

## Vragenlijst Nulmeting AVG 2023

### DE ORGANISATIE

<p><b>1. Voor welke organisatie(s) doet u deze nulmeting?</b></p>
<p><b>2. Hoe ziet de structuur van uw organisatie eruit?</b> <i>Maak een onderscheid tussen dochtermaatschappijen en moedermaatschappij in Nederland of elders in de EER (EU en Noorwegen, Liechtenstein en Andorra) en buiten de EER.</i></p>
<p><b>3. Heeft u specifieke verzoeken c.q. aandachtspunten met betrekking tot de privacy compliance, welke hier wordt uitgevoerd?</b></p>
<p><b>4. Heeft u in uw kantoorpand en uw terrein camerabewaking? Zo ja, heeft u dan een camerareglement?</b></p>
<p><b>5. Gebruikt u (s.v.p. aanvinken wat van toepassing is):</b></p> <ul style="list-style-type: none"><li><input type="radio"/> Vingercans</li><li><input type="radio"/> Palmscanners</li><li><input type="radio"/> Gezichtsherkenning</li><li><input type="radio"/> Andere technologieën, welke weerstand kunnen oproepen, namelijk:</li></ul>
<p><b>6. Heeft u een ondernemingsraad of een pvt?</b></p>
<p><b>7. Geldt er specifieke wetgeving voor uw organisatie? Zo ja, welke?</b></p>

## PERSOONSgegevens – ALGEMEEN

<p><b>8. Welke algemene en bijzondere persoonsgegevens worden er bij u verwerkt?</b></p>
<p><b>9. Met welke doelen verwerkt u deze persoonsgegevens?</b></p>
<p><b>10. Van wie zijn deze persoonsgegevens?</b></p>
<p><b>11. Met welke grondslag verwerkt u de persoonsgegevens?</b> U kunt kiezen uit:</p> <ul style="list-style-type: none"><li>○ Vanwege de uitvoering van een wettelijke verplichting;</li><li>○ Vanwege de uitvoering van overeenkomst;</li><li>○ Vanwege een gerechtvaardigd belang;</li><li>○ Vanwege de bescherming van een vitaal belang;</li><li>○ Vanwege de bescherming van een algemeen belang;</li><li>○ Op basis van toestemming van de betrokkene.</li></ul> <p>(Meerdere keuzes mogelijk)</p>
<p><b>12. Op welke wijze geschiedt verstrekking van persoonsgegevens aan u? Via een formulier, digitaal of anders bijv. via een doorverwijzing?</b></p>
<p><b>13. Zijn de gegevens die aan u worden verzonden, versleuteld of op een andere wijze technisch beveiligd verzonden?</b></p>
<p><b>14. Bewaart u de gegevens op een server bij uw ict-leverancier? Of elders? Indien elders, waar vindt in de EER de opslag van deze gegevens plaats?</b></p>
<p><b>15. Heeft u een register met alle verwerkingen van persoonsgegevens? Zo ja, kunt u die toevoegen als bijlage?</b></p>

**16. Heeft u inzicht in de specifieke bewaartermijnen, welke voor uw organisatie c.q. voor de persoonsgegevens welke u verzamelt, gelden?**

## **INTERN BELEID**

**17. Heeft u een beleid betreffende het omgaan met persoonsgegevens en met datalekken? Bijv. in het personeelshandboek of in aparte protocollen?**

**18. Weet u wat te doen in geval van een datalek? Heeft u een draaiboek daarvoor? Zo ja, voegt u deze als bijlage bij?**

**19. Houdt u bij welke datalekken er zijn geweest en welke opvolging u daaraan heeft gegeven? Zo ja, voegt u deze als bijlage bij?**

**20. Heeft u andere stukken waarin de verwerking van persoonsgegevens of het omgaan met persoonsgegevens met uw werknemers, uw cliënten of derden is geregeld?**

**21. Op welke wijze vindt zowel interne als externe registratie van persoonsgegevens van uw personeel plaats?**

**22. Welke werknemers hebben toegang tot de persoonsgegevens?  
*Geef de functiegroepen aan***

**23. Is het noodzakelijk dat de werknemers voor de uitoefening van hun functie toegang hebben tot de persoonsgegevens?**

**24. Zijn uw werknemers zich ervan bewust hoe om te gaan met persoonsgegevens?**

**25. Vallen uw werknemers (en contractors) onder een tuchtrecht en zo ja, welk tuchtrecht?**

**26. Maakt een specifiek geheimhoudingsbeding dan wel een ander beding ten aanzien van het omgaan met persoonsgegevens onderdeel uit van de arbeidsovereenkomst of van het personeelsreglement c.q. de huisregels?**

**27. Zorgt u ervoor dat bij een arbeidsconflict of bij uitdiensttreding werknemers direct geblokkeerd worden van de toegang tot de persoonsgegevens?**

**28. Maakt u gebruik van specifieke, voor uw branche voorgeschreven software? Zo ja, welke?**

Op grond van de AVG dienen organisaties technische en organisatorische maatregelen te treffen bij verwerking van persoonsgegevens.

**29. Welke technische maatregelen treft u (graag per systeem en risico)?**

**30. Welke organisatorische maatregelen heeft u getroffen ter beveiliging van de persoonsgegevens?**

## **EXTERN BELEID**

**31. Welke derden hebben toegang tot uw kantoor?**

**32. Hebben deze derden ook toegang tot uw persoonsgegevens?**

**33. Aan welke derden verstrekt u persoonsgegevens om diensten voor u uit te voeren?**

**34. Heeft u overeenkomsten met deze derden gesloten? Zo ja, met wie en kunt u deze als bijlage(n) toevoegen?**

**35. Zijn er algemene voorwaarden met privacyvoorwaarden van toepassing en zo ja, welke?**

**36. Maakt u gebruik van een privacyverklaring op uw website?**

**37. Van welke cookies maakt u gebruik op uw website?**

*Geef aan of dit noodzakelijke cookies zijn of andere cookies.*

**38. Geeft u betrokkenen de mogelijkheid hun persoonsgegevens in te zien, te rectificeren, te wissen of over te dragen?**

**OVERIG**

**39. Voegt u documenten toe, andere dan reeds genoemde? Zoals (vink aan wat u toevoegt):**

- Arbeidsovereenkomst
- Verwerkersovereenkomst
- Personeelsreglement
- Een Privacy Data Impact Assessment (DPIA)
- Algemene voorwaarden
- Overeenkomst van opdracht
- Huisregels / Personeelshandboek
- Behandelovereenkomst
- Overeenkomsten met derden
- Anders, namelijk: