AVG | ADVIES

Wetgeving - Beleid - Implementatie

The Privacy Factory
Robert Schumandomein 2
6229 ES Maastricht

Telefoon: 088-2036323
E-mail: info@theprivacyfactory.com
Website: theprivacyfactory.com

KvK: 63263076
Btw-id: NL855159674B01
IBAN: NL27INGB0006835512

The Privacy Factory

Inhoudsopgave

1. Inleiding **2**

2. Probleemstelling **3**

3. Onderzoeksvragen **3**

3.1 Is de Wpg van toepassing op GRS Drechtsteden? 3

3.2 Is het regionale AVG-beleid leidend, of moet GRS Drechtsteden haar eigen weg gaan? 4

3.3 Indien GRS ervoor kiest haar eigen weg te gaan, hoe wordt dit dan geïmplementeerd? 4

4. Advies **6**

ANNEX 1: Procedure Beleidsverklaring **7**

The Privacy Factory

1. Inleiding

Op grond van de door dhr. Polderman gegeven telefonische briefing alsmede op basis van daarna verstrekte documenten[1] kan het volgende worden vastgesteld:

1. De Gemeenschappelijke Regeling Sociaal (hierna GRS) is een rechtspersoonlijkheid bezittend openbaar lichaam van het type 'collegeregeling' in de zin van de Wet gemeenschappelijke regelingen.
2. GRS kent als zodanig een algemeen bestuur, een dagelijks bestuur en een voorzitter.
3. GRS is in deze hoedanigheid een takenpakket toegewezen op basis van delegatie en mandaat. Een en ander in het kader van de:

    - Participatiewet
    - Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW)
    - Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ)
    - Wet maatschappelijke ondersteuning 2015 (Wmo 2015), voor zover dit de maatwerkvoorzieningen betreft, zoals nader aangeduid in de desbetreffende begripsbepaling van artikel 1.1.1 van de Wmo 2015, met inbegrip van de bevoegdheden genoemd in artikel 6.1 Wmo 2015
    - Wet structuur uitvoeringsorganisatie werk en inkomen
    - Wet kinderopvang, voor zover betrekking hebbend op de tegemoetkoming van de gemeente in de kosten van kinderopvang (hoofdstuk 1)
    - Wet gemeentelijke schuldhulpverlening
    - Wet sociale werkvoorziening, voor zover betrekking hebbend op de in het vijfde lid genoemde taken
    - Algemene wet bestuursrecht
    - Wet op de lijkbezorging
    - Burgerlijk Wetboek artikel 1:432 BW en artikel 1:449 BW (verzoek tot instellen/verlengen/opheffen van bewind)
4. GRS heeft Bijzondere Opsporingsambtenaren in dienst
5. Zowel de Algemene Verordening Gegevensbescherming als de Wet Politiegegevens zijn zowel geografisch als materieel op GRS van toepassing.

[1] GR Sociaal en Memorie van toelichting GR Sociaal

2. Probleemstelling

In het kader van bovenstaande taakstelling is door dhr. Polderman aan The Privacy Factory (hierna TPF) gevraagd om duidelijkheid te scheppen over de op haar van toepassing zijnde wetgeving omtrent bescherming persoonsgegevens, over het door haar te volgen privacybeleid en hoe de AVG geïmplementeerd moet worden. Op deze probleemstelling wordt middels het beantwoorden van een drietal onderzoeksvragen een antwoord gegeven.

3. Onderzoeksvragen

Onderstaande onderzoeksvragen zijn erop gericht een antwoord te geven op de vraag hoe GRS invulling moet geven aan het beschermen van door haar te verwerken persoonsgegevens in termen van het te voeren beleid, de van toepassing zijnde wetgeving (m.n. ook Wpg) en de wijze waarop de naleving hiervan in de organisatie moet worden geïmplementeerd.

3.1 Is de Wpg van toepassing op GRS Drechtsteden?

Antwoord

Ja, ervan uitgaande dat de bij GRS Drechtsteden in dienstverband werkende bijzondere opsporingsambtenaren (boa's) in het kader van de uitvoering van hun opsporingstaak persoonsgegevens verwerken.

Toelichting

BOA's kunnen belast zijn met het opsporen van bepaalde categorieën van strafbare feiten. In dat geval is voor wat betreft de bescherming van daarbij te verwerken politiegegevens de Wpg[2] van toepassing. Belangrijk daarbij is te onderkennen dat, ofschoon deze opsporingstaak plaatsvindt onder gezag van de officier van justitie, de verwerking van deze politiegegevens plaatsvindt onder het beheer van GRS die dan ook gezien moet worden als de verwerkingsverantwoordelijke[3] in de zin van artikel 1.f 4 Wpg.

[2] De toezichtstaken van de boa vallen onder de Algemene Verordening Gegevensbescherming (AVG). De werkgever is ook dan verwerkingsverantwoordelijke maar in dat geval in de zin van de AVG.

[3] In de hoedanigheid van toezichthouder op de naleving van de Wpg heeft GRS ook toegang tot de in het kader van deze opsporingstaak te verwerken persoonsgegevens.

3.2 Is het regionale AVG-beleid leidend, of moet GRS Drechtsteden haar eigen weg gaan?

Antwoord

De verwerkingsverantwoordelijke is in de zin van artikel 24 lid 2 van de AVG zelfstandig verantwoordelijk voor het opstellen van een eigen gegevensbeschermingsbeleid. Dit betekent feitelijk dat het GRS Drechtsteden niet vrijstaat om het regionale beleid onverkort van toepassing te verklaren. Het staat GRS natuurlijk wel vrij om elementen uit het regionale beleid te integreren in haar eigen beleid.

Toelichting

Van de verwerkingsverantwoordelijke wordt verwacht dat hij, gezien de te verwerken persoonsgegevens en de daarbij horende risico's, de te nemen passende technische en organisatorische maatregelen in de zin van art 24 lid 1 AVG uitwerkt tot gegevensbeschermingsbeleid en dat ook in de praktijk uitvoert[4].

Letterlijke lezing van artikel 24 lid 1 AVG zou aanleiding kunnen zijn dit beleid te beperken tot informatiebeveiligingsbeleid. Het is echter aan te bevelen dit beleid te formuleren als een meer algemeen privacybeleid dat tevens de naleving van de AVG op hoofdlijnen beschrijft[5].

In de uitvoering van het beleid is het daarnaast aan te bevelen om voor de planning van de op grond van beleid uit te voeren privacyactiviteiten te zorgen voor nadere inhoudelijke toelichting bij deze privacyactiviteiten.

