AVG: PIA's en Compliance

Welke eisen stelt de Algemene Verordening Gegevensbescherming?

Utrecht, Juni 2017
Versienummer: 1.0

Colofon

AVG: PIA's en Compliance
Welke eisen stelt de Algemene Verordening Gegevensbescherming?

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

Auteurs
SURFnet

Juni 2017

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

1. Inleiding

Op 25 mei 2016 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. De AVG is de Europese verordening die de zorgvuldige verwerking van persoonsgegevens regelt. Deze verordening heeft directe werking binnen de Europese Unie. Hoewel de AVG al wel in werking is getreden, is deze nog niet formeel van kracht. Er geldt een implementatietermijn van twee jaar. Vanaf 25 mei 2018 geldt de AVG dus daadwerkelijk en komt de huidige wet rond persoonsgegevens, de Wet bescherming persoonsgegevens (Wbp) te vervallen.
Er is al een hoop gezegd en geschreven over de nieuwe verordening en de impact die dit gaat hebben op organisaties. Hoewel de beginselen rond de bescherming van persoonsgegevens niet veel veranderen (de AVG en Wbp hebben veel gelijkenissen) zijn bepaalde onderwerpen verder gespecificeerd en ligt de nadruk op accountability; je moet als organisatie kunnen aantonen dat je je aan de regels houdt en hier transparant over zijn. Ook zijn er aanzienlijke boetes als je je niet aan de AVG houdt.
Een veel gehoorde term als het gaat om de AVG is het Privacy Impact Assessment, afgekort de PIA. De AVG stelt een dergelijke impact assessment in bepaalde gevallen verplicht. Wat deze PIA precies inhoudt is niet altijd even bekend bij organisaties en het voldoen aan deze eis wordt dan lastig. Daarbij zijn er verschillende soorten PIA's in omloop en ook de tooling om hierbij te ondersteunen wordt steeds meer aangeboden
.
Deze notitie is bedoeld om meer inzicht te geven in wat een PIA nu precies is en welke onderdelen in een PIA kunnen zitten. Daarbij wordt de PIA ook in een breder kader rondom gegevensbescherming geplaatst en wordt ingegaan op hoe de PIA zich verhoudt tot het compliant zijn aan de AVG. Dit is belangrijk, omdat deze zaken vaak door elkaar heen lopen. Door een beter besef te hebben over het doel van de PIA en de (on)mogelijkheden, kun je als organisatie een betere keuze maken welk soort PIA het beste past en welke tooling hierbij kan ondersteunen. Uitgangspunt van de notitie hierbij is: er is niet één soort PIA die altijd voor iedereen geschikt is. "One size fits all…but it doesn't".

2. Privacy Impact Assessment

2.1. Inleiding

Dit hoofdstuk gaat in op wat er in de AVG te vinden is over de PIA. Daarbij is gekeken naar de bepalingen en overwegingen uit de verordening. Doel van deze juridische context is om uiteen te zetten wat een PIA volgens de AVG is en ten minste zou moeten bevatten. En wanneer een PIA wel of niet verplicht is. Dit biedt vervolgens de basis voor het verder onderzoeken wat er nog meer aan een PIA kan worden toegevoegd.

2.2. Juridische context

2.2.1. Wanneer moet je een PIA doen?

De term Privacy Impact Assessment komt in de AVG als zodanig niet voor. Er is gekozen voor de term 'gegevensbeschermingseffectbeoordeling"(GEB). In het Engels wordt gesproken over een "data protection impact assessment" (DPIA). In het kader van de leesbaarheid en herkenbaarheid gaat deze notitie toch uit van de term PIA, maar strikt genomen wordt dus de GEB bedoeld.

De PIA komt aan bod in artikel 35 van de AVG. Lid 1 van het artikel luidt als volgt:

> **Gegevensbeschermingseffectbeoordeling**
>
> 1.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 voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

Wat allereerst opvalt is dat er geen definitie wordt gegeven voor wat een PIA nu eigenlijk is. Wel wordt aangegeven wanneer je een PIA zou moeten doen. Kort gezegd moet je een PIA doen als de verwerking een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Daarbij gaat het dus niet om eventuele risico's voor de organisatie.
De vraag is hoe je de risico's beoordeelt. Het artikel geeft een aantal aanknopingspunten. Er moeten worden gekeken naar:

- De aard van de verwerking
- De omvang van de verwerking
- De context van de verwerking
- De doeleinden van de verwerking
- Het gebruik van nieuwe technologieën

Aan de hand van deze punten moet worden bepaald of de verwerking waarschijnlijk een hoog risico inhoudt voor de betrokkene(n). De AVG noemt daarnaast in lid 3 nog een aantal voorbeelden wanneer een PIA met name vereist is:

- Systematische en uitgebreide beoordeling van persoonlijke aspecten, gebaseerd op geautomatiseerde verwerking (profilering)
- Grootschalige verwerking van bijzondere persoonsgegevens

- Stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten

> 3. Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:
>
> a) 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;
>
> 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; of
>
> c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Het is aan een organisatie om zelf de afweging te maken of er sprake is van een waarschijnlijk hoog risico en een PIA dus een verplichting is. De AVG geeft nog wel een extra handvat. In lid 4 staat dat de toezichthoudende autoriteit (in Nederland de Autoriteit Persoonsgegevens) een lijst van soorten verwerkingen opstelt waarvoor een PIA verplicht is. En in lid 5 staat dat de Autoriteit ook een lijst kan opstellen voor soorten verwerkingen waar geen PIA voor is vereist.

De AVG noemt in artikel 35 AVG nog een aantal relevante punten:

- Indien een organisatie een Functionaris Gegevensbescherming (FG) heeft aangesteld, dient bij een PIA advies bij de FG worden ingewonnen (lid 2);
- De organisatie kan in voorkomend gevallen ook betrokkenen (of hun vertegenwoordiging) naar hun mening vragen over de voorgenomen verwerking (lid 9).

