Bijlage I: Toelichting op het invullen van risico's en mitigerende maatregelen in sectie 5

In sectie 5 moeten de volgende twee onderdelen uitgewerkt te worden:

A. Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.
B. Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen te mitigeren.

Risicomethodiek

De privacyregelgeving schrijft niet voor op welke wijze de risicoanalyse uitgevoerd moet worden. Binnen UWV wordt vaak de CRSA methode gehanteerd. Deze methodiek bestaat uit tenminste 1 bijeenkomst waarin de risico's worden geïnventariseerd en beoordeeld. Vervolgens wordt gekeken naar de maatregelen om de geïnventariseerde risico's te voorkomen, dan wel te verminderen. Belangrijk bij deze methode is dat de risico's en maatregelen vanuit verschillende disciplines worden bekeken.
Welke methode ook wordt gehanteerd om de risico's te beschrijven, een multidisciplinaire blik is sterk aan te bevelen. Gezien het onderwerp is het sowieso aan te raden kennis uit het IB&P domein te betrekken, denk aan de collega's van het decentrale IB&P team (BSO/Coördinator IB&P), maar ook de collega's van CISO-Office en Juridische Zaken.

Uitwerking risicomatrix

Het is belangrijk dat risico's op een eenduidige manier worden beschreven. Allereerst om de risico's binnen de GEB goed te kunnen beoordelen. Het is daarnaast ook noodzakelijk dat de verschillende GEBs op een vergelijkbare manier tot hun risicobeoordeling komen. Dit leidt ertoe dat er eisen gesteld worden aan de wijze waarop de risico's worden beschreven en de wijze waarop de risico's worden geclassificeerd. In de GEB wordt hiervoor onderstaande matrix gebruikt:

Identificeren risico's	**Risico 1**	Het risico op: [wat treedt erop] Als gevolg van: [gebeurtenis/activiteit] Veroorzaakt door: [oorzaak, kwetsbaarheid of issue (vaak een maatregel die niet of slecht is geïmplementeerd of niet effectief is)].
	Consequenties voor betrokkene	[Wat zijn de mogelijke negatieve gevolgen voor betrokkenen?] *Voorbeeld:* *Identiteitsfraude, stigmatisering, uitsluiting, chantage*
Classificeren risico	**Classificatie (Kans / Impact)**	Kans score: [tussen 1 en 5] Impact score: [tussen 1 en 5] Classificatie: [kans*impact]
Uitwerking mitigerende maatregelen	**Maatregel**	Geïmplementeerde maatregelen: [beschrijf de maatregelen die reeds zijn geïmplementeerd en het effect op het risico] Geplande maatregelen: [beschrijf de voorgenomen maatregelen en het beoogde effect op het risico]
	Geplande maatregelen binnen scope project/wijziging	[Valt de geplande maatregel binnen de scope van het project of wijziging? Zo nee, op welke wijze is implementatie van de maatregel geborgd?]
Risico-acceptatie	**Restrisico**	Restrisico na geïmplementeerde maatregelen: [Is er een restrisico aanwezig na implementatie van

		genomen maatregelen? Indien ja, motiveer waarom restrisico acceptabel is en wie is risico-acceptant] Restrisico na geplande maatregelen: [Is er een restrisico aanwezig na implementatie van geplande maatregelen? Indien ja, motiveer waarom restrisico acceptabel is en wie is risico-acceptant]

Per onderdeel (identificeren risico's, classificeren risico, uitwerking mitigerende maatregelen en risicoacceptatie) volgt een korte toelichting.

Identificeren risico's

De eerste stap is om potentiële privacyrisico's vast te stellen. Een privacyrisico is een potentieel negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens. Het gaat bij de GEB dus niet om de bestuurlijke risico's voor de organisatie (bijvoorbeeld imagoschade voor UWV).

Identificeren risico's	**Risico 1**	Het risico op: [wat treedt erop] Als gevolg van: [gebeurtenis/activiteit] Veroorzaakt door: [oorzaak, kwetsbaarheid of issue (vaak een maatregel die niet of slecht is geïmplementeerd of niet effectief is)].
	Consequenties voor betrokkene	[Wat zijn de mogelijke negatieve gevolgen voor betrokkenen?] *Voorbeeld:* *Identiteitsfraude, stigmatisering, uitsluiting, chantage*

Hieronder staan enkele voorbeelden van veel voorkomende privacyrisico's.

