van de DPIA.

Hugo Leisink en Frans Dondorp

Voordat u begint

Dit Data Protection Impact Assessment (DPIA) model is bedoeld voor gebruik bij de Algemene Verordening Gegevensbescherming (AVG). Het is daarom zeer raadzaam om de AVG bij de hand te hebben tijdens de uitvoering van deze DPIA. U kunt de AVG als PDF downloaden [2] of online bekijken [3].

Om de vragen makkelijk leesbaar te maken, wordt u in dit model direct aangesproken. Uiteraard wordt u daarbij niet persoonlijk bedoeld, maar de organisatie waarvoor u de DPIA uitvoert.

De scope van de DPIA is één specifieke verwerking. Voer voor andere verwerkingen een aparte DPIA uit. Beantwoord de vragen zo volledig mogelijk. Geef dus naast een gevraagde 'ja' of 'nee' ook een beargumentatie voor uw antwoord.

Appendix A bevat extra toelichtingen bij enkele vragen. Deze zijn in een apart hoofdstuk gezet om de DPIA-vragenlijst leesbaarder te maken.

Dit document is een volledige kopie van het online DPIA model [4]. De online versie biedt u de mogelijkheid om gericht vragen in te vullen die voor u van toepassing zijn, een hulpmiddel om de antwoorden vast te leggen en een rapportage aan het einde van de DPIA. Wij raden u aan om, indien mogelijk, gebruik te maken van deze online versie.

Disclaimer:

- Dit DPIA model heeft een bepaalde verwerking als scope. De uitkomst van de DPIA zegt niets over compliancy of de mate waaraan u in totaliteit aan de AVG voldoet. Dit model geeft alleen invulling aan artikel 35.

- De DPIA geeft u inzicht in risico's. Het is geen beoordeling over de vraag of de verwerking wenselijk is of dat de verwerking is toegestaan. Als u na de uitvoering van de DPIA van mening bent dat de verwerking geen risico's oplevert, zegt dat niet dat de verwerking een goed idee is onder de AVG.

- Dit DPIA model is een hulpmiddel en geen wettekst. De auteurs van dit model beogen u te helpen bij de beoordeling van risico's, niet om de (mede)verantwoordelijkheid te dragen voor uw verwerkingen. Zij zijn dus niet aansprakelijk voor enig gevolg dat voortvloeit uit het gebruik van dit model.

1. Algemeen

Algemene informatie over de verwerking die in deze DPIA wordt behandeld.

1. Voor welke organisatie en afdeling wordt deze DPIA uitgevoerd?
2. Geef een omschrijving van de verwerking.

   Een algemene omschrijving van de verwerking in uw eigen bewoording, bedoeld om deze DPIA later in context te kunnen plaatsen. Het gaat hier dus niet om de gedetailleerde doelbeschrijving zoals benoemd in artikel 5, maar om uw eigen procesomschrijving.
3. Welke gegevens verwerkt u en wat doet u daarmee?

   Geef aan welke persoonsgegevens of categorieën van persoonsgegevens u verwerkt en wat u daar precies mee doet.
4. Wat is het doel / reden van de verwerking?

   Waarom voert u deze verwerking uit? In deze DPIA gaan we bespreken wat qua verwerking van persoonsgegevens noodzakelijk is voor dit doel.
5. Heeft de DPIA betrekking op meerdere vergelijkbare verwerkingen?

   In de AVG is een DPIA is gericht op één verwerking, maar voor efficiëntie is het toegestaan om meerdere verwerkingen met een enkele DPIA te onderzoeken. Dit volgt uit EDPB guideline 248.

   Als deze DPIA betrekking heeft op meerdere verwerkingen, dient u uiteraard de verschillende verwerkingen te beschrijven en te beargumenteren waarom u deze verwerkingen analyseert met één DPIA.

   Ook is het denkbaar (en toegestaan) dat u een DPIA wilt uitvoeren voor meerdere projecten of voor meerdere organisaties. Overweging 92 staat dat nadrukkelijk toe: het is dus mogelijk om DPIA's ook sectoraal te hergebruiken.

   Uw antwoord op de vraag:

   - ja
     De DPIA heeft betrekking op meerdere verwerkingen.
   - nee, ga door met vraag 2.1
6. Omschrijf de verschillende verwerkingen en waarom u deze met een enkele DPIA analyseert.

2. DPIA verplichting

Deze sectie helpt u bepalen of een DPIA verplicht is.

1. Wilt u de vragen over de DPIA verplichting doorlopen?

Een DPIA is in bepaalde gevallen verplicht. Het is natuurlijk aan u als verantwoordelijke om te bepalen of u sowieso deze DPIA wilt uitvoeren, of dat u dit alleen wilt doen als een DPIA in uw situatie wettelijk verplicht zou zijn. Als u al weet dat een DPIA verplicht is of de DPIA sowieso wilt doorlopen, kunnen we de vragen over de verplichting overslaan.

Uw antwoord op de vraag:

- ja
- nee, ga door met vraag 3.1
  De sectie over noodzakelijkheid wordt overgeslagen, in de gedachte dat de wenselijkheid van deze DPIA al vaststaat.

2. Houdt de verwerking waarschijnlijk een hoog risico in voor de betrokkene?

Dit is het kerncriterium voor de DPIA. In geval van twijfel adviseert de EDPB een DPIA uit te voeren. Het nut van deze vraag is dus vooral om te bepalen of er niet sprake is van een hoog risico.

Artikel 35 schrijft een DPIA voor:

> *Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen [...]*

Uw antwoord op de vraag:

- ja, ga door met vraag 3.1
  De DPIA is verplicht. De vragenlijst gaat verder bij het volgende hoofdstuk.
- nee
  De DPIA is niet verplicht. U kunt er voor kiezen om de DPIA toch uit te voeren, maar dat is optioneel.
- weet ik niet
  De vragenlijst gaat verder met de subcriteria om te bepalen of een DPIA verplicht is.

3. Is een van de uitzonderingen van toepassing?

De Autoriteit Persoonsgegevens heeft geen negatieve lijst [5] gepubliceerd waarop staat wanneer u geen DPIA hoeft uit te voeren. De EDPB geeft echter als criteria:

- als er waarschijnlijk geen hoog risico voor betrokkene is;
- als de aard, omvang, context en doel zeer vergelijkbaar zijn met een andere verwerking waar al een DPIA voor is uitgevoerd;
- als de verwerking voor mei 2018 door de AP / CBP is gecontroleerd;
- als de verwerking een wettelijke grond heeft en er al een DPIA is uitgevoerd bij het vaststellen van die grond;

Uw antwoord op de vraag:

- ja: er is een uitzondering van toepassing, ga door met vraag 2.7
  De DPIA is niet verplicht. U kunt er voor kiezen om de DPIA toch uit te voeren, maar dat is optioneel.
- nee
  De vragenlijst gaat verder bij de subcriteria om te bepalen of een DPIA verplicht is.
- weet ik niet
  De vragenlijst gaat verder bij de subcriteria om te bepalen of een DPIA verplicht is.