2.2.2. Waar bestaat een PIA uit?

Als je op basis van bovengenoemde punten hebt geconcludeerd dat een PIA noodzakelijk is, wat moet je dan doen? De richtlijnen zijn te vinden in artikel 35 lid 7 AVG. Daar worden vier punten genoemd.

7.De beoordeling bevat ten minste:

a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;

b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;

c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en

d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

De vier onderdelen van een PIA volgens de AVG zijn als volgt:

1. Een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden. En indien van toepassing de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd.

Allereerst moet je beschrijven welke persoonsgegevens je wilt verwerken en met welke doeleinden. Oftewel: wat wil je en waarom? Daarnaast is het relevant of je de gegevens wilt verwerken onder de grondslag ‘gerechtvaardigd belang’.[1]

2. Een beoordeling van de noodzaak en de evenredigheid van de verwerking, met betrekking tot de doeleinden die je eerder hebt vastgesteld.

In deze stap moet je je afvragen of de persoonsgegevens die je wilt verwerken wel noodzakelijk zijn om je doel te behalen. En of je bijvoorbeeld niet hetzelfde kan bereiken met minder gegevens. Het gaat hier om proportionaliteit en subsidiariteit. Je zou na deze stap ook de conclusie kunnen trekken dat je niet aan de verwerking moet beginnen.

3. Een beoordeling van de risico’s voor de rechten en vrijheden van natuurlijke personen.

Bij deze stap staat de vraag centraal welke risico’s de betrokkenen lopen als deze verwerking gaat plaatsvinden. Denk daarbij aan risico’s als inbreuk op de persoonlijke levenssfeer, identiteitsfraude, benadeling, (maatschappelijke) uitsluiting, willekeur etc. Het gaat niet alleen om risico’s die ontstaan als er persoonsgegevens uitlekken of verkeerd worden gebruikt, maar ook als de verwerking plaatsvindt zoals deze is bedoeld. Ook dan kan er bijvoorbeeld een risico tot willekeur ontstaan.

4. De beoogde maatregelen om de risico’s aan te pakken om de bescherming van persoonsgegevens te garanderen.

[1] Er zijn verschillende grondslagen om persoonsgegevens te mogen verwerken, zoals toestemming van de betrokkenen, op grond van een contract of op grond van een wettelijke plicht. Gerechtvaardigd belang is ook een grondslag, maar dat kan alleen als je een afweging maakt tussen jouw noodzakelijke gerechtvaardigde belangen en de privacy schending richting de betrokkenen en je kunt concluderen dat jouw belang zwaarder weegt dan de privacy van de betrokkenen (zie artikel 6 lid f AVG).

Als je bij stap 3 de risico's in kaart hebt gebracht, is het bij stap 4 het moment om met maatregelen te komen die risico's zoveel mogelijk te beperken. Daarbij kun je denken aan extra beveiligingsmaatregelen, maar ook aan kwaliteitswaarborgen die bijdragen aan het accuraat, juist en actueel zijn van de persoonsgegevens. Of extra transparantie richting de betrokkene, onafhankelijk toezicht, extra audits etc. Denk niet alleen aan technische maatregelen, maar ook aan organisatorische maatregelen die risico's kunnen beperken. Het gaat hier niet alleen om maatregelen die je volgens de AVG sowieso al moet treffen, zoals passende beveililging, het sluiten van bewerkersovereenkomsten en ingaan op inzageverzoeken van de betrokkenen. Het gaat juist om extra maatregelen of een specifieke inrichting van de wettelijke vereisten. Ook bij deze stap is het mogelijk dat ondanks de maatregelen de risico's hoog blijven en dat de voorgenomen verwerking niet op de voorgenomen manier moet plaatsvinden.

2.3. Een voorbeeldcasus

Om de bovenstaande stappen meer te laten leven volgt nu een voorbeeldcasus. Hierbij is ten behoeve van de duidelijkheid gekozen voor een extreem voorbeeld en is de PIA slechts in heel beperkte mate uitgewerkt.

Fictieve casus: een instelling is voornemens om gebruik van leeromgevingen te monitoren en aan de hand daarvan een docent te laten beoordelen of een student wel of niet mag deelnemen aan een tentamen.

Stap 1: Het gaat om de verwerking van logging en metadata rond het gebruik van leeromgevingen: welke documenten, filmpjes en opdrachten heeft een student bekeken, voor hoe lang en op welk tijdstip. Het doel van de verwerking is het verbeteren van het onderwijs, door studenten te verplichten om digitaal lesmateriaal tot zich te nemen voorafgaande aan een tentamen. Als grondslag geldt gerechtvaardigd belang van de instelling; het kost de instelling veel geld als studenten onvoorbereid naar tentamens gaan en niet binnen de gestelde tijd slagen voor een opleiding.

Stap 2: De verwerking is niet noodzakelijk, omdat je ook op andere wijzen het beoogde doel kan worden bereikt. Maar dan met minder ingrijpende verwerking van persoonsgegevens. Het is ook niet erg proportioneel om zoveel gevoelige gegevens te verwerken. De gegevens kunnen inzicht geven in het levenspatroon van de student en dat weegt waarschijnlijk niet op tegen het belang van de instelling.

Je zou nu al de conclusie kunnen trekken om de verwerking niet te laten plaatsvinden en verder te kijken naar alternatieven, maar om alle stappen te doorlopen, gaan we toch door met de volgende stap.