3.3 Indien GRS ervoor kiest haar eigen weg te gaan, hoe wordt dit dan geïmplementeerd?

Antwoord

Het implementeren van de AVG - dit geldt overigens ook voor de Wpg - vergt voor alles het combineren van een stabiel(e):

[4] Het is de rol van de FG om in de zin van artikel 38 lid 1 AVG betrokken te worden bij het opstellen en (doen) uitvoeren van dit beleid, daarbij nauw samenwerkend met de security officer op vlak van het benoemen en uitvoeren van de feitelijke uit te voeren beveiligingsmaatregelen.

[5] Zie Annex 1

- register van verwerkingen
- risicoanalyse
- privacyactiviteitenplanning

Toelichting

Register van verwerkingen

Centraal in de uitvoering van het GRS privacybeleid staat het Register van verwerkingen. De hierin opgenomen verwerkingen met bijbehorende doelomschrijvingen, categorieën van persoonsgegevens, categorieën van betrokkenen, wettelijke grondslagen en bewaartermijnen zijn bepalend voor de inhoud van o.a. privacyverklaringen en verwerkersovereenkomsten, maar ook voor de in acht te nemen bewaartermijnen.

Het is dan ook essentieel dat dit register stabiel is en niet steeds bij de aankoop van nieuwe software, een wetswijziging, of een wijziging in de organisatiestructuur aan verandering onderhevig is. Al was het maar omdat dit tevens mogelijke gevolgen heeft voor de inhoud van de eerder genoemde privacyverklaringen en verwerkersovereenkomsten.

Ervaring heeft ons overigens geleerd dat organisaties - op vlak van bijvoorbeeld personeelsbeheer en financieel beheer - vrijwel identieke ‘basis-verwerkingen’ hebben, verwerkingen waarvan TPF in de loop van de tijd een bibliotheek heeft aangelegd.
Het is enkel op vlak van wat een ‘kern-verwerking’ genoemd wordt - denk in het kader van GRS aan de verwerking ‘zorg-welzijnsbeheer’ - dat een nadere analyse nodig is.

Risicoanalyse

De AVG gaat ervan uit dat de verwerkingsverantwoordelijke in de context van de eigen organisatie zorgt voor het invoeren van passende technische en organisatorische maatregelen. Om vast te kunnen stellen wat ‘passend’ is, vergt een risicoanalyse die inzicht geeft in de impact van het niet meer:

- beschikbaar zijn van persoonsgegevens
- kunnen bouwen op de integriteit van persoonsgegevens
- vertrouwelijk zijn van persoonsgegevens

Het is dit inzicht dat bepalend is voor de te treffen informatiebeveiligingsmaatregelen. Het zijn deze maatregelen die ervoor moeten zorgen dat de kans dat die impact wordt bewaarheid, wordt teruggedrongen tot een voor de organisatie acceptabel risico.

Privacyactiviteitenplanning

Om AVG-accountable te kunnen worden, vergt naast het hebben van een stabiel register van verwerkingen en 'passende' technische en organisatorische maatregelen ook het opstellen en uitvoeren van een privacyactiviteitenplanning.

Dit vergt een Plan-Do-Check-Act vertaling van de AVG, i.e. een overzicht van uit te voeren activiteiten gericht op het voor AVG-accountability opleveren van de nodige bewijsvoering.

Door TPF uitgevoerde analyse van de AVG laat zien dat er 13 hoofddoelen zijn met in totaal 57 uit te voeren activiteiten. Afhankelijk of er persoonsgegevens naar niet EER-landen worden geexporteerd en/of er gegevens van kinderen worden verwerkt, blijven er voor de meeste organisaties een 49-tal verplicht in te plannen/uit te voeren privacyactiviteiten over.

4. Advies

4.1 GRS Drechtsteden is zowel voor de AVG als ook voor de Wpg de verwerkingsverantwoordelijke en moet zich conform organiseren.

4.2 Voor beide rollen - verwerkingsverantwoordelijke AVG en Wpg - geldt dat GRS Drechtsteden in onafhankelijkheid haar beleid dienaangaande moet formuleren en uitvoeren.

In onafhankelijkheid, omdat zij de enige 'verwerkingsverantwoordelijke' is voor de door haar organisatie te verwerken persoonsgegevens/politiegegevens. Blijkt op enig moment dat GRS niet AVG-compliant is - niet door de Wpg audit komt - dan betekent dit dat betrokkenen en/of de Autoriteit Persoonsgegevens zich enkel bij haar zullen melden voor verhaal.

4.3 Voor zowel de AVG als ook voor de Wpg geldt dat het implementeren van beide wetten zich moet baseren op een deugdelijk register van verwerkingen, een BIV-risicoanalyse en een op uit te voeren activiteiten gebaseerde planning.

ANNEX 1: Procedure Beleidsverklaring

The Privacy Factory bestaat uit ervaren specialisten in gegevensbescherming. Deze procedures en notificaties die wij als templates aanbieden, zijn bedoeld als voorbeelden. Ze geven algemene richtlijnen. U kunt deze documenten gebruiken als uitgangspunt, maar het is aan u om ze waar nodig, in overleg met uw eigen juridische adviseurs, aan te passen aan de specifieke omstandigheden binnen uw organisatie. The Privacy Factory is in geen enkele zin aansprakelijk voor mogelijke gevolgen van het gebruik van deze documenten.

---

1. Bereik

Het bereik van deze procedure is het door de verwerkingsverantwoordelijke opstellen en onderhouden van de beleidsverklaring bescherming van persoonsgegevens van **[naam organisatie]**.

2. Verantwoordelijkheden

Het voor **[naam organisatie]** opstellen en onderhouden van een beleidsverklaring betreffende de bescherming van persoonsgegevens is de verantwoordelijkheid van de **[functietitel]**.

3. Procedure

De **[functietitel]** stelt een concept-beleidsverklaring bescherming van persoonsgegevens op, die tenminste de volgende elementen bevat:

- Toepasselijkheid AVG
- Beleidsverklaring
- Verantwoordelijkheden en rollen AVG
- Grondbeginselen van bescherming persoonsgegevens
- Rechten van betrokkenen
- Toestemming
- Veiligheid van persoonsgegevens
- Verstrekking van persoonsgegevens aan derden
- Bewaring en verwijdering van persoonsgegevens
- Doorgifte van persoonsgegevens
- Risico's

De concept-beleidsverklaring wordt voor advies voorgelegd aan de functionaris voor gegevensbescherming en bij afwezigheid aan een interne of externe deskundige op het gebied van de AVG.

