

Data Protection Impact Assessment (DPIA)

Bronnen:

- De AVG
- De Handleiding Algemene Verordening Gegevensbescherming, uitgave van de Autoriteit Persoonsgegevens. Auteurs: Bart W. Schermer, Dominique Hagenauw, Nathalie Falot
- Richtsnoeren voor gegevensbeschermingseffectbeoordelingen door groep Gegevensbescherming, Zoals laatstelijk gewijzigd en vastgesteld op 4 oktober 2017
- Privacy Impact Assessment (PIA): Introductie, handreiking en vragenlijst Versie 1.2 - November 2015 uitgegeven door NOREA
- Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA) Versie 1.0 September 2017, Ministerie van BZK, directie Constitutionele Zaken en Wetgeving, Pien Eijnden en Lester Meijenfeldt, Ministerie van VenJ, directie Wetgeving en Juridische Zaken

Documenthistorie template

Versie	Datum	Auteur	Aanpassingen
1.0	15-09-18	Jeroen Muijs	Invulling
1.1	02-10-18	Ellen Kremers	Aanvulling grondslag/belangenafweging
1.2	27-11-18	Jeroen Muijs	Redesign & aanpassingen
1.3	03-12-18	Jeroen Muijs & Jolanda Aalten	DPIA ontwikkeling
1.4	10-9-2019	Ellen Kremers	Veld met algemene toelichting over de voorgenomen verwerkingsactiviteit toegevoegd.

1. Organisatie & contactgegevens

Soort gegevens	Omschrijving
Naam & adres organisatie	Provincie Utrecht Archimedeslaan 6 3584 BA Utrecht
Naam & contactgegevens opsteller DPIA	Jeroen Muijs, jeroen.muijs@provincie-utrecht.nl
Naam & contactgegevens FG	Jolanda Aalten, jolanda.aalten@provincie-utrecht.nl of privacy@provincie-utrecht.nl
Contactgegevens gesprekspartner	
Contactpersoon teamleider(s)	
Contactpersoon Functioneel Beheerder(s)	

2. Gegevens van de verwerking

Soort gegevens	Omschrijving
Beschrijf hier in het algemeen de voorgenomen verwerkingsactiviteit.	
Beschrijf hier om welke persoonsgegevens het gaat (naam, email, medisch, ...).	
Met welk doel en in welk proces worden deze gegevens gebruikt? Kunnen deze doelen ook zonder de gegevens worden behaald?	
Welke rechtvaardigingsgrond uit de AVG is van toepassing?	☐ De betrokkene heeft toestemming gegeven voor de verwerking. Op welke wijze is/wordt toestemming verkregen?: ☐ De verwerking is noodzakelijk voor de uitvoering van een overeenkomst. (Daarbij moet de betrokkene zelf (mede)partij zijn, anders kan deze grondslag niet worden gekozen.) Welke overeenkomst: ☐ De verwerking is noodzakelijk om een wettelijke verplichting van de Provincie te kunnen nakomen. Verwijs naar wet/artikel: ☐ De verwerking is noodzakelijk om vitale belangen van betrokkene te beschermen. Bv medische gegevens bij een ongeval of noodsituaties. Graag toelichten: ☐ De verwerking is noodzakelijk bij de uitvoering van een publieke taak van de PU. Welke publieke taak (uit welke wet vloeit dit voort) en waarom is het noodzakelijk?: ☐ De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van de PU als rechtspersoon/organisatie. Denk hierbij vooral aan de eigen bedrijfsvoering en informatiebeveiliging. Graag belang toelichten:
Van welke groepen betrokkenen worden de persoonsgegevens verwerkt? (websitebezoekers, burgers, medewerkers, ...)	

3. Systematische omschrijving gegevensverwerking

Soort gegevens	Omschrijving
Beschrijf hier in meer detail hoe de gegevensverwerking gaat.	
Hoe wordt de informatie verzameld?	
Waar wordt deze opgeslagen (systemen/applicaties)? Wie kan hier bij?	
Hoe wordt de informatie gebruikt? Wordt elke soort persoonsgegevens gebruikt?	
Wat is de bewaartermijn van de gegevens? Hoe is de verwijdering van de gegevens geregeld?	
Welke afdelingen, leveranciers en andere partijen zijn als verwerker bij de verwerking betrokken?	
Is er sprake van internationale doorgifte? Welke landen betreft dit?	
Waar wordt de data gearcheeerd? Is dit papier of digitaal?	
Wat is de verwachte omvang van de gegevensverwerking (aantallen betrokkenen)	
Wordt er voldoende informatie verstrekt aan betrokkene? Is het voor betrokkenen duidelijk welke rechten zij hebben en hoe zij deze kunnen uitoefenen?	

