

Versie: Manager in control

Inleiding

We zijn als CBS wettelijk verplicht (zowel vanuit de CBS-wet als de AVG) om gegevens van personen en bedrijven te beschermen. Het gaat hierbij zowel om microdata als gegevens over de werknemers van het CBS. Deze bescherming is essentieel om onze taak als statistisch bureau te kunnen blijven uitvoeren.

Als manager ben je de 'First line of defence'. Je geeft sturing aan, en bent verantwoordelijk voor de verantwoording en opvolging in jouw team/ sector en divisie in de bescherming van de persoons- en bedrijfsgegevens waarmee gewerkt wordt. Deze checklist is een hulpmiddel dat je kan gebruiken ter voorbereiding voor Q-rapportages, directiebeoordelingen en audits. De volgorde en het framework zelf zijn afgeleid van het Privacy control framework van NOREA en volgt dezelfde lijn (en onderwerpen) waarop de externe audit gebaseerd is.

Hoe gebruik je de checklist?

De checklist is een hulpmiddel die concrete vragen stelt per onderwerp. Het is geen uitputtende lijst, dus voeg ook vragen toe die relevant zijn voor jouw team. Ook zullen niet alle vragen of onderwerpen van toepassing zijn voor jouw team. Door te onderzoeken waar de sterke punten van jouw team liggen en waar mogelijkheden tot verbetering zijn en daarop te acteren, ben je als manager 'in control'. Vraag jezelf ook af of je alles ook aan kan tonen. Dat maakt alles concreet en helpt jouw team tijdens audits.

Heb je vragen of opmerkingen, stel ze dan aan de privacycoördinator van de divisie of aan de CPO.

Checklist

1. Algemeen Management

- a) Privacybeleid
 - Ben je bekend met het privacybeleid van het CBS en hoe dat zich vertaalt naar de werkzaamheden binnen jouw team?
 - Hoe zorg je ervoor dat het privacybeleid wordt nageleefd in jouw team?
- b) Afbakening van rollen en verantwoordelijkheden
 - Ben je bekend met de rollen van Functionaris Gegevensbescherming (FG), de Chief Privacy Officer (CPO) en de Privacy Coördinatoren (PC), en wie dat zijn in de organisatie?
 - Weet je wie je op welk moment kan of moet aanhaken?
 - Weet je wat de vereisten zijn als verwerkingsverantwoordelijke en in hoeverre je team samenwerkt met verwerkers en verwerkingsverantwoordelijken buiten het CBS?
- c) Identificatie en classificatie van persoonsgegevens
 - Is in je team duidelijk wat er wordt verstaan onder 'persoonsgegevens' en welke soorten persoonsgegevens er onderscheiden worden in de AVG? (Bijvoorbeeld bijzondere persoonsgegevens, strafrechtgegevens en BSN gegevens)?
 - Is het duidelijk in je team wanneer een gegeven direct of indirect identificeerbaar is (zowel bij personen als bij bedrijven) en op welk moment er gepseudonimiseerd moet worden?
 - Zijn alle Procesbeschrijvingen en de Baselinetoets privacybescherming (of de T-baselinetoets) van de processen waarmee jouw team werkt up-to-date?
 - Is bekend wanneer er een Melding Verwerking Persoonsgegevens nodig is (MVP)?
- d) Risicomanagement:
 - Hoe zorg je ervoor dat jouw team situaties vroegtijdig herkent waarin er sprake kan zijn van een verhoogd privacyrisico? Denk hierbij bijvoorbeeld aan nieuwe bronnen, methoden of technieken.
 - Hoe borg je dat er in een vroeg stadium aandacht besteed wordt aan een DPIA.
 - Hoe worden bevindingen uit de privacy audit die van toepassing zijn voor jouw team opgepakt?
 - Hoe worden adviezen van de FG in jouw team gecommuniceerd en opgevolgd?
 - Hoe gaat je team om met mogelijke datalekken?
- e) Bewustwording en training medewerkers:
 - Op welke wijze heb je de awareness binnen je team verhoogd?
 - Zijn er specifieke privacybeschermende eisen waar jouw team mee te maken heeft? Denk bijvoorbeeld aan het omgaan met bijzondere persoonsgegevens.

- Zijn er specifieke trainingen die je medewerkers hebben gevolgd om met de gegevens waar jouw team mee werkt om te gaan? Dit kunnen ook korte trainingen zijn vanuit het team zelf om bijvoorbeeld nieuwe medewerkers goed privacyvriendelijk te laten werken.
- Maakt je team gebruik van advies en ondersteuning van de PC, de CPO en/of de FG?

2. Minimale gegevensverwerking

- Hoe borg je dat medewerkers in jouw team niet méér gegevens ontvangen en verwerken dan voor het doel nodig is?
- Op welke wijze wordt dataminimalisatie al in een vroeg stadium meegenomen bij een nieuw proces (privacy by design)?
- In hoeverre worden bestaande processen met enige regelmaat opnieuw kritisch bekeken of het met minder gegevens kan?
- In hoeverre worden de autorisaties per proces bijgewerkt?

3. Gebruiken, opslaan en verwijderen

- In hoeverre borg je dat de bewaar- en vernietigingstermijnen in jouw team worden nageleefd?
- Is het duidelijk hoe vaak en om welke reden er afgeweken wordt van de bewaar- en vernietigingstermijnen van de processen in jouw team?
- Privacy by design: in hoeverre wordt er bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk in het ontwerpproces rekening wordt gehouden met privacyprincipes- en risico's?

4. Verstrekken

- Is in jouw team sprake van dataverstrekkingen aan derden? Zo ja, in hoeverre is dat geborgd in het Veilig Data Delen beleid?
- Is er sprake van terugleveren van microdata aan berichtgevers? Hoe is geborgd dat dit alleen gebeurt als het noodzakelijk is voor het statistisch proces zelf?
- Hoe heb je geborgd dat 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 team is bekend met het informatiebeveiligingsbeleid van het CBS
- Hoe wordt de naleving van de gedragsregels van het CBS geborgd?

6. Monitoren en handhaven

- Hoe borg je dat het privacybeleid gehandhaafd wordt?
- Hoe wordt jij op de hoogte gesteld van risico's en ontwikkelingen die voor jouw team relevant zijn op het gebied van privacy? Heb je hiervoor extra hulp nodig van bijvoorbeeld een Privacycoördinator of CPO?