Stap 3: De risico's voor de betrokkenen, de studenten, zijn onder andere benadeling en willekeur. Een student kan benadeeld worden, omdat hij ten onrechte niet aan een tentamen mag meedoen. Stel dat hij de leeromgeving via een medestudent heeft bezocht, of zijn kennis voornamelijk uit een boek heeft gehaald. Of in een eerdere fase van zijn studie de kennis al heeft opgedaan en dus geen behoefte heeft aan nog een keer digitaal stof tot zich te nemen. En willekeur kan optreden als de beoordeling van de gegevens niet goed vastligt. Een docent kan de voorkeur geven aan bepaalde studenten, die bijvoorbeeld overdag inloggen in plaats van enkel 's nachts en enkel de dagen voor het tentamen. Ook kunnen docenten elk tentamen weer andere beoordelingscriteria hanteren.

Stap 4: Te nemen maatregelen

Verkleining van het risico van willekeur is bijvoorbeeld mogelijk door:

- Een gedegen procedure rond de beoordeling op te stellen
- Transparant zijn richting studenten over hoe de beoordeling plaatsvindt

- De beoordeling niet door de docent zelf laten doen en/of deels geautomatiseerd laten uitvoeren.

Mogelijke opties om het risico van benadeling te verminderen zijn:

- Het tijdstip dat iemand inlogt wordt niet bij de beoordeling meegenomen
- De student de mogelijkheid geven op een andere manier aan te tonen dat hij de stof tot zich heeft genomen.

Aan de hand van de te nemen maatregelen moet vervolgens worden beoordeeld of de verwerking wel of niet kan plaatsvinden. Het kan zijn dat ook met de maatregelen de risico's voor de betrokkenen nog te groot zijn.

Bovenstaande uitwerking is heel beperkt. Het voorbeeld geeft wel een beeld hoe je door middel van een PIA tot nadenken wordt gezet over wat de verwerking betekent voor een betrokkene en hoe je de risico's zoveel mogelijk kunt beperken. Daarbij gaat het juist om maatregelen waardoor de verwerking wordt beperkt, anders wordt ingericht en/of om goede procedures op te stellen.
Om de stappen uit de PIA goed te doorlopen en een volledig zicht te hebben op wat de verwerking precies inhoudt en wat de risico's zijn, is het goed om de PIA door meerdere personen uit verschillende disciplines te laten uitvoeren en hierbij ook de proces- of systeemeigenaar te betrekken. Ook kan het wenselijk zijn de betrokkenen, of hun vertegenwoordigers naar hun mening te vragen over de voorgenomen verwerking. Een verwerking die grosso modo prima gevonden wordt, zou eerder acceptabel zijn.
De uitwerking kan anders zijn dan hierboven beschreven. Er zijn ook verschillende werkwijzen mogelijk, bijvoorbeeld via een vragenlijst of een workshop. Wat de voorkeur heeft hangt sterk van de organisatie af. Meer over de tooling en vorm van de PIA in hoofdstuk 4.

2.4. Wat als een PIA niet noodzakelijk is?

Als je als organisatie oordeelt dat de betrokkenen waarschijnlijk geen hoog risico lopen, bijvoorbeeld omdat er slechts beperkt persoonsgegevens worden verwerkt, ben je er dan qua bescherming van persoonsgegevens? Nee zeker niet. Ook als een PIA niet noodzakelijk is, moet je je nog steeds houden aan de eisen en principes uit de AVG rond een zorgvuldige verwerking van persoonsgegevens. Denk bijvoorbeeld aan het rechtmatig verwerken van persoonsgegevens (heb je een rechtmatige grondslag om te verwerken), het vaststellen van doeleinden rond de verwerking, het nemen van passende technische en organisatorische beveiligingsmaatregelen, het afsluiten van bewerkersovereenkomsten, het voldoen aan de documentatieplicht, zorgen voor dataminimalisatie en het kunnen voldoen aan verzoeken vanuit betrokkenen die hun rechten uitoefenen (recht op inzage, aanpassing, wissing, bezwaar etc).
Bovenstaande vereisten en daaruit voortvloeiende maatregelen zijn op zichzelf geen maatregelen die voortvloeien uit een PIA, omdat je je hieraan, los van de risico's voor de betrokkenen, altijd aan moet houden. Het zijn dus geen extra waarborgen en maatregelen. Meer over de eisen uit de AVG in hoofdstuk 3.

Bij veel organisaties ligt de focus vooral op compliance met de AVG: het is een hele kluif om aan de vereisten en maatregelen te voldoen. Daardoor komt het regelmatig voor dat in de PIA de aandacht vooral uitgaat naar deze vereisten. Daardoor verdwijnen de risicoanalyse en het beoordelen van de noodzakelijkheid van de verwerking, punten die in de PIA centraal staan, nog wel eens naar de achtergrond. Er zijn daarbij twee gevaren:

1. Compliance komt niet aan de orde bij verwerkingen waar geen PIA wordt gedaan;
2. De PIA wordt als voldoende beschouwd voor compliance.

Het is daarom goed om de PIA en compliance los van elkaar te kunnen zien. Een PIA kan dus wel een deel compliance bevatten, maar kan ook los daarvan worden behandeld.
Een voordeel van het lostrekken van de PIA en compliance is dat je deze onderdelen op verschillende momenten aan de orde kunt stellen, bijvoorbeeld in de voortgang van een project. Stel je de

eerdergenoemde voorbeeldcasus voor. Je wilt de PIA in een vroeg stadium uitvoeren, zodat je nog makkelijk kunt stoppen of aanpassingen kunt doen in de voorgenomen verwerking. Maar dat hoeft niet altijd ook een goed moment te zijn om aan alle vereisten uit de AVG te voldoen. Zo is het niet ondenkbaar dat de leveranciers, met wie je contracten moet afsluiten, in dat vroege stadium nog niet bekend zijn. Ook kan de beveiliging nog niet (helemaal) op orde zijn of ontbreken de procedures rond de rechten van betrokkenen nog. Op die manier houd je de PIA nog betrekkelijk klein aan het begin. Je focust je dan in de loop van het traject op de andere maatregelen.
Er zijn natuurlijk scenario's denkbaar waar het wél wenselijk is om de compliance meteen mee te nemen. Het is aan de organisatie om hier een weloverwogen keuze te maken.

