|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Vraag** | **Antwoord** | **Leidt het antwoord tot een verhoogd risico? Geef dan een beschrijving van de aanbevolen maatregelen.** | **Toelichting** |
| **1.** | **Algemeen** |  |  |  |
| 1.1 | Geef een korte omschrijving van de verwerking |  | *nvt* | *Geef een algemene omschrijving van de verwerking. Dit kan worden aangevuld met een stroomschema waarmee de afdelingen en systemen waarbinnen de persoonsgegevens worden verwerkt inzichtelijk wordt.* |
| 1.2 | Wie vult de DPIA in? |  | *nvt* |  |
| 1.3 | Op welke datum wordt de DPIA uitgevoerd? |  | *nvt* |  |
| 1.4 | Wie / welke afdeling is verantwoordelijk voor de verwerking? | *Dit kunnen ook meerdere afdelingen zijn.* | *nvt* | *Dit kunnen ook meerdere afdelingen zijn.* |
| 1.4.1 | Is de organisatie verwerkingsverantwoordelijke of verwerker?  Zie [de begrippen](https://a.pgosupport.nl/in-10-stappen-voorbereid-op-de-nieuwe-privacywet-avg#Begrippen) op blz 4 van de brochure |  |  | *Indien niet duidelijk is welke rol de organisatie heeft (verwerkingsverantwoordelijke of verwerker) kan dit een verhoogd risico met zich mee brengen* |
| **2** | **De persoonsgegevens / betrokkenen** |  |  |  |
| 2.1 | Welke persoonsgegevens worden verwerkt?  Voorbeelden  Naam, Adres, Telefoonnummer, Emailadres, Geboortedatum, Wachtwoorden, Gegevens over gezondheid, religieuze of levensbeschouwelijke overtuiging of  Bankrekeningnummer | *Dit zijn waarschijnlijk meerdere soorten gegevens* |  | *Per soort gegevens kunnen de privacyrisico’s verschillen. Het verwerken van gegevens over gezondheid, religieuze of levensbeschouwelijke overtuiging, seksueel gedrag of financiële gegevens brengt bijvoorbeeld een verhoogd risico van misbruik of onrechtmatige verwerking mee.* |
| 2.1.1 | Is sprake van verwerken van: |  |  |  |
|  | Bijzondere persoonsgegevens?  Bijvoorbeeld gegevens over gezondheid, religieuze of levensbeschouwelijke overtuiging, seksueel gedrag | *Zo ja, welke?* |  | *Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee dat (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging.*  *Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden (bijvoorbeeld als de betrokkene uitdrukkelijk toestemming voor welbepaalde doelen heeft gegeven)* |
|  | Uniek identificerende gegevens?  Bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen. | *Zo ja, welke?* |  | *Het werken met dit type gegevens brengt een verhoogd risico van misbruik met zich mee dat (potentieel grote) impact op de betrokkene heeft en vraagt daarmee om betere beveiliging.*  *Het verwerken van deze gegevens is alleen toegestaan onder bepaalde wettelijke voorwaarden* |
|  | Wettelijk voorgeschreven persoons­nummers?  Bijvoorbeeld het burgerservicenummer  (BSN). | *Zo ja, welke?* |  | *Het BSN nummer mag alleen worden verwerkt indien daarvoor een wettelijke basis is, anders is dit verboden.* |
| 2.2 | Van welke betrokkenen worden persoonsgegevens verwerkt?  Bijvoorbeeld klanten, leden, donateurs, medewerkers, vrijwilligers | *Geef een omschrijving van de categorieën van betrokkenen* |  | *Risico’s kunnen per categorie betrokkenen verschillen.*  *Voor betrokkenen in kwetsbare groepen zoals kinderen, gehandicapten of mensen met een ziekte brengt het verlies of onrechtmatige verwerking van persoonsgegevens extra risico's met zich mee.*  *Dit betekent dat er extra beveiligingsmaatregelen op een hoger beveiligingsniveau genomen moeten worden.* |
