

Checklist management 1

1. Algemeen

a) Privacybeleid

- Ben je bekend met privacy beleid CBS en hoe dat zich vertaalt naar werkzaamheden in jouw team?
- Hoe zorg je dat privacy beleid wordt nageleefd in jouw team?

b) Afbakening van rollen en verantwoordelijkheden

- Ben je bekend met rollen 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 binnen en 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? (bijzondere, strafrechtelijk en BSN).
- 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 Procesbeschrijvingen en T-baselinetoets) binnen jouw team up-to-date.
- Is bekend wanneer er een Melding Verwerking Persoonsgegevens nodig is (MVP).

Checklist management 2

1. Algemeen

d) Risicomanagement:

- Hoe zorg je ervoor dat jouw team situaties vroegtijdig herkent waarin er sprake kan zijn van een verhoogd privacy risico? (nieuwe bronnen, methoden of technieken).
- Hoe borg je dat er in een vroeg stadium aandacht besteedt 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 van 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 en de CPO?

Checklist management 3

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.

Checklist management 4

4. Verstrekken

- Is in jouw team sprake van dataverstrekkingen aan derden? Is dat geborgd in beleid Veilig Data Delen?
- 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;
 - Is gecheckt of dit onder de standaard CBS DPIA valt. Zo niet, aanvullende DPIA maken.

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 privacy beleid 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? Vraag indien nodig extra hulp van Privacycoördinator of CPO.



Privacy borging

Bewustzijn medewerkers



Checklist medewerkers 1

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.

a) 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.

a) 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), en dat die jaarlijks moet worden geactualiseerd.
- Je weet wanneer er een Melding Verwerking Persoonsgegevens nodig is (MVP).



Checklist medewerkers 2

1. Algemeen

e) 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.

f. 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 privacy vragen.



Checklist medewerkers 3