4. Is er sprake van een geautomatiseerde beoordeling met gevolgen voor betrokkenen?

Een DPIA is volgens artikel 35 lid 3 sub a verplicht als er sprake is van:

> *een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn*

> *verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen.*

Het gaat hier om screening en profilering met een geautomatiseerde beslissing. Denk aan geautomatiseerde screening van klanten voor krediet of verzekering. Of aan korting die klanten automatisch krijgen als ze aan bepaalde criteria voldoen.

Uw antwoord op de vraag:

- ja, ga door met vraag 3.1
  De DPIA is verplicht. De vragenlijst gaat verder bij het volgende hoofdstuk.
- nee

5. Verwerkt u bijzondere persoonsgegevens op grote schaal?

Als u bijzondere gegevens op grote schaal verwerkt, is een DPIA verplicht onder artikel 35 lid 3 sub b:

> *grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10*

... waarbij de vraag is wat 'grootschalig is'. Daarin voorzien overweging 91 en EDPB opinie 248:

- aantal betrokkenen;
- het volume van gegevens;
- de duur van de verwerkingsactiviteit;
- geografische omvang van de verwerkingsactiviteit.

Uw antwoord op de vraag:

- ja, ga door met vraag 3.1
  De DPIA is verplicht. De vragenlijst gaat verder bij het volgende hoofdstuk.
- nee

6. Is er sprake van stelselmatige en grootschalige monitoring van openbare ruimten?

De AVG stelt in artikel 35 lid 3 sub a dat een DPIA verplicht is als er sprake is van:

> *stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.*

De EDPB stelt in opinie 248:

> *Dit type monitoring is een criterium omdat de persoonsgegevens kunnen worden verzameld in omstandigheden waarin de betrokkenen mogelijk niet weten wie hun gegevens verzamelt en hoe die gegevens zullen worden gebruikt. Bovendien kan het voor natuurlijke personen onmogelijk zijn om te voorkomen dat ze aan een dergelijke verwerking in een openbare (of openbaar toegankelijke) ruimte worden onderworpen.*

Uw antwoord op de vraag:

- ja, ga door met vraag 3.1
  De DPIA is verplicht. De vragenlijst gaat verder bij het volgende hoofdstuk.
- nee

7. De DPIA is niet verplicht.

Op basis van eerder gegeven antwoorden is een DPIA in uw geval niet verplicht. U kunt nu stoppen met deze DPIA. Uiteraard kunt u er ook voor kiezen om door te gaan met de DPIA, om zo beter zicht te krijgen op de verwerking.

3. Behoorlijk & transparant

De AVG is gebaseerd op een aantal beginselen: de verwerking moet behoorlijk zijn (duidelijk doel, gegevensminimalisatie, bescherming, verwijdering etc) en transparant (navolgbaar).

1. Wilt u de detailvragen over behoorlijkheid en transparantie doorlopen?

   De AVG eist dat een verwerking 'behoorlijk en transparant' is (artikel 5). De DPIA bevat hier subvragen voor, maar het is goed mogelijk dat u op basis van eerdere onderzoeken al weet dat u hieraan voldoet. En dus dat u deze vragen kunt overslaan.

   Uw antwoord op de vraag:

   - ja
   - nee, ga door met vraag 3.8
     We gaan door naar de laatste vraag van deze sectie, waar u uw eindoordeel geeft over de behoorlijkheid en de transparantie.

2. Verwerkt u voor een duidelijk omschreven doel?

   De verwerking moet verbonden zijn aan een 'uitdrukkelijk omschreven en gerechtvaardigd' doel ("doelbinding"), zodat voor eenieder duidelijk is waarom de persoonsgegevens verwerkt worden.

   Uw antwoord op de vraag:

   - ja
   - nee
     De verwerking is onbehoorlijk omdat er geen uitdrukkelijk omschreven doel is. Daardoor is het onduidelijk welke gegevens daarvoor noodzakelijk zijn.

3. Verwerkt u voor een gerechtvaardigd doel?

   Deel 2 van de doelbinding is dat de verwerking gerechtvaardigd is. In overweging 39 wordt uitgelegd dat dit betekent dat persoonsgegevens alleen mogen worden verwerkt als "het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt". Dit betekent dus dat u serieus onderzocht heeft of de doelstelling waarvoor u de persoonsgegevens verwerkt, ook behaald kan worden met minder of zelfs zonder de te verwerken persoonsgegevens.

   Uw antwoord op de vraag:

   - ja
   - nee
     Het doel van de verwerking kan ook worden verwezenlijkt op een andere wijze. Dat maakt deze verwerking onnodig en de principes van minimalisatie en 'privacy by design' hebben dan tot gevolg dat u deze verwerking dient te schrappen.
   - weet ik niet, is niet in voldoende mate onderzocht
     Doe eerst onderzoek naar alternatieve processen, waarbij minder of zelfs geen persoonsgegevens nodig zijn.

4. Verwerkt u de gegevens uitsluitend voor het doel of voor een verenigbaar doel?

   De vorige twee vragen waren gericht op het 'uitdrukkelijk omschreven en gerechtvaardigd doel'. De doelbinding houdt in dat de verwerking zich beperkt tot dat doel. De AVG geeft echter ruimte om ook te verwerken voor een 'verenigbaar' doel. Daar is geen aparte grond voor nodig (uit art. 6, waarover in de sectie rechtmatigheid meer). Een webshop kan bijvoorbeeld de persoonsgegevens over aankopen ook gebruiken voor suggesties of marketing. Dat doel is verenigbaar met het doel 'nakomen overeenkomst en levering' en vindt plaats op basis van dezelfde rechtsgrond (in dit geval 6b: overeenkomst met betrokkene).

   Eisen dat u alleen verwerkt voor het gespecificeerde doel is dus te streng. Een verenigbaar doel mag ook. Wat verenigbaar is, wordt uitgelegd in overweging 50.