| **3** | **Verwerkingsdoeleinden** |  |  |  |
| 3.1 | Voor welke doeleinden worden de persoonsgegevens gebruikt?  Voorbeelden van doeleinden zijn: - Het werven van klanten - Het uitvoeren van de overeenkomst - Het organiseren van activiteiten  - Het doen van onderzoek  - Verstrekken of verkoop aan derden | *Geef een omschrijving van de doeleinden.* |  | *Persoonsgegevens mogen alleen voor duidelijk omschreven en gerechtvaardigde doeleinden worden verwerkt. Deze doeleinden moeten voorafgaand aan de verwerking zijn vastgesteld. Een verwerking kan voor meerdere doeleinden plaatsvinden.*  *De verwerking is mogelijk onrechtmatig indien niet bekend is voor welke doeleinden de persoonsgegevens verwerkt worden.* |
| 3.2 | Zijn alle gegevens noodzakelijk om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)? | *Zo ja, geef een toelichting* |  | *De wetgeving gaat uit van dataminimalisatie, hetgeen inhoudt dat niet meer gegevens verwerkt worden dan noodzakelijk voor de gestelde doeleinden. De organisatie loopt dus een risico als er te veel gegevens worden verwerkt.*  *Met name indien de gegevens uit vraag 2.1.1 worden verwerkt moet de organisatie zich afvragen of er geen andere mindere ingrijpende gegevens gebruikt kunnen worden.* |
| 3.3 | Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)? | *Zo ja, geef een toelichting* |  | *Privacyrisico’s kunnen worden verkleind door gebruik te maken van geanonimiseerde en/*  *of gepseudonimiseerde gegevens.* |
| 3.4 | Worden persoonsgegevens ook gebruikt voor direct marketing-activiteiten?  Bijv. benadering per telefoon of mail | *Zo ja, wat voor activiteiten:* |  | *Indien persoonsgegevens ook voor direct marketing-activiteiten worden gebruikt, gelden ook aanvullende verplichtingen uit de Telecommunicatiewet. Niet-naleving van deze regels kan leiden tot zware boetes en reputatieschade* |
| **4** | **Rechtmatigheid van de gegevensverwerking** |  |  |  |
| 4.1 | Op basis van welke grondslag vindt de verwerking van persoonsgegevens plaats? | *Er kan gekozen worden uit de volgende 6 wettelijke grondslagen:*  *a. toestemming van de betrokkene.  b. uitvoering van een overeenkomst tussen de organisatie en de betrokkene.  c. wettelijke verplichting, bijvoorbeeld op grond van de Belastingwetgeving. d. vitaal belang van de betrokkene. e. ten behoeve van een publiekrechtelijke taak door het bestuursorgaan waaraan de gegevens worden verstrekt. f. Gerechtvaardigd belang van de organisatie of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of van de betrokkene zwaarder weegt.* |  | *Persoonsgegevens mogen alleen op basis van een wettelijke grondslag worden verwerkt. Indien er geen grondslag aanwezig is, mogen er geen persoonsgegevens worden verwerkt.*  *Dan bestaat het risico dat de verwerking onrechtmatig is.* |
| **5.** | **Toestemming van betrokkenen** |  |  |  |
| 5.1 | Indien de gegevens worden verwerkt op basis van toestemming, op welke wijze wordt deze gevraagd? | *Beschrijven hoe toestemming wordt gevraagd.* |  | *Uit de AVG vloeit voort dat van een rechtsgeldige toestemming pas sprake is indien deze vrijelijk is gegeven; gegeven is voor een specifiek doel en bovendien gebaseerd is op duidelijke informatie.*  *Indien de toestemming daar niet aan voldoet, bestaat het risico dat de verwerking onrechtmatig is.* |