De **[functietitel]** verwerkt het advies en legt de concept-beleidsverklaring ter accordering voor aan de hoogste functionaris van **[naam organisatie]**.

De **[functietitel]** draagt zorg dat de geaccordeerde beleidsverklaring ten grondslag ligt aan alle in het kader van bescherming van persoonsgegevens binnen **[naam organisatie]** uitgevoerde activiteiten.

4. Template beleidsverklaring gegevensbescherming

1. Inleiding

1.1 Achtergrond van de Algemene Verordening Gegevensbescherming ('AVG')

De Algemene Verordening Gegevensbescherming van 2016 vervangt de EU-Richtlijn Gegevensbescherming 95/46/EC uit 1995 en komt tevens in de plaats van alle op basis daarvan door individuele lidstaten ontwikkelde wetgeving. Doel van de AVG is tweeledig: beschermen van de "rechten en vrijheden" van natuurlijke personen (levende individuen) en zeker stellen dat persoonsgegevens uitsluitend worden verwerkt met medeweten en, voor zover mogelijk, met toestemming van de betrokkenen.

1.2 Door [naam organisatie] gehanteerde definities (afgeleid van de AVG)

Materieel toepassingsgebied (artikel 2)
De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde (d.w.z. computergestuurde) verwerking, alsmede op de verwerking, anders dan met geautomatiseerde middelen, van persoonsgegevens (in de vorm van persoonsgegevens op papier) die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Territoriaal toepassingsgebied (artikel 3)
De AVG is van toepassing op alle in de EU gevestigde verwerkingsverantwoordelijken die persoonsgegevens verwerken in de context van de activiteiten van hun organisatie, alsmede op verwerkingsverantwoordelijken buiten de EU die persoonsgegevens verwerken om goederen of diensten aan te bieden aan of het gedrag te volgen van betrokkenen die zich in de EU bevinden.

Vestigingen (artikel 4)
De hoofdvestiging van een verwerkingsverantwoordelijke in de EU is de plaats waar de belangrijkste beslissingen over doelstellingen van en middelen voor de verwerking van persoonsgegevens worden genomen, m.a.w. de plaats van zijn centrale administratie in de EU. Buiten de EU gevestigde verwerkingsverantwoordelijken of verwerkers moeten een vertegenwoordiger in de EU aanwijzen die gemachtigd is op te treden namens de verwerkingsverantwoordelijke of verwerker en het contact verzorgt met de toezichthoudende autoriteit en de betrokkenen in alle kwesties die verband houden met de verwerking van persoonsgegevens.

Persoonsgegevens (artikel 4)
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een

naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Bijzondere categorieën van persoonsgegevens (artikel 9)
Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Verwerkingsverantwoordelijke (artikel 4)
De natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

Betrokkene (artikel 4)
Elke levende persoon die het onderwerp is van persoonsgegevens die in het bezit zijn van een organisatie.

Verwerking (artikel 4)
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Profilering (artikel 4)
Elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij 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.

Inbreuk in verband met persoonsgegevens (artikel 4)
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Toestemming van de betrokkene (artikel 4)

Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem of haar betreffende verwerking van persoonsgegevens aanvaardt.

Kind (artikel 8)
De AVG definieert een kind als elke persoon jonger dan 16 jaar, maar geeft lidstaten de vrijheid die leeftijd bij wet terug te brengen tot 13 jaar. Verwerking van de persoonsgegevens van een kind is (voor de meeste verwerkingsdoeleinden) alleen rechtmatig op voorwaarde van ouderlijke toestemming of toestemming door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. De verwerkingsverantwoordelijke moet redelijke inspanningen doen om in dergelijke gevallen te controleren of de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt, toestemming heeft gegeven of machtiging tot toestemming heeft verleend.

Derde (artikel 4)
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

Bestand (artikel 4)
Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

2. Beleidsverklaring

2.1 De **[naam hoogste orgaan binnen organisatie] [en het management]** van **[naam organisatie]**, gevestigd te **[adres organisatie]**, hebben de overtuigde intentie zich volledig te houden aan alle relevante EU- en nationale wetgeving met betrekking tot de bescherming van persoonsgegevens en de bescherming van de rechten en vrijheden van personen van wie **[naam organisatie]** persoonsgegevens verzamelt en verwerkt.

2.2 Dit beleid en andere relevante beleidsstukken zoals **[specificeer, bijv. het Informatiebeveiligingsbeleid]** beschrijven de betekenis van compliance met de Algemene Verordening Gegevensbescherming (AVG) alsmede de daarmee verbonden processen en procedures.

2.3 De AVG en dit beleid zijn van toepassing op alle bij **[naam organisatie]** in gebruik zijnde functies voor verwerking van persoonsgegevens, met inbegrip van verwerkingsfuncties die worden gebruikt voor verwerking van persoonsgegevens van klanten, medewerkers,

leveranciers en partners en alle andere persoonsgegevens die, afkomstig uit welke bron dan ook, door **[naam organisatie]** worden verwerkt.

2.4 [Naam organisatie] heeft doelstellingen voor bescherming van persoonsgegevens opgesteld en vastgelegd in **[specificeer: document/applicatie]**.

2.5 De **[functietitel]** is verantwoordelijk voor jaarlijkse controle van het register van verwerkingen in het licht van mogelijke veranderingen in de activiteiten van **[naam organisatie]** en mogelijke extra vereisten zoals gebleken uit gegevensbeschermingseffectbeoordelingen (DPIA's - Data Protection Impact Assessments). Genoemd register dient beschikbaar te worden gesteld op verzoek van de toezichthoudende autoriteit.

2.6 Dit beleid is van toepassing op alle medewerkers en belanghebbende partijen, zoals externe leveranciers van **[naam organisatie]**. Inbreuken op de AVG zullen worden behandeld volgens het disciplinaire beleid van **[naam organisatie]** en kunnen tevens als wetsdelict worden beoordeeld, in welk geval de kwestie zo snel mogelijk aan de bevoegde autoriteiten zal worden gemeld.