   Archivering in het algemeen belang (w.o. archiefrechtelijk), wetenschappelijk en historisch onderzoek of statistische doeleinden worden als verenigbaar beschouwd en zijn dus toegestaan als de oorspronkelijke verwerking is toegestaan. Een geheimhoudingsplicht gaat altijd voor: een verwerking die een wettelijke, begroepsmatige of contractuele geheimhouding schendt kunt u niet rechtvaardigen met 'verenigbaar doel'. Klinkt logisch, maar met commerciële geheimhouding kan het complex worden.

Uw antwoord op de vraag:

- ja
- nee

Er wordt verwerkt buiten het gedocumenteerde doel en voor doelen die niet verenigbaar zijn. Daardoor is de verwerking onbehoorlijk.

5. Worden alleen de noodzakelijke persoonsgegevens verzameld?

Artikel 5 lid 1 sub c zegt

> *Persoonsgegevens moeten toereikend zijn, ter zake dienen en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.*

Dit principe van gegevensminimalisatie vereist dat het proces en de administratie daarvan geen persoonsgegevens vastlegt die niet noodzakelijk zijn. Maar ook dat de persoonsgegevens toereikend zijn: te weinig (een 'onvolledig beeld') is ook niet goed. Zie ook overweging 39.

Het uitdrukkelijke doel komt hier terug: het gaat om de noodzakelijkheid om het doel te bereiken. Niet meer (gegevens), maar ook niet minder (gegevens). In feite kunt u dus van alle persoonsgegevens binnen deze verwerking verdedigen dat de verwerking daarvan noodzakelijk is.

Uw antwoord op de vraag:

- ja
- nee

De verwerking is in strijd met het minimalisatiebeginsel. Er worden persoonsgegevens verwerkt die niet noodzakelijk zijn en dat is een risico voor betrokkene - omdat hij dat niet verwacht en omdat u een onnodig groter risico neemt op datalekkage.

6. Is het voor alle betrokkenen duidelijk welke gegevens over hen verzameld worden, waarom dat is en wat hun rechten zijn?

De betrokkene heeft natuurlijk het recht om persoonsgegevens in te zien en te laten corrigeren (onder andere). Deze rechten dienen alleen hun doel als de betrokkene daadwerkelijk weet dat de verwerking plaatsvindt. Het gaat hier om transparantie over de inhoud: dat is in de AVG vastgelegd in art. 12. Het gaat er om dat aan de betrokkene duidelijk en begrijpelijk gecommuniceerd wordt wat de verwerking inhoudt, om welke gegevens het gaat en wat zijn rechten zijn. Dit wordt nader uitgewerkt in art. 13 en 14.

Uw antwoord op de vraag:

- ja
- nee

De inhoud van de verwerking is niet transparant voor de betrokkene (art. 12). Hierdoor kan betrokkene niet zijn rechten effectueren en dat is een risico.

7. Kunt u de rechtmatigheid, behoorlijkheid en transparantie aantonen?

De AVG eist niet alleen dat de verwerking rechtmatig, behoorlijk en transparant is, maar ook dat u dat kunt aantonen. Dat betekent dat u een administratie moet voeren waaruit blijkt dat uw verwerking zich houdt aan het doel, dat persoonsgegevens minimaal worden verzameld, actueel zijn, tijdig verwijderd worden en passend beschermd worden.

Dat is geen eenvoudige opgave. U moet een verwerkingsregister bijhouden (art. 30 lid 1) en dat ook eisen van uw verwerkers (art. 30 lid 2). U moet kunnen aantonen dat u de een passende bescherming biedt. Maar ook dat u de gegevens actueel houdt en minimaliseert (niet te veel, niet te weinig).

Uw antwoord op de vraag:

- ja
- nee

De aantoonbaarheid (transparantie over het proces) is niet of onvoldoende ingevuld.

8. Heeft u de behoorlijkheid en transparantie van de verwerking op orde?

Baseer uw antwoord op uw eerdere antwoorden van de vragen 3.2, 3.3, 3.4, 3.5, 3.6 en 3.7. Uiteraard alleen als u deze hebt ingevuld.

Uw antwoord op de vraag:

- ja
- nee

Neem maatregelen om de verwerking 'behoorlijk en transparant' te maken.

4. Rechtmatigheid

Is de verwerking rechtmatig?

1. Wilt u de vragen over de rechtmatigheid van de verwerking doorlopen?

   Strikt genomen gaat de DPIA niet over de vraag of een verwerking wel mag onder de AVG. In veel DPIA's is dit echter wel een onderdeel, omdat het doorlichten van een verwerking een goed moment is om te bepalen of u nog beter kunt voldoen aan de eisen die de AVG stelt.

   Als u echter al weet dat deze verwerking rechtmatig is, kunnen we de vragen daarover overslaan.

   Uw antwoord op de vraag:

   - ja
   - nee, ga door met vraag 4.16
     We gaan door naar de laatste vraag van deze sectie, waar u uw eindoordeel geeft over rechtmatigheid van de verwerking.

2. Wat is de grondslag van de verwerking?

   Kies daarbij een van de grondslagen zoals bedoeld in artikel 6(1). Kies alleen toestemming als grondslag als alle andere grondslagen niet van toepassing zijn. Beargumenteer hoe u tot de gekozen grondslag gekomen bent.

   Voor overheidsinstanties is het belangrijk om op de hoogte te zijn van deze punten:

   - Overweging 43 stelt dat voor "toestemming" (grondslag a) voor overheidsinstanties een hogere drempel bestaat;
   - Overweging 47 en de laatste zin van art. 6 lid 1 stellen dat "gerechtvaardigd belang" (grondslag f) niet van toepassing is voor overheidsinstanties bij de uitoefening van hun taken;
   - Art. 6 lid 1 sub e heeft het over een taak in het kader van de uitoefening van het openbaar gezag. Dat is wezenlijk anders dan publiekrechtelijke taak. Het kan onder grondslag "e" dus ook gaan over taken waar geen expliciete wettelijke basis voor is, maar die logisch zijn in de uitoefening van het correct overheidshanden.