4. Beoordeling van de privacy risico's

Risico omschrijving	Risico	Kans dat dit in een jaar gebeurt	Impact op betrokkenen	Maatregelen
	<i>Ja/Nee, want...</i>	<i>Laag/Midden/Hoog want...</i>	<i>Laag/Midden/Hoog want...</i>	<i>Getroffen maatregelen (organisatorisch & technisch)</i>
Onrechtmatige toegang door interne medewerkers Denk hierbij aan: • Teveel fysieke en logische toegang tot informatie via applicaties, systemen en netwerken (rechten gebruikers); • Mogelijkheden voor bulk kopiëren / exporteren; • Pogingen om systemen binnen te dringen zijn niet terug te vinden (logging); • Audits/Reviews met betrekking tot de fysieke en logische toegangsbeveiliging ontbreken.				
Onrechtmatige toegang door buitenstaanders Denk hierbij aan: • Gebrekkige controle over de toegang via inbelsystemen; • Onnodig gebruik van internet; • De mate waarin het systeem benaderbaar is, bv. bij cloud systemen en vanaf internet; • Het gebruik van draagbare computers; • Toegang tot systemen door derden; • Audits/Reviews met betrekking tot de fysieke en logische toegangsbeveiliging worden niet uitgevoerd.				
Ongewenste wijziging van gegevens door interne medewerkers Denk hierbij aan: • Fysieke en logische maatregelen om de toegang tot gegevensbestanden te beheren/controleren (incl. Back-ups); • Het beheer van wachtwoorden; • Toezicht op het gebruik van krachtige beheerfuncties; • Procedures met betrekking tot reparaties; • Toegang tot systemen door derden; • Gebruik van controletotalen (bijv. checksum, hash-waarde, etc.); • Procedures voor de beveiligingsadministratie; en, • Procedures voor het onderzoeken van en rapporteren over beveiligingsincidenten;				

Ongewenste wijziging van gegevens door buitenstaanders Denk hierbij aan: • Kwaadaardige software, malware, phishing • De interesse van anderen voor het aanpassen van de informatie. • Patching en gebruik van verouderde software en systemen.				
Verdwijnen en/of zoekraken van gegevens Denk hierbij aan: • De kwaliteit van de beheerprocedures; • Mate van betrokkenheid / kennis van de beheerder bij de normale productieverwerking; • Gebruik van geautomatiseerde planning- en opdrachtverwerking systemen; • Aard van de herstelprocedures na een productiestoring; • Hoe omgegaan wordt met emergency fixes; • Vastleggen (loggen) van de activiteiten van de beheerder; • Controletotalen (checksum) van bestanden; • Management reviews van de systeemresultaten; en, • Het valideren van computer records met bestaande (fysieke) entiteiten of derde partijen (verbandscontrole).				

Opmerking: Indien er een hoog risico is geconstateerd dient de aanvullende risicobeoordeling ingevuld te worden. *Zie Bijlage 1 – Aanvullende risicobeoordeling*

5. Advies Functionaris Gegevensbescherming

Naam FG:	Jolanda Aalten
Datum van advies:	

Vragen	Antwoord	Opmerkingen
Zijn de gegevensverwerking en doeleinden duidelijk omschreven?		
Is er de verwerking van de persoonsgegevens noodzakelijk of proportioneel voor de doeleinden?		
Zijn de privacy risico's voldoende in kaart gebracht? Welke risico's ontbreken nog?		

Bijlage 1 - Aanvullende risicobeoordeling

Risico	Ja / Nee	Onderbouwing
Is er sprake van invoering van nieuwe technologie? <i>Bijvoorbeeld intelligente transportsystemen, locatie of volgsystemen op basis van GPS, mobiele technologie, gezichtsherkenning in samenhang met cameratoezicht.</i>		
Is er sprake van invoering van technologie die bij het publiek vragen of weerstand op kan roepen? <i>Bijvoorbeeld biometrie, RFID, behavioural targeting (profilering).</i>		
Is er sprake van invoering van bestaande technologie in een nieuwe context? <i>Bijvoorbeeld cameratoezicht of drugscontrole op de werkvloer.</i>		
Is er sprake van andere grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt? <i>Bijvoorbeeld het samenvoegen of koppelen van verschillende overheidsregistraties, invoering van nieuwe vormen van identificatie of vervanging van een systeem waarin persoonsgegevens worden opgeslagen.</i>		
Is er (naast de AVG) veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft? <i>Houd bij de beantwoording rekening met:</i> 1. Sectorale wetgeving. 2. Gedragscodes. 3. Algemene maatregelen van bestuur. 4. Jurisprudentie. 5. Internationale aspecten.		
Zijn er veel maatschappelijke belanghebbenden? <i>Denk aan Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichhouders.</i>		
Zijn er bij veel partijen betrokken de uitvoering van het project? <i>Houd bij de beantwoording rekening met:</i> 1. Aannemers en dienstverleners; 2. Hardware en software leveranciers; 3. IT Service providers.		
Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt? <i>Dit terwijl daar op dit moment geen gebruik van wordt gemaakt?</i>		
Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)? <i>Denk hierbij bijvoorbeeld ook aan geolocatie, personeelsvolgsystemen, beslisondersteuning bij het als dan niet aanbieden van producten of diensten.</i>		
Verwerkt u gegevens over kwetsbare groepen of personen?		

<i>Bijvoorbeeld minderjarige personen, verstandelijk gehandicapten, gedetineerden, onder toezicht gestelden, mensen van wie de fysieke veiligheid in gevaar is?</i>		
Hebben de gegevens betrekking op de gehele of grote delen van de bevolking van een land?		
Worden de gegevens verkocht aan derde partijen?		
Verwerkt u bijzondere persoonsgegevens, gevoelige persoonsgegevens, unieke biometrische kenmerken, BSN-nummers of andere gegevens waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid? <i>Bijvoorbeeld vingerafdrukken, DNA-profielen, creditcardinformatie, financiële informatie, erfrechtelijke aspecten, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt?</i>		

Impact	Ja / Nee	Onderbouwing
Heeft het uitlekken van gegevens impact op de betrokkenen?		
Heeft dit nadelige gevolgen voor de persoon?		
Is er kans op financiële schade?		
Is er kans op identiteitsdiefstal of fraude?		

Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen? Wie is dit: