

Versie: Medewerker in control

Toelichting

We zijn als CBS wettelijk verplicht (zowel vanuit de CBS-wet als de AVG) om gegevens van personen en bedrijven te beschermen. Deze bescherming is essentieel om onze taak als statistisch bureau te kunnen blijven uitvoeren. Als medewerker lever je een belangrijke bijdrage in de bescherming van alle persoons- en bedrijfsgegevens van het CBS. Deze checklist is een hulpmiddel voor jou om te toetsen of je 'in control' bent als het gaat om kennis, procedures en gedragsregels rondom het privacybeleid van het CBS. Heb je vragen of opmerkingen, stel ze dan aan de privacycoördinator van jouw divisie of aan de CPO van het CBS.

Checklist

1. Algemeen

a) Privacybeleid

- Je weet informatie over privacy te vinden op het CBS Intranet.
- Je weet hoe het beleid van toepassing is op jouw eigen werk.

b) Afbakening van rollen en verantwoordelijkheden

- Je bent bekend met rollen van Functionaris Gegevensbescherming (FG), de Chief Privacy Officer (CPO en de Privacy Coördinatoren (PC), en wie dat zijn in de organisatie.
- Je weet wat een verwerkingsverantwoordelijke en wat een verwerker is in de zin van de AVG.

c) Identificatie en classificatie van persoonsgegevens

- Je bent bekend met de begrippen 'persoonsgegevens' en 'bijzondere persoonsgegevens' en weet met welke gegevens je werkt.
- Je weet wanneer een gegeven direct of indirect identificeerbaar is (zowel bij personen als bij bedrijven) en op welk moment er gepseudonimiseerd moet worden.
- Je bent bekend met de Procesbeschrijvingen van de processen waarmee je werkt en de Baselinetoets privacybescherming (of de T-baselinetoets).
- De T-baselinetoets wordt jaarlijks geactualiseerd.
- Je weet wanneer er een Melding Verwerking Persoonsgegevens nodig is (MVP).

d) Risicomanagement:

- Je herkent situaties waarin er sprake kan zijn van een verhoogd privacyrisico, bijvoorbeeld bij het gebruik van nieuwe bronnen, methoden of technieken.
- Je bent bekend met de standaard CBS DPIA en je weet wanneer een aanvullende DPIA nodig is.
- Je bent bekend met de bevindingen uit privacy audits die voor jouw werk relevant zijn.
- Je bent bekend met de adviezen van de Functionaris Gegevensbescherming die voor jouw werk relevant zijn.
- Je meldt een (potentieel) datalek in TOPdesk en aan je leidinggevende.
- Na een datalek in jouw team denk je mee hoe dit in de toekomst voorkomen kan worden.

e) Bewustwording en training medewerkers:

- Je weet welke procedures en regels er gelden voor de gegevens waarmee je werkt.
- Je hebt een cursus/awareness bijeenkomst privacy gevolgd.
- Je weet bij wie je moet zijn voor al je privacyvragen.

2. Minimale gegevensverwerking

- Je vraagt niet méér gegevens op dan je nodig hebt voor je werk. Teveel ontvangen gegevens worden zo snel mogelijk verwijderd.
- Bij nieuwe onderzoeken of processen stel je vooraf de vraag of het doel bereikt kan worden met minder gegevens of minder gevoelige gegevens.
- Autorisaties zijn per proces ingeregeld (dataminimalisatie via beperkte toegang).
- Je past Privacy by Design toe voor dataminimalisatie.

3. Gebruiken, opslaan en verwijderen

- Je bent bekend met de bewaar- en vernietigingstermijnen van je processen.
- Je weet of, en om welke reden je gebruik kan maken van een uitzondering op de bewaar- en vernietigingstermijnen van je processen.

- Je zorgt ervoor dat de bewaar-en vernietigingstermijnen worden nageleefd.
- Je past Privacy by Design toe voor het naleven van de standaard bewaar-en vernietigingstermijnen.

4. Verstrekken

- Je weet dat microdata het CBS niet mogen verlaten. Uitzonderingen zijn vastgelegd in het Veilig Data Delen beleid.
- Je weet dat terugleveren van informatie aan berichtgevers niet is toegestaan, tenzij het noodzakelijk is voor het statistisch proces zelf en dit is vastgelegd.
- Samenwerking met derden is vastgelegd in een contract met de volgende aandachtspunten voor privacy:
 - Indien nodig is er een verwerkersovereenkomst afgesloten;
 - Rollen en verantwoordelijkheden zijn onderscheiden en vastgelegd;
 - Gezamenlijke verwerkingsverantwoordelijkheid is geminimaliseerd;
 - Er is gecheckt of dit onder de standaard CBS DPIA valt. Zo niet, dan is er een aanvullende DPIA gemaakt.

5. Gegevensbeveiliging

- Je bent bekend met het informatiebeveiligingsbeleid van het CBS
- Je bent bekend met de gedragsregels van het CBS.

6. Monitoren en handhaven

- Je weet wanneer je processen moet updaten.
- Je zorgt ervoor dat het beleid wordt nageleefd.