Toelichting Pre-DPIA-model

Lees eerst de hieronder opgenomen begrippen uit de AVG. Ken je deze al, ga dan direct naar het Pre-DPIA-model.

Begrippen uit de AVG

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Identificatie kan ook indirect, het hoeft niet altijd een naam te zijn om informatie te kunnen herleiden naar een persoon. Ook maakt de vorm van de informatie niet uit; het kan zowel schriftelijke informatie betreffen, als bijvoorbeeld een foto, film of geluidsopname. Voorbeelden van persoonsgegevens: NAW-gegevens, rekeningnummer, identificatienummer, locatiegegevens, online identificator of elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van een persoon.

Bijzondere persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens, gezondheidsgegevens of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Gevoelige persoonsgegevens: gegevens die naar hun aard gevoelig zijn en daarom extra bescherming behoeven. Hierbij kan gedacht worden aan inloggegevens, financiële gegevens, BSN, locatiegegevens, gegevens waarmee identiteitsfraude gepleegd kan worden, gegevens die onder een wettelijke geheimhoudingsplicht vallen of over minderjarigen/kwetsbare groepen gaan, etc.

Verwerking: alle handelingen die een organisatie kan uitvoeren met persoonsgegevens. Denk aan 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.

Betrokkene: een geïdentificeerde of identificeerbare natuurlijke persoon over wie persoonsgegevens worden verwerkt. Ook bedrijven zonder rechtspersoonlijkheid kunnen, afhankelijk van de structuur, als 'betrokkene' worden aangemerkt. Hierbij kan gedacht worden aan een zzp'er of aan een maatschap waarbij de maten natuurlijke personen zijn (en niet bv's).

Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een dienst of een ander orgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.

Toelichting per vraag (en waar mogelijk de verwijzing naar de AVG).

	A. Inventarisatie	
Nr.	**Toelichting**	**Art. AVG**
A.1.	Licht toe wat de beoogde verwerking van persoonsgegevens inhoudt en in welke context deze plaats gaat vinden. Dus: wat is het doel, waarom is deze nodig, wat zijn de voordelen voor betrokkenen, etc. Geef aan wat de scope is van de (Pre-)DPIA, geef daarbij ook aan wat buiten de scope valt.	5
A.2.	Onder wiens directe verantwoordelijkheid zal de verwerking plaatsvinden? Bijvoorbeeld: 'De proceseigenaar is manager van HR.' Geef ook aan wie eindverantwoordelijk is voor de verwerking. Bijvoorbeeld: 'Eindverantwoordelijk voor dit proces is de directie van ...'	4 sub 7

A.3.	Geef aan van welke categorieën van betrokkenen persoonsgegevens worden verwerkt. Hier bestaat geen uitputtende lijst van. De gegeven voorbeelden zijn veelvoorkomende categorieën en daaraan kun je andere categorieën toevoegen. Geef ook aan wat de relatie van uw organisatie met de betrokkenen is. Bijvoorbeeld: 'De verwerkingsverantwoordelijke heeft een rechtstreekse relatie met de betrokkene, want die heeft een verzekering bij haar afgesloten.' Het is ook mogelijk dat de betrokkene verder af staat van je organisatie, bijvoorbeeld als je zijn data hebt gekregen bij aankoop van een klantenbestand. De relatie, of mogelijk juist het ontbreken van een directe relatie, is van belang bij de beantwoording van de andere vragen, bijvoorbeeld aan welke informatieverplichtingen je tegenover die betrokkene moet voldoen en wat de rechtsgrondslag voor de verwerking is.	30 lid 1.c
A.4.	Geef aan welke categorieën van persoonsgegevens worden verwerkt. Er kan alleen gekozen worden uit de in vraag 4 aangegeven categorieën. Deze zijn gebaseerd op de AVG en de UAVG. Om tot een juiste kwalificatie te komen kun je gebruikmaken van de voorbeelden zoals deze per categorie zijn aangegeven: - Gewone persoonsgegevens, bijvoorbeeld: NAW, telefoonnummer, e-mailadres, leeftijd, geboortedatum. - Gevoelige persoonsgegevens, bijvoorbeeld: BSN, financiële gegevens, beoordelingen, kopie ID en gegevens van kwetsbare personen, bijvoorbeeld van minderjarigen, werknemers, verstandelijk beperkten, ouderen en patiënten. - Bijzondere persoonsgegevens, bijvoorbeeld: medische gegevens, politieke of seksuele voorkeur, religie, ras, etniciteit, vakbondslidmaatschap (art. 9 AVG). - Strafrechtelijke persoonsgegevens, bijvoorbeeld: strafblad, verrichte misdaden (art. 10 AVG).	30 lid 1.c / 9 / 10
A.5.	Geef aan op welke wijze de persoonsgegevens worden verkregen. Bijvoorbeeld, worden de persoonsgegevens: • aangeleverd door betrokkenen zelf? • verkregen van een andere partij? • verzameld door observatie, monitoring of tracking? • Etc. Indien de gegevens afkomstig zijn van een andere partij, moet je altijd nagaan of de verwerking verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (*doelbinding*).	12, 13 en 14
A.6.	Ontvangers zijn partijen buiten jouw organisatie aan wie de persoonsgegevens worden verstrekt. Geef aan of deze ontvangers A) verwerkers zijn of B) andere verwerkingsverantwoordelijken. Een verwerker is een partij waaraan namens jouw organisatie de verwerking van persoonsgegevens wordt uitbesteed (bijvoorbeeld: cloudprovider, administratiekantoor, of een app-leverancier). Een andere verwerkingsverantwoordelijke ontvangt wel persoonsgegevens vanuit jouw organisatie, maar verwerkt die onder eigen verantwoordelijkheid (bijvoorbeeld: UWV, gemeente, arbodienst, ketenpartner).	30 lid 1.d / 28
A.7.	Geef aan in welke landen de verwerking wordt uitgevoerd en of je bij de verwerking persoonsgegevens aan derde landen (= landen buiten de EER) of aan internationale organisaties doorgeeft. Indien het landen buiten de EER betreft, geef dan aan of deze als adequaat zijn aangemerkt door de EU. Zo niet, welke andere passende waarborgen zijn of moeten worden getroffen om de gegevensverwerking mogelijk te laten zijn? Denk hierbij aan de lijst van de Europese Commissie https://ec.europa.eu/info/law/law-topic/data-	28, 30, 45, 46 en 47