   In de praktijk hebben wij veel discussie meegemaakt over klantcontactcentra bij overheden. Het vastleggen van telefoonnummers, contactgegevens, details over persoonlijke omstandigheden bij hulpvragen. De grondslag daarvoor is dus niet toestemming of gerechtvaardigd belang, omdat dat onder ow. 43, 47 + art. 6 lid 1 gewoon niet kan. De grondslag daarvoor is "e", met de context dat de gegevens nodig zijn voor een taak in de uitoefening van overheidshandelen. Hetzelfde speelt in de Wet BRP, waarbij de Nota van Toelichtingen [6] stelt in paragraaf 10.3.4:

   > *De wet (=Wet BRP) spreekt uitsluitend over verstrekking ten behoeve van de taak van een overheidsorgaan. De reden daarvan is dat ook in het geval de uitvoering van de taak van het overheidsorgaan plaatsvindt in een privaatrechtelijke vorm, er in brede zin sprake blijft van een publiekrechtelijk handelen dat verstrekking van gegevens uit de basisregistratie rechtvaardigt. Gegevensverstrekking uit de basisregistratie ten behoeve van het KCC voor dergelijke taken stuit derhalve niet op bezwaar.*

   Voor overheidsinstanties dus het advies om grondslag "e" ruim te lezen. De keerzijde is er natuurlijk ook: als een gegeven redelijkerwijs niet nodig is voor "een taak" in het kader van de uitoefening van het openbaar gezag is er geen grondslag onder "e". Minimalisatie blijft natuurlijk aan de orde.

   Uw antwoord op de vraag:

   - 6(1)a: Toestemming, ga door met vraag 4.3
   - 6(1)b: Uitvoering van een overeenkomst
   - 6(1)c: Wettelijke verplichting
   - 6(1)d: Bescherming van vitale belangen
   - 6(1)e: Algemeen belang
   - 6(1)f: Gerechtvaardigd belang

   Ga door met vraag 4.9.

3. Is er sprake van toestemming volledig uit vrije wil?

Het kader voor toestemming staat in overweging 32:

> *Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt.*

Houd daarbij rekening met een eventuele machtsverhouding tussen de verwerkingsverantwoordelijke en de betrokkenen.

Toestemming afdwingen door een dienst volledig te blokkeren tenzij eerst toestemming wordt gegeven gaat te ver.

> *Artikel 7 lid 4: Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.*

Zie ook overweging 43. Toestemming gaat niet op als die toestemming niet noodzakelijk is voor de uitvoering van een overeenkomst.

Uw antwoord op de vraag:

- ja
- nee

Indien toestemming niet uit vrije wil is gegeven, kan toestemming niet worden gekozen als grondslag.

4. Zijn er voor een betrokkene negatieve gevolgen bij het niet geven of intrekken van de toestemming?

Indien uw antwoord 'ja' is, beschrijf dan wat deze gevolgen zijn.

Zie ook overweging 43. Als de uitvoering van een overeenkomst afhankelijk is van deze toestemming, is de toestemming niet vrijelijk gegeven. In welk geval toestemming dus geen grondslag kan zijn. Dat speelt natuurlijk in arbeidsovereenkomsten, waar (dus) een andere grondslag (zoals wettelijke plicht) moet bestaan voor het vastleggen van persoonsgegevens. Je mag dus niet grondslag "b" aanvullen met "a": als het gegeven niet noodzakelijk is voor de overeenkomst ("b") mag je het niet alsnog via toestemming ("a") goedpraten door de uitvoering van de overeenkomst af te laten hangen van die toestemming.

Uw antwoord op de vraag:

- ja

Volgens overweging 42 kan toestemming niet worden geacht vrijelijk te zijn verleend, indien de betrokkene zijn of haar toestemming niet kan weigeren of intrekken zonder nadelige gevolgen.

- nee

5. Kan de toestemming worden aangetoond?

Als u verwerkt op basis van toestemming, moet u een toestemmingsregister voeren. Niet alleen voor de verantwoording maar ook omdat een betrokkene de toestemming kan intrekken of betwisten.

> *Artikel 7 lid 1: 1.Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.*

De betrokkene kan toestemming verlenen, maar die ook weer intrekken. Het register moet uiteraard de correcte status weergeven: alleen vastleggen dat er ooit toestemming is gegeven (door bijvoorbeeld de formulieren uit de registratiefase te bewaren) volstaat dus niet.

Uw antwoord op de vraag:

- ja
- nee

6. Kan de toestemming op dezelfde eenvoudige wijze worden ingetrokken als waarop deze is gegeven?

Het is niet de bedoeling dat het geven van toestemming eenvoudig is, maar het intrekken lastig.

> *Artikel 7 lid 3: De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan.*

Intrekking betekent dus niet dat de reeds uitgevoerde verwerking onrechtmatig was (want er was destijds wel toestemming). Het betekent echter wel dat het voortzetten van die verwerking onrechtmatig is. Logischerwijs heeft de betrokke dus ook het recht op wissing (art. 17 lid 1 sub b). Je kunt dus verwachten dat betrokkene toestemming intrekt en in hetzelfde bericht om wissing verzoekt.

Voor de liefhebber: het recht op wissing na intrekking bestaat alleen als er geen andere rechtsgrond is voor de verwerking (weer art. 17 lid 1 sub b). Het zou opmerkelijk zijn als die situatie zich voordoet, want als er een andere grond zou zijn, zou je je niet moeten beroepen op toestemming. Het toestemmingsregister, intrekking: die complexiteit zou je niet kiezen als je een andere grond had.

Uw antwoord op de vraag:

- ja
- nee

U bent hiermee in overtreding van artikel 7 lid 3.

7. Verwerkt u persoonsgegevens van kinderen, zoals bedoeld in artikel 8?

Het gaat hier om verwerkingen in het kader van elektronische diensten ('diensten van de informatiemaatschappij') die direct aan kinderen worden aangeboden en waarvan de grondslag 'toestemming' is. Deze toestemming is alleen rechtmatig als het kind minimaal 16 is of als de toestemming wordt verleend door de ouder of voogd.

Uw antwoord op de vraag:

- ja
- nee, ga door met vraag 4.9

8. Verkrijgt u de toestemming van de ouders van het kind, zoals bedoeld in artikel 8 lid 2?

Als u elektronische diensten aanbiedt aan kinderen en daarbij verwerkt op de grondslag 'toestemming', heeft u de toestemming nodig van de ouder of voogd als het kind jonger is dan 16.

U moet daar een 'redelijke inspanning' voor doen. Bij de registratie voor de dienst kunt u bijvoorbeeld een aantal vragen stellen die voor een kind onder de 16 lastig zijn.

> *Artikel 8 lid 2: Met inachtneming van de beschikbare technologie doet de verwerkingsverantwoordelijke redelijke inspanningen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.*

Uw antwoord op de vraag:

- ja
- nee

U bent hiermee in overtreding van artikel 8.

9. Verwerkt u bijzondere persoonsgegevens, zoals bedoeld in artikel 9?

Het gaat om verwerkingen:

- van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken;
- van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon;
- van gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Let op de cursieve tekst. Als u niet expliciet registreert wat iemands ras is, maar wel gegevens

verwerkt waaruit dat ras blijkt (zoals een foto), is er dus sprake van bijzondere persoonsgegevens.

