**Bijlage 1**

**Voorbeeld Formulier Gegevensbeschermingseffectbeoordeling**

Deel A: Inleiding

Definities van termen gebruikt in deze Bijlage 1 kunnen worden teruggevonden in het bijgevoegde Deel E (Begrippenlijst).

Deel B bevat een diagram met een overzicht van de GBEB-procedure. Deel C stelt enkele eerste vragen om de aard van het Project en de noodzaak van een GBEB te bepalen (de **'Eerste Kennisgeving'**). Deel D is het Formulier Gegevensbeschermingseffectbeoordeling met een aantal vragen over het voorgestelde Project en het daarin opgenomen gebruik van Persoonsgegevens (het **'Formulier GBEB'**).

Disclaimer: Het Formulier GBEB is niet bedoeld voor een situatie waarin de Verwerkingsverantwoordelijke moet overleggen met de autoriteit gegevensbescherming. Dit overleg dient te worden geleid door de **Legal Department**.

Deel C: Eerste vragen om te bepalen of een GBEB nodig is en zo ja, hoe deze beoordeling moet worden uitgevoerd ('Eerste Kennisgeving')

**Algemene projectinformatie**

|  |  |
| --- | --- |
| **Vraag** | **Antwoord** |
| **[*Relevante HES entiteit*]** die het Project aanvraagt/uitvoert |  |
| Gegevens Projectleider | Naam:Rol:Telefoon:Email: |
| Betreft jouw Project de Verwerking van Persoonsgegevens? Zo nee: geen verdere actie vereist. Stuur dit formulier ter controle en goedkeuring naar de lokale Compliance Officer. |  |
| Beschrijf zo gedetailleerd mogelijk op welke manier jouw Project de Verwerking van Persoonsgegevens betreft. |  |
| Worden de Persoonsgegevens verwerkt door HES als Verwerkingsverantwoordelijke of door een Verwerker? Geef de reden voor de betreffende optie. |  |
| Wat is het doel van het Project? |  |
| Wat zijn de voordelen voor HES?  |  |
| Wat zijn de mogelijke voordelen voor andere partijen (waaronder, zover van toepassing, klanten van HES en betrokken personen)? |  |
| Zijn er voor het Project relevante documenten (zoals een projectvoorstel) die nuttig zijn voor de uitvoering van deze GBEB, bijvoorbeeld omdat ze uiteenzetten hoe Persoonsgegevens worden gebruikt? Zo ja: geef een lijst van deze documenten en voeg deze toe aan dit Formulier. |  |
| Tegen welke datum moet het Project worden geïmplementeerd? |  |

**Project en Persoonsgegevens**

|  |  |  |
| --- | --- | --- |
| **Vraag** | **Ja/Nee** | **Privacyrisico** |
| Betreft het Project de verzameling van Persoonsgegevens van betrokken personen? |  | Laag-gemiddeld |
| Vereist het Project dat personen informatie over zichzelf geven om de Verwerking te kunnen uitvoeren, of is dit op vrijwillige basis? |  | Gemiddeld |
| Hoe worden de personen op de hoogte gesteld/geïnformeerd? |  | Gemiddeld |
| Worden Persoonsgegevens op een nieuwe manier bekend gemaakt aan of bewaard binnen de HES-organisatie of een derde partij? |  | Gemiddeld |
| Worden de Persoonsgegevens gebruikt voor een nieuw of ander doel? |  | Laag-gemiddeld |
| Maakt het Project gebruik van nieuwe technologie? |  | Gemiddeld-hoog |
| Leidt het Project tot het nemen van besluiten of acties tegen personen die een aanzienlijke invloed op hen kunnen hebben (bijvoorbeeld door ze te profileren)? |  | Hoog |
| Maakt het Project gebruik van geautomatiseerde besluitvorming of profilering van personen? |  | Hoog |
| Betreft het Project grootschalige Verwerking van Persoonsgegevens? |  | Gemiddeld-hoog |
| Betreft het Project grootschalige Verwerking van speciale categorieën of gegevens over strafrechtelijke veroordelingen of delicten? |  | Hoog |
| Betreft het Project grensoverschrijdende Verwerking? |  | Hoog |

**Samenvatting**

|  |  |
| --- | --- |
| **Vraag** | **J/N** |
| Lijken de hierboven gegeven informatie en antwoorden te duiden op een hoog risico voor Betrokkenen of een risicovolle verwerkingsactiviteit bij de Verwerking van Persoonsgegevens? |  |
| Zo nee: geef de redenen voor deze conclusie en stuur dit formulier ter goedkeuring aan de lokale Compliance Officer. |  |
| Zo ja: ga verder met het volgende deel. |  |