Onrechtmatige verwerking van persoonsgegevens

Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Als een grondslag ontbreekt, bijvoorbeeld wanneer er geen wettelijke taak is vastgelegd en toestemming als grondslag niet mogelijk is;
- Wanneer bijzondere persoonsgegevens worden verwerkt zonder dat er sprake is van een geldige uitzonderingsgrond;

De mogelijke consequentie van dit risico voor betrokkene is dat zijn gegevens ten onrechte door een organisatie of individu kunnen worden geraadpleegd, worden vastgelegd en verder worden verwerkt.

De verwerking van persoonsgegevens is niet transparant en/of niet 'behoorlijk'

Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- De verwerking is niet of onvolledig opgenomen in het register van verwerkingen;
- De verwerking is niet of onvolledig opgenomen in de privacyverklaring;
- De verwerking is niet maatschappelijk geaccepteerd en niet in lijn met wat de betrokkene in redelijkheid van UWV kon verwachten. Dit kan zich bijvoorbeeld voordoen bij het hergebruik van gegevens voor nieuwe doeleinden.

De mogelijke consequentie van dit risico voor betrokkene is dat hij geen weet heeft van de verwerking van zijn gegevens en daardoor geen gebruik kan maken van zijn rechten onder de AVG om de rechtmatigheid van de verwerking van zijn persoonsgegevens te controleren.

De verwerking van persoonsgegevens voldoet niet aan de vereisten van doelbinding

Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Gegevens die voor de ene taak van UWV zijn verzameld worden voor een andere taak gebruikt zonder dat dit verenigbaar is. Bijvoorbeeld gegevens die UWV als beheerder van de Polisadministratie verwerkt worden ingezet voor een analyse van het dienstverleningsproces.

De mogelijke consequentie van dit risico voor betrokkene is dat hij, nadat gegevens door UWV zijn verzameld, geen grip meer heeft op waar UWV deze gegevens voor inzet.

De verwerking van persoonsgegevens voldoet niet aan de beginselen van minimale gegevensverwerking

Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Er worden meer gegevens verwerkt dan strikt noodzakelijk doordat dit bijvoorbeeld handig is voor het proces of doordat het systeem niet voorziet in fijnmazig autorisatiebeheer.

De mogelijke consequentie van dit risico voor betrokkene is dat meer mensen kennis nemen van zijn persoonsgegevens dan strikt noodzakelijk of dat mensen kennis nemen van meer van zijn persoonsgegevens dan strikt noodzakelijk.

Gegevens worden langer bewaard dan noodzakelijk voor het doel van de verwerking (bewaartermijn)

Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Gegevens blijven langer in het archief staan/worden niet tijdig vernietigd doordat de ingangsdatum van de bewaartermijn niet is geregistreerd;
- Gegevens worden niet tijdig vernietigd doordat de applicatie hier niet in voorziet;
- Gegevens worden niet tijdig vernietigd doordat er geen proces is ingericht dat hier in voorziet;
- Gegevens worden niet tijdig vernietigd omdat de bewaartermijn onduidelijk is;
- Gegevens worden niet tijdig vernietigd doordat zij buiten doelsystemen zijn opgeslagen, zoals op sharepoint, op gezamenlijke of persoonlijke schijven en in mailboxen.

De mogelijke consequentie van dit risico voor betrokkene is dat medewerkers langer kennis kunnen nemen van zijn persoonsgegevens dan strikt noodzakelijk is. Zijn gegevens kunnen mogelijk voor andere verwerkingen van UWV worden ingezet of worden gedeeld nadat deze al vernietigd hadden moeten zijn. Het zal niet in de lijn der verwachting van betrokkene liggen dat zijn gegevens nog steeds worden verwerkt, waardoor hij mogelijk ook minder snel geneigd is om gebruik te maken van zijn rechten om de verwerking te controleren.

Inbreuk op de vertrouwelijkheid van persoonsgegevens

Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Door een inbreuk op of gebrek in de technische of organisatorische beveiliging van persoonsgegevens (datalek). Bijvoorbeeld als gevolg van
  - onveilige uitwisseling van gegevens via open email;
  - het gebruik van een verkeerd (post)adres;
  - een kwetsbaarheid in de applicatie of infra die door een hacker wordt gebruikt.
- Als gevolg van het feit dat er gegevens ontsloten worden van teveel betrokkenen of dat er van betrokkenen teveel gegevens ontsloten worden, doordat autorisatiebeheer niet voldoende fijnmazig is ingericht;
- Als gevolg van het feit dat persoonsgegevens bij ingang van de bewaartermijn niet worden afgeschermd tegen inzage door medewerkers in het primaire proces. Bijvoorbeeld doordat een systeem niet zo is ingericht of doordat gegevens buiten doelsystemen staan waar niet wordt geschoond;
- Als gevolg van het feit dat persoonsgegevens buiten doelsystemen worden opgeslagen (bijvoorbeeld op sharepoint, in mailboxen, op groepsschijven of persoonlijke schijven) waardoor zij onttrokken worden aan autorisatiebeheer;
- Als gevolg van gebruik van productiedata buiten de productieomgeving, bijvoorbeeld in de testomgeving.