2.7 Van partners van en externe partijen werkend met of voor **[naam organisatie]** met toegang of mogelijke toegang tot persoonsgegevens, wordt verwacht dat zij kennis hebben genomen van dit beleid, dit beleid begrijpen en zich aan dit beleid zullen houden. Geen enkele externe partij heeft het recht van toegang tot persoonsgegevens in het bezit van **[naam organisatie]** zonder voorafgaande afsluiting van een gegevensvertrouwelijkheidsovereenkomst, die aan de externe partij dezelfde zwaarwegende verplichtingen oplegt als waaraan **[naam organisatie]** zelf gehouden is en die **[naam organisatie]** het recht geeft conformering aan deze overeenkomst te controleren.

3. Verantwoordelijkheden en rollen onder de AVG

3.1 [Naam organisatie] is onder de AVG een **[specificeer: verwerkingsverantwoordelijke en/of verwerker]**.

3.2 Het hoogste management van **[naam organisatie]** en alle personeelsleden in management- of leidinggevende rollen binnen de organisatie zijn verantwoordelijk voor de ontwikkeling, invoering en stimulering van goede praktijken op het gebied van de bescherming van persoonsgegevens binnen **[naam organisatie]**; de exacte verantwoordelijkheden worden gespecificeerd in individuele functieomschrijvingen.

3.3 (Indien vereist) De functionaris voor gegevensbescherming, een in de AVG gespecificeerde rol, **[is een lid van het senior managementteam]**, rapporteert aan de **[naam hoogste orgaan]** binnen **[naam organisatie]** inzake de bescherming van persoonsgegevens binnen

[naam organisatie] en de status van compliance met en praktische toepassing van wetgeving op het gebied van bescherming van persoonsgegevens.

3.4 (Indien vereist) De functionaris voor gegevensbescherming, die volgens de **[naam hoogste orgaan]** beschikt over de juiste kwalificaties en passende ervaring, is aangesteld met de bedoeling dat hij of zij de verantwoordelijkheid op zich neemt voor monitoring van en advisering met betrekking tot conformering, binnen **[naam organisatie]** en op dagelijkse basis, aan dit beleid en, in het bijzonder, voor monitoring en advisering van managers en leidinggevenden inzake AVG-compliance bij **[naam organisatie]**, binnen hun respectievelijke verantwoordelijkheidsterreinen.

3.5 (Indien vereist) De functionaris voor gegevensbescherming heeft specifieke verantwoordelijkheden met betrekking tot relevante procedures en is het eerste aanspreekpunt voor medewerkers die uitleg nodig hebben over welk aspect dan ook van gegevensbescherming-compliance.

3.6 Naleven van wetgeving op het gebied van bescherming van persoonsgegevens is de verantwoordelijkheid van alle medewerkers van **[naam organisatie]** die persoonsgegevens verwerken.

3.7 De "Procedure Training en bewustwording" van **[naam organisatie]** specificeert vereisten op het gebied van training en bewustwording in relatie tot de rollen van medewerkers betrokken bij de verwerking van persoonsgegevens.

3.8 Het is de verantwoordelijkheid van medewerkers van **[naam organisatie]** om ervoor te zorgen dat persoonsgegevens over hen en door hen verstrekt aan **[naam organisatie]** correct en actueel zijn.

4. Principes van bescherming van persoonsgegevens

Alle vormen van verwerking van persoonsgegevens moeten worden uitgevoerd in overeenstemming met de grondbeginselen zoals omschreven in artikel 5 van de AVG. Beleid en procedures met betrekking tot de bescherming van persoonsgegevens binnen **[naam organisatie]** zijn opgesteld om compliance met deze grondbeginselen te waarborgen.

4.1 Verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn

[Naam organisatie] onderhoudt een "Procedure Opstellen en bekendmaken privacyverklaringen" en privacyverklaringen.

De specifieke informatie die in dit kader door **[naam organisatie]** aan de betrokkenen wordt verstrekt, moet minimaal het volgende omvatten:

- Identiteit en contactgegevens van de verwerkingsverantwoordelijke en, voor zover van toepassing, diens vertegenwoordiger;
- Contactgegevens van de Functionaris Gegevensbescherming (indien niet benoemd, dan de contactgegevens van **[functietitel]**);
- Doelstellingen van de verwerking waarvoor de persoonsgegevens zijn bedoeld en de wettelijke grondslag voor de verwerking;
- De bewaartermijn van de persoonsgegevens;
- Het recht van de betrokkene op inzage, rectificatie en verwijdering van zijn of haar persoonsgegevens en het recht om bezwaar te maken tegen de verwerking, en de voorwaarden (of het ontbreken van voorwaarden) voor de uitoefening van deze rechten, bijvoorbeeld in verband met mogelijke effecten op de rechtmatigheid van eerdere verwerking;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens, waar van toepassing;
- Dat de verwerkingsverantwoordelijke, waar van toepassing, het voornemen heeft tot doorgifte van de persoonsgegevens aan een ontvanger in een derde land en het niveau van bescherming dat voor de persoonsgegevens wordt geboden;
- Alle andere informatie die nodig is om zeker te stellen dat sprake is van verwerking die voldoet aan de beginselen van rechtmatigheid, behoorlijkheid en transparantie.

4.2 Persoonsgegevens mogen alleen worden verzameld voor specifieke, expliciete en gerechtvaardigde doeleinden

Gegevens die zijn verkregen voor uitdrukkelijk omschreven doeleinden mogen niet worden gebruikt voor een doel dat afwijkt van de doeleinden als omschreven in het register van verwerkingen van **[naam organisatie]**.

4.3 Persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de voorgenomen verwerking

- De **[functietitel]** zorgt er door monitoring en advisering voor dat **[naam organisatie]** geen informatie verzamelt die niet strikt noodzakelijk is voor de gestelde doeleinden.
- Alle vormen van gegevensverzameling (elektronisch of op papier), met inbegrip van gegevensverzamelingsvereisten in nieuwe informatiesystemen, moeten vergezeld gaan van een koppeling naar een (of meer) privacyverklaring(en).
- De **[functietitel]** zorgt voor monitoring van en advisering inzake methoden van gegevensverzameling om zeker te stellen dat de verzamelde persoonsgegevens toereikend en ter zake dienend blijven en niet excessief zijn.

