Ministerie van Justitie en Veiligheid

Toelichting: Big Data Analyse >

Big Data

Model GEB Rijksdienst (PIA)

Dit document bevat een Big Data specifieke aanvulling op het rijksbrede instrument Toetsmodel GEB Rijkdienst (PIA) en is opgesteld voor organisaties die met Big Data aan de slag gaan en mogelijke privacyrisico's in kaart willen brengen. Zie voor het oorspronkelijk model GEB Rijksdienst, met het volledige proceskader en toelichting op de website van de Rijksoverheid.

Big Data

Toelichting: Big Data Analyse

Inhoudsopgave

Big Data

Toelichting: Big Data Analyse

Inleiding

Big Data wordt ingezet om nieuwe inzichten te verkrijgen. Wanneer het om persoonsgegevens gaat kan verwerking, gelet op de aard, omvang, context en doeleinden van analyse, risico's inhouden voor het recht op bescherming van persoonsgegevens van betrokkenen. Het is van belang om de privacyrisico's bij Big Data toepassingen zoveel mogelijk te voorkomen en beperken. Daarvoor kan een gegevensbeschermingseffectbeoordeling worden gehanteerd. Hiermee worden de volgende onderdelen in kaart gebracht:

- De feitelijke verwerkingen bij Big Data analyse;
- De beoordeling van de effecten daarvan voor betrokkenen;
- De maatregelen die op basis hiervan kunnen worden getroffen om deze effecten voor betrokkenen te voorkomen of verkleinen.

Wat is Big Data?

Big Data is een wijdverspreide en veelgebruikte term. Toch bestaat er geen breed gedeelde definitie van Big Data, zo constateerde de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in haar rapport 'Big Data in een vrije en veilige samenleving'. De WRR benoemd in haar rapport drie hoofdkenmerken van Big Data:

1. Data: grote hoeveelheden gestructureerde of ongestructureerde gegevens of een combinatie van beide uit verschillende databronnen.
2. Data-gedreven analyse: er wordt gezocht naar patronen in de data zonder vooraf opgestelde hypotheses. Analyses zijn vooral gericht op het heden (realtimeanalyses/nowcasting) en de toekomst (predictive analyses/forecasting).
3. Gebruik: data uit het ene domein wordt gebruikt voor beslissingen in een ander domein met ontschotting van domeinen als gevolg. Actionable knowledge: conclusies op geaggregeerd niveau kunnen worden toegepast voor beslissingen op groeps- of individueel niveau (persoon of object).

Zie hiervoor ook de Big Data Factsheet https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/documenten/publicaties/2018/04/20/big-data-factsheet

Dit document bevat een Big Data specifieke aanvulling op het rijksbrede instrument Toetsmodel GEB Rijkdienst (PIA) en is opgesteld voor organisaties die met Big Data aan de slag gaan en mogelijke privacyrisico's in kaart willen brengen. Zie voor het oorspronkelijk model GEB Rijksdienst, met het volledige proceskader en toelichting op de website van de Rijksoverheid.

Opbouw

Het Toetsmodel GEB Rijkdienst (PIA) bestaat uit drie onderdelen:

1. Het Proceskader;
2. Het Model (de PIA);
3. De Toelichting.

In dit document is onderdeel 3 (de Toelichting) van de PIA helemaal toegespitst op verwerkingen in het kader van Big Data, zodat de verwerkingsverantwoordelijke die het instrument van de PIA wil toepassen op efficiënte wijze gebruik kan maken van de bouwstenen zoals nader omschreven onder het kopje 'Bouwstenen Big Data Model'. Hiermee kan het opstellen van een PIA bij Big Data verwerkingen worden vereenvoudigd en versneld. De opgestelde toelichting bestaat uit twee onderdelen:

- Allereerst een **groen gemarkeerde** selectie van aandachtspunten uit de oorspronkelijke toelichting van het Toetsmodel die in het bijzonder van belang kunnen zijn bij Big Data analyse;
- Alsmede een **geel gemarkeerde** aanvullende toelichting op het officiele Toetsmodel GEB Rijksdienst die is gebasseerd op de hieronder omschreven kennis en ervaring die met Big Data is opgedaan.

Big Data

Toelichting: Big Data Analyse

Bouwstenen Big Data Model

Voor de totstandkoming van de aanvullende toelichting zijn onder meer de volgende bronnen gehanteerd:

- Beleidsuitgangspunten vanuit de kabinetsreactie op het WRR Rapport 'Big Data in een vrije en veilige samenleving (Kamerstukken II 2016-2017, 26643, nr. 426);
  - Minisymposia met Big Data-professionals die naar aanleiding hiervan zijn georganiseerd en de best practices die hieruit zijn voortgekomen;
- Ervaringen van lopende Big Data trajecten van het Big Data Living Labs and Competence Network project JenV;
- Het juridisch toetsingskader dat ten behoeve Big Data Living Labs JenV is opgesteld;
- Het Toetsingskader City Deal zicht op ondermijning (Stcrt. 2017, 48699).

Toepassing GEB Big Data analyse

De PIA dient in het geval van Big Data analyse in een zo vroeg mogelijk stadium te worden gehanteerd en bij verandering van de scope van data-analyse te worden herzien. De (beoogde) opdrachtgever voor Big Data toepassingen is verantwoordelijk voor de uitvoering van deze stappen en voor de verantwoording hiervan, eventueel in afstemming met de Functionaris voor Gegevensbescherming.

Gelet op de stand van de techniek en veranderde wet- en regelgeving zal dit document op regelmatige basis worden herzien. Zie voor de meest actuele versie de Big Data Toolbox op de website van de Rijksoverheid.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Toelichting

Bij overheidsverwerkingen kan in hoofdlijnen worden beschreven hoe de gegevensverwerkingen er uit zullen zien. Als dat er is kan worden aangesloten bij het projectvoorstel of een beschrijving van de architectuur.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

Big Data

Toelichting: Big Data Analyse

Toelichting

Beschrijf allereerst alle te verwerken categorieën van persoonsgegevens. Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Natuurlijke personen wil zeggen mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in beginsel geen persoonsgegeven. Deze informatie kwalificeert weer wel als persoonsgegeven indien die ook betrekking heeft op een levende persoon.

Om te bepalen of iemand identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om de persoon te identificeren.

Gepseudonimiseerde gegevens
Gepseudonimiseerde (ook wel: versleutelde) gegevens worden als persoonsgegevens beschouwd. Onder pseudonimisering wordt verstaan: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens (sleutels) worden gebruikt. Hieraan wordt wel de eis verbonden dat deze aanvullende gegevens apart worden bewaard en maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een persoon worden gekoppeld.

Geanonimiseerde persoonsgegevens
Anonieme en geanonimiseerde gegevens zijn geen persoonsgegevens. Met anoniem en geanonimiseerd wordt bedoeld dat de persoon op wie het gegeven betrekking heeft, niet (meer) identificeerbaar is. Het anonimiseren van persoonsgegevens als zodanig is overigens weer wel een verwerking van persoonsgegevens.

Voorbeelden
Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK-nummer, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag.

Metadata
Ook metadata – informatie over informatie – zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt en de geschreven taal.

Geolocatiegegevens
Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

Typen

Stel vervolgens de aard van de te verwerken categorieën van persoonsgegeven vast. De AVG onderscheidt drie typen van persoonsgegevens – gewone, bijzondere en strafrechtelijke persoonsgegevens – en stelt verschillende eisen aan een rechtmatige verwerking daarvan. De gedachte hierachter is dat hoe gevoeliger de aard van de persoonsgegevens, hoe groter de effecten voor de betrokkenen zijn.

Bijzondere persoonsgegevens

Hieronder een limitatieve opsomming van categorieën van bijzondere persoonsgegevens:

- ras of etnische afkomst;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;

Big Data

Toelichting: Big Data Analyse

- het lidmaatschap van een vakbond;
- genetische gegevens;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens over seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers, ledenlijst van een politieke partij, relatiestatus op sociale media. Let op: uit beeldmateriaal zoals foto's en camerabeelden kunnen soms ook bijzondere persoonsgegevens, zoals etnische afkomst of medische gesteldheid, worden afgeleid.

Genetische gegevens
Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over zijn fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

Biometrische gegevens
Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, toetsaanslaganalyse, looppatroon, stemgeluid en slaapritme. Foto's vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken.

Gegevens over gezondheid
Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Strafrechtelijke persoonsgegevens
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (hierna: strafrechtelijke persoonsgegevens) zijn een apart type persoonsgegeven. Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Voorbeelden hiervan zijn: proces-verbaal, sepotbeslissing, strafblad, relaas verhoor en aanvraag voor een toevoeging in een strafzaak.

Wettelijke identificatienummers
Nummers ter identificatie van een persoon die bij wet zijn voorgeschreven, mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Denk hierbij aan: een Burgerservicenummer (BSN), BIG-nummer (beroepen in de individuele gezondheidszorg), A-nummer (basisregistratie personen), onderwijsnummer, strafrechtketennummer en kenteken. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers.

Overige persoonsgegevens
Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens wil overigens niet zeggen dat geen sprake is van een hoog privacyrisico. Bepaalde persoonsgegevens kunnen door de context waarin zij worden gebruikt gevoelig zijn en daardoor een hoog privacyrisico met zich brengen. Hierbij kan gedacht worden aan:

Big Data

Toelichting: Big Data Analyse

- gegevens over de financiële of economische situatie van de betrokkene;
- gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties;
- (andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- gegevens die betrekking hebben op kwetsbare groepen;
- gebruikersnamen, wachtwoorden en andere inloggegevens;
- gegevens die kunnen worden misbruikt voor (identiteits)fraude;
- communicatie- en locatiegegevens.

Betrokkenen

Benoem tot slot de categorieën van betrokkenen van wie de persoonsgegevens worden verwerkt. Denk hierbij aan: medewerkers, consumenten, cliënten, patiënten, zakelijke contacten, bezoekers, gebruikers of ingezetenen van een gemeente. De omvang en categorie van betrokkenen kunnen invloed hebben op de effecten van het voorstel. Bepaalde betrokkenen zijn kwetsbaarder dan anderen. Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere (zie ook de anderszins gevoelige persoonsgegevens). Denk bijvoorbeeld aan: minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven, medewerkers van inlichtingen- en veiligheidsdiensten, klokkenluiders of informanten van politie of justitie. Betrokkenen hebben op grond van de privacyregelgeving bepaalde rechten, zoals het inzage- en correctierecht.

Gegevens minderjarigen

De AVG biedt specifieke bescherming aan kinderen, omdat zij zich minder bewust zullen zijn van de effecten van de gegevensverwerking en van hun rechten in dat kader. Die specifieke bescherming geldt met name voor het gebruik van persoonsgegevens van kinderen voor marketingsdoeleinden, het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Zo is wanneer het kind jonger is dan 16 jaar zo'n verwerking slechts rechtmatig, indien de toestemming of machtiging tot toestemming wordt verleend door de ouder of voogd. Ook heeft de leeftijd van betrokkenen gevolgen voor de wijze waarop hij geïnformeerd moet worden.

In het kader van de Richtlijn kan het onderscheid worden gemaakt tussen:

a. personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;

b. personen die voor een strafbaar feit zijn veroordeeld;

c. slachtoffers van een strafbaar feit, of personen ten aanzien van wie bepaalde feiten aanleiding geven tot het vermoeden dat zij het slachtoffer zouden kunnen worden van een strafbaar feit; en

d. andere personen die bij een strafbaar feit betrokken zijn, zoals personen die als getuige kunnen worden opgeroepen in een onderzoek naar strafbare feiten of een daaruit voortvloeiende strafrechtelijke procedure, personen die informatie kunnen verstrekken over strafbare feiten, of personen die contact hebben of banden onderhouden met een van de personen bedoeld onder a en b.

Aandachtspunt 1: Overzicht datasets

Voor de verantwoordingsplicht die in artikel 24 AVG is opgenomen en verder is uitgewerkt in de vereisten die in artikel 30 AVG aan het verwerkingsregister worden gesteld[11], moet worden vastgelegd welke (categorieën van) persoonsgegevens voor de analyse worden verstrekt en verder verwerkt. Indien dat technisch niet anders kan, zal het om de complete dataset uit een systeem kunnen gaan. Voor zover het

[1] In de Wpg artikel 4a en 31d en in de Wjsg de artikelen 7 en 26c.

Big Data

Toelichting: Big Data Analyse

echter zonder onevenredige inspanning mogelijk is om relevante extracten of deelverzamelingen uit die dataset te halen, dan moet worden volstaan met verwerking van die data-extracten of deelverzamelingen.

Aandachtspunt 2: Registreer kwaliteit en herkomst gegevens

Het is van belang om naast de te hanteren datasets ook de bijbehorende omschrijving van de kwaliteit en herkomst van de betreffende dataset te registreren, zodat de resultaten van Big Data analyse op juiste wijze kunnen worden vastgesteld. Het is verder van belang dat de gegevens die voor Big Data analyse worden verstrekt, door de verstrekker rechtmatig zijn verkregen.
Breng in kaart of de databron eventueel is verzwaard met intellectuele eigendomsrechten zoals Auteursrecht of Databankenrecht op de databron, het algoritme of de analysemethode. Dit kan door te controleren of de gegevens op basis van een licentie zijn verkregen of door te controleren of de eventuele gegevensverstrekker bepaalde rechten, zoals het auteursrecht, heeft voorbehouden.

Aandachtspunt 3: Primaire- en secundaire bronnen

Maak indien mogelijk een onderscheid tussen primaire- en secundaire databronnen. Primaire bronnen zijn de bronnen waar gegevens daadwerkelijk worden gegenereerd. Secundaire bronnen zijn bronnen die bestaande datasets koppelen en (her)gebruiken.

Aandachtspunt 4: Kies tussen Big Data analyse ten behoeve van patronen, dan wel herleidbare personen

Als het doel van Big Data analyse het opstellen van een trendrapportage is, zal de analyse waarschijnlijk zonder verwerking van persoonsgegevens kunnen worden uitgevoerd. Daaronder valt ook het verwerken van gegevens die van persoonsgegevens zijn afgeleid, maar vooraf zijn geanonimiseerd, d.w.z. op onomkeerbare wijze zijn omgezet naar gegevens die identificatie niet langer mogelijk maakt. Als het doel echter het blootleggen van bepaalde patronen is, zal het naar alle waarschijnlijkheid onvermijdelijk zijn om persoonsgegevens te verwerken. Voor het opstellen van een groepsprofiel is dat zelfs volstrekt zeker. Immers, zo'n profiel zal alleen kunnen worden opgesteld als daartoe verbanden tussen bepaalde personen en bepaalde kenmerken kunnen worden gelegd.

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

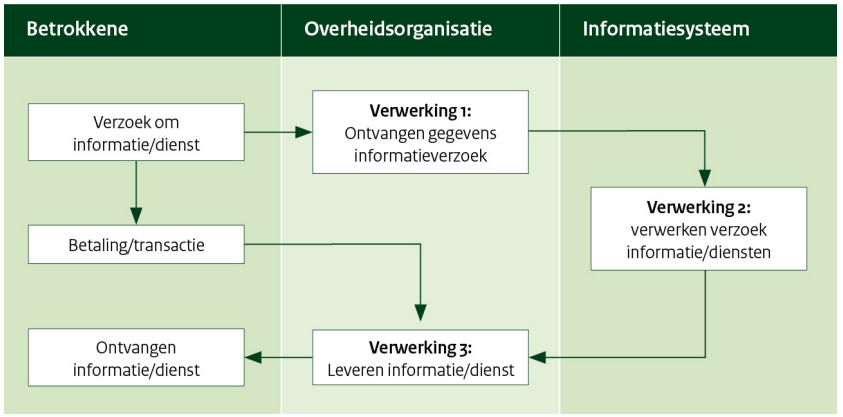
Toelichting

Om de rechtmatigheid van de voorgenomen gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om alle gegevensverwerkingen in beeld te hebben. Onder verwerking wordt verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Denk hierbij aan: 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. Met andere woorden, het begrip omvat het gehele proces dat een persoonsgegeven doormaakt, vanaf het moment van verzamelen tot en met het moment van vernietigen.

Indien mogelijk verdient het aanbeveling om de gegevensverwerkingen te visualiseren, bijvoorbeeld aan de hand van een input-proces-output model, *flowchart of workflow*.

Big Data

Toelichting: Big Data Analyse



4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Toelichting

De privacyregelgeving geeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. De vaststelling van de verwerkingsdoeleinden is een noodzakelijk voorwaarde om te kunnen beoordelen of de voorgenomen gegevensverwerkingen rechtmatig zijn (onder B) en om vast te stellen welke maatregelen moeten worden getroffen om de risico's (onder C) te voorkomen of verkleinen (onder D). Omschrijf daarom per voorgenomen gegevensverwerking de verwerkingsdoeleinden zo specifiek mogelijk.

Bij verwerkingsdoeleinden kan gedacht worden aan: beveiligen van gebouwen en objecten, behandelen van personeelszaken, opsporen van strafbare feiten, direct marketing, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen. Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoeleinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, waarbij het algemene overkoepelende doel kan worden gebruikt als kapstok waaraan verschillende subdoelen kunnen worden gehangen, bijvoorbeeld:

- e-mailadres: noodzakelijk voor communicatie met betrokkene;
- ip-adres: noodzakelijk ter verificatie dat alleen vanuit een bepaalde locatie contact wordt gemaakt met het systeem;
- adresgegevens: noodzakelijk om een beschikking naar de betrokkene te kunnen toezenden;
- financiële gegevens: noodzakelijk om vast te stellen of de betrokken partij in aanmerking komt voor een toeslag;
- strafrechtelijke gegevens: noodzakelijk om een screening te kunnen uitvoeren.

Wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verkregen (met andere woorden: de persoonsgegevens zijn afkomstig van een andere persoon of organisatie dan wel uit een bestaand databestand), is het noodzakelijk om de doeleinden waarvoor de gegevens oorspronkelijk zijn verzameld te herleiden. De privacyregelgeving geeft namelijk als beginsel dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Met andere woorden: de verwerking van persoons-gegevens voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk zijn verzameld, mag enkel indien de verwerking verenigbaar is met de doeleinden waarvoor de persoonsgegevens aanvankelijk zijn verzameld. Met verdere

Big Data

Toelichting: Big Data Analyse

verwerking wordt gedoeld op gebruik van persoonsgegevens die al eerder voor een bepaald doel zijn verzameld. Denk hierbij aan verstrekkingen van persoonsgegevens aan een andere organisatie die niet oorspronkelijk, ten tijde van het verzamelen van de gegevens, was beoogd.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Toelichting

Bij overheidsverwerkingen zullen, voor zover niet reeds wettelijk voorgeschreven, de organisaties die (functioneel) betrokken zijn bij de gegevensverwerkingen zelf en in onderling overleg moeten bepalen wie in welke hoedanigheid de persoonsgegevens verwerkt. Tevens zal moeten worden bepaald, voor zover eveneens niet wettelijk voorgeschreven, welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens, bijvoorbeeld aan de hand van een autorisatiematrix, in relatie tot de doeleinden van de gegevensverwerking. Hierin kan tevens worden bepaald in welke gevallen en onder welke voorwaarden deze functionarissen toegang krijgen tot de persoonsgegevens.

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt.

Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Aandachtspunt 5: Bepaal wie verantwoordelijk is voor Big Data analyse

Voor de verwerking van persoonsgegevens is in beginsel de verwerkingsverantwoordelijke degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[2]

Voor de verwerking van politiegegevens door de politie is de Korpschef in beginsel de verwerkingsverantwoordelijke[3], van justitiële gegevens de Minister van Justitie en Veiligheid[4] en van strafvorderlijke gegevens het College van procureurs-generaal[5].

Onder verwerking van persoonsgegevens valt ook het verstrekken daarvan. Het belang om te bepalen wie als verantwoordelijke voor de verstrekking van data voor de uit te voeren analyse moet worden aangemerkt, ligt in het feit dat sommige stappen in dit model naar hun aard door deze verantwoordelijke zullen moeten worden gezet.

Van degene die als verantwoordelijke voor de verstrekking van data valt aan te merken, moet worden onderscheiden degene die als verantwoordelijke valt aan te merken voor de verdere verwerking van de verstrekte gegevens ten behoeve van de uit te voeren analyse. Dat is degene die als opdrachtgever van de analyse optreedt. Hij bepaalt immers welke persoonsgegevens op welke wijze en voor welk doel worden verwerkt. Binnen de ministeries ligt de rol van verantwoordelijke/opdrachtgever in beginsel bij de minister. Een blik op de geldende mandaatsbesluiten kan leren in hoeverre deze rol is (door)gemandateerd aan leidinggevende ambtenaren.

[2] Artikel 4 lid 7 AVG.
[3] Artikel 1, onder f, Wpg. Dat voor de verwerking van politiegegevens door de rijksrecherche of de Koninklijke marechaussee het College van procureurs-generaal, resp. de minister van Defensie als de verantwoordelijke wordt aangemerkt, kan hier verder buiten beschouwing blijven, omdat van verwerking door deze organisaties ten behoeve van het Living Lab geen sprake is.
[4] Artikel 2, eerste lid, Wjsg.
[5] Artikel 39a, eerste lid, Wjsg.

Big Data

Toelichting: Big Data Analyse

Aandachtspunt 6: Verwerker Big Data analyse

Afhankelijk van wie de opdrachtgever is, zullen betrokken Big Data analisten in het algemeen niet in een ondergeschikte positie ten opzichte van de opdrachtgever staan. Zij zijn dan aan te merken als verwerker of subverwerker.[6] Uit praktisch oogpunt dient de opdrachtgever die organisatie als verwerker aan te wijzen waar naar verwachting het zwaartepunt in de uitvoering van de opdracht zal liggen.

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Toelichting

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt. Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens ter beschikking stelt.

Aandachtspunt 7: Betrek partijen en/of personen die (in)direct belang hebben bij Big Data analyse

Betrek indien mogelijk partijen en/of personen die een belang hebben bij de resultaten van Big Data analyse, zodat een goede belangenafweging kan worden gemaakt over de manier waarop Big Data analyse kan worden toegepast en ten behoeve van welke baten Big Data kan worden toegepast.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Toelichting

De locaties waar de voorgenomen gegevensverwerkingen plaatsvinden, kunnen aanvullende privacyrisico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Tevens heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacytoezichthouder.

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, bepalen de AVG en de Richtlijn dat gegevensverwerkingen buiten de Europese Unie enkel onder bepaalde omstandigheden zijn toegestaan. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit) of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch zijn toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene.

Naast de AVG en de Richtlijn kunnen andere wettelijke regels of beleid invloed hebben op de locaties waar persoonsgegevens kunnen worden verwerkt. Denk hierbij aan het VIRBI 2013 inzake gerubriceerde overheidsinformatie en situaties waarin opslag in een overheidsdatacenter geëigend is.

[6] Artikel 4 lid 8 AVG c.q. artikel 1, onder g, Wjsg en artikel 1, onder i, Wpg.

Big Data

Toelichting: Big Data Analyse

8. Techniek en methode van gegevensverwerking

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi)geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Toelichting

Geautomatiseerde besluitvorming

Uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor de betrokkenen rechtsgevolgen hebben of hem anderszins in aanmerkelijke mate treffen, zijn in beginsel verboden.

Voor verwerkingen die onder de werkingssfeer van de AVG vallen, geldt dat dit verbod niet van toepassing indien het besluit:

a. noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;

b. is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of

c. berust op de uitdrukkelijke toestemming van de betrokkene.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn geldt dit verbod niet indien het besluit:

a. wettelijk is toegestaan; en

b. voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkenen, waaronder ten minste het recht op menselijke tussenkomst.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Bij verwerkingen die vallen onder de werkingssfeer van de Richtlijn, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering. Big data staat voor het verschijnsel dat grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau.

Big Data

Toelichting: Big Data Analyse

In de kern komt het bij big data-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van big data brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Aandachtspunt 8: Ga na of de analyse zich voor patroonherkenning leent

Data-analyses kunnen naar hun aard het best worden uitgevoerd voor vraagstukken die zich goed voor patroonherkenning lenen, d.w.z. vraagstukken met een regelmatig en terugkerend karakter. Naarmate de mogelijkheden tot patroonherkenning minder zijn, neemt het belang toe van een goede validatie door experts op het desbetreffende vakgebied om het risico op foutieve uitkomsten van de analyse zoveel mogelijk te reduceren. Ga in een zo vroeg mogelijk stadium na of de analyse zich voor patroonherkenning leent en neem dit op in de PIA.

Aandachtspunt 9: Gebruik indien mogelijk een gestandaardiseerde en/of wetenschappelijk gevalideerde methodiek

Hanteer een standaard methodiek van werken, bijvoorbeeld CRISP DM (Cross Industry Standard Process for Data Mining). Deze methodiek is toepasbaar bij data mining (techniek om patronen in datasets te ontdekken). Wanneer je een hypothese wil toetsen aan de hand van data-analyse is deze methodiek minder van toepassing. Algoritmen en methoden die bij data-analyses worden gebruikt, moeten verder deugdelijk zijn en aan de wetenschappelijke criteria voor goed (statistisch) onderzoek voldoen. Bij voorkeur worden algoritmen gebruikt die wetenschappelijk zijn getoetst, blijkend uit bijvoorbeeld publicaties of peer reviews.[7] Een zorgplicht met betrekking tot de deugdelijkheid van gebruikte algoritmen en methoden ligt opgesloten in artikel 6 AVG, waarin is bepaald dat persoonsgegevens op behoorlijke en zorgvuldige wijze worden verwerkt.