De mogelijke consequentie van dit risico voor betrokkene is dat zijn persoonsgegevens zijn ingezien door en mogelijk nog in bezit zijn van iemand voor wie deze gegevens niet zijn bedoeld.

Afhankelijk van om welke gegevens het gaat kan deze persoon de persoonsgegevens bovendien misbruiken voor stigmatisering van betrokkene, chantage, spear phishing of ID-fraude.

Inbreuk op de integriteit van gegevens
Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Gegevens kunnen ongecontroleerd gewijzigd worden doordat de applicatie niet logt en/of monitort of doordat gegevens buiten doelsystemen worden opgeslagen.
- Gegevens kunnen ongecontroleerd gewijzigd worden door een inbreuk op of gebrek aan technische of organisatorische beveiliging van persoonsgegevens (datalek). Bijvoorbeeld als gevolg van een onveilige uitwisseling van gegevens, een fout waardoor een bestand verkeerd wordt overschreven of een kwetsbaarheid in de applicatie of infra die door een hacker wordt misbruikt.

De mogelijke consequentie voor betrokkene is dat niet kan worden vastgesteld wie zijn gegevens heeft gewijzigd en of de gegevens nog juist zijn. Mogelijk zijn de gegevens op zodanige wijze veranderd dat dit nadelig is voor betrokkene, bijvoorbeeld omdat hij door een wijziging in de Polisadministratie niet meer aan de wekeneis voor een WW-uitkering voldoet.

De rechten van betrokkenen zijn onvoldoende gewaarborgd
Voorbeelden van wanneer dit kan optreden (gebeurtenis/activiteit en oorzaak):

- Er kan geen gevolg worden gegeven aan een inzageverzoek doordat onvoldoende overzicht bestaat van waar de persoonsgegevens zicht bevinden;
- Er kan geen gehoor worden gegeven aan een inzageverzoek doordat het proces niet goed is ingericht;
- Er kan geen gevolg worden gegeven aan een inzageverzoek doordat de applicatie geen overzicht van de verwerkte persoonsgegevens in een gangbaar format kan genereren;
- Er kan geen gevolg worden gegeven aan het recht op vergetelheid omdat onduidelijk is waar de gegevens allemaal zijn opgeslagen (bijvoorbeeld ook buiten archief en doelsystemen);
- Er kan geen gevolg worden gegeven aan het recht op vergetelheid doordat de applicatie geen gegevens kan verwijderen.

De mogelijke consequentie van dit risico voor betrokkene is dat hij geen controle kan uitoefenen op de rechtmatigheid van de verwerking van zijn persoonsgegevens.

Classificeren risico's
Nadat de risico's en de gevolgen voor betrokkenen in kaart zijn gebracht, moet het risico worden geclassificeerd. Zoals aangegeven is het belangrijk dat de risico's binnen een GEB goed onderling vergeleken kunnen worden. Het is daarnaast ook belangrijk dat GEBs op een vergelijkbare manier de risico's classificeren, zodat bijvoorbeeld de beoordeling of een verwerking een hoog risico verwerking is op eenzelfde manier tot stand is gekomen.

Voor de GEB wordt gebruikt gemaakt van onderstaande kwalificatie:

Classificeren risico	**Classificatie (Kans / Impact)**	Kans score: [tussen 1 en 5] Impact score: [tussen 1 en 5] Classificatie: [kans*impact]

Kans
De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking (is het middel gevoelig voor een inbreuk), maar ook van de aard van de persoonsgegevens (zijn de persoonsgegevens zo waardevol dat kwaadwillenden er veel effort in willen steken om ze te bemachtigen) en het dreigingsbeeld. 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 (gezondheids)gegevens van VIPs.

Impact
De impact/ernst van de risico's hangt af van de context van de verwerkingen:

- de aard van de persoonsgegevens (gaat het om 'gewone' persoonsgegevens of bijv. om gezondheidsgegevens?)
- de aard van de verwerkingen (gaat het alleen om het vastleggen van gegevens of worden gegevenssets gekoppeld en wordt gebruik gemaakt van geautomatiseerde besluitvorming?)
- de doeleinden waarvoor de gegevens worden verwerkt (maakt de verwerking onderdeel uit van het primaire proces van UWV of gaat het bijv. om ondersteuning van de bedrijfsvoering?).