De UAVG biedt nadere uitwerkingen en uitzonderingen in artt. 24-29.

Uw antwoord op de vraag:

- ja
- nee

10. Verwerkt u persoonsgegevens over strafrechtelijke veroordelingen of strafbare feiten, zoals bedoeld in artikel 10?

Het is (behoudens de uitzonderingen) niet toegestaan om gegevens vast te leggen over iemands strafrechtelijke verleden.

> *Artikel 10: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid [...]*

De UAVG biedt nadere uitwerkingen en uitzonderingen in artikel 31-33.

Uw antwoord op de vraag:

- ja
- nee

11. Vind de verwerking reeds plaats?

Dit is relevant omdat een DPIA voorafgaand aan de verwerking moet plaatsvinden. Als dat niet is gebeurd, moet u dat kunnen verklaren.

Uw antwoord op de vraag:

- ja
  Een DPIA dient uitgevoerd te worden voorafgaand aan de verwerking.
- nee

12. Ontvangt u persoonsgegevens direct van de betrokkenen of via derden?

Dit is relevant voor de informatieplicht voor de verantwoordelijke: die moet de betrokkene informeren over de verwerking. De regels daarvoor staan in artikel 13 als de gegevens direct van betrokkene worden verzameld; in artikel 14 als deze via een derde worden verkregen.

Uw antwoord op de vraag:

- Direct van de betrokkenen
- Via derden

13. Worden de persoonsgegevens doorgezet naar derden?

Welke derde partijen zijn onderdeel van deze verwerking? Benoem daarbij welke gegevens zij verwerken en op welke manier.

Uw antwoord op de vraag:

- ja
- nee, ga door met vraag 4.15

14. Indien deze derden verwerker zijn zoals bedoeld in artikel 28, is met hen een verwerkingsovereenkomst afgesloten?

De Handleiding AVG [7] biedt een stroomschema om te bepalen of een organisatie verwerker is of niet. Als toelichting zegt de Handleiding:

> *U verwerkt ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens wanneer de verwerking van persoonsgegevens uw primaire opdracht is. Met andere woorden, uw dienstverlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Wanneer de verwerking van persoonsgegevens niet uw primaire opdracht is, maar het een uitvloeisel is van een andere vorm van dienstverlening, dan bent u als dienstverlener zélf de verwerkingsverantwoordelijke voor deze verwerking. Oftewel, het enkele feit dat u een opdracht krijgt van de verwerkingsverantwoordelijke is niet voldoende om te kunnen spreken van verwerkerschap, de opdracht moet gericht zijn op het verwerken van persoonsgegevens.*

De vraag hier is dus: geeft u een derde expliciet opdracht om voor u, namens u, persoonsgegevens te verwerken?

Zo ja: heeft u met die derde een verwerkersovereenkomst afgesloten zoals bedoeld in artikel 28 lid 3?

Uw antwoord op de vraag:

- ja
- nee

15. Bevinden zich onder de organisaties waar u (of anderen) gegevens naar doorzet, organisaties buiten de Europese Economische Ruimte (EER)?

Als u gegevens doorgeeft aan derdelanden (buiten de EEG), dan kan dat alleen onder de voorwaarden uit hoofdstuk 5 van de AVG.

Uw antwoord op de vraag:

- ja
- nee

16. Heeft u de rechtmatigheid van de verwerking op orde?

Baseer uw antwoord op uw eerdere antwoorden van de vragen 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14 en 4.15. Uiteraard alleen als u deze hebt ingevuld.

Uw antwoord op de vraag:

- ja
- nee

De verwerking is onrechtmatig. Staak de verwerking of neem maatregelen om deze rechtmatig te maken.

5. Rechten betrokkenen

Zijn de rechten van de betrokkenen gewaarborgd?

1. Wilt u de vragen over de betrokkenerechten doorlopen?

   De DPIA richt zich op de bescherming van persoonsgegevens en de risico's voor betrokkenen. Als een betrokkene bepaalde rechten niet of slechts heel moeilijk kan uitoefenen is dat een risico. Dat is bijvoorbeeld het geval als een betrokkene zijn gegevens niet kan inzien of corrigeren.

   Het is natuurlijk mogelijk dat u de betrokkenerechten al heeft beoordeeld voor andere processen. In dat geval kunnen we deze vragen overslaan.

   Uw antwoord op de vraag:

   - ja
   - nee, ga door met vraag 5.10
     We gaan door naar de laatste vraag van deze sectie, waar u uw eindoordeel geeft over betrokkenerechten.

2. Heeft u een proces voor inzage door betrokkenen?

   Op grond van artikel 15 heeft de betrokkene het recht om te achterhalen of u persoonsgegevens van hem verwerkt en vervolgens ook het recht om inzage in die gegegevens te krijgen (lid 1). U verstrekt een gratis kopie; voor eventuele volgende kopieen kunt u een vergoeding vragen (lid 3).

   Uw antwoord op de vraag:

   - ja
   - nee

3. Heeft u een proces voor correctie / aanvulling door betrokkene?

   Artikel 16 biedt de betrokkene het recht op rectificatie van onjuiste persoonsgegevens en (afhankelijk van het doel van de verwerking) het recht op 'vervollediging'.

   Uw antwoord op de vraag:

   - ja
   - nee

4. Heeft u een proces voor gegevenswissing?

   Het gaat hier om het bekende 'recht op vergetelheid'. De betrokkene heeft het recht op wissing van gegevens als:

   - deze niet langer nodig zijn; feitelijk dus als u verzuimt de gegevens te verwijderen ex artikel 5 lid 1 sub e;
   - de verwerking plaatsvindt op basis van toestemming en de toestemming wordt ingetrokken;
   - de betrokkene bezwaar maakt (het recht ex artikel 21) en er geen redenen zijn om dat te weigeren;
   - de persoonsgegevens onrechtmatig zijn verwerkt; of
   - de persoonsgegevens zijn verzameld bij het aanbieden van een elektronische dienst aan een kind op basis van toestemming waarbij het kind jonger is dan 16 jaar.

   Zoals ook geldt bij andere betrokkenerechten, gaat dit recht dus niet altijd op. Er is bijvoorbeeld geen recht op wissing als de grondslag "uitvoering openbaar gezag" is (art. 6 lid 1 sub e) tenzij er bezwaar is gemaakt (art. 21).

   De weergave hierboven is een niet-juridische samenvatting van art. 17: lees in geval van twijfel de oorspronkelijke tekst. Lees dan ook overweging 59 (wissing zou gratis moeten zijn) en overweging 66 (keteninstructie: laat ook andere verantwoordelijken links verwijderen).

   Uw antwoord op de vraag:

   - ja
   - nee

5. Heeft u een proces voor beperking van de verwerking?

In de gevallen zoals beschreven in artikel 18 lid 1, kan de betrokkene eisen dat de verwerking wordt beperkt / gestopt, terwijl de gegevens wel onder de verwerkingsverantwoordelijke blijven. Denk aan 'bevriezing' van gegevens. De betrokkene kan dit bijvoorbeeld doen als de gegevens niet kloppen en de verantwoordelijke dit nog moet controleren. Of juist om te voorkomen dat de gegevens worden gewist als ze voor de verantwoordelijke niet meer nodig zijn, maar voor de betrokkene nog wel.

Uw antwoord op de vraag:

- ja
- nee

6. Geeft u wijziging(en) in persoonsgegevens door aan derden ('ontvangers')?

Op grond van artikel 19 moet iedere ontvanger in kennis worden gesteld van elke rectificatie, wissing of beperking, zoals benoemd in artikel 16, 17 lid 1 en 18.

Denk bijvoorbeeld aan een verwerker. Als u persoonsgegevens laat administeren door een derde, is het logisch dat u deze correcties, wissingen en bevriezingen doorgeeft aan de verwerker. Hetzelfde geldt natuurlijk als u persoonsgegevens verstrekt aan een derde.

Uw antwoord op de vraag:

- ja
- nee
- niet van toepassing

7. Heeft u een proces voor de overdracht van gegevens?

Artikel 20 stelt dat indien de verwerking berust op toestemming (artikel 6 lid 1 sub a of artikel 9 lid 2 sub a) of de uitvoering van een overeenkomst (artikel 6 lid 1 sub b) en de verwerking via geautomatiseerde procedés wordt verricht, de betrokkene recht heeft om zijn persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. Hij heeft daarnaast het recht om die gegevens ongehinderd aan een andere verwerkingsverantwoordelijke over te dragen.

Nota bene: het recht op overdraagbaarheid bestaat dus niet als de grondslag van de verwerking een andere is dan toestemming of overeenkomst. Als u een andere grondslag hanteert (art. 6 lid 1 sub c t/m f, zoals uitoefening publiek gezag of gerechtvaardigd belang), hoeft u het recht op overdraagbaarheid dus niet in te vullen.

Baseer uw antwoord op uw eerdere antwoorden van de vragen 4.2. Uiteraard alleen als u deze hebt ingevuld.

Uw antwoord op de vraag:

- ja
- nee
- niet van toepassing

8. Heeft u een proces voor het recht van bezwaar?

Artikel 21 stelt dat indien de verwerking berust op de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (artikel 6 lid 1 sub e) of voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke (artikel 6 lid 1 sub f), de betrokkene het recht heeft om, vanwege met zijn specifieke situatie verband houdende redenen, bezwaar te maken tegen de verwerking van zijn persoonsgegevens.

Uw antwoord op de vraag:

- ja
- nee
- niet van toepassing

9. Heeft u een proces voor bezwaar tegen besluitvorming / profilering?

Artikel 22 stelt dat de betrokkene het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Artikel 22 stelt uitzonderingen en daarbij horende regels op voor het verbod op profilering.

Uw antwoord op de vraag:

- ja
- nee

10. Heeft u het naleven van de rechten van de betrokkenen op orde?

Baseer uw antwoord op uw eerdere antwoorden van de vragen 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 en 5.9. Uiteraard alleen als u deze hebt ingevuld.

Uw antwoord op de vraag:

- ja
- nee

Neem maatregelen om de rechten van de betrokkenen op orde te brengen.

6. Informatiebeveiliging

Informatiebeveiliging is de verzameling van organisatorische en technische maatregelen om het risico dat ontstaat bij het werken met informatie, terug te brengen naar een acceptabel niveau.

1. Wilt u de vragen over informatiebeveiliging doorlopen?

   Het goed beveiligen van persoonsgegevens is een belangrijk onderdeel van de bescherming van persoonsgegevens. Deze sectie geeft invulling aan artikel 32.

   Het beantwoorden van de vragen uit deze sectie geeft u geen compleet beeld van uw beveiliging, maar slechts een indicatie.

   Indien u van mening bent dat de beveiliging van persoonsgegevens op orde is, kunt u deze sectie overslaan.

   Uw antwoord op de vraag:

   - ja
   - nee, ga door met vraag 6.8
     We gaan door naar de laatste vraag van deze sectie, waar u uw eindoordeel geeft over informatiebeveiliging.

2. Stuurt de directie in voldoende mate op het veilig omgaan met bedrijfsinformatie?

   De directie draagt het belang van informatiebeveiliging uit, zorgt dat het eigenaarschap van informatie is geregeld, rekent eigenaren af op het eigenaarschap en wordt periodiek op de hoogte gehouden over de staat van informatiebeveiliging middels rapportages. Een ISO-27001 certificering draagt hieraan bij.

   Uw antwoord op de vraag:

   - ja
   - nee
     Gebrek aan aandacht voor bedrijfsinformatie en het veilig omgaan daarmee, is de belangrijkste reden waarom informatiebeveiliging binnen een organisatie geen succes wordt. Breng dit onder de aandacht van de directie.

3. Heeft u iemand aangesteld die informatiebeveiliging voor u organiseert?

   Dit is bijvoorbeeld een information security officer of een externe informatiebeveiligingsadviseur die met enige regelmaat bij u langs komt om uw informatiebeveiliging te organiseren.

   Uw antwoord op de vraag:

   - ja
   - nee
     Het niet hebben van iemand die informatiebeveiliging binnen uw organisatie organiseert, vergroot de kans dat informatie onvoldoende is beveiligd.

4. Heeft u een officieel informatiebeveiligingsbeleid?

   Een beleid dat door de directie is goedgekeurd, welke bij de organisatie bekend is en waar ook naar gehandeld wordt.

   Uw antwoord op de vraag:

   - ja
   - ja, maar het wordt onvoldoende nageleefd
     Door het niet goed naleven van het informatiebeveiligingsbeleid, is het niveau van informatiebeveiliging mogelijk lager dan wenselijk is. Breng dit onder de aandacht van de directie en diegene die verantwoordelijk is voor de verwerking van de persoonsgegevens.
   - nee
     Door het niet hebben van een informatiebeveiligingsbeleid, is het lastig uit te leggen aan de organisatie wat van hen verwacht wordt wat betreft informatiebeveiliging. Zorg dat een informatiebeveiligingsbeleid wordt ingevoerd.

5. Is een risicoanalyse uitgevoerd voor de processen waarbinnen de persoonsgegevens worden verwerkt?

   De risicoanalyse hoeft niet per se recentelijk of speciaal voor deze DPIA te zijn uitgevoerd. Wat

telt is dat de resultaten van de risicoanalyse nog actueel en bruikbaar zijn.

Op www.ravib.nl [8] vindt u een gratis en open source methodiek voor het uitvoeren van een risicoanalyse voor informatiebeveiliging.

Uw antwoord op de vraag:

- ja
- nee, ga door met vraag 6.7
  Goed zicht hebben op de risico's helpt bij het voorkomen van o.a. datalekken. Voer een risicoanayse uit op de processen waarbinnen de persoonsgegevens worden verwerkt om dat zicht te verkrijgen.

6. Geeft het resultaat van de risicoanalyse aan dat de persoonsgegevens in voldoende mate zijn beveiligd?

Denk daarbij aan afspraken rondom toegang tot en gebruik van gegevens, backup van gegevens, hardening van systemen, pseudonimiseren of versleutelen van gegevens, penetratietesten op de betreffende systemen en voldoende bescherming bij koppelingen van of naar het internet.

Uw antwoord op de vraag:

- ja
- nee
  Onvoldoende bescherming vergroot de kans op datalekken. Verbeter de beveiliging van de persoonsgegevens.

7. Kunnen geraakte persoonsgegevens tijdig worden hersteld in het geval van een incident?

Persoonsgegevens worden regelmatig veiliggesteld door middel van een backup. De volledigheid en correctheid van deze backups worden periodiek getest. Gegevens uit een backup kunnen binnen een acceptabele tijd worden teruggezet. Backupmedia worden op een veilige plek bewaard, zodat de beschikbaarheid en vertrouwelijkheid van de daarop opgeslagen gegevens worden gewaarborgd.

Uw antwoord op de vraag:

- ja
- nee
  Het kwijtraken van persoonsgegevens valt ook onder de noemer 'datalek'. Het niet tijdig kunnen terughalen van gegevens uit een backup, kan ook nadelige gevolgen hebben voor een betrokkene.
- weet ik niet
  Verbeter uw zicht op de wijze waarop gegevens binnen uw organsatie worden gebackupt en weer worden hersteld.

8. Heeft u de beveiliging van de persoonsgegevens op orde?

Baseer uw antwoord op uw eerdere antwoorden van de vragen 6.2, 6.3, 6.4, 6.5, 6.6 en 6.7. Uiteraard alleen als u deze hebt ingevuld.

Uw antwoord op de vraag:

- ja
- nee
  U bent hiermee in overtreding van artikel 32. Verbeter uw informatiebeveiliging.

7. Bescherming

Het effect van uw handelen op de bescherming van persoonsgegevens.

1. Wilt u de vragen over bescherming van persoonsgegevens doorlopen?

   De DPIA verwacht een beoordeling van de bescherming van de persoonsgegevens. Dat is meer dan informatiebeveiliging: het gaat ook om procesinhoudelijke aspecten, zoals de doorgifte aan andere organisaties, privacy by design etc.

   Als u deze beoordeling al heeft uitgevoerd voor vergelijkbare processen, kunnen we deze vragen overslaan.

   Uw antwoord op de vraag:

   - ja
   - nee, ga door met vraag 7.7

     We gaan door naar de laatste vraag van deze sectie, waar u uw eindoordeel geeft over bescherming van persoonsgegevens.

2. Is de directie van uw organisatie voldoende bekend met het belang van privacy, de AVG en de verwerkingen die de organisatie uitvoert?

   De juiste aansturing vanuit de directie is noodzakelijk voor een goede omgang met persoonsgegevens binnen uw organisatie.

   Uw antwoord op de vraag:

   - ja
   - nee

     Ga met de directie het gesprek aan over het belang van privacy en gegevensbescherming.

3. Hebben de medewerkers van uw organisatie die met persoonsgegevens in aanraking komen de juiste training en uitleg gehad over privacy, de AVG en de verwerking die zij doen?

   Foutief menselijk handelen is een veel voorkomende oorzaak van incidenten met persoonsgegevens.

   Uw antwoord op de vraag:

   - ja
   - nee

     Zorg voor een juiste training en uitleg over hoe om te gaan met persoonsgegevens.

4. Worden persoonsgegevens verwijderd als deze niet meer noodzakelijk zijn?

   Artikel 5 lid 1 sub e stelt

   > *Persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is, [...]*

   Als u de persoonsgegevens niet meer nodig heeft (als deze niet meer 'noodzakelijk' zijn) moet u die deze dus verwijderen. Dit kan ook betekenen dat u de betreffende records anonimiseert - waardoor het niet meer mogelijk is de records aan een individu te koppelen.

   Uw antwoord op de vraag:

   - ja
   - nee

     Deze verwerking is onbehoorlijk omdat persoonsgegevens niet (afdoende) worden verwijderd. Dit is een risico voor betrokkene omdat er een kans bestaat op datalekkage van gegevens die al verwijderd hadden moeten zijn en omdat er (mogelijk onjuiste / verouderde) gegevens blijven bestaan zonder dat de betrokkene dat verwacht of weet.

5. Heeft u processen ingericht om inbreuken in verband met persoonsgegevens, zoals bedoeld in artikel 34, te melden aan de betrokkenen?

   Door datalekken tijdig te melden, biedt u betrokkenen de mogelijkheid om snel actie te ondernemen om zo de gevolgen voor hen te minimaliseren. Vanwege het belang hiervan loopt u het risico op een boete vanuit de Autoriteit Persoonsgegevens indien u daar niet aan voldoet.

Uw antwoord op de vraag:

- ja
- nee

Richt een proces in om datalekken te melden bij de geraakte betrokkenen.

6. Heeft u de betrokkenen of hun vertegenwoordigers gevraagd naar hun mening over deze verwerking?

Indien 'ja', wat was hun reactie?

Uw antwoord op de vraag:

- ja
- nee

De betrokkenen zijn bij uitstek de meest geschikte personen om aan te vragen of deze verwerking wenselijk of acceptabel is. Neem hun oordeel mee bij uw beslissingen rondom deze verwerking.

