

## AVG Self-assessment voor externe partijen (bijv. leveranciers en ketenpartners)

### Details assessment

Verstreckende organisatie:

Ontvangende organisatie:

Datum assessment:

Ingevuld door:

Organisatie:

Functie:

E-mail:

Telefoonnummer:

**1. Omvatten uw diensten/producten het verzamelen, opslaan, openen, behandelen of anderszins toegang hebben tot persoonsgegevens die direct of indirect verband houden met kandidaten, werknemers, werknemers van de klant of andere Betrokkenen of vertegenwoordigers van de Verstreckende organisatie?**

*Persoonsgegevens* betekent 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 identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

- Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

---

**2. Bent u voor de geleverde dienst een verwerker of een verwerkingsverantwoordelijke?**

- Opties:*  Verwerker  
 Verwerkingsverantwoordelijke  
 Gezamenlijk verwerkingsverantwoordelijke

*Motiveer hier uw antwoord*

### 3. Selecteer de categorieën van persoonsgegevens die u als Ontvangende organisatie zal verwerken (bijv. toegang, opslag, openbaarmaking, wissen).

Geef via het onderstaande vak meer details over het type persoonsgegevens dat uw organisatie zal verwerken.

- Opties:*
- |   |  |
|---|--|
| <input type="checkbox"/> Naam, voornaam, voorletters, titel                       | <input type="checkbox"/> Onderwijs-/vaardigheidsgegevens     |
| <input type="checkbox"/> Geslacht, geboortedatum, geboorteplaats en nationaliteit | <input type="checkbox"/> Werkgelegenheidsgegevens (bijv. CV) |
| <input type="checkbox"/> Adres, postcode en woonplaats                            | <input type="checkbox"/> Achtergrondchecks                   |
| <input type="checkbox"/> Telefoonnummer en e-mailadres                            | <input type="checkbox"/> Gezondheidsgegevens                 |
| <input type="checkbox"/> IBAN bankrekeningnummer                                  | <input type="checkbox"/> Geloofsovertuiging                  |
| <input type="checkbox"/> BSN / Persoonsgebonden nummer                            | <input type="checkbox"/> Account-/loginformatie              |
| <input type="checkbox"/> (Kopie) ID-bewijs/paspoort                               | <input type="checkbox"/> Browsegegevens                      |
| <input type="checkbox"/> Beeldmateriaal   | <input type="checkbox"/> Diagnostische gegevens              |
| <input type="checkbox"/> Financiële gegevens (gerelateerd aan een individu)       | <input type="checkbox"/> Overig                              |

*Motiveer hier uw antwoord*

#### 4. Worden er gevoelige of bijzondere persoonsgegevens verwerkt ten behoeve van de te leveren diensten/goederen?

Geef via het onderstaande vak meer details over het type persoonsgegevens dat uw organisatie zal verwerken.

**Bijzondere persoonsgegevens** zijn persoonsgegevens met betrekking tot raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen of lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met als doel een natuurlijke persoon uniek te identificeren, gegevens over gezondheid of gegevens over het seksleven of seksuele geaardheid van een natuurlijke persoon.

- Opties:**
- |   |  |
|---|--|
| <input type="checkbox"/> Ras of etnische afkomst                          | <input type="checkbox"/> Lidmaatschap van een vakbond            |
| <input type="checkbox"/> Religieuze of levensbeschouwelijke overtuigingen | <input type="checkbox"/> Seksueel gedrag of seksuele gerichtheid |
| <input type="checkbox"/> Genetische gegevens                              | <input type="checkbox"/> Biometrische gegevens                   |
| <input type="checkbox"/> Fysieke en geestelijke gezondheid                | <input type="checkbox"/> BSN / (kopie) ID-bewijs/paspoort        |
| <input type="checkbox"/> Politieke opvattingen                            | <input type="checkbox"/> Niet van toepassing                     |

*Motiveer hier uw antwoord*

## 5. Selecteer de categorieën van Betrokkenen (van de Verstreckende organisatie) van wie u persoonsgegevens zal verwerken.

Geef via het onderstaande vak meer details over categorieën van Betrokkenen (van de Verstreckende organisatie) van wie u persoonsgegevens zal verwerken.

- Opties:*
- |  |   |
|--|---|
| <input type="checkbox"/> Werknemers              | <input type="checkbox"/> Klanten (huidig en potentieel) |
| <input type="checkbox"/> Leerlingen of studenten | <input type="checkbox"/> Patiënten                      |
| <input type="checkbox"/> Minderjarigen           | <input type="checkbox"/> Personen uit kwetsbare groepen |
| <input type="checkbox"/> Anders                  |   |

*Motiveer hier uw antwoord*

---

## 6. Wat is het geschatte aantal Betrokkenen om wie het gaat?

- Opties:*
- |                                  |                                   |
|----------------------------------|-----------------------------------|
| <input type="checkbox"/> 0 - 5   | <input type="checkbox"/> 50 - 75  |
| <input type="checkbox"/> 5 - 25  | <input type="checkbox"/> 75 - 100 |
| <input type="checkbox"/> 25 - 50 | <input type="checkbox"/> 100 +    |

*Motiveer hier uw antwoord*

## 7. Voor welk doel(en) worden deze gegevens door u verwerkt?

Geef hieronder een toelichting op de verwerkingsdoelen.

*Motiveer hier uw antwoord*

---

## 8. Worden de gegevens alleen voor bovenstaande primaire doel(en) gebruikt of vindt er intern of extern nog hergebruik (waaronder analyses, benchmarks e.d.) van de persoonsgegevens plaats?

Geef via het onderstaande vak meer details over de verdere verwerking van de persoonsgegevens door uw organisatie.

*Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

**9. Beschikt u over een (of meer) vastgesteld en geïmplementeerd privacy- en informatiebeveiligingsbeleid en/of -protocol?**

Heeft u het beleid/protocol intern gepubliceerd of gecommuniceerd om ervoor te zorgen dat mensen het beleid/protocol kennen en ernaar handelen? Verstrek een link naar uw beleid of stuur het als bijlage bij dit assessment.

*Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

---

**10. Beschikt u over een certificatie voor privacy en/of informatiebeveiliging of ondergaat u een dergelijk proces?**

Hanteert uw organisatie een standaard informatiebeveiligingsnorm (Baseline Informatiebeveiliging Overheid, NEN 7510, ISO 9001, ISO 17799 of ISO 27000). Zo ja, geef hierover dan een toelichting in het onderstaande vak.

*Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

## 11. Worden (of zijn) er DPIA's (Data Protection Impact Assessments) verricht?

- Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*

---

## 12. Welke technische en organisatorische maatregelen heeft u getroffen ter bescherming van de persoonsgegevens?

Geef hieronder weer welke technische en organisatorische maatregelen u heeft getroffen. Verstrek een link naar een overzicht hiervan of stuur het als bijlage bij dit assessment.

- Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*



**13. Zijn de genomen privacy- en informatiebeveiligingsmaatregelen bijgesteld op basis van incidenten, ontwikkelingen, audits en / of reviews?**

Zo ja, geef hierover dan een toelichting in het onderstaande vak en welke criteria hiervoor gelden.

- Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*

---

**14. Beschikt u over een Functionaris Gegevensbescherming (FG) en/of Privacy Officer (of gelijkwaardige functie)?**

Zo ja, geef dan de volgende gegevens aan in het onderstaande vak:

- Haar/zijn naam
- Contactgegevens (e-mail en telefoonnummer)
- Achtergrond en ervaring
- Plaats binnen de organisatie

- Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*

### 15. Hanteert u een standaard(model) voor verwerkersovereenkomsten of overeenkomsten tussen (gezamenlijk) verwerkingsverantwoordelijken?

Zo ja, geef dan in het onderstaand vak aan welk standaardmodel dit is. Verstrek een link naar de overeenkomst of stuur het als bijlage bij dit assessment.

- Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

---

### 16. In welke landen verwerkt u de persoonsgegevens?

Veilige landen zijn volgens de Europese Commissie landen waarnaar persoonsgegevens kunnen worden overgedragen zonder aanvullende contractuele afspraken. De Europese Commissie heeft tot dusver **Andorra, Argentinië, Canada (commerciële organisaties), Faeröer Eilanden, Guernsey, Israël, Ilse of Man, Japan, Jersey, Nieuw-Zeeland, Zwitserland en Uruguay** erkend als landen met een afdoende privacybescherming.

- Opties:*  EU/EEA  India  
 Verenigde Staten van Amerika  China  
 Verenigd Koninkrijk  Overig

*Motiveer hier uw antwoord*

**17. Indien u persoonsgegevens verwerkt in 'derde landen', welke andere maatregelen treft u momenteel om te zorgen voor een adequate bescherming van gegevensoverdrachten buiten de EU/EER?**

Geef via het onderstaande vak meer details over de melding.

- Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

---

**18. Maakt u gebruik van externe serviceproviders/derde partijen? (bijv. (sub)verwerkers)**

Zo ja, geef in het onderstaande vak dan een overzicht van de betrokken (sub)verwerkers en vermeld hoe u controleert en monitort hoe zij persoonsgegevens behandelen en hoe zij passende technische en organisatorische maatregelen treffen.

- Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

**19. Zijn er adequate afspraken m.b.t. de verwerking van persoonsgegevens gemaakt met uw externe serviceproviders/derde partijen?**

Geef hieronder de bestaande afspraken weer. Indien "niet zeker", gelieve dit verder uit te werken via het onderstaande vak.

- Opties:*  Ja  
 Nee / Niet zeker

*Motiveer hier uw antwoord*

---

**20. Als u gebruikmaakt van niet in de EER gevestigde externe dienstverleners/derde partijen, beschikt u dan over een deugdelijk mechanisme voor gegevensoverdracht?**

Bijvoorbeeld: EU Model Standard Contractual Clauses of Binding Corporates Rules (BCR).

- Opties:*  Ja  
 Nee

*Motiveer hier uw antwoord*

**21. Monitort of controleert u de beveiligingsmaatregelen die worden gebruikt door uw externe serviceproviders/derde partijen?**

Vul in het onderstaande vaak in hoe u toezicht houdt op de beveiligingscontroles van uw externe serviceproviders en derde partijen.

Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*

---

**22. Heeft u een beleid of procedure die de toegang tot persoonlijke gegevens beperkt en hoe controleert u de naleving? (bijv. Access Rights Procedure)**

Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*

**23. Heeft u een overzicht van al uw systemen waarin persoonsgegevens worden verwerkt en de geïmplementeerde beveiligingsmaatregelen?**

Opties:  Ja  
 Nee

*Motiveer hier uw antwoord*

---

**24. Welke bewaartermijnen gelden er bij u dan wel uw externe serviceproviders/derde partijen?**

Hoe worden de gegevens na afloop van die termijn verwijderd? Hoe weet Organisatie dat dit ook daadwerkelijk gebeurt? Vul in het onderstaande vak een toelichting hierop in.

*Motiveer hier uw antwoord*

## 25. Hoe kan een Betrokkene een beroep doen op een recht van de AVG bij uw organisatie?

Wie is uw aanspreekpunt en wat is de procedure (naam aanspreekpunt en procedure kan hieronder of separaat worden bijgevoegd)? Vul in het onderstaande vak een toelichting hierop in.

*Motiveer hier uw antwoord*

---

## 26. Is er een datalekken en -incidentenprotocol?

Mocht u een datalek vaststellen hoe gaat u de Betrokkene dan wel de Organisatie hierover tijdig informeren en wat is hiervoor de procedure (naam coördinator en procedure kan hieronder of separaat worden bijgevoegd)? Vul in het onderstaande vak een toelichting hierop in.

*Motiveer hier uw antwoord*