Deel D: Formulier Gegevensbeschermingseffectbeoordeling ("Formulier GBEB")

| # | **Vraag** | **Antwoord** |
| --- | --- | --- |
| Persoonsgegevens |
|  | Welke Persoonsgegevens worden verzameld? (Omcirkel wat van toepassing is) | Naam: J / NAdres: J / NGeboortedatum: J / NEtnische achtergrond: J / NBurgerlijke staat: J / NFamilieleden en persoonlijke relaties: J / NReligie: J / NGezondheid: J / NSeksuele geaardheid: J / NPolitieke overtuiging: J / NGenetica: J / NStrafrechtelijke veroordelingen: J / NFysieke eigenschappen (lengte, gewicht, etc.):J / NCreditcard/bankrekeningnummer: J / NBezittingen (voertuigen, woningen, etc.): J / NFinanciële geschiedenis: J / NSociale netwerken: J / NAnders (te weten): J / N |
|  | Hoe worden deze Persoonsgegevens verzameld? |  |
|  | Wat is de Verwerkingsactiviteit? |  |
|  | Is de Verwerking noodzakelijk of kan de activiteit op een andere manier worden uitgevoerd? |  |
|  | Kan het Project succesvol worden uitgevoerd zonder het verzamelen van (een deel van) deze Persoonsgegevens?  |  |
|  | Van wie kunnen Persoonsgegevens worden verzameld/Verwerkt? (Omcirkel wat van toepassing is) | Medewerkers: J / NNiet-medewerkers: J / NIndien niet-medewerkers: geef aan wie (klanten, verkopers, andere derde partijen, etc.): |
|  | Voor welk specifiek doel worden de Persoonsgegevens Verwerkt (bijv. om een nieuwe, persoonlijke portal voor arbeidsvoorwaarden te creëren)? Beschrijf zo gedetailleerd mogelijk waarom de Persoonsgegevens worden Verwerkt. |  |
|  | Hoe lang worden de Persoonsgegevens bewaard? |  |
| Rechtsgrond |
|  | Worden de Persoonsgegevens Verwerkt na toestemming van de Betrokkene(n)? Zo ja: hoe is deze toestemming verkregen? |  |
|  | Worden de Persoonsgegevens Verwerkt in de uitvoering van een contract met de Betrokkene(n)? |  |
|  | Worden de Persoonsgegevens Verwerkt naar aanleiding van een legitiem zakelijk belang van HES (bijv. interne HR-administratie)? |  |
|  | Worden de Persoonsgegevens Verwerkt naar aanleiding van een andere rechtsgrond (zie Deel F voor een lijst met rechtsgronden)? |  |
| Informatiestromen |
|  | Waar worden Persoonsgegevens van Betrokkenen bewaard nadat ze zijn verzameld? |  |
|  | Wie heeft toegang tot de Persoonsgegevens? |  |
|  | Worden rapporten gegenereerd door het gebruik en de openbaring van de Persoonsgegevens? |  |
|  | Worden de Persoonsgegevens overgedragen aan rechtspersonen buiten HES? Zo ja: aan welke rechtspersonen en voor welk doel? |  |
|  | Worden de Persoonsgegevens overgedragen aan landen of ingezien door personen buiten de Europese Economische Ruimte? |  |
|  | Zijn de Persoonsgegevens geïnventariseerd? |  |
|  | Indien het antwoord op vraag (18) 'ja' is: geef een inventarisatie van de Persoonsgegevens met de informatiestromen binnen het Project.(met vermelding van het soort Persoonsgegevens, de ondernemingen die de Persoonsgegevens delen, de locaties van deze ondernemingen en de locaties van de opslag van de Persoonsgegevens). |  |
|  | Hoe lang worden de Persoonsgegevens bewaard? |  |
| Overlegverplichting |