2.5. Samenvattend

De AVG is vrij duidelijk in wat een PIA zou moeten bevatten, maar is minder specifiek over de uitvoering en uitwerking. De norm van een waarschijnlijk hoog risico is een open norm. Duidelijk is dat de betrokkene centraal staat en dat het doel van de PIA is dat de mogelijke risico's voor de betrokkenen zoveel mogelijk worden beperkt. Dit kan los staan van het voldoen aan de andere eisen van de AVG. Compliant zijn aan de AVG geldt ook als een PIA strikt genomen volgens de AVG niet hoeft.
Een en ander is samen te vatten in een zeer vereenvoudigd pijlenschema:

In dit hoofdstuk zijn de vier stappen van de PIA volgens de AVG aan bod gekomen. In het volgende hoofdstuk wordt verder ingegaan op de vereisten die verder in de AVG staan en welke maatregelen hieruit voortvloeien. Vervolgens wordt in hoofdstuk 4 nog ingegaan op hoe je een PIA zou kunnen inrichten, hoe je deze wel of niet aan compliance koppelt en welke vormen van tooling er zijn.

3. Compliance

3.1. Inleiding

Zoals in hoofdstuk 2 is beschreven, betekent een PIA uitvoeren niet meteen dat je aan alle eisen voldoet die de AVG stelt op het gebied van een zorgvuldige verwerking van persoonsgegevens. Je kunt natuurlijk compliance onderdeel maken van de PIA. Om te kunnen bepalen in hoeverre dat binnen een organisatie wenselijk is, is het goed om te weten hoe de vereisten van de AVG zich verhouden tot de eisen van de PIA. Daar gaat dit hoofdstuk over. Eerst wordt globaal de juridische context beschreven. Vervolgens wordt de vraag uitgewerkt in hoeverre dit overlapt met de PIA en waar de mogelijkheden zitten om deze twee te combineren.

3.2. Juridische context

De AVG is alleen van toepassing als er sprake is van verwerking van persoonsgegevens, binnen het toepassingsgebied van de AVG.

Onder persoonsgegevens en betrokkene wordt verstaan (artikel 4):

Definities

1. „persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene) "als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online 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.

Een verwerking is iedere handeling met persoonsgegevens, zoals bijvoorbeeld het inzien, opslaan wissen en ordenen. [2]

Definities

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

Het materiële toepassingsgebied
Op welke verwerking de AVG van toepassing is, is in principe de geheel of gedeeltelijk geautomatiseerde verwerking, maar ook de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. [3] Met bestand wordt elk

[2] Artikel 4 lid 2 AVG
[3] Zie artikel 2 AVG voor uitzonderingen op deze regel

gestructureerd geheel van persoonsgegevens bedoeld, die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.[4] Ook een papieren kopie van een geautomatiseerde verwerking valt onder het regime van die geautomatiseerde verwerking.

Het territoriale toepassingsgebied
Naast het materiele toepassingsgebied is er ook nog een territoriale scope en een territoriaal toepassingsgebied.[5] Scope: De AVG is van toepassing bij verwerkingen van persoonsgegevens van betrokkenen die verblijven binnen de Europese Economische ruimte (de EU, Liechtenstein, Noorwegen en IJsland), ongeacht waar de verwerkingsverantwoordelijke is gevestigd.
Territoriaal toepassingsgebied: De AVG is van toepassing op de verwerking van persoonsgegevens door een verantwoordelijke of verwerker die een hoofd- of nevenvestiging in de Unie heeft, ongeacht of de verwerking in de Unie plaatsvindt en ongeacht of de Europese vestiging ook verwerkingen uitvoert.
Als je hebt bepaald dat je persoonsgegevens verwerkt binnen het toepassingsgebied van de AVG, dan moet je je houden aan de regels in de AVG. De AVG kent allereerst een aantal beginselen rond de verwerking van persoonsgegevens.[6] Aan de hand van deze beginselen zullen een aantal belangrijke vereisten uit de AVG worden besproken. Dit is geen volledig overzicht, maar geeft wel inzicht in waar je bij het verwerken van persoonsgegevens zoal rekening mee moet houden.

3.2.1. Beginselen

De AVG gaat uit van een aantal basisbeginselen waaraan elke verwerking moet voldoen.

3.2.1.1. Rechtmatigheid, behoorlijkheid en transparantie:
Dit beginsel houdt in dat het voor betrokkenen inzichtelijk moet zijn welke persoonsgegevens worden gebruikt en op welke manier. Informatie en communicatie hierover moet dus eenvoudig toegankelijk en begrijpelijk zijn in duidelijke en eenvoudige taal. Daarnaast moet het voor betrokkenen ook inzichtelijk zijn welke risico's, regels, waarborgen en rechten ze hebben en hoe ze onder de AVG hun rechten kunnen uitoefenen. Rechtmatig betekent hier (vrij vertaald): 'netjes handelen'.

Om de verwerking rechtmatig te laten zijn, moet je een van de in de AVG genoemde grondslagen hebben om te mogen verwerken. De AVG kent zes grondslagen: 1 toestemming van de betrokkene voor een of meer specifieke doeleinden; 2 noodzakelijk voor uitvoering van de overeenkomst waarbij de betrokkene partij is of op verzoek van betrokkene vóór het sluiten van de overeenkomst; 3 noodzakelijk voor voldoen aan een wettelijke verplichting; 4 een vitaal belang van een of meer personen beschermen, 5 vervulling van een taak van algemeen belang of een taak voor het openbaar gezag en 6 gerechtvaardigd belang.