De risicoclassificatie (kans*impact) is vervolgens volgens onderstaande matrix in te delen:

Legenda Risico matrix						
	Kans	1	2	3	4	5
Impact		zeer klein	klein	redelijk	groot	zeer groot
5	zeer groot	5	10	15	20	25
4	groot	4	8	12	16	20
3	redelijk	3	6	9	12	15
2	beperkt	2	4	6	8	10
1	minimaal	1	2	3	4	5

	Risicoclassificatie
	Zeer klein
	Klein
	Gemiddeld
	Groot/zeer groot

Uitwerking mitigerende maatregelen
De verwerkingsverantwoordelijke 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 huidige stand van de techniek. Het begrip passend duidt tevens op proportionaliteit tussen de maatregelen en erkende privacyrisico's. 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.
Naarmate de risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens.

In de risicomatrix wordt gevraagd inzicht te geven in de bestaande maatregelen en de geplande maatregelen. Hierdoor wordt het makkelijker om het restrisico te duiden op het moment van schrijven van de GEB en het restrisico in te schatten nadat ook de geplande maatregelen zijn genomen.
Houdt bij het beschrijven van mitigerende maatregelen ook rekening met de oorzaak. Ofwel draagt de bestaande, dan wel geplande maatregel bij aan het terug brengen van de kans en impact.

Uitwerking mitigerende maatregelen	**Maatregel**	Geïmplementeerde maatregelen: [beschrijf de maatregelen die reeds zijn geïmplementeerd en het effect op het risico] Geplande maatregelen: [beschrijf de voorgenomen maatregelen en het beoogde effect op het risico]
	Geplande maatregelen binnen scope project/wijziging	[Valt de geplande maatregel binnen de scope van het project of wijziging? Zo nee, op welke wijze is implementatie van de maatregel geborgd?]

Op basis van het Privacy by Design/by Default Beleid kunnen de benodigde privacyborgende- en beveiligingsmaatregelen worden afgeleid. Het beleidskader PbDD van het CISO Office kan hier gevonden worden: Privacy en Security by Design

In het PbDD beleidskader zijn voornamelijk technische maatregelen beschreven. Daarnaast kan ook gedacht worden aan de volgende organisatorische maatregelen, zoals:

- Privacybewustzijn- en beveiligingstrainingen (Awareness en Gouden regels)
- UWV richtlijnen voor gebruik ICT-hulpmiddelen en systemen (Gedragscode)
- Screening personeel en VOG-verklaring (screening en VOG)
- Geheimhoudingsverklaring
- Afspraken over thuiswerken en toegang tot systemen (Gedragscode)
- 4 Ogen principe

De onderstaande tabel geeft een bondig overzicht van de verschillende (technische) maatregelen die overwogen kunnen worden en die van links naar rechts doorlopen kan worden.

Anonimi-seren	**1. Dataminima-lisatie**	**2. Pseudonimi-seren**	**3. Encryptie**	**4. Access control**	**5. Data protection by default**	**6. Bewaarter-mijnen**	**7. Rechten van betrokkenen**
Anonimiseren van persoonsgegevens waar dat kan. Indien niet mogelijk, dan de tabel vervolgen.	Welke gegevens zijn strikt noodzakelijk voor het doel van verwerking (proportionaliteit)?	Identificerende gegevens worden verwijderd en gescheiden bewaard.	Versleuteling van persoonsgegevens bij opslag of transport.	Toegangscontrole van zowel fysieke als logische toegang.	Privacyvriendelijke settings als uitgangspunt	Indien gegevens niet meer mogen worden bewaard moeten ze worden vernietigd (Archiefwet)	- Actieve informatieplicht - Recht van inzage - Recht van correctie
UWV richtlijn : TDA (CISO)	UWV richtlijn: Data Life Cylce Management (DataOffice)	UWV richtlijn: TDA (CISO)	UWV richtijn: Cryptografie (CISO) SSD (CISO)	UWV richtlijn: - Fysieke beveiliging (FB) - Autorisatiebeheer (BZ) - Logging & Monitoring (CISO)	UWV richtlijn: SSD (CISO)	UWV richtlijn: - Data Life Cycle Management (GD) - Selectielijst (FB DIV)	UWV richtlijn: - Inzage-verzoek (BZ) - Correctie-verzoek (BZ) - Privacystate-ment (K&S)