4.4 Om ervoor te zorgen dat persoonsgegevens accuraat en actueel zijn, moeten alle redelijke maatregelen worden genomen om persoonsgegevens die onjuist zijn onverwijld te wissen of te rectificeren

- Persoonsgegevens die bij **[naam organisatie]** zijn opgeslagen, moeten regelmatig worden gecontroleerd en waar nodig geactualiseerd. Persoonsgegevens waarvan niet in redelijkheid kan worden aangenomen dat ze correct zijn, moeten ook niet worden bewaard.
- De **[functietitel]** zorgt er door monitoring en advisering voor dat alle medewerkers training ontvangen over het belang van het verzamelen van accurate persoonsgegevens en het op peil houden van die accuratesse.
- Het is ook de verantwoordelijkheid van de betrokkene om ervoor te zorgen dat de persoonsgegevens in bezit van **[naam organisatie]** accuraat en actueel zijn. Dat is de reden waarom betrokkenen bij het invullen van registratie- of aanvraagformulieren tevens, door middel van een standaard opgenomen tekst, verklaren de in het formulier verstrekte persoonsgegevens correct zijn op het tijdstip van indienen.
- Medewerkers **[indien van toepassing: anderen]** zijn gehouden **[naam organisatie]** te verwittigen van wijzigingen in hun omstandigheden, zodat hun persoonsgegevens overeenkomstig kunnen worden aangepast.
  Het is de verantwoordelijkheid van **[naam organisatie]** om ervoor te zorgen dat alle berichtgeving met betrekking tot wijziging van omstandigheden wordt gedocumenteerd en dat er actie op wordt ondernomen.
- De **[functietitel]** zorgt er door monitoring en advisering voor dat passend beleid en passende procedures geïmplementeerd zijn om persoonsgegevens accuraat en actueel te houden, rekening houdend met de hoeveelheid verzamelde gegevens, de snelheid waarmee veranderingen kunnen optreden en andere relevante factoren.
- Minimaal op jaarlijkse basis bekijkt de **[functietitel]** de einddatums voor bewaring van alle door **[naam organisatie]** verwerkte persoonsgegevens aan de hand van het register van verwerkingen, ter identificatie van persoonsgegevens die niet langer nodig zijn in de context van het geregistreerde doel. Deze persoonsgegevens worden vervolgens op een veilige manier verwijderd/vernietigd conform de “Procedure Veilige Verwijdering van Opslagmedia”.
- De **[functietitel]** ziet erop toe dat wordt gereageerd op door betrokkenen ingediende verzoeken tot rectificatie, en wel binnen één maand. Die termijn kan indien nodig en gelet op de complexiteit van het verzoek, met nog eens twee maanden worden verlengd. Als **[naam organisatie]** besluit geen gevolg te geven aan een verzoek, deelt de **[functietitel]** de betrokkene mee waarom het verzoek zonder gevolg is gebleven, en informeert hij hem/haar over de mogelijkheid om een klacht in te dienen bij een toezichthoudende autoriteit en beroep bij de rechter in te stellen.
- In het geval dat derden mogelijk onjuiste of achterhaalde persoonsgegevens hebben ontvangen, zorgt de **[functietitel]** ervoor dat die derden van de problemen op de

hoogte worden gesteld en worden geïnstrueerd de persoonsgegevens niet te gebruiken als basis voor besluitvorming ten aanzien van de betrokkenen. Waar nodig zorgt de **[functietitel]** er ook voor dat correcties worden doorgegeven aan de betreffende derden.

4.5 Persoonsgegevens moeten worden bewaard in een vorm die identificatie van de betrokkenen niet langer mogelijk maakt dan noodzakelijk is voor de doeleinden van verwerking van de gegevens

- Als persoonsgegevens langer worden bewaard dan tot aan de einddatum van verwerking, worden ze **[geminimaliseerd/versleuteld/gepseudonimiseerd]** ter bescherming van de identiteit van de betrokkenen. Dit is gedocumenteerd in de/het **[specificeer: document / applicatie]**.
- Persoonsgegevens worden bewaard in overeenstemming met de "Procedure Bewaartermijnen" en worden bij verstrijken van de bewaartermijn op een veilige manier vernietigd, zoals beschreven in deze procedure.
- Wanneer persoonsgegevens langer worden bewaard dan de bewaartermijnen die zijn vastgelegd in de "Procedure Bewaartermijnen", ziet de **[functietitel]** erop toe dat rechtvaardiging voor die verlengde periode duidelijk is omschreven en in overeenstemming is met wettelijke eisen ten aanzien van bescherming van persoonsgegevens.

4.6 Persoonsgegevens moeten worden verwerkt op een dusdanige manier dat passende beveiliging ervan gewaarborgd is

De **[functietitel]** ziet toe op uitvoering van een of meer risicobeoordelingen, rekening houdend met de specifieke omstandigheden van de werkzaamheden van **[naam organisatie]** in haar rol als verwerkingsverantwoordelijke of verwerker.

Bij beoordeling van het al dan niet passend zijn van voorgestelde beveiligingsmaatregelen moet de **[functietitel]** ook rekening houden met de mate van mogelijke schade of verlies voor individuele personen (bijv. voor medewerkers of klanten) in het geval van een beveiligingsincident, met het effect van beveiligingsincidenten voor **[naam organisatie]** zelf, en met elke vorm van te verwachten reputatieschade, met inbegrip van mogelijk verlies van klantvertrouwen.

Bij evaluatie van passende technische maatregelen moet de **[functietitel]** de volgende mogelijkheden overwegen (opsomming niet limitatief):

- Wachtwoordbeveiliging (Procedure Beheer van Gebruikerstoegang)
- Automatische vergrendeling van niet in gebruik zijnde terminals

- Intrekking van toegangsrechten voor USB-sticks en andere geheugenmedia (Procedure Regels voor toegangscontrole en toegangsrechten)
- Inzet van antivirus-software en firewalls (Procedure Beveiliging van draadloze computers)
- Rol-gebaseerde toegang (Regels voor Toegangscontrole en Toegangsrechten voor Gebruikers/Gebruikersgroepen)
- Versleuteling van apparaten die buiten bedrijfsgebouwen van **[naam organisatie]** komen, zoals laptops (Procedure Beveiliging van draadloze computers)
- LAN- en WAN-beveiliging (Procedure Beveiliging van draadloze computers)
- Privacy-verhogende technologieën als pseudonimisering en anonimisering
- Inventarisatie van passende internationale beveiligingsstandaarden die relevant zijn voor **[naam organisatie]**

Bij evaluatie van passende organisatorische maatregelen moet de **[functietitel]** de volgende mogelijkheden overwegen (opsomming niet limitatief):

- De passende niveaus van training in alle geledingen van **[naam organisatie]**
- Maatregelen ter beoordeling van de betrouwbaarheid van medewerkers (zoals referenties etc.)
- Opname van bescherming van persoonsgegevens in arbeidscontracten
- Identificatie van disciplinaire maatregelen in het geval van datalekken
- Monitoring van tegemoetkoming aan relevante beveiligingsstandaarden onder het personeel
- Fysieke toegangscontrole voor elektronische persoonsgegevens en persoonsgegevens op papier
- Invoering van clean desk beleid
- Opslag van persoonsgegevens op papier in afsluitbare brandveilige kasten
- Beperking van gebruik van mobiele elektronische apparatuur buiten de werkomgeving
- Beperking van gebruik door medewerkers van eigen apparatuur in de werkomgeving
- Invoering van duidelijke regels voor wachtwoorden
- Maken van regelmatige back-ups van persoonsgegevens waarbij de media op externe locaties worden opgeslagen
- Oplegging van contractuele verplichtingen aan de importerende organisaties tot het nemen van passende beveiligingsmaatregelen bij overdracht van persoonsgegevens naar landen buiten de Europese Economische Ruimte

Deze maatregelen zijn geselecteerd op basis van geïdentificeerde risico's voor persoonsgegevens en de potentiële schade, materieel dan wel immaterieell, voor personen van wie persoonsgegevens worden verwerkt.

4.7 De verwerkingsverantwoordelijke moet in staat zijn compliance aan te tonen met de andere principes van de AVG (accountability)

Bij wijze van aanvulling op de eisen ten aanzien van transparantie, staan in de AVG ook bepalingen die stimuleren tot accountability en zorgvuldige bedrijfsvoering. Het accountability-principe in artikel 5, lid 2 stelt dat de verwerkingsverantwoordelijke niet alleen moet voldoen aan de in de AVG genoemde principes van verantwoorde gegevensverwerking, maar tevens in staat moet zijn naleving aan te tonen.
[Naam organisatie] zal naleving van deze principes aantonen door implementatie van beleid voor bescherming van persoonsgegevens, door zich te houden aan vastgelegde gedragsregels, door het nemen van technische en organisatorische maatregelen en door adoptie van technieken als data protection by design, door het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's), door het onderhouden van procedures voor melding van datalekken en reactie op incidenten.

5. Rechten van de betrokkenen

Als het gaat om de persoonsgegevens die over hen worden verzameld en vastgelegd en over de verwerking van die gegevens, hebben betrokkenen de volgende rechten:

- Inzage van zijn of haar persoonsgegevens om te controleren wat voor persoonsgegevens zijn verzameld en aan wie ze beschikbaar zijn gesteld.
- Bezwaar te maken tegen verwerking die tot schade, materieel dan wel immaterieel, kan leiden.
- Bezwaar te maken tegen verwerking ten behoeve van direct marketing.
- Geïnformeerd te worden over de mechanismen van geautomatiseerd proces van besluitvorming dat verstrekkende gevolgen voor de betrokkene kan hebben.
- Niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hem of haar verstrekkende gevolgen verbonden zijn.
- Compensatie te eisen voor geleden schade als gevolg van een overtreding van de AVG.
- Actie te ondernemen om te zorgen dat onjuiste persoonsgegevens worden gerectificeerd, geblokkeerd, gewist (met inbegrip van het recht op vergetelheid) of vernietigd.
- De toezichthoudende autoriteit te verzoeken na te gaan of er sprake is van een overtreding van de AVG.
- De hem of haar betreffende persoonsgegevens te verkrijgen in een gestructureerd, gangbaar en machineleesbaar formaat en die aan een andere verwerkingsverantwoordelijke door te laten zenden.

- Niet te worden onderworpen aan geautomatiseerde besluitvorming zonder daar toestemming voor te hebben gegeven.

[Naam organisatie] zorgt ervoor dat betrokkenen de volgende rechten kunnen uitoefenen:

- Betrokkenen hebben het recht te vragen om inzage in hun persoonsgegevens zoals beschreven in de “Procedure Afhandeling verzoek tot inzage”. Deze procedure beschrijft ook hoe **[naam organisatie]** ervoor zal zorgen dat haar reactie op een verzoek om inzage tot persoonsgegevens voldoet aan de vereisten van de AVG.
- Betrokkenen hebben het recht een verzoek, klacht of bezwaar in te dienen bij **[naam organisatie]** in verband met de verwerking van hun persoonsgegevens. De behandeling van een door hen ingediend verzoek of een door hen ingediende klacht of ingediend bezwaar is vastgelegd in de daarvoor opgestelde procedures betreffende verzoeken, klachten en bezwaren.

6. Toestemming

[Naam organisatie] begrijpt ‘toestemming’ in de betekenis van expliciet en vrijwillig verleend, als een specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling aangeeft in te stemmen met verwerking van hem of haar betreffende persoonsgegevens. De betrokkene kan die toestemming op elk gewenst moment intrekken.

[Naam organisatie] verstaat onder ‘toestemming’ ook dat de betrokkene volledig is geïnformeerd over de voorgenomen verwerking en zich daarmee akkoord heeft verklaard, in het volle bezit van zijn of haar verstandelijke vermogens en zonder dat er druk op hem of haar is uitgeoefend. Onder druk of dwang verkregen toestemming of toestemming die is verleend op basis van misleidende informatie, wordt niet beschouwd als een wettelijke grondslag voor verwerking.

[Naam organisatie] moet in staat zijn aan te tonen dat toestemming is verkregen voor een verwerking van persoonsgegevens. **[Voeg in hoe u dat wilt doen – bijv. door middel van een te ondertekenen formulier of door een prominent aanwezige privacyverklaring op uw website te plaatsen die mensen moeten accepteren alvorens ze persoonsgegevens kunnen doorgeven.]**

Voor bijzondere persoonsgegevens moet expliciete, schriftelijke toestemming zijn verkregen tenzij er sprake is van een alternatieve wettelijke grondslag voor verwerking.

Waar **[naam organisatie]** online diensten verleent aan kinderen, is ouderlijke toestemming nodig of toestemming verleend door de persoon die de ouderlijke verantwoordelijkheid voor het kind draagt. Voor die lidstaten waar de leeftijdsgrens niet lager is gelegd, geldt dit vereiste voor kinderen jonger dan 16 jaar.

7. Gegevensveiligheid

Alle medewerkers van **[naam organisatie]** hebben de taak ervoor te zorgen dat de persoonsgegevens die in het bezit zijn van **[naam organisatie]** en waarvoor zij verantwoordelijk zijn, veilig worden bewaard en onder geen enkele voorwaarde worden verstrekt aan derden, tenzij die derde uitdrukkelijk door **[naam organisatie]** is geautoriseerd voor ontvangst van de betreffende informatie en daartoe een vertrouwelijkheidsovereenkomst is aangegaan **[voeg in: verwijzing naar document]**.
Alle persoonsgegevens dienen uitsluitend toegankelijk te zijn voor personen die ermee moeten werken en toegang mag alleen worden verleend volgens de "Procedure Toegangscontrole".
Alle persoonsgegevens moeten worden behandeld met inachtneming van de hoogste veiligheidseisen en moeten als volgt worden bewaard:

- in een afsluitbare ruimte met voorzieningen voor toegangscontrole; en/of
- in een afgesloten lade of archiefkast; en/of
- in het geval van digitale gegevens, wachtwoordbeveiligd in overeenstemming met de bedrijfsregels van de "Procedure Toegangscontrole"; en/of
- opgeslagen op (uitneembare) computermedia, versleuteld in overeenstemming met de "Procedure Veilige verwijdering van opslagmedia".

Er dient op te worden gelet dat beeldschermen en terminals alleen zichtbaar zijn voor geautoriseerd personeel van **[naam organisatie]**. Alle medewerkers zijn verplicht een individuele Gebruikersovereenkomst aan te gaan voordat hen toegang wordt verleend tot bedrijfsinformatie van welke aard dan ook. In die overeenkomst worden o.a. zaken geregeld als automatische schermuitschakeling en screen time-outs.
Gegevens op papier mogen niet worden achtergelaten op plaatsen waar ze kunnen worden gezien door ongeautoriseerd personeel en mogen niet worden meegenomen uit de bedrijfsgebouwen zonder uitdrukkelijke toestemming. Zodra zulke papieren persoonsgegevens niet langer nodig zijn voor dagelijkse klantenondersteuning, dienen ze uit hun beveiligd archief te worden verwijderd in overeenstemming met de "Procedure Veilige verwijdering van opslagmedia".
Persoonsgegevens mogen alleen worden gewist of verwijderd in overeenstemming met de "Procedure Bewaartermijnen". Papieren persoonsgegevens waarvoor het einde van de bewaartermijn is bereikt, worden versnipperd en afgevoerd als 'vertrouwelijk afval'. Vaste schijven van overbodig geworden computers worden verwijderd en onmiddellijk vernietigd

volgens de voorschriften van de “Procedure Veilige verwijdering van opslagmedia”. Pas daarna is afvoer mogelijk.
‘Off-site’ verwerking van persoonsgegevens verhoogt het gevaar van verlies, diefstal of beschadiging van gegevens. Voor off-site gegevensverwerking is dan ook specifieke autorisatie vereist.

8. Verstrekking van persoonsgegevens aan derden

[Naam organisatie] moet ervoor zorgen dat persoonsgegevens niet worden verstrekt aan ongeautoriseerde derden. Daaronder vallen ook familieleden en vrienden van medewerkers, overheidsinstanties en in bepaalde omstandigheden, de politie. Alle medewerkers dienen voorzichtigheid te betrachten wanneer hen wordt gevraagd persoonsgegevens te verstrekken aan enige andere partij dan de betrokkene zelf. In voorkomende gevallen dient altijd de vraag te worden gesteld of verstrekking van de persoonsgegevens relevant en noodzakelijk is voor de bedrijfsvoering van **[naam organisatie]**.
Onder de AVG is verstrekking van persoonsgegevens aan derden in sommige gevallen toegestaan zonder toestemming van de betrokkene, namelijk als er een van de volgende doelen mee gediend wordt:

- waarborging van nationale veiligheid;
- voorkoming van of onderzoek naar strafbare feiten, met inbegrip van aanhouding en vervolging van de daders;
- belastingtechnisch onderzoek of heffing van belasting;
- onderzoek naar schendingen van beroepscode (bijv. met betrekking tot gezondheid, veiligheid en welzijn op het werk);
- voorkoming van ernstige schade voor een derde; en
- bescherming van de vitale belangen van een persoon.

Verzoeken tot verstrekking van persoonsgegevens om een van deze redenen moeten vergezeld gaan van een deugdelijke onderbouwing en voor feitelijke verstrekking is altijd specifieke autorisatie nodig van de **[functietitel]**.

9. Bewaring en verwijdering van gegevens

[Naam organisatie] bewaart persoonsgegevens, in een vorm die identificatie van de betrokkenen mogelijk maakt, niet langer dan nodig is met het oog op het doel of de doeleinden waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

[Naam organisatie] kan persoonsgegevens langer bewaren als die persoonsgegevens dan uitsluitend worden verwerkt met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. In dat geval zullen passende technische en organisatorische maatregelen worden genomen om rechten en vrijheden van de betrokkenen te waarborgen.
De bewaartermijn voor elke categorie persoonsgegevens wordt vastgelegd in de "Procedure Bewaartermijnen", samen met de criteria voor bepaling van die periode, waarbij ook wettelijke verplichtingen een rol kunnen spelen.
De procedures van **[naam organisatie]** ten aanzien van bewaring en verwijdering van persoonsgegevens zijn in alle gevallen van toepassing.
Persoonsgegevens moeten op een veilige manier worden verwijderd, in overeenstemming met artikel 5 lid 1 sub f AVG – dusdanig dat veiligheid gewaarborgd is, ter bescherming van de "rechten en vrijheden" van de betrokkenen. Verwijdering van persoonsgegevens gebeurt altijd volgens de "Procedure Veilige verwijdering van opslagmedia".

10. Doorgifte van gegevens [optioneel]

Doorgifte van persoonsgegevens vanuit de Europese Economische Ruimte (EER) naar niet-EER landen (in de AVG 'derde landen' genoemd) is verboden tenzij het derde land in kwestie passende waarborgen biedt voor een adequaat "beschermingsniveau voor de grondrechten van de betrokkenen".

Doorgifte van persoonsgegevens naar landen buiten de EER is verboden tenzij een of meer van de in de AVG gespecificeerde waarborgen of uitzonderingen van toepassing zijn:

Een adequaatheidsbesluit
De Europese Commissie kan derde landen, een gebied en/of specifieke sectoren in derde landen beoordelen en voert zulke beoordelingen ook in de praktijk uit, om vast te stellen of er sprake is van een adequaat beschermingsniveau voor de rechten en vrijheden van natuurlijke personen. Waar dat geval is, is geen autorisatie vereist.
Landen die behoren tot de Europese Economische Ruimte (EER) maar geen lidstaat zijn van de EU, worden geaccepteerd als voldoend aan de voorwaarden voor een adequaatheidsbesluit.
In het Publicatieblad van de Europese Unie worden lijsten gepubliceerd van landen die op dat moment voldoen aan de adequaatheidsvereisten van de Commissie.