	protection/international-dimension-data-protection/adequacy-decisions_en, of aan andere methodes, zoals de Model Clauses of Binding Corporate Rules.	
A.8.	Bepaal welke bewaartermijn(en) van toepassing is/zijn. Soms zijn er meerdere van toepassing (*bijv. fiscale bewaartermijn van 7 jaar, civielrechtelijke verjaringstermijnen van 5 of 20 jaar, voor patiëntendossier van 20 jaar, etc.*). Maak, wanneer er meerdere bewaartermijnen van toepassing zijn, een keuze en leg die keuze en motivering van die keuze vast in dataretentiebeleid en/of privacybeleid. Wanneer je er niet uit komt, vraag het dan aan de gedelegeerd FG of de Privacy Officer (Privacy@saxion.nl).	30 lid 1.f
A.9.	Geef aan wat de doelen van de verwerking van de persoonsgegevens zijn. Voorbeelden hiervan zijn: uitvoeren van een personeelsadministratie, uitvoeren van de zorgovereenkomst, uitvoeren van een leerlingenadministratie, etc.	30 lid 1.b
A.10.	De AVG kent zes grondslagen voor de rechtmatige verwerking van persoonsgegevens. Geef aan welke van toepassing is/zijn. Er kunnen dus meerdere grondslagen van toepassing zijn. Indien dit het geval is, geef deze dan ook aan. De grondslagen zijn: a. Toestemming van de betrokkene b. De noodzaak voor de uitvoering van een overeenkomst c. Om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust d. Ter bescherming van een vitaal belang van de betrokkene of een andere natuurlijke persoon e. De noodzaak voor de vervulling van een taak van algemeen belang of van een taak van de verwerkingsverantwoordelijke in het kader van de uitoefening van openbaar gezag, en f. De noodzaak voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde	6, 9
	B. Analyse of er sprake is van een hoog privacyrisico, zodat een DPIA verplicht is	
B.1.	Volgens art. 35 lid 3 AVG is er in ieder geval sprake van een hoog risico en is een DPIA dus verplicht wanneer de verwerkingsverantwoordelijke: a. geautomatiseerd systematisch en uitgebreid persoonlijke aspecten evalueert, waaronder begrepen profilering, en op basis daarvan besluiten neemt met rechtsgevolgen voor de betrokkene, of die de betrokkene anderszins in aanzienlijke mate treffen; b. op grote schaal bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard verwerkt; c. grootschalig en stelselmatig mensen volgt in openbaar toegankelijke ruimten (bijvoorbeeld door middel van cameratoezicht). Geef aan of een van deze drie criteria toepasselijk is en licht dit toe. Of sprake is van grootschalige verwerking van persoonsgegevens kun je lezen in: - De richtlijnen voor de Functionaris Gegevensbescherming van Working Party 29 16/NL WP 243 rev.01 paragraaf 2.1.3 - De uitleg van de AP over grootschaligheid voor zorgaanbieders in het nieuwsbericht van de AP https://autoriteitpersoonsgegevens.nl/nl/nieuws/uitleg-begrip-%E2%80%98grootschalig%E2%80%99-verduidelijkt-voor-alle-zorgaanbieders	35 lid 3
B.2.	Naast de criteria uit art. 35 lid 3 AVG, heeft de AP een lijst opgesteld met 17 soorten verwerkingen waarbij het uitvoeren van een DPIA verplicht is. Beoordeel de verwerking in relatie tot deze lijst en geef aan of 'Ja' dit inderdaad de situatie is, dan wel 'Nee' indien dit niet het geval is, en beschrijf ook waarom (dus bijvoorbeeld wanneer je van oordeel bent dat een verwerking valt onder de categorie '1. Heimelijk onderzoek', motiveer dan waarom je denkt dat deze onder die categorie valt). De soorten zijn: 1. Heimelijk onderzoek. 2. Zwarte lijsten. 3. Fraudebestrijding. 4. Creditscores. 5. Financiële situatie. 6. Genetische persoonsgegevens. 7. Gezondheidsgegevens. 8. Samenwerkingsverbanden. 9. Cameratoezicht. 10. Flexibel cameratoezicht. 11. Controle	35 lid 4

	werknemers. 12. Locatiegegevens. 13. Communicatiegegevens. 14. Internet of things. 15. Profilering. 16. Observatie en beïnvloeding van gedrag. 17. Biometrische gegevens.	
B.3.	Naast de criteria zoals genoemd in art. 35 lid 3 AVG en de lijst van de AP heeft ook WP29 (EDPB) een lijst opgesteld van negen criteria waarbij, indien er minimaal twee van toepassing zijn, een DPIA verplicht is. Beoordeel of er twee of meer van toepassing zijn, en zo ja, beschrijf ook waarom. De criteria zijn: 1. Beoordelen van mensen op basis van persoonskenmerken/profilering. 2. Geautomatiseerde beslissingen. 3. Stelselmatige en grootschalige monitoring. 4. Gevoelige gegevens. 5. Grootschalige gegevensverwerkingen. 6. Gekoppelde databases. 7. Gegevens over kwetsbare personen. 8. Gebruik van nieuwe technologieën. 9. Blokkering van een recht, dienst of overeenkomst.	70
B.4.	Geef aan welke (andere) omstandigheden kunnen spelen die maken dat er sprake is van een dusdanige hoogrisicoverwerking dat een DPIA nodig is. Bijvoorbeeld indien een van de in B.3 genoemde criteria speelt, zoals het gebruik van nieuwe technologieën in combinatie met een andere genoemde categorie. Geef daarbij ook aan wat de eventuele nadelige gevolgen zijn voor de rechten en vrijheden van de betrokkenen bij deze verwerking.	
B.5.	Wanneer je een of meer van de vragen B.1 tot en met B.4 met 'Ja' beantwoordt, dan is er sprake van een dusdanig hoog privacyrisico voor betrokkenen dat een DPIA verplicht is. Vermeld hier de beslissing en motiveer deze. -> de PO kijkt hierop mee!	

	C.1. Vaststellen beheersmaatregelen	
Nr.	**Toelichting**	**Art. AVG**
C.1.	Ook wanneer er geen DPIA nodig is, is het toch van belang om voor de tijdens de Pre-DPIA geconstateerde risico's passende beheersmaatregelen te formuleren en deze vervolgens voor de start van de verwerking te implementeren. Wanneer je bijvoorbeeld het risico constateert dat je organisatie persoonsgegevens via onbeveiligde e-mail verstuurt, is de beheersmaatregel: 'Zorg voor beveiligde mail of encryptie van de inhoud in de mail waarin je persoonsgegevens verstuurt.'	24

	C.2. Uitvoering Pre-DPIA, ondertekening door proceseigenaar/directie en oordeel FG	**Art. AVG**
C.2.	Leg hier vast door wie de Pre-DPIA is ingevuld. Het is mogelijk dat verschillende delen van de Pre-DPIA door verschillende personen zijn ingevuld. Vermeld hun naam en functie en het tijdstip waarop zij dit hebben gedaan. De uitkomsten van de Pre-DPIA moeten worden beoordeeld door de Privacy Officer (PO). Neem het advies van de PO op. Ook moet namens de verwerkingsverantwoordelijke de proceseigenaar, of, indien die ontbreekt, de directie voor akkoord tekenen.	39 lid 1 sub c