Risico acceptatie

Tot slot, beveiligingsrisico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een restrisico zal overblijven. Bij dit onderdeel moet beschreven worden wat het restrisico is na implementatie van de genomen en/of geplande maatregelen. Daarnaast moet aangegeven waarom het restrisico acceptabel is en wie risicoacceptant is.
Als uit de GEB komt dat de (voorgenomen) verwerking een hoog privacyrisico met zich mee brengt en het niet lukt om (voldoende) maatregelen te vinden om dit risico te beperken, dan is overleg met de Autoriteit Persoonsgegevens (AP) noodzakelijk. Middels een voorafgaande raadpleging geeft de AP advies hoe de risico's van de voorgenomen verwerking kunnen worden beperkt. Het kan ook zijn dat de AP adviseert om af te zien van de verwerking. UWV kan bij de constatering dat een verwerking een hoog privacy met zich mee brengt ook zelf besluiten de verwerking niet uit te voeren of te staken.

Risico-acceptatie	**Restrisico**	Restrisico na bestaande maatregelen: [Is er een restrisico aanwezig na implementatie van genomen maatregelen? Indien ja, motiveer waarom restrisico acceptabel is en wie is risico-acceptant] Restrisico na geplande maatregelen: [Is er een restrisico aanwezig na implementatie van geplande maatregelen? Indien ja, motiveer waarom restrisico acceptabel is en wie is risico-acceptant]

Onderstaande tabel geeft aan hoe de risico's geclassificeerd worden en wie, afhankelijk van de risicoclassificatie, de risico's kan accepteren. Uitgangspunt is dat de directie van het bedrijfsonderdeel de risico's moet accepteren, wel kan risicoacceptatie bij (zeer) kleine risico's gedelegeerd worden aan de domeinhouder/verantwoordelijk management. De Business Security Officer (BSO) kan **geen** risico's accepteren. De BSO geeft in paragraaf 6.2 een reactie op de GEB waarin ook een advies wordt gegeven over de restrisico's.

Legenda Risico matrix						
	Kans	**1**	**2**	**3**	**4**	**5**
Impact		**zeer klein**	**klein**	**redelijk**	**groot**	**zeer groot**
5	**zeer groot**	**5**	**10**	**15**	**20**	**25**
4	**groot**	**4**	**8**	**12**	**16**	**20**
3	**redelijk**	**3**	**6**	**9**	**12**	**15**
2	**beperkt**	**2**	**4**	**6**	**8**	**10**
1	**minimaal**	**1**	**2**	**3**	**4**	**5**

	Risicoclassificatie	**Risicoacceptatie door**
	Zeer klein	Directie bedrijfsonderdeel, gedelegeerd aan domeinhouder/verantwoordelijk management
	Klein	Directie bedrijfsonderdeel, gedelegeerd aan
	Gemiddeld	Directie bedrijfsonderdeel
	Groot/zeer groot	Directie bedrijfsonderdeel **en mogelijk** Raad van Bestuur

Bijlage II: Hulpmiddel bij het uitvoeren van een GEB voor verwerkingen met complexe data-analyses, algoritmen, (klant)profilering, risicomodellen, geautomatiseerde besluitvorming e.d.

Wanneer kan je deze bijsluiter gebruiken?

Deze bijsluiter is bedoeld om **te helpen bij het uitvoeren van een GEB** voor voorgenomen verwerkingen die bestaan uit **(complexe) data-analyses**[1] (bijv. op basis van gegevens in artikel 5 lid 2 sub d artikel 5 lid 2 sub d Woo of een andere analyseomgeving) en toepassing van **algoritmen**. Het kan daarbij gaan om verwerkingen die tot doel hebben **klanten te profileren** (indelen in groepen) door het ontwikkelen van klantprofielen, klantsegmenten, risicomodellen e.d. Deze toelichting is verder handig wanneer de verwerking is gericht op **geautomatiseerde besluitvorming** met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokken.

Waarom deze bijsluiter?

De hierboven genoemde verwerkingen zijn verwerkingen met een **hoog risico** voor de privacy van de betrokkenen. Het gaat om verwerkingen waarbij vaak **zeer veel persoonsgegevens** worden gecombineerd. Ook kunnen dergelijke verwerkingen soms aanzienlijke **gevolgen voor de betrokkene** hebben. Daarom is het van belang om voor deze verwerkingen een goede GEB uit te voeren. Om te helpen de GEB zo volledig mogelijk in te vullen, heeft Bureau Gegevensbescherming deze bijsluiter als hulpmiddel opgesteld.

Hoe gebruik je deze bijsluiter?

Hieronder wordt voor de onderdelen 3 (beschrijving van de verwerking), 4 (beoordeling rechtmatigheid verwerking) en 5 (risico's en maatregelen) van het GEB-sjabloon toegelicht welke informatie in het GEB-rapport voor dergelijke verwerkingen moet worden opgenomen. Hoe ga je nu te werk?