Privacy Shield
Als **[naam organisatie]** persoonsgegevens vanuit de EU wil doorgeven aan een organisatie in de Verenigde Staten, moet worden gecontroleerd of die organisatie is aangesloten bij het Privacy Shield programma van het Amerikaanse Ministerie van Economische Zaken. Bedrijven

die in dit Privacy Shield programma participeren, zijn gehouden te voldoen aan beginselen die zijn vastgelegd in de “Privacy Principles”. Beheer en bestuur van het Privacy Shield is in handen van het Amerikaanse Ministerie van Economische Zaken dat erop toeziet dat bedrijven zich aan hun verplichtingen houden. Om in aanmerking te komen voor certificering moeten bedrijven over een privacybeleid beschikken dat in overeenstemming is met de Privacy Principles, wat bijvoorbeeld wil zeggen dat gebruik, opslag en verdere doorgifte van persoonsgegevens gebonden is aan een set van strikte regels en waarborgen voor bescherming van persoonsgegevens. Dat niveau van bescherming van persoonsgegevens moet altijd worden aangehouden, ongeacht of de persoonsgegevens betrekking hebben op een ingezetene van de EU of niet. Lidmaatschap van het Privacy Shield programma moet jaarlijks worden vernieuwd. Gebeurt dat niet, dan is ontvangst en gebruik van uit de EU ontvangen persoonsgegevens in dat kader niet langer mogelijk.

Bindende bedrijfsvoorschriften

[Naam organisatie] kan een beroep doen op goedgekeurde bindende bedrijfsvoorschriften voor doorgifte van persoonsgegevens naar landen buiten de EU. De voorschriften waar **[naam organisatie]** zich op wil beroepen, moeten dan ter goedkeuring worden voorgelegd aan de relevante toezichthoudende autoriteit.

Modelcontractclausules

[Naam organisatie] kan een beroep doen op goedgekeurde modelcontractclausules voor doorgifte van persoonsgegevens naar landen buiten de EER. Als **[naam organisatie]** zich beroept op door de relevante toezichthoudende autoriteit goedgekeurde modelcontractclausules, wordt automatisch uitgegaan van adequaatheid.

Uitzonderingen

Bij ontstentenis van een adequaatheidsbesluit, lidmaatschap van Privacy Shield, bindende bedrijfsvoorschriften en/of modelcontractclausules, is doorgifte van persoonsgegevens naar een derde land of internationale organisatie alleen toegestaan op een van de volgende voorwaarden:

- De betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd, na te zijn ingelicht over de risico's die dergelijke doorgiften voor hem kunnen inhouden bij ontstentenis van een adequaatheidsbesluit en van passende waarborgen;
- De doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van op verzoek van de betrokkene genomen precontractuele maatregelen;
- De doorgifte is noodzakelijk voor de sluiting of de uitvoering van een in het belang van de betrokkene tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon gesloten overeenkomst;
- De doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang;

- De doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering; en/of
- De doorgifte is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven.

11. Risico's

[Naam organisatie] is zich bewust van de risico's die zijn verbonden aan verwerking van bepaalde typen persoonsgegevens.
[Naam organisatie] evalueert het niveau van risico voor betrokkenen dat is verbonden met de verwerking van hun persoonsgegevens. Voor verwerkingen met verhoogd risico worden door **[naam organisatie]** gegevensbeschermingseffectbeoordelingen (Data Protection Impact Assessments, DPIA's) uitgevoerd, zoals dat ook gebeurt voor verwerkingen met verhoogd risico die ten behoeve van **[naam organisatie]** worden uitgevoerd door andere organisaties.
Waar deze evaluatieprocessen wijzen op het bestaan van concrete risico's, zal **[naam organisatie]** er alles aan doen om die risico's te beheersen en de kans op afwijking van dit beleid te reduceren.
Waar een bepaald type verwerking, met name wanneer daarbij nieuwe technologieën worden gebruikt en gelet op aard, reikwijdte, context en doeleinden waarschijnlijk grote risico's voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, zal **[naam organisatie]** voorafgaand aan feitelijke verwerking een DPIA uitvoeren om de effecten van de voorgenomen verwerking op de bescherming van persoonsgegevens vast te stellen. Eén DPIA kan daarbij gelden voor een set van gelijksoortige verwerkingen met vergelijkbaar hoog risico.
Waar uit de resultaten van een DPIA duidelijk wordt dat **[naam organisatie]** op het punt staat een verwerking van persoonsgegevens te starten die ernstige lichamelijke, materiële en/of immateriële schade zou kunnen veroorzaken voor de betrokkenen, moet de beslissing over wel of niet doorgaan van deze verwerking door **[naam organisatie]** via een escalatieproces worden voorgelegd aan de **[functietitel]**.
Als er sprake is van ernstige zorgen, in termen van de ernst van de mogelijke lichamelijke, materiële of immateriële schade of in termen van het aantal betrokkenen, zal de **[functietitel]** de kwestie via een volgende stap in het escalatieproces voorleggen aan de toezichthoudende autoriteit.
Passende mechanismen zullen worden geselecteerd en toegepast om het met verwerking van afzonderlijke persoonsgegevens verbonden risico terug te brengen tot een aanvaardbaar niveau, onder verwijzing naar de door **[naam organisatie]** gedocumenteerde criteria voor risico-acceptatie en de vereisten van de AVG.

Documenteigenaar en Goedkeuring

Het is de verantwoordelijkheid van de **[functietitel]**, eigenaar van dit document, om ervoor te zorgen dat deze procedure periodiek wordt getoetst in overeenstemming met de voor het AVG-project geldende toetsingsvereisten.

Een actuele versie van dit document is beschikbaar voor **[alle/gespecificeerde]** medewerkers op het **[voeg locatie in, bijv. bedrijfsintranet]** en wordt gepubliceerd **[voeg medium in]**.

Deze werkinstructie is goedgekeurd door de **[functietitel]** op **[datum]** en wordt op basis van versiecontrole vrijgegeven.

Wijzigingshistorie

Versie	Beschrijving van wijziging	Goedgekeurd door	Datum
1	Eerste versie	**[Functietitel]**	**[dd/mm/jjjj]**
2			
3			