| 5.2 | Indien de gegevens worden verwerkt op basis van toestemming, hoe kan de organisatie aantonen dat deze toestemming is verkregen? | *Beschrijven hoe de toestemming kan worden aangetoond.* |  | *Uit de AVG vloeit voort dat de organisatie moet kunnen aantonen dat de betrokkene toestemming heeft gegevens. Kan de organisatie dat niet aantonen dan bestaat het risico dat de verwerking onrechtmatig is.* |
| 5.3 | Op welke wijze kan de betrokkene de toestemming weer intrekken? | *Beschrijven hoe de toestemming kan worden ingetrokken.* |  | *Uit de AVG vloeit voort dat de betrokkene te allen tijde het recht heeft om de toestemming in te trekken. Voldoet de organisatie hier niet aan dan bestaat het risico dat de verwerking onrechtmatig is.* |
| 5. | **Informeren van betrokkene** |  |  |  |
| 5.1 | Wordt de betrokkene voorafgaand aan de gegevensverwerking geïnformeerd over de verwerking van persoonsgegevens? | *Zo ja, op welke wijze wordt de informatie verstrekt? Bijvoorbeeld via een Privacybeleid?* |  | *De betrokkene moet worden geïnformeerd over de verwerking van zijn persoonsgegevens, de doeleinden, zijn rechten etc. Als dit niet zorgvuldig gebeurt, heeft dit tot gevolg dat de verwerking onrechtmatig is.* |
| **6.** | **Rechten van betrokkenen** |  |  |  |
| 6.1 | Uit de AVG volgt dat aan de betrokkene onder meer de volgende rechten toekomen:  Het recht op (i) informatie over en inzage in de verwerking van diens gegevens, (ii) correctie of beperking van de persoonsgegevens, (iii) vergeten te worden (‘vergetelheid’), (iv) dataportabiliteit, (v) bezwaar maken tegen profilering en geautomatiseerde besluitvorming.  Kan de betrokkene deze rechten uitoefenen? | *Zo ja, beschrijf op welke wijze.* |  | *Indien betrokkene diens rechten niet kan uitoefenen dan bestaat het risico dat de verwerking onrechtmatig is.* |
| 6.2 | Wordt de betrokkene van diens rechten en de mogelijkheid tot uitoefening daarvan op de hoogte gesteld? | *Zo ja, op welke wijze*  *(Bijvoorbeeld via Privacybeleid).* |  | *De verwerkingsverantwoordelijke dient de betrokkene van diens rechten op de hoogte te stellen. Anders bestaat het risico dat de verwerking onrechtmatig is.* |
|  |  |  |  |  |
| **7** | **Bewaren en vernietigen** |  |  |  |
| 7.1 | Is een bewaartermijn voor de persoonsgegevens vastgesteld?  Zo ja, wat is de bewaartermijn? | *Bewaartermijn aangeven, eventueel differentiëren naar soort gegevens.* |  | *Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld.*  *Indien er geen bewaartermijnen zijn vastgesteld voor de persoonsgegevens, is het risico groot dat de persoonsgegevens langer worden bewaard dan noodzakelijk voor het verwezenlijken van de doeleinden waarvoor de persoonsgegevens zijn verzameld. Dan bestaat het risico dat de verwerking onrechtmatig is.* |
| 7.2 | Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwij­derd (uit een bestand) of vernietigd? | *Zo ja, op welke wijze?* |  | *De gegevens dienen na afloop van de bewaartermijn daadwerkelijk verwijderd of geanonimiseerd te worden. Indien dit niet mogelijk is, wordt het risico dat de gegevens voor andere doeleinden worden gebruikt groter. Bovendien wordt dan in strijd met de AVG gehandeld.* |