Stap 1: Download een leeg GEB-sjabloon van DWU.
Stap 2: Vul het voorblad en onderdeel 2 in.
Stap 3: Pak deze bijsluiter erbij en lees welke informatie in ieder geval bij de vragen in hoofdstuk 3 en 4 moet worden opgenomen. Aanbevolen wordt om zeker bij hoofdstuk 4 de expertise van JZ te betrekken.
Stap 5: Vul de risico-maatregelenmatrix (hoofdstuk 5) in en neem, indien van toepassing, daarbij de risico's die in deze bijsluiter worden genoemd mee.
Stap 6: Vul hoofdstuk 6 in en lever de GEB in bij je BSO. Deze beoordeelt de kwaliteit, vult zijn of haar advies in en stuurt de GEB naar de FG.

Bestaat de verwerking uit verschillende fasen? Beschrijf dan alle fasen.

Sommige verwerkingen waarvoor deze bijsluiter is bedoeld, bestaan uit verschillende fasen. Denk bijvoorbeeld aan project of pilot waarbij eerst een grote hoeveelheid historische data wordt geanalyseerd met als doel bepaalde verbanden te ontdekken en daarmee een model (beslisregels) of een klantprofiel te ontwikkelen. Vervolgens wordt het ontwikkelde model in het primaire proces van UWV ingezet. Daarna kan weer sprake zijn van een fase waarin de gegevens die zijn verzameld bij de toepassing van het model worden gebruikt om de juistheid van het model te verifiëren en/of om het model verder te ontwikkelen.

Bestaat de verwerking uit verschillende fasen, beschrijf dan in de GEB al die fasen en beantwoord de vragen voor alle fasen.

---

[1] Denk hierbij aan data-analyses waarbij meer dan 6 categorieën van persoonsgegevens worden verwerkt.

Nog een tip.

Lees paragraaf 5.8 van het UWV Beleidskader Privacy voor meer informatie over de eisen die de AVG stelt aan dit soort verwerkingen.

GEB-rapport en algoritmen

Hieronder volgt voor een aantal onderdelen van het GEB-rapport specifieke aandachtspunten voor verwerkingen met algoritmen. Neem deze aandachtspunten mee in het GEB-traject en verwerk ze in het GEB-rapport.

Hoofdstuk 3 Beschrijving van de (voorgenomen) gegevensverwerking

3.1 Wat is de aanleiding van de verwerking?

Geef aan waarom wordt gekozen voor een toepassing van algoritmen, klantprofilering e.d. Geef hier ook aan wie het besluit heeft genomen om het project te starten. Geef ook aan of dit project al besproken is in de Adviescommissie data-gestuurd werken. Zo ja, geef aan wat het oordeel van de commissie is.

3.3 Verwerkte categorieën van personen en verwerkte persoonsgegevens

Neem in de Excel-bijlage bij het rapport zo nauwkeurig mogelijk op:

a. van welke personen gegevens worden gebruikt voor de analyse of ontwikkeling van het model (bijv. welke selectie van personen die in artikel 5 lid 2 sub staan is gemaakt); en
b. Een zo volledig mogelijke opsomming van de persoonsgegevens (denk ook aan (gedrags)kenmerken of andere variabelen die worden meegenomen bij de analyse). Als de verwerking uit verschillende fasen bestaat, geef dan duidelijk aan welke persoonsgegevens in welke fase van de verwerking worden verwerkt.
c. Geef het doel waarvoor zij oorspronkelijk zijn verkregen. Dit laatste is van belang voor de beantwoording van de vraag of het gebruik van deze gegevens voor de ontwikkeling van het model verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verkregen (zie vraag 4.5).

Beschrijf in het rapport op welke personen het model uiteindelijk zal worden toegepast.

3.4 Beschrijf de verwerking

Beschrijf hier de verschillende fasen van de verwerking (het verzamelen van de gegevens, het analyseren daarvan, het testen van een model, het toepassen van het model in het primaire proces, controleren van de betrouwbaarheid (valideren) van het model etc).

Maak bij de beschrijving van de verwerking een onderscheid tussen de verschillende fasen en beschrijf per fase wat de verwerking inhoudt. Indien gebruik wordt gemaakt van algoritmen, beschrijf dan in begrijpelijke taal hoe het algoritme werkt en hoe het model wordt getraind. Beschrijf ook hoe het model wordt getest en of daarbij gebruik wordt gemaakt van externe expertise (universiteit, IT auditors etc.)