[7] *Aanbeveling 1 in § 6.4.4* in de bijlage bij de kabinetsreactie op het WRR-rapport "Big Data in een vrije en veilige samenleving" (Kamerstukken II 2016-2017, 26643, nr. 426).

9. Juridisch en beleidsmatig kader

Benoem de wet en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Toelichting

Naast of in de plaats van de AVG kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken. In bepaalde wet- en regelgeving staan bepalingen die specifiek van belang kunnen zijn voor Big Data analyse, zoals artikel 40 Uitvoeringswet AVG, artikel 7a Wpg en artikel 7 onder e Wjsg, die een uitwerking van het verbod op geautomatiseerde besluitvorming geven.

Er kan ook departementaal of rijksbreed beleid zijn dat de mogelijkheden voor de voorgenomen gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

Aan de hand van deze inventarisatie kan bij onderdeel B beoordeeld worden of de voorgenomen gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

Aandachtspunt 10: Juridisch kader strafrechtelijke gegevens

Het accent kan naast de AVG op de Wet politiegegevens (Wpg), de Wet justitiële en strafvorderlijke gegevens (Wjsg) en – in het geval van de laatste twee wetten – het daarop berustende Besluit politiegegevens (Bpg), respectievelijk Besluit justitiële en strafvorderlijke gegevens (Bjsg) liggen.

Big Data

Toelichting: Big Data Analyse

Aandachtspunt 11: Beleidsmatig kader

Verder zijn in dit kader de beleidsuitgangspunten verwerkt die zijn neergelegd in de kabinetsreactie op het rapport “Big Data in een vrije en veilige samenleving” van de Wetenschappelijke Raad voor het Regeringsbeleid. Andere juridische aspecten dan die welke met bescherming van de privacy te maken hebben, worden buiten beschouwing gelaten. Dat laat onverlet dat daarmee uiteraard wel rekening moet worden gehouden. Daarbij valt met name te denken aan eventuele geheim-houdingsplichten in sectorale wetten ten aanzien van gegevens die voor verwerking ten behoeve van het experiment in aanmerking zouden kunnen komen.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Toelichting

De privacyregelgeving geeft als beginsel dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, mogen worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is. Met andere woorden: indien het voor de verwezenlijking van de verwerkings-doeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd. Op dit beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering indien de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen.

Bij overheidsverwerkingen moet worden nagegaan of regelgeving een bewaartermijn voorschrijft. Indien dat het geval is, moet de verwerkingsverantwoordelijke zich aan die termijn houden. Indien geen wettelijke bewaartermijn is voorgeschreven, moet de verwerkingsverantwoordelijke zelf bewaartermijnen vaststellen of de gegevens periodieke toetsen aan het beginsel van opslagbeperking. Hierbij moet rekening worden gehouden met andere regelgeving over bewaartermijnen, zoals de Archiefwet 1995.

Voorbeeld opsomming bewaartermijn voor persoonsgegevens bij overheidsverwerkingen (IT/uitvoering):

Categorie Persoonsgegeven	Ingang bewaartermijn	Termijn van bewaring	Motivatie bewaring	Verantwoordelijkheid voor verwijdering
Naam	Vanaf moment dat de betrokene voor het eerste inlogt in het systeem.	365 dagen, als de gebruiker ‘onthouden inloggegevens’ aanklikt 30 dagen.	Deze persoonsgegevens zijn functioneel: het gegeven zorgt er voor dat je met slechts één handeling inlogt in het verschillende databases.	Functioneel beheerder

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de PIA is in het bijzonder juridische expertise nodig.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Toelichting

De AVG geeft als beginsel dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Als uitwerking van dit beginsel is geregeld dat een gegevensverwerking alleen rechtmatig is indien deze gebaseerd kan worden op ten minste één van de volgende zes rechtsgronden:

a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

Ten aanzien van de rechtsgronden c (wettelijke plicht) en e (taak van algemeen belang) geldt dat deze moet worden vastgesteld bij of krachtens de wet.

De wettelijke verplichting (rechtsgrond c) hoeft niet noodzakelijkerwijs te bestaan uit een expliciete verplichting om persoonsgegevens te verwerken. Ook is mogelijk dat de verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht of wettelijke verplichting. Zonder verwerking van de persoonsgegevens moet het uitvoeren van een wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Met betrekking tot rechtsgrond e (de taak van algemeen belang) geldt dat deze taak zal moeten blijken uit regelgeving die op de verwerkingsverantwoordelijke van toepassing is. Niet noodzakelijk is dat in de regelgeving ook expliciet is opgenomen dat ten behoeve van de vervulling van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.

De Richtlijn gegevensbescherming opsporing en vervolging voor dat een gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid alleen rechtmatig is indien die verwerking gebaseerd is op de wet.

Big Data

Toelichting: Big Data Analyse

Bij overheidsverwerkingen zal het overheidsorgaan de voorgenomen gegevensverwerkingen moeten baseren op één van de zes rechtsgronden. De rechtsgrond genoemd onder f geldt niet voor gegevensverwerkingen in het kader van de uitoefening van publieke taken. Wel kan deze rechtsgrond gebruikt worden voor gegevensverwerkingen in de bedrijfsvoering, zoals cameratoezicht, bezoekersregistratie en toegangscontrole. In veel situaties zal de rechtsgrond genoemd onder a (toestemming) evenmin kunnen dienen als rechtsgrond voor gegevensverwerkingen door overheidsorganen, omdat de betrokkene in de gegeven situatie niet vrijelijk toestemming kan geven.

Indien de gegevensverwerkingen gebaseerd worden op de rechtsgrond genoemd onder f (het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde), dan stelt de AVG als eis dat de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder mogen wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of de derde.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Toelichting

De AVG verbiedt de verwerking van bijzondere persoonsgegevens. Op dit verwerkingsverbod gelden de volgende uitzonderingen:

a. de betrokkene heeft uitdrukkelijke toestemming gegeven;
b. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
c. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
d. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;
e. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
f. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
g. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
h. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnosen, het verstrekken van gezondheidzorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsel en diensten;
i. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
j. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Verdere uitzonderingen zijn te vinden in nationale regelgeving.

De AVG bepaalt daarnaast dat verwerking van strafrechtelijke gegevens alleen is toegestaan door of onder toezicht van de overheid of als dit bij wet geregeld is.

De verwerking van nationale identificatienummers is alleen toegestaan ter uitvoering van de wet of voor doeleinden die bij wet zijn bepaald. Overheidsorganen kunnen bij de uitvoering van hun publieke taak gebruik maken van het burgerservicenummer, zonder dat daarvoor nadere regelgeving vereist is.

De Richtlijn schrijft voor dat verwerking van bijzondere persoonsgegevens slechts is toegestaan wanneer de verwerking strikt noodzakelijk is, geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van

betrokkene, en:
a. wettelijk is toegestaan;
b. noodzakelijk is om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen; of
c. die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Toelichting

De privacyregelgeving geeft als beginsel dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze.

De AVG regelt dat de verdere verwerking voor een ander doel toegestaan is indien de verdere verwerking berust op toestemming van de betrokkene of op een specifiek wettelijk voorschrift, dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van een belangrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, monetaire, budgettaire of fiscale aangelegenheden. Daarnaast wordt de verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkene te beschermen.

Bij **overheidsverwerkingen** moet de verwerkingsverantwoordelijke zelf beoordelen of de verdere gegevensverwerking voor een ander doel toegestaan en verenigbaar is aan de hand van:
a. het verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
b. de context waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke betreft;
c. de aard van de persoonsgegevens, met name bijzondere of strafrechtelijke persoonsgegevens;
d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkene;
e. het bestaan van passende waarborgen.

De Richtlijn staat de verdere verwerking van persoonsgegevens toe voor een doelstelling die binnen het toepassingsgebied van de Richtlijn valt, niet zijnde die waarvoor zij zijn verzameld, voor zover:
a. de verwerkingsverantwoordelijke overeenkomstig de wet gemachtigd is deze persoonsgegevens voor een dergelijk doel te verwerken; en
b. de verwerking noodzakelijk is en in verhouding staat tot dat andere doel.

Aandachtspunt 12: Leg indien mogelijk vooraf in het doel van analyse vast.

Het is raadzaam het type product te noemen dat uit de Big Data analyse zou moeten komen. Daarbij kan worden gedachten aan de volgende producten:
- Trendrapportages (bijvoorbeeld een rapportage over ontwikkelingen rond fraude),
- Rapportages waarin op bepaalde terreinen patronen worden blootgelegd (bijvoorbeeld een rapportage over fraudepatronen)
- Groepsprofielen (bijvoorbeeld een profiel met kenmerken van een beroepsfraudeur en diens “modus operandi”) en
- Overzichten van personen die een verhoogd risico laten zien dat zij een bepaald

gedrag vertonen of bepaalde activiteiten verrichten (bijvoorbeeld een lijst van personen die een verhoogd risico laten zien dat zij op een bepaald terrein fraude plegen).

Deze producten kunnen worden meegenomen in de vorm van een rapportage die leidt tot meer inzicht in de benoemde casussen en personen.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?.

Toelichting

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord 'noodzakelijk' in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?). Daarbij zal onder meer moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken. Daarbij kunnen empirische onderzoeksresultaten helpen.

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt. Bijvoorbeeld:

- Kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?
- Kan het verwerken van de persoonsgegevens in een beperktere vorm of met minder verwerkingen?

Zo kan in bepaalde gevallen met foto's hetzelfde doel worden bereikt (bijvoorbeeld: identificatie) als met het verwerken van filmbeelden. Het subsidiariteitsbeginsel houdt bijvoorbeeld ook in dat als persoonsgegevens openbaar gemaakt gaan worden, niet automatisch alle persoonsgegevens openbaar worden gemaakt, maar een selectie wordt gemaakt op grond van gerechtvaardigde criteria. Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Aandachtspunt 13: Bepaal de foutmarge

Toepassing van profielen op concrete situaties levert vrijwel altijd een foutmarge op, omdat een profiel altijd over- of onderinclusief is. Het is daarom wenselijk bij iedere analyse gaande het proces de acceptabele foutmarge te bepalen. Daarbij dient niet alleen te worden gelet op de potentiële impact op de privacy en de veiligheid, maar ook de zeldzaamheid van het fenomeen waarop de analyse betrekking heeft. Naarmate de potentiële gevolgen van het gebruik van de profielen voor het individu of

de maatschappij groter worden, neemt ook het belang van adequate benchmarks toe. Ook de behoefte om de toelaatbare foutmarge te bepalen kan worden herleid tot artikel 5 AVG, waarin is bepaald dat persoonsgegevens op behoorlijke wijze worden verwerkt.

15. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen dat is toegestaan.

Toelichting

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen. Het betreft het recht op informatie, het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, een kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens, het recht op overdraagbaarheid van gegevens, het recht van bezwaar en het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit. Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen moeten altijd op een nationale wet berusten, direct zijn toegestaan op grond van de bepalingen in de Europese privacyregelgeving.

Geef bij overheidsverwerkingen aan hoe invulling wordt gegeven aan de rechten van betrokkenen, bijvoorbeeld op welke wijze de betrokkenen worden geïnformeerd en hoe wordt omgegaan met een aanvraag voor correctie en wissing van gegevens.

Indien de verwerkingsverantwoordelijke uitzonderingen wil maken op de uitoefening van bepaalde rechten van betrokkenen, geef aan waarom dat noodzakelijk is en op welke grond dat is toegestaan.

Aandachtspunt 14: Ga na of betrokkenen geïnformeerd dienen te worden over het feit dat over hen persoonsgegevens worden verwerkt.

Degene die als verwerkingsverantwoordelijke in de zin van de AVG optreedt, heeft in beginsel de plicht om een betrokkene te informeren over het feit dat over hem persoonsgegevens worden verstrekt c.q. verder worden verwerkt. Dat geldt zowel voor de verantwoordelijke die ten behoeve van de analyse gegevens verstrekt, als de verantwoordelijke (de opdrachtgever) die deze gegevens daartoe verder verwerkt. Let wel op uitzonderingsmogelijkheden op deze verplichting betrokkenen te informeren, zoals onder meer vastgesteld in artikel 15 lid 5 onder b AVG, artikel 24a lid 5 Wpg en 39ha, lid 3 Wjsg. Daarnaast dient met betrekking tot de informatieplicht een splitsing te worden gemaakt tussen de analyses die wel en niet worden geoperationaliseerd.

Aandachtspunt 15: Transparantie

Ontwikkel een ‘Whitebox’ waarmee men kan achterhalen welke variabelen zijn gebracht, indien mogelijk welke triggers worden gehanteerd en welke beslissingen op basis daarvan zijn genomen. Pas daarnaast gelaagde transparantie en controle toe. Wanneer een overheidsorganisatie over haar Big Data toepassingen wel in algemene termen transparantie betracht maar bepaalde, meer gedetailleerde aspecten met het oog op bijvoorbeeld het belang van de opsporing of rekening houdend met gaming the system niet openbaar maakt, dient zij een dergelijke handelswijze tenminste te compenseren met voldoende toezicht op die aspecten.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Toelichting

Volgens de privacyregelgeving dient een PIA een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen te bevatten. Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico. Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:
1. risico's identificeren;
2. risico's inschatten/analyseren;
3. risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging. Daarom kan ook gebruik gemaakt worden van informatie die daaruit naar voren is gekomen. Anders dan bij deze risicoafweging die gericht is op de betrouwbaarheidseisen voor informatiesystemen, en daarmee de risico's voor de verantwoordelijke (zoals aanpassing, vertrouwen, publiciteit, toezicht en handhaving, dienstverlening, betrouwbare informatie), ziet de risicoafweging van de PIA op de risico's voor de betrokkenen.

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse moet worden uitgevoerd. Het verdient aanbeveling om aan te sluiten bij internationale standaarden, bijvoorbeeld van de International Organization of Standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) en Organisation for Economic Co-operation and Development (OECD).

1. Risico's identificeren

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens. Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

Big Data

Toelichting: Big Data Analyse

Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie. Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties:

- waar de gegevensverwerking kan leiden tot:
  - discriminatie, stigmatisering en uitsluiting;
  - (blootstelling aan) identiteitsdiefstal of -fraude;
  - financiële verliezen;
  - reputatie- of anderszins relationele schade;
  - verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
  - ongeoorloofde ongedaanmaking van pseudonimisering;
  - of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;
- wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2. Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit antwoorden, maar op een afweging. Aan de hand hiervan moet een risiconiveau worden bepaald.

De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking. Alsook van de aard van de persoonsgegevens. Persoonsgegevens die de sleutel vormen voor toegang tot geldelijke middelen of waarmee een betrokkene te chanteren is, zijn aantrekkelijk voor hackers. Denk hierbij aan de inloggegevens voor DigiD of een datingwebsite.

De kans dat zich gevolgen voordoen voor de rechten en vrijheden van de betrokkenen, kan tevens verband houden met de (mate van) beveiliging van de persoonsgegevens. De al dan niet opzettelijke:

- vernietiging en verlies (beschikbaarheid);
- wijziging (integriteit);
- ongeoorloofde toegang en verstrekking (vertrouwelijkheid);van persoonsgegevens, kan leiden tot schade voor de betrokkene.

Voor het inschatten van de risico's kan het behulpzaam zijn om de betrokkenen of hun vertegenwoordigers te consulteren.

Big Data

Toelichting: Big Data Analyse

Big data-verwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen. Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

3. Risico's beoordelen

Definieer aanvaardbare risicowaarden en beoordeel of de risico's aanvaardbaar zijn.

Aandachtspunt 16: Let op bewustwording van risico's

Eigenaren, ontwerpers, bouwers, gebruikers en andere belanghebbenden van analytische systemen die gebruikt worden voor toepassingen met specifieke consequenties voor individuele burgers moeten zich bewust zijn van de mogelijke discriminerende- of stigmatiserende factoren die in ontwerp, implementatie en gebruik kunnen opleveren en de impact of schade die biases kunnen creëren voor individuele burgers en samenleving.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt bezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Toelichting

Denk bij maatregelen bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

Daarnaast kunnen de maatregelen ook beveiligingsmaatregelen omvatten. De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op een dusdanige manier wordt verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Big Data

Toelichting: Big Data Analyse

De verwerkingsverantwoordelijk moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In het begrip passend ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip passend duidt mede op een proportionaliteit tussen de maatregelen en erkende privacyrisico's. Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens. Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen. Beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom dit aanvaardbaar wordt geacht.

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en controlcyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismen.

Ter illustratie noemt de AVG de volgende maatregelen:

a. pseudonimiseren en versleutelen van persoonsgegevens;

b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- opslag van gegevens in een kluis;
- project-, risico- en incidentenmanagement;
- data opsplitsen;
- dataminimalisatie;
- back-ups;
- integriteitscontroles;
- meerfactor-authenticatie;
- monitoring en logging;
- controle van toegekende bevoegdheden;
- privacybewustzijn- en beveiligingstrainingen;
- managementrapportages over risicobeheer;
- beperken inzageniveau;
- periodiek een audit of hack- of penetratietest uitvoeren;
- richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- responsible-disclosurebeleid;
- geheimhoudingsverklaringen;
- service level agreements (met boeteclausules);
- overwerkersovereenkomsten;
- screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Rijksdienst (BIR).

Big Data

Toelichting: Big Data Analyse

De Richtlijn noemt tot slot de volgende maatregelen:
a. controle op de toegang tot de apparatuur;
b. controle op de gegevensdragers;
c. opslagcontrole;
d. gebruikscontrole
e. controle op de toegang tot gegevens;
f. transmissiecontrole;
g. invoercontrole;
h. transportcontrole; en
i. herstelmogelijkheid.

De Richtlijn verplicht tot het bijhouden van logbestanden van bepaalde vormen van verwerkingen, opdat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens

Big Data

Bij Big data-analyses (zie punt 8) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden.
- Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegevens in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van big data-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen.

- Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming.
- Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Aandachtpunt 17: Denk aan gebruikersgemak

Voorkom bureaucratisering door te zware protocollen en procedures in te richten t.b.v. risicobeperking, laat ruimte voor kansen en onderzoeksvrijheid in verhouding tot het doel en de impact van het onderzoeksgebied.

Organisatorische maatregelen

Aandachtspunt 18: Hanteer de modelverwerkersovereenkomst/de model verwerkersafsprakenovereenkomst/protocol

De verwerker verwerkt gegevens voor de uitvoering van de analyse overeenkomstig de instructies en onder verantwoordelijkheid van de opdrachtgever. De uitvoering van de verwerking door de bewerker dient op grond van de privacywetgeving te worden geregeld in een overeenkomst. Daarin dienen waarborgen te worden opgenomen voor een professionele en zorgvuldige verwerking van gegevens. Het nieuwste model Verwerkersovereenkomst is te vinden op Rijksportaal.