|  | Met welke collega's pleeg je intern overleg over de privacy- en veiligheidsrisico's voortkomend uit het Project? |  |
|  | Heb je advies ingewonnen van de lokale Compliance Officer, de Chief Compliance Officer of HES Legal Department?  |  |
|  | Moeten ondernemingsraden of andere medezeggenschapsorganen worden geraadpleegd (in het geval van HR-/medewerkersgegevens)?  |  |
|  | Moet in geval van een grensoverschrijdende overdracht goedkeuring worden gezocht in een ander rechtsgebied? |  |
|  | Indien het antwoord op vraag (23) of (24) 'ja' is: heb je het verplichte overleg met de relevante partijen ondernomen? Geef hier een bevestiging van dit verplichte overleg met details over het daadwerkelijke overleg, de betrokken personen en de betreffende datum/data.  |  |
| Risicobepaling  |
|  | Heb je specifieke privacyrisico's gevonden naar aanleiding van bovenstaande vragen? Zo ja, welke? Bijvoorbeeld: het risico dat Persoonsgegevens worden ingezien door een onbevoegd persoon;* het risico dat de veiligheid van de Persoonsgegevens in gevaar komt;
* het risico dat de betrokken personen bezwaar maken tegen de Verwerking indien zij hiervan op de hoogte worden gesteld;
* het risico dat de juistheid van de Persoonsgegevens niet behouden blijft;
* het risico dat de Persoonsgegevens langer dan noodzakelijk worden bewaard.
 |  |
|  | Wat is de specifieke schade die dergelijke risico's met zich meebrengen voor de betrokken personen (bijvoorbeeld het risico dat Persoonsgegevens worden gestolen, waardoor de betrokken personen het slachtoffer kunnen worden van (identiteits)fraude)? |  |
|  | Is er een specifiek nalevingsrisico? |  |
|  | Is er een breder organisatorisch risico (bijvoorbeeld hoge boetes naar aanleiding van een overtreding en daaraan gerelateerde negatieve media-aandacht)? |  |
| Stappen en maatregelen om Persoonsgegevens te waarborgen, beveiligen en beschermen |
|  | Met betrekking tot de risico's hierboven: welke maatregelen worden genomen om de Persoonsgegevens te beveiligen en beschermen (bijv. versleuteling of meervoudige authenticatie)? |  |
|  | Met betrekking tot de risico's hierboven: hoe faciliteren we de uitvoering van rechten van Betrokkenen (bijv. het recht op inzage)? |  |
|  | Hoe wordt de juiste informatie over het Project en de gerelateerde privacyrisico's, indien nodig, gedeeld met de Betrokkenen? |  |
|  | Sluiten deze stappen het risico volledig uit of beperken deze stappen het risico slechts? |  |
|  | Is de uiteindelijke invloed op de privacyrechten van de Betrokkenen, op basis van de geïdentificeerde risico's en de voorgestelde oplossingen, laag genoeg en dus acceptabel gezien de doelstellingen en voordelen van het Project? |  |
| Verwerking bevindingen en maatregelen om risico's uit te sluiten/te beperken |
|  | Hoe worden deze bevindingen verwerkt in het Project? |  |
|  | Wiens verantwoordelijkheid is het om te garanderen dat de bevindingen juist worden verwerkt?  |  |
|  | Op welke termijn? |  |
|  | Wat is de procedure voor Betrokkenen die hun privacygerelateerde zorgen omtrent het Project willen bespreken? |  |