Beschrijf vervolgens hoe het model wordt gebruikt in het primaire proces (productie). Worden in de uitvoering naast de gevallen/dossiers die het model heeft opgeleverd ook willekeurig geselecteerde gevallen/dossiers meegenomen, bijv. om het model te toetsen, aan medewerkers aangeboden? Is er sprake van een feedbackloop (wordt het model doorontwikkeld door nieuwe gegevens terug te 'pompen'?) Welke rol speelt de uitkomst van het model in de besluitvorming? Wie beslist wat er met de uitkomst van het model wordt gedaan? Welke andere factoren spelen een rol bij de uiteindelijke besluitvorming? Welke gevolgen heeft het model voor de klant?

3.8 Wordt er gebruik gemaakt van geautomatiseerde besluitvorming?

Het gaat hier om de vraag of de verwerking is gericht op volledig geautomatiseerde besluitvorming met *rechtsgevolgen* voor de betrokkene of volledig geautomatiseerde besluitvorming *die de betrokkene anderszins in aanmerkelijke mate treft*. Voorbeeld hiervan is de straight-through-processing bij de aanvraag van een WW-uitkering. Het systeem stelt automatisch het recht, de hoogte en de duur van de WW-uitkering vast. Dit is een beslissing met rechtsgevolgen voor de klant.

Beantwoord in dit onderdeel in ieder geval de volgende vragen:

- Wordt er een algoritme gebruikt bij het verwerken van persoonsgegevens?
- Wordt er (deels) een beslissing gebaseerd op deze verwerking?
- Is er sprake van een volledige geautomatiseerde beslissing? Oftewel een beslissing zonder betekenisvolle tussenkomst door een medewerker.

Is de beslissing een besluit met rechtsgevolgen, bijvoorbeeld een besluit in de zin van de Awb, of treft de beslissing de betrokkenen anderszins in aanmerkelijke mate?

Als in het proces gebruik wordt gemaakt van volledig geautomatiseerde besluitvorming met rechtsgevolgen of andere aanmerkelijke gevolgen voor de betrokkene, beschrijf dan welke uitzonderingsgrond deze verwerking toestaat, welke logica (business rules) er wordt gebruikt bij de geautomatiseerde besluitvorming en uit welke regelgeving de criteria afkomstig zijn. Dit is van belang omdat UWV dit ook aan de betrokkene moet kunnen uitleggen (zie ook sectie 4.7) en zelfs (verkort) in de privacyverklaring moet opnemen.

3.9 Wordt er gebruikt gemaakt van profilering?

Het gaat hier om de vraag of de verwerking tot doel heeft personen (bijv. klanten) in te delen in bepaalde groepen (klantsegmenten of -profielen), bijvoorbeeld door toepassing van een model. Denk bijvoorbeeld aan een model dat klanten indeelt in groepen die een hoog of laag risico op fraude vormen.

Beantwoord in dit onderdeel in ieder geval de volgende vragen:

- Worden betrokkenen geautomatiseerd ingedeeld in bepaalde groepen?
- Worden generieke kenmerken gebruikt voor het indelen in bepaalde groepen?
- Worden bepaalde gevolgen getrokken uit het feit dat de betrokkene in een bepaalde groep is ingedeeld? Bijv. voorspelt het model dat een betrokkene uit een bepaalde groep bepaald gedrag zal vertonen?

Als in het proces gebruik wordt gemaakt van profilering, beschrijf dan hier de werking van het model, de verschillende groepen (klantsegmenten) die in het model worden onderscheiden en op basis van welke kenmerken een betrokkene in een bepaalde groep (klantsegment) wordt ingedeeld.

Beschrijf voorts wat er met de uitkomst van het model wordt gedaan. Indien gebruik wordt gemaakt van profilering moet er altijd sprake zijn van 'betekenisvolle menselijke tussenkomst' voordat op basis van de uitkomst van het model een beslissing wordt genomen met rechtsgevolgen voor de betrokkene of een beslissing die de betrokkene anderszins in aanmerkelijke mate treft. Beschrijf hier in ieder geval wie uiteindelijk de beslissing neemt en welke andere factoren die medewerker daarbij betrekt om tot de uiteindelijke beslissing te komen.

Beschrijf ook welke rol de profilering in het gehele proces speelt.

Hoofstuk 4 Rechtmatigheid van de gegevensverwerking

4.3 Worden bijzondere persoonsgegevens verwerkt?

Geef hier aan of bij de verwerking bijzondere persoonsgegevens worden gebruikt, zoals gezondheidsgegevens. Als dat het geval is, geef dan aan op grond van welke uitzonderingsgrond (zie UWV Beleidskader Privacy en de UAVG) UWV bevoegd is deze bijzondere persoonsgegevens te gebruiken voor de ontwikkeling van het model. Motiveer waarom deze uitzonderinggrond op de verwerking van toepassing is.

4.4 Worden persoonsgegevens van strafrechtelijke aard verwerkt?

Geeft hier aan of bij de ontwikkeling van het model persoonsgegevens van strafrechtelijke aard worden gebruikt, zoals gegevens over detentie.
Als dat het geval is, geef dan aan op grond van welke uitzonderingsgrond (zie UWV Beleidskader Privacy en de UAVG) UWV bevoegd is deze persoonsgegevens van strafrechtelijke aard te gebruiken voor de ontwikkeling van het model. Motiveer waarom deze uitzonderinggrond op de verwerking van toepassing is.

4.5 Doelbinding: worden de persoonsgegevens verwerkt voor het doel waarvoor ze zijn verzameld of voor een ander doel?

Beschrijf hier of de persoonsgegevens die in paraaf. 3.3 zijn geïdentificeerd, zijn verkregen voor een doel dat verenigbaar is met het doel waarvoor de analyse wordt uitgevoerd of het doel waarvoor het model wordt ontwikkeld. Let op: dit kan per persoonsgegeven verschillen aangezien in de analyseomgevingen (in het bijzonder in artikel 5 lid 2 sub d zich persoonsgegevens bevinden die voor zeer uiteenlopende doeleinden zijn verkregen.

4.6 Wat is de noodzaak van de verwerking?

Dit een belangrijk onderdeel van de GEB dus besteed hier aandacht aan. Geef voor het geheel van de verwerking, maar ook per fase of processtap een goede motivering waarom deze noodzakelijk is. Motiveer dit goed. Een enkele opmerking dat de verwerking noodzakelijk is voor de uitvoering van de wettelijke taak volstaat niet. Geef bijvoorbeeld duidelijk aan wat er gebeurt als de verwerking (en de verschillende stappen die daarbinnen worden gevolgd) niet kan plaatsvinden.

4.7 Transparantie van de verwerking voor betrokkene

Vul zoals gebruikelijk in en vul aan met de beschrijving (of in een bijlage) in begrijpelijke taal (de klant moet het ook kunnen begrijpen) hoe de logica van het algoritme werkt (hoe komt de uitkomst van het model of het besluit tot stand). Beschrijf voorts de gevolgen van de profilering of geautomatiseerde besluitvorming voor de klant beschikbaar zijn.

4.8 Rechten van betrokkene

Betrokkenen hebben recht op inzage en correctie van hun persoonsgegevens. Onder omstandigheden hebben ze ook recht op vernietiging van hun gegevens (denk bijvoorbeeld aan gegevens die via websitebezoek zijn verzameld met toestemming van de betrokkene) en kunnen ze bezwaar maken tegen de verwerking van hun gegevens.

Geef hier aan of aan dergelijke verzoeken gehoor kan worden gegeven. Indien bij de analyse ook gebruik wordt gemaakt van (klik)gegevens die zijn verzameld over het websitebezoek van de betrokken, geef dan aan of aan een verzoek tot vernietiging kan worden voldaan, indien de betrokkene zijn toestemming intrekt.

Hoofdstuk 5 Inventarisatie van risico's en mitigerende maatregelen

Als er sprake is van een verwerking waarin op basis van big data analyses worden verricht voor het opstellen van modellen of klantprofielen, zal in ieder geval aandacht moeten worden besteed aan de volgende risico's:

- Betrokkene zijn niet op de hoogte van het feit dat hun persoonsgegevens worden gebruikt voor deze verwerking.
- Er worden bijzondere persoonsgegevens of gegevens van strafrechtelijke aard gebruikt bij de verwerking.
- De gebruikte data is niet actueel of juist.
- De bewaartermijnen worden niet nageleefd.
- De data zijn niet of onvoldoende beveiligd.

- Een externe partij/leverancier/cloud provider is betrokken bij de uitvoering van de analyses en gebruikt de gegevens voor eigen doeleinden.
- Een externe partij/leverancier/cloud provider is betrokken bij de uitvoering van de analyses en deze beveiligt de gegevens onvoldoende
- UWV kan de logica niet uitleggen.
- Het model heeft een (verborgen) discriminatoir karakter.

Dit laatste punt van een (verborgen) discriminatoir karakter van het model is een heel belangrijk risico waarop zal moeten worden ingegaan in de GEB en waarbij uitleg moet worden gegeven welke maatregelen zijn getroffen om dit risico te mitigeren. Denk hierbij bijvoorbeeld aan externe partijen die het model testen en toetsen.