| 7.3 | Zo ja, worden de gegevens na verstrij­ken van de bewaartermijn op zo’n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?  Let hierbij ook op alle mogelijke locaties en media waarop de gegevens bewaard kunnen zijn. Al deze locaties en media moeten worden meegenomen. | *Zo ja, op welke wijze?* |  | *Op grond van specifieke wetgeving, bijv Archiefwet of belastingwetgeving, kan het mogelijk zijn dat bepaalde gegevens langer bewaard moeten worden. Uitsluitend de gegevens die voor deze specifieke wetgeving noodzakelijk zijn, mogen dan bewaard blijven.* |
| **8.** | **Betrokken partijen** |  |  |  |
| 8.1 | Zijn er bij de verwerking van de gegevens meerdere *interne* partijen (medewerkers) betrokken? | *Zo ja, welke partijen/medewerkers?* |  | *Indien er meerdere afdelingen personen betrokken zijn, is er een verhoogd risico. Er moet per afdeling / partij een duidelijke beschrijving van taken en verantwoordelijkheden zijn. Bijv. over beveiliging, afhandeling fouten, controles, vernietiging, beveiliging etc.* |
| 8.2 | Zijn deze *interne* partijen (medewerkers) geïnformeerd over de specifieke privacyrisico’s? | *Zo ja, op welke wijze?* |  | *Als medewerkers zich niet bewust zijn van de risico’s die met de verwerking gepaard gaan (bijvoorbeeld het risico dat persoonsgegevens onveilig worden opgeslagen, te lang worden bewaard of voor een ander doel worden gebruikt), dan bestaat er een verhoogd risico dat de gegevensverwerking in strijd is met de AVG en dus onrechtmatig is.* |
| 8.3 | Zijn er bij de verwerking van de gegevens meerdere *externe* partijen (verwerkers) betrokken? | *Zo ja, welke externe partijen?* |  | *Hoe meer partijen bij de verwerking betrokken zijn, hoe groter de kans op verlies, onrechtmatige verwerking, onduidelijkheden in verantwoordelijkheden etc.* |
| 8.4 | Heeft de organisatie met alle verwerkers een verwerkersovereenkomst gesloten? | *Zo nee, met welke externe partijen niet?* |  | *De organisatie is verplicht om met verwerkers een verwerkersovereenkomst te sluiten.*  *Zonder zo’n overeenkomst handelt de organisatie in strijd met de AVG en is de verwerking onrechtmatig.* |
| 8.5 | Zijn de verwerkers gevestigd buiten de Europese Economische Ruimte (EER)? | *Zo ja, aangeven welke partijen dat zijn*. |  | *Zo nee, dan bestaat er een verhoogd risico dat de gegevensverwerking in strijd is met de AVG en dus onrechtmatig is.* |
|  |  |  |  |  |
| **9** | **Beveiliging** |  |  |  |
| 9.2 | Zijn er passende beveiligingsmaatregelen genomen om de geïdentificeerde risico’s te beperken? | *Zo ja, omschrijf welke specifieke beveiligingsmaatregelen zijn genomen voor de verwerking van de persoonsgegevens.* |  | *Indien geen passende beveiligingsmaatregelen zijn getroffen, bestaat er een vergroot risico op beveiligingsincidenten en datalekken. Bovendien handelt de organisatie dan in strijd met de AVG, waardoor het verhoogd risico bestaat dat de verwerking onrechtmatig is.* |
| 9.1 | Is er sprake van intern geformuleerd beleid over het beveiligen van informatie? |  |  | *Een informatiebeveiligingsbeleid schept duidelijkheid over de maatregelen die de organisatie neemt / dient te nemen. Hiermee wordt de bewustwording van beveiliging vergroot.* |
| **10** | **Datalekken** |  |  |  |
|  | Zijn er maatregelen genomen om mogelijke datalekken in het systeem te identificeren? | *Zo ja, omschrijf de maatregelen.* |  | *Indien er geen maatregelen zijn genomen om datalekken te identificeren, bestaat het risico dat de organisatie niet (tijdig) op de hoogte is van mogelijke datalekken en/of kwetsbaarheden. Hierdoor kan de organisatie niet aan haar verplichtingen uit de AVG (bijv. beveiliging en meldplicht datalekken) voldoen.* |