7. Heeft u de bescherming van persoonsgegevens op orde?

Baseer uw antwoord op uw eerdere antwoorden van de vragen 7.2, 7.3, 7.4, 7.5 en 7.6. Uiteraard alleen als u deze hebt ingevuld.

Uw antwoord op de vraag:

- ja
- nee

Verbeter de beveiliging van persoonsgegevens.

8. Risico's betrokkenen

Uw beoordeling van de risico's voor de betrokkenen.

1. Lopen de betrokkenen een hoog risico met deze verwerking?

   Houd bij het beantwoorden van deze vraag rekening met de wijze waarop u de persoonsgegevens verwerkt en de maatregelen die u hebt genomen om deze te beschermen.

   Baseer uw antwoord op uw eerdere antwoorden van de vragen 2.4, 2.5, 4.7, 4.9, 4.10, 4.16, 5.10, 6.8 en 7.7. Uiteraard alleen als u deze hebt ingevuld.

   Uw antwoord op de vraag:

   - ja, ga door met vraag 8.3
     De betrokkenen lopen een hoog risico.
   - nee

2. Kan de verwerking grote gevolgen hebben voor de betrokkenen?

   Bijvoorbeeld een automatische beoordeling of score-toekenning, geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg of blokkering van een recht, dienst of contract.

   Uw antwoord op de vraag:

   - ja
     De rechten en vrijheden van de betrokkenen lopen gevaar.
   - nee, ga door met vraag 8.5

3. Gaat u maatregelen nemen om het hoge risico of de grote gevolgen van deze verwerking weg te nemen?

   Baseer uw antwoord op uw eerdere antwoorden van de vragen 8.1 en 8.2. Uiteraard alleen als u deze hebt ingevuld.

   Uw antwoord op de vraag:

   - ja, ga door met vraag 8.5
   - nee
     Het niet wegnemen van de risico's van de betrokkenen, schendt hun rechten en vrijheden.

4. Gaat u contact opnemen met de Autoriteit Persoonsgegevens over het hoge risico van deze verwerking?

   Volgens artikel 36 lid 1 bent u hiertoe verplicht.

   Uw antwoord op de vraag:

   - ja
   - nee
     Het voor u zelf houden van de risico's voor de betrokkenen, schendt hun rechten en vrijheden.

5. Ziet u nog andere mogelijkheden tot verbetering van de gegevensbescherming bij deze verwerking?

   Dit is dus exclusief de maatregelen voor het wegnemen van een eventueel hoog risico.

   Uw antwoord op de vraag:

   - ja
   - nee

De DPIA is hiermee afgerond.

Appendix A: Toelichting bij de vragen

2.1 Wilt u de vragen over de DPIA verplichting doorlopen?

Hulpmiddelen om op voorhand te bepalen of een DPIA verplicht is:

1. De lijst [9] van de Autoriteit Persoonsgegevens
2. Het richtsnoer van de EDPB, opinie 248 [10] over 'hoog risico'

2.2 Houdt de verwerking waarschijnlijk een hoog risico in voor de betrokkene?

De Autoriteit Persoonsgegevens [11] heeft een lijst [12] opgesteld met verwerkingen waarvoor een DPIA verplicht is. Denk vooral aan monitoring, profilering en het volgen van gedrag. De EDPB heeft (in opinie 248) 9 criteria opgesteld, Als u aan twee of meer criteria voldoet, is de DPIA verplicht:

1. Evaluatie of scoretoekenning: zie ook overwegingen 71 en 91;
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wenzelijk gevolg (zoals uitsluiting of discriminatie);
3. Stelselmatige monitoring, met name van openbare ruimten;
4. Gevoelige gegevens of zeer persoonlijk: artikel 9 en 10 data, maar ook e-mails, dagboeken en life-logging etc. (mits uiteraard niet openbaar gemaakt door betrokkene);
5. Grote schaal: zie ook overweging 91. Factoren:
   - aantal betrokkenen;
   - het volume van gegevens;
   - de duur van de verwerkingsactiviteit;
   - geografische omvang van de verwerkingsactiviteit;
6. Combinatie van datasets, vooral als de betrokkene dat niet verwacht (meerdere verwerkingen/verantwoordelijken);
7. Kwetsbare betrokkenen: zie ook overweging 75. Denk aan machtsongelijkheid tussen verantwoordelijke en betrokkenen (werknemers, kinderen, ouderen etc.);
8. Innovatieve toepassingen: zie ook overweging 91. Essentie is dat de persoonlijke en sociale gevolgen nog onbekend zijn;
9. Als betrokkenen door de verwerking een recht niet kunnen uitoefenen of geen beroep op een dienst of overeenkomst kunnen doen (artikel 22, in samenhang met overweging 91). Denk aan screening van klanten.

2.5 Verwerkt u bijzondere persoonsgegevens op grote schaal?

Voor individuele artsen en advocaten geldt:

> *Overweging 91: De verwerking van persoonsgegevens mag niet als een grootschalige verwerking worden beschouwd als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat.*

6.1 Wilt u de vragen over informatiebeveiliging doorlopen?

> *EDPB opinie 250: Een van de vereisten van de AVG is dat persoonsgegevens met behulp van passende technische en organisatorische maatregelen op zodanige wijze worden verwerkt dat een passende beveiliging van de persoonsgegevens wordt gewaarborgd, met inbegrip van bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.*

7.4 Worden persoonsgegevens verwijderd als deze niet meer noodzakelijk zijn?

Het is natuurlijk lastig om te bepalen wanneer de gegevens niet meer nodig zijn. In overweging 39 staat dat "de opslagperiode tot een strikt minimum wordt beperkt". Per proces (verwerking) moet u bepalen op welk moment de gegevens niet meer nodig zijn. Bijvoorbeeld 5 jaar na de transactie vanwege de verjaring van vorderingen of 7 jaar om fiscale redenen. Of op basis van een selectielijst een meer gedetailleerde aanpak. De essentie is dat persoonsgegevens niet onnodig blijven rondhangen.

Appendix B: Verwijzingen naar websites

[1] https://www.privacy-friendly.nl/
[2] https://www.privacy-friendly.nl/files/AVG/verordening 2016 - 679 definitief.pdf
[3] https://www.privacy-regulation.eu/nl/index.htm
[4] https://www.privacy-friendly.nl/dpia
[5] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wanneer-hoef-ik-geen-dpia-uit-te-voeren-5881
[6] https://zoek.officielebekendmakingen.nl/stb-2013-493.html#d16e5466
[7] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf
[8] https://www.ravib.nl/
[9] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667
[10] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[11] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia
[12] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667