***Samenvatting***

|  |  |
| --- | --- |
| **Vraag** | **Ja / Nee** |
| Worden de geïdentificeerde risico’s uitgesloten, beperkt of geaccepteerd? |  |
| Zo nee, dan mag de Verwerking niet worden gestart totdat de GBEB is doorgestuurd en geschikte maatregelen kunnen worden genomen. |  |

|  |
| --- |
| **Ondertekening en goedkeuring/afkeuring** |
| **Projectleider** |
| Naam |  |
| Functie |  |
| Handtekening |  |
| Datum |  |
| **Vertegenwoordig(st)er Compliance Team (indien van toepassing)** |
| Naam |  |
| Functie |  |
| Handtekening |  |
| Datum |  |
|  |  |

|  |
| --- |
| **Bepaling Lokale Compliance Officer** |
| Naam |  |
| Datum |  |
| Reactie |  |
| Uitleg (indien van toepassing) |  |
| Handtekening |  |

Deel E: Termen en definities

|  |  |
| --- | --- |
| **Term** | **Definitie** |
| AVG:  | De Algemene Verordening Gegevensbescherming (AVG), van kracht sinds 25 mei 2018. De AVG is alleen van toepassing op Persoonsgegevens, niet op gegevens van ondernemingen en rechtspersonen. |
| Verwerkingsver­antwoordelijke:  | De onderneming die de doelstelling en wijze van Verwerking van Persoonsgegevens bepaalt.  |
| Verwerker:  | De onderneming die Persoonsgegevens Verwerkt namens de Verwerkingsverantwoordelijke.  |
| Lokale Compliance Officer: | De persoon binnen de HES-onderneming die verantwoordelijk is voor de Gegevensbeschermingseffectbeoordeling.  |
| Persoons­gegevens:  | Alle informatie over identificeerbare personen. Voorbeelden van Persoonsgegevens zijn: |
| 1. naam (o.a. volledige naam, meisjesnaam of alias);
 |
| 1. identificatienummer (o.a. Burgerservicenummer, paspoortnummer, rijbewijsnummer, bankrekeningnummer of creditcardnummer);
 |
| 1. adresgegevens (o.a. straatnaam of e-mailadres);
 |
| 1. systeemgegevens (o.a. Internet Protocol-adres (IP-adres) of media access control-adres (mac-adres));
 |
| 1. telefoonnummer (o.a. mobiel telefoonnummer);
 |
| 1. uiterlijk, waaronder foto's (bijv. van het gezicht), röntgenfoto's, vingerafdrukken of andere biometrische foto's/voorbeelden (bijv. irisscan, verbale handtekening of gezichtsherkenning);
 |
| 1. bezittingen (o.a. voertuigregistratie en gerelateerde informatie);
 |
| 1. informatie die gerelateerd is of kan worden aan een van bovenstaande gegevens (o.a. geboortedatum en -plaats, afkomst, religie, activiteiten, geografische informatie, arbeidsverleden, medische gegevens, opleidingsachtergrond en financiële gegevens);
 |
| 1. ogenschijnlijk onbelangrijke informatie, zoals het feit dat een persoon een e-mail heeft gestuurd op een bepaald moment of het feit dat een persoon een medewerker is van een klant van HES (of een andere organisatie);
 |
| 1. meningen over een persoon (zoals opgenomen in een referentie of beoordeling).
 |
| Verwerking: | Vrijwel alle activiteiten omtrent Persoonsgegevens, waaronder: |
| 1. verzamelen, opslaan en vastleggen;
 |
| 1. organiseren en structureren;
 |
| 1. bewerken en wijzigen;
 |
| 1. vinden, overleggen en gebruiken;
 |
| 1. openbaren en verspreiden;
 |
| 1. uitlijnen en combineren; en
 |
| 1. beperken, wissen en vernietigen.
 |

Deel F: Lijst van rechtsgronden voor Verwerking

* **De betrokken persoon heeft toestemming gegeven voor de Verwerking.**
* Toestemming moet uitdrukkelijk, weloverwogen en vrijwillig worden gegeven. Een betrokken persoon moet zijn/haar toestemming ook kunnen intrekken. Raadpleeg het Beleid Privacy van HES voor meer informatie over toestemming.
* **De Verwerking is noodzakelijk:**
* met betrekking tot een contract die de persoon is aangegaan; of
* omdat de persoon heeft gevraagd iets te laten uitvoeren om een contract aan te kunnen gaan.
* **De Verwerking is noodzakelijk vanwege een wettelijke verplichting die op jou rust (m.u.v. een verplichting onder een contract).**
* Bijvoorbeeld wanneer gegevens moeten worden bewaard om te voldoen aan vereisten onder regelgeving, omtrent financiële verslaglegging of anti-omkoping- en -corruptiewetgeving.
* **De Verwerking is noodzakelijk om de 'essentiële belangen' van de persoon te beschermen.**
* Deze voorwaarden geldt alleen in gevallen van leven of dood, zoals wanneer iemands medische gegevens worden gedeeld met een ziekenhuis waar deze persoon wordt behandeld na een ernstig auto-ongeluk.
* **De Verwerking komt overeen met de voorwaarde omtrent 'rechtmatig belang'.**
* Een rechtmatig belang is de flexibelste rechtsgrond voor Verwerking, maar je kunt er niet altijd van uitgaan dat deze rechtsgrond de meest geschikte is.
* Het is waarschijnlijk de meest geschikte rechtsgrond, wanneer je Persoonsgegevens gebruikt op een manier die mensen kunnen verwachten en die minimale privacyrisico's met zich meebrengt of wanneer er een dwingende reden is voor de Verwerking.
* De voorwaarde voor een rechtmatig belang kent drie onderdelen, dus het is een goed idee om deze onderdelen te zien als een driedelige toets. Je moet: (i) een rechtmatig belang identificeren; (ii) aantonen dat de Verwerking noodzakelijk is om dat belang te beschermen en (iii) het rechtmatig belang afwegen tegen de belangen, rechten en vrijheden van de betrokken persoon.
* Het rechtmatig belang kan jouw eigen belang zijn of een belang van een derde partij. Hieronder vallen commerciële belangen, persoonlijke belangen of bredere, maatschappelijke belangen. De Verwerking moet noodzakelijk zijn. Indien je redelijkerwijs hetzelfde resultaat kunt krijgen op een minder ingrijpende manier, dan is het rechtmatig belang niet van toepassing.