Big Data

Toelichting: Big Data Analyse

Aandachtpunt 19: Maak afspraken over transport van data

Indien er sprake is van een gegevensverwerker: maak afspraken over welke veiligheids-maatregelen er getroffen dienen te worden met betrekking tot het transport, de verwerking en eventueel de vernietiging van de gegevens. Daarbij kan, afhankelijk van de aard van de analyse en de kosten, onder meer worden gedacht aan het anonimiseren of pseudonimiseren van gegevens. Zo kunnen onder meer de volgende acties worden uitgezet ter beveiliging van het transport van data dat op gegevensdragers is vastgelegd:

- Op het transport device opgeslagen data versleutelen (minimaal AES-256);
- De sleutel via een separaat kanaal beschikbaar stellen aan de ontvanger. Contactgegevens hiervoor worden vooraf beschikbaar gesteld;
- Transport device kan fysiek beveiligd worden, bijvoorbeeld een afgesloten container;
- Transport device kan zodanig worden verpakt en verzegeld dat niet te zien is waar het om gaat en verbreken verzegeling te zien is;
- Een koeriersdienst het transport en tekening voor ontvangst laten uitvoeren;
- Gegevensdrager op het moment van levering controleren en partijen laten tekenen voor ontvangst.

Aandachtpunt 20: Richt een zorgvuldig autorisatiebeleid in.

Bevoegdheden van gebruikersaccounts dienen zo goed mogelijk te worden gekoppeld aan de functie van een bepaalde medewerker. Denk aan Role based autorisatie structuur'.

Aandachtpunt 21: Zorg er voor dat Big Data analyse door derden kan worden gecontroleerd

Betrek indien mogelijk proactief controlerende partijen. Denk hierbij aan de 'Proof of Ability' toets van een controlerende partij zoals de ADR. Er kan worden gewerkt met audit-logbestanden (controle van systeemgebruik en bescherming van informatie in logbestanden).

Technische maatregelen

Aandachtpunt 22: Zorg voor voldoende beveiliging tijdens de verstrekking en verdere verwerking van data ten behoeve van de analyse.

Ingevolge artikel 32 AVG dient de verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen dienen, rekening houdend met de stand van de techniek en de uitvoeringskosten, een passend beveiligingsniveau te garanderen, gelet op de risico's die die de verwerking en de aard van te beschermen gegevens meebrengen. In artikel 4a Wpg en artikel 7 Wjsg zijn hiermee vergelijkbare bepalingen opgenomen. Omdat het bij Big Data analyses om verwerking van grote hoeveelheden data gaat, is de verantwoordelijkheid voor een goede beveiliging van de data navenant groot.

Mogelijke maatregelen om gegevens te beveiligen zijn de volgende:

1. Indien de combinatie van de gegevensbronnen heel gevoelig is, zou deze hetzelfde regime kunnen volgen als (hoog)gerubriceerde informatie, zoals in het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie voorschrijft ;
2. Indien de gegevensverwerkende organisatie de informatiebeveiliging onvoldoende op orde heeft, kan het werken op een geïsoleerd netwerk dat geen verbinding heeft met het internet een oplossing zijn.
3. Zorg na afloop van het experiment voor vernietiging van de data en indien nodig, bewijs voor vernietiging van de data.

Big Data

Toelichting: Big Data Analyse

Interne maatregelen

Aandachtspunt 23: Ga na of de verwerking moet worden gemeld bij de Functionaris voor de gegevensbescherming.

Ingevolge [verwijzing interne procedure] moet Big Data analyse worden gemeld bij de Functionaris voor de gegevensbescherming. Of er daadwerkelijk moet worden gemeld, hangt af van de toets die in het concrete geval dient uit te maken of Big Data analyse moet worden gemeld bij de FG.

Aandachtspunt 24: Zorg voor een goede evaluatie van het analyse-traject en de uitkomst daarvan.

Het is van belang om het analyse-traject en de uitkomst daarvan goed te evalueren, omdat deze evaluatie een rechtvaardiging kan opleveren voor een eventuele overstap in de toekomst naar analyse voor operationeel gebruik, waarbij ook een toetsing heeft plaatsgevonden aan een aantal principes met betrekking tot het beschermen van persoonsgegevens. Daartoe is het wenselijk om tijdens het analysetraject aantekening te houden van een aantal zaken die relevant voor het uitvoeren van de evaluatie zijn. Het gaat daarbij om zaken die kunnen helpen om bij de evaluatie antwoord te geven op tenminste de volgende vragen:

1. Zijn (de extracten uit) de datasets die bij de analyse zijn betrokken, alle voldoende relevant geweest of zijn er die niet meer betrokken behoeven te worden in een analyse voor operationeel gebruik?
2. Is de opbrengt van de analyse van voldoende waarde om de noodzaak van verwerking van de gebruikte data te kunnen rechtvaardigen als de overstap wordt gemaakt naar analyse voor operationeel gebruik?
3. Hebben zich bij de uitvoering van de stappen uit dit kader bijzonderheden voorgedaan waarmee bij een overstap naar analyse voor operationeel gebruik rekening moet worden gehouden?
4. Is de analyse met het oog op transparantie en verantwoording achteraf reproduceerbaar?

Aandachtspunt 25: pas indien mogelijk certificering, normenkaders en gedragscodes toe

Aan de hand van certificeringen (NEN-ISO/IEC 27000, subnormen: ISO/IEC 27001 en 27002) en normenkaders zoals het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) kan in bepaalde gevallen aantonen dat wordt voldaan aan bepaalde vereisten op het gebied van beveiliging van gegevens. Certificeringen, normenkaders en gedragscodes kunnen ook worden meegenomen als eis in een aanbesteding rond Big Data analyse.

Aandachtspunt 26: richt een goed monitoring- en loggingsbeleid in

Mede gelet op de vereisten van de Richtlijn Strafvorderlijke gegevens is het van belang om een goed monitoring- en loggingsbeleid aan te leggen, zodat Big Data analyse op zorgvuldige wijze tot stand kan worden gebracht.

Aandachtspunt 27: maak resultaten openbaar

Maak de resultaten van de Big Data analyse indien mogelijk openbaar.

Colofon

Ministerie van Justitie en Veiligheid
Directie Informatisering & Inkoop
Postbus 20301 | 2500 EH Den Haag

informatieplan@minvenj.nl

Den Haag | april 2018