Elke grondslag kent ook weer voorwaarden. Zo moet de toestemming een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting zijn, die actief moet worden gedaan. Ook moet het even eenvoudig zijn om toestemming te geven als om deze in te trekken.
En bij gerechtvaardigd belang moet je een belangenafweging maken en heeft betrokkene het recht bezwaar te maken tegen de verwerking onder deze grondslag.
De verwerking moet transparant zijn richting de betrokkene. De betrokkene moet geïnformeerd worden als zijn of haar persoonsgegevens worden verwerkt en moet ook weten voor welk doel en op basis van welke grondslag. Dergelijke informatie wordt vaak opgenomen in een privacy statement dat bijvoorbeeld voorafgaande aan de verwerking wordt getoond en die verder in te zien is via de website van de organisatie. Een betrokkene mag ook inzicht vragen in welke persoonsgegevens worden

[4] Artikel 4 lid 6 AVG
[5] Zie artikel 1 lid 2 en artikel 3 AVG
[6] Artikel 5 AVG

verwerkt en met wie deze worden gedeeld. De organisatie moet de betrokkene informeren hoe een dergelijk verzoek kan worden ingediend.
Naast het recht op informatie en inzage hebben betrokkenenrecht op wijziging, recht om vergeten te worden (in bepaalde gevallen), recht om bezwaar te maken tegen de verwerking en het recht om persoonsgegevens overgedragen te krijgen.

3.2.1.2. Doelbinding:
Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld worden en vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt

3.2.1.3. Minimale gegevensverwerking (Dataminimalisatie):
Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt blijven tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt. Je mag dus niet méér persoonsgegevens verwerken dan strikt noodzakelijk is voor het doel. Dat betekent ook dat ze zo snel mogelijk moeten worden gewist of onherkenbaar worden gemaakt (tenzij dat in strijd is met andere wetgeving). Je mag ook weer niet te weinig gegevens verzamelen, omdat dan het beeld van de betrokkene onjuist kan zijn, Ook mogen geen persoonsgegevens worden verwerkt als het doel redelijkerwijs op een andere manier te bereiken is, bijvoorbeeld met geaggregeerde gegevens. Het ‘handig’ zijn, of ‘omdat het kan’ zijn geen argumenten om persoonsgegevens te verwerken, om er meer te verwerken of langer te bewaren dan strikt noodzakelijk.

3.2.1.4. Juistheid:
Persoonsgegevens moeten juist én actueel zijn. Blijken gegevens onjuist of achterhaald dan moeten ze worden gewist. De verantwoordelijke dient daarvoor actief zorg te dragen. Het is belangrijk dat persoonsgegevens kloppen en dat er waarborgen zijn om de kwaliteit hoog te houden. Dit wordt nog belangrijker als persoonsgegevens gedeeld worden met derden en mogelijke onjuistheden verder verspreid worden. De betrokkene heeft het recht om wijziging van de gegevens te verzoeken of te wissen als zijn of haar persoonsgegevens onjuist zijn.
Zoals ook onder het beginsel van transparantie genoemd, is het daarvoor belangrijk dat de betrokkene weet welke gegevens worden verwerkt en weet waaraan te kloppen als er iets mis is.

3.2.1.5. Opslagbeperking:
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 bewaard noodzakelijk is. Dit beginsel dient ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan voor de verwerking noodzakelijk is. Voor elke verwerking moet je vaststellen hoe lang je de persoonsgegevens nodig hebt. Na het aflopen van de termijn moeten de persoonsgegevens worden verwijderd of worden geanonimiseerd. Bij het vaststellen van de termijnen moet je kijken naar de wettelijke bewaartermijnen en de noodzaak van bewaren. Daarbij is oneindig opslaan in principe nooit juist. Er zal altijd een termijn moeten worden bepaald. Deze kan per (categorie) persoonsgegeven (die) dat je verwerkt verschillen.

3.2.1.6. Integriteit en vertrouwelijkheid:
“Persoonsgegevens moeten door passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging gewaarborgd is, en dat ze onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.” Wat passend is hangt af van de persoonsgegevens die je verwerkt. Zo gelden er voor bijzondere persoonsgegevens (zoals medische gegevens, of gegevens over iemands religie) strengere eisen, omdat de risico’s voor de betrokkenen groter zijn als de gegevens onverhoopt uitlekken. Bijzondere persoonsgegevens mogen overigens enkel worden verwerkt als de AVG dat toestaat.

Mochten persoonsgegevens onrechtmatig zijn verwerkt of heeft iemand er toegang toe gehad die er niet bij mocht, is dit een datalek. Het datalek zal beoordeeld moeten worden door de organisatie en aan de hand daarvan moet het datalek mogelijk aan de toezichthouder en/of betrokkenen worden gemeld. De Autoriteit Persoonsgegevens heeft beleidsregels gepubliceerd over de meldplicht datalekken. [7]

3.2.1.7. Verantwoordingsplicht:

De AVG legt het voldoen aan de zes beginselen expliciet bij de verwerkingsverantwoordelijke. Deze dient er niet alleen op toe te zien dat de beginselen worden nageleefd, maar (belangrijker) moet dit ook kunnen aantonen. Bijvoorbeeld als de toezichthouder hier om verzoekt. Dit vraagt om goede documentatie en beschrijving van procedures. Deze plicht is een belangrijke toevoeging op de nu geldende Wet bescherming persoonsgegevens.

Documentatieplicht:
De AVG noemt ook een documentatieplicht. Elke verwerkingsverantwoordelijke moet een register van de verwerkingsactiviteiten bijhouden die onder zijn verantwoordelijkheid plaatsvinden. De AVG benoemt de gegevens die hierin moeten staan. Op deze plicht geldt de uitzondering voor ondernemingen of organisaties met minder dan 250 werknemers tenzij het waarschijnlijk is dat de verwerking een risico inhoudt voor de rechten en vrijheden van de betrokkenen, de verwerking niet incidenteel is, of de verwerking bijzondere categorieën van gegevens, of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten betreft.

3.3. Een voorbeeldcasus

We nemen net als in hoofdstuk 2 de volgende, ietwat extreme, voorbeeldcasus.

Fictieve casus: een instelling is voornemens om gebruik van leeromgevingen te monitoren en aan de hand daarvan een docent te laten beoordelen of een student wel of niet mag deelnemen aan een tentamen.

In hoofdstuk twee hebben we een korte PIA uitgevoerd. Daar hebben we de gegevensverwerking als volgt gespecificeerd: de verwerking van logging en metadata rond het gebruik van leeromgevingen: welke documenten, filmpjes en opdrachten heeft een student bekeken, voor hoe lang en op welk tijdstip. Het doel van de verwerking is het verbeteren van het onderwijs, door studenten te verplichten om digitaal lesmateriaal tot zich te nemen voorafgaande aan een tentamen. Als grondslag geldt gerechtvaardigd belang van de instelling; het kost de instelling veel geld als studenten onvoorbereid naar tentamens gaan en niet binnen de gestelde tijd slagen voor een opleiding. Er zijn twee mogelijke risico's benoemd: benadeling en willekeur. Vervolgens zijn een aantal maatregelen beschreven, die de risico's die we zien voor de betrokkenen (de studenten in dit geval) te beperken. Dit zijn de volgende maatregelen:

- Het opstellen van een gedegen procedure rond de beoordeling;
- Transparant zijn over de beoordeling richting studenten;
- De beoordeling niet door de docent laten uitvoeren;
- Tijdstip van inloggen niet laten meewegen;
- Studenten laten aantonen hoe ze op andere wijze de stof tot zich hebben genomen.

Als we nu kijken naar de maatregelen die voortvloeien uit de AVG, zien we allereerst een deel overlap. Het benoemen van de verwerking, de doeleinden en de grondslag van verwerking. Als

[7] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf

verantwoordelijke van de verwerking moet je deze punten altijd vaststellen. Ook het beoordelen of je alle gegevens daadwerkelijk nodig hebt, overlapt (zie het beginsel van dataminimalisatie). De overige maatregelen die voortvloeien uit de AVG komen echter niet per se overeen met de maatregelen die uit de PIA zijn gerold. Kijkend naar de eerdere beschreven beginselen, kun je denken aan de volgende maatregelen:

- Passende technische en organisatorische maatregelen treffen om de persoonsgegevens te beschermen tegen onrechtmatige verwerking;
- Bewerkersovereenkomsten afsluiten met eventuele hulpleveranciers. Denk hierbij aan de beheerpartij die het systeem en de persoonsgegevens host en beheert;
- Het informeren van de betrokkene over de verwerking, bijvoorbeeld door middel van het publiceren van een privacy statement;
- Het informeren van de betrokkene over de rechten die hij/zij heeft, en waar de betrokkene terecht kan met verzoeken;
- Het melden van mogelijke datalekken bij de toezichthouder en/of betrokkenen;
- Waarborgen inbouwen om de kwaliteit van de persoonsgegevens hoog te houden;
- Bewaartermijnen voor elke categorie vaststellen en persoonsgegevens verwijderen na afloop.

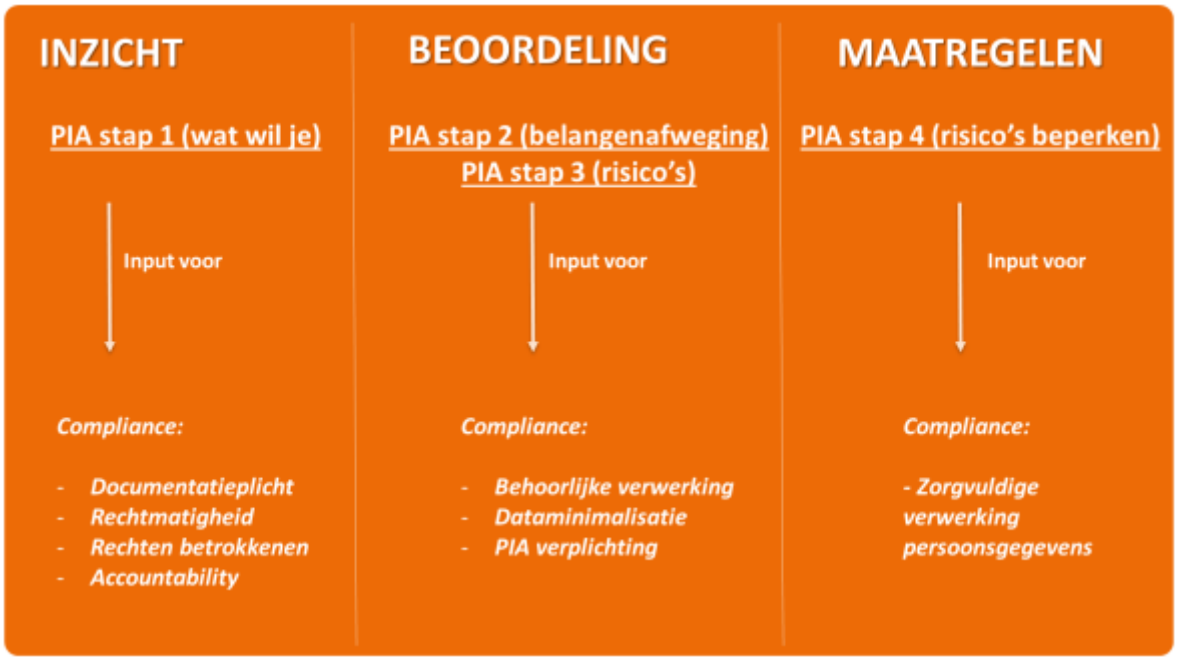
De maatregelen van de AVG en PIA geven samen een goed beeld van wat je als organisatie moet doen om op een zorgvuldige wijze persoonsgegevens te verwerken. Daarbij gaat het overigens niet om eenmalig maatregelen te nemen, maar ook om dit structureel te borgen binnen de organisatie. Denk daarbij aan het volgen van normenkaders en het inrichten van je organisatie volgens de principes van privacy by design.

3.4. Verhouding PIA en Compliance

Zoals eerder aangegeven zit er deels overlap in de PIA en de vereisten uit de AVG. Om de overlap beter inzichtelijk te maken, onderscheiden we drie punten:

1. Inzicht in de verwerkingen van persoonsgegevens;
2. Beoordelen van de risico's en afweging van de verschillende belangen;
3. Maatregelen om een zorgvuldige verwerking te waarborgen.

Deze punten vatten heel erg kort samen waar je bij verwerking van persoonsgegevens op moet letten. Altijd inzicht hebben in wat je doet (en dit naar buiten toe kunnen verantwoorden), altijd afwegen of wat je doet niet onnodig de rechten en vrijheden van betrokkenen schaadt en zoveel mogelijk maatregelen nemen om de betrokkene en de persoonsgegevens te beschermen/te beveiligen.
De PIA stipt elk van deze drie onderwerpen aan, maar niet voldoende om in zijn geheel aan de AVG te voldoen. Wel kan het als input dienen voor het voldoen aan de AVG. In onderstaand schema wordt samengevat welke onderdelen van een PIA als input kunnen dienen voor onderwerpen en beginselen van de AVG.



3.5. Samenvattend

De AVG kent een aantal beginselen en vanuit die beginselen zijn bepalingen uitgewerkt die eisen stellen aan het verwerken van persoonsgegevens. Om aan deze vereisten te kunnen voldoen en compliant te zijn met de AVG, zal je verschillende zaken op orde moeten hebben, zoals 1) inzicht hebben in wat je verwerkt en waarom, 2) het beoordelen van wat je doet d.m.v. het inschatten van risico's voor betrokkenen en het afwegen van belangen, en 3) het nemen van maatregelen en inregelen van mechanismen om de betrokkenen en persoonsgegevens te beschermen. Deze drie onderwerpen komen ook aan bod in de PIA, maar is niet voldoende om compliant te zijn. Wel biedt de PIA op sommige punten input voor het voldoen aan de vereisten van de AVG.
Nu beschreven is wat een PIA is, wat de beginselen zijn van de AVG en hoe deze zich verhouden tot elkaar, is het de vraag hoe je in je organisatie PIA en compliance wilt inzetten. Wordt het één groot alles omvattend instrument, of juist losse onderdelen die je inzet als het nodig is? En kies je ervoor om een PIA alleen te doen als de AVG dat vraagt, of wil je bij elke verwerking een PIA uitvoeren? Kies je dan voor een vragenlijst of een workshop met personen met verschillende disciplines? Dit zijn allemaal keuzes die je als organisatie hebt. Het volgende hoofdstuk benoemt de verschillende onderdelen en wat de mogelijkheden zijn om deze uit te voeren, aan de hand van tooling en andere werkwijzen.

4. Werkwijzen en tooling

4.1. Inleiding

In de vorige hoofdstukken is dieper ingegaan op de PIA en de beginselen en vereisten van de AVG en hoe deze zich tot elkaar verhouden. Dit hoofdstuk gaat in op de vraag hoe je deze zaken nu binnen je organisatie kunt regelen en uitvoeren. Het uitgangspunt hierbij is dat er niet één manier is die goed is en voor alle organisaties geldt. Kies dus voor een benadering die past bij je organisatie en kijk naar wat je behoefte is.
Allereerst worden in dit hoofdstuk de onderdelen genoemd waar je als organisatie iets mee moet (de inhoud). Vervolgens wordt er gekeken naar hoe je deze onderdelen kan inzetten binnen de organisatie (de werkwijze) en hoe je deze kunt presenteren (de vorm). Ten slotte wordt ingegaan op de vraag hoe privacy is te koppelen aan andere aspecten van een organisatie (privacy overstijgend).

4.2. De inhoud

Op basis van wat eerder in de notitie aan bod is gekomen, zou je inhoudelijk gezien als organisatie behoefte kunnen hebben aan:

1. Een inhoudelijke invulling van de vraag of je wel of geen PIA moet doen.
   De inhoud die hier centraal staat, is het bepalen van waarschijnlijke risico's voor de rechten en vrijheden van betrokkenen, omdat dit bepaalt of je wel of geen PIA moet doen. De AVG geeft een aantal handvaten om de risico's in te kunnen schatten (zoals aard en omvang van de gegevens, gebruik van nieuwe technologie), maar een bruikbare toets om dit te beoordelen ontbreekt. Net als een lijst met mogelijke risico's. Dus op dit punt is een extra inhoudelijke invulling wenselijk.

2. Een inhoudelijke invulling van de PIA
   De inhoud die hier centraal staat, zijn de vier stappen die de AVG benoemt die in een PIA moeten zitten. De PIA kan heel basic gezien bestaan uit die vier stappen, maar het is goed mogelijk dat deze vier stappen niet voor iedereen voldoende duidelijk zijn. Er kan daarom behoefte zijn aan extra inhoudelijke duiding of extra tussenstappen. Met als gevolg dat de PIA toegankelijker wordt en ook te gebruiken is zonder enige voorkennis van de privacy wetgeving.

3. Een inhoudelijke invulling van alle vereisten uit de AVG
   De AVG benoemt verschillende beginselen en er zijn bepalingen opgenomen die beschrijven hoe een organisatie met persoonsgegevens moet omgaan. De AVG is een juridische tekst, dus niet voor iedereen goed te begrijpen. Ook zijn niet alle bepalingen zo concreet dat de te nemen maatregelen er meteen uit voortvloeien. Een vertaalslag van wettelijke vereisten naar concrete en toetsbare maatregelen is daarom gewenst, een soort privacy normenkader.

4.3. De werkwijze

Zodra je weet wat de inhoud wordt van je toets of assessment (één of meer onderdelen die hierboven zijn beschreven) kun je nadenken over welke werkwijze je als organisatie kiest. Voor de hand liggend is een vragenlijst, die je door één of meer medewerkers laat invullen. Maar een workshop is ook een optie. Het bepalen van risico's voor betrokkenen en het uitvoeren van een PIA zijn onderdelen die niet altijd in een schriftelijke vragenlijst goed te vangen zijn, een discussie met meerdere personen kan in die gevallen vaak meer resultaat opleveren. Op die manier denk je samen na over de impact die het

verwerken van persoonsgegevens kan hebben. Andere onderdelen lenen zich juist minder voor een workshop. Toetsen of je compliant bent met de AVG is bijvoorbeeld niet geheel geschikt om er in een groep over te discussiëren. Een checklist is daar meer voor de hand liggend.
Ook qua timing kun je kiezen voor een andere werkwijze. Waar een risico inschatting en een PIA vaak aan het begin van een nieuw project of een nieuwe verwerking het beste kunnen worden uitgevoerd, geldt dit niet voor alle compliance maatregelen die voorvloeien uit de AVG. Een deel zal je al wel in een vroeg stadium moeten oppakken, maar er zijn ook maatregelen die je pas later in het proces kunt nemen (denk aan het contracteren van bewerkers en het opstellen van procedures).

4.4. De vorm

Er zijn verschillende manieren om de uitkomsten van de PIA of de compliance toets te presenteren. Voor de hand liggend is het resultaat van de PIA te documenteren, bijvoorbeeld als rapportage beschikbaar te stellen aan degene die iets moet met de uitkomst. Denk aan het geven van een go/ no-go of een advies. Bij wijziging van de verwerking kan deze rapportage er weer bij kan worden gepakt, om te zien of de PIA opnieuw moet worden uitgevoerd. Wat er in de rapportage moet komen hangt weer af van wat de inhoud is geweest en wat het doel is van de rapportage; welke beslissing moet er worden genomen op basis van de rapportage en welke informatie is hiervoor nodig? Bij een PIA is het aannemelijk dat de uitkomst van de verschillende stappen wordt beschreven, met daarbij de mogelijk te nemen maatregelen. Aan de hand van die rapportage kan dan worden beoordeeld of een verwerking wel of niet moet plaatsvinden, en onder welke voorwaarden.
Compliance bijhouden kan op verschillende manieren. Bijvoorbeeld een Word of Excel bestand waarin een checklist is opgenomen waarmee de voortgang kan worden bijgehouden. Of een wiki pagina maken waar gemakkelijk de laatste stand van zaken kan worden genoteerd. Tegenwoordig zijn er verschillende tools op de markt waarmee dit inzichtelijk kan worden gemaakt. In die tools kun je bijvoorbeeld vragenlijsten en normenkaders plaatsen en wordt in kaart gebracht wat de uitkomsten zijn en welke actiepunten er bijvoorbeeld nog openstaan, vaak in de vorm van dashboards. Deze tools zijn soms ook zo ingericht dat ze ook kunnen dienen als register om je verwerkingen in bij te houden (de documentatieplicht uit de AVG). Bij deze tools moet je er wel op letten dat de inhoud niet altijd onderdeel is van de tool. Zo moet je vaak zelf bepalen welke vragen je wilt stellen of welk normenkader je wilt hanteren. Ook voor het houden van workshops leent dergelijke tooling zich minder. Wel zou je de resultaten van een workshop wellicht in de tool kunnen opslaan en raadplegen.

4.5. Privacy overstijgend

Je kunt de privacy onderdelen die hier beschreven zijn op verschillende manier combineren en presenteren. Verder kijken dan bescherming van persoonsgegevens door dit andere aandachtsgebieden te combineren is mogelijk. Denk aan de combinatie met informatiebeveiliging. Zo kun je onderdelen als dataclassificatie en het nemen van beveiligingsmaatregelen voor zowel privacy als security gezamenlijk oppakken. Verlies daarbij niet uit het oog dat bescherming van persoonsgegevens meer omvat dan enkel beveiliging. En ook kan er een verschil zitten in het beoordelen van risico's. Zo gaat het bij persoonsgegevens om de risico's voor de betrokkenen en wordt data geclassificeerd op basis van gevoeligheid van de gegevens. Dit kan vanuit het oogpunt van informatiebeveiliging anders zijn.

4.6. Samenvattend

Er is niet één manier om goed om te gaan met de PIA en de vereisten uit de AVG. Kijk naar je organisatie en onderzoek aan welke inhoud er behoefte is en welk werkwijze en vorm passen bij de organisatie. Op internet zijn verschillende PIA's, normenkaders en tools te vinden, dus kijk goed naar wat ze te bieden hebben en stel zelf een pakket samen waarmee je uit de voeten kan. Kijk voor inspiratie ook op de website van SURF: www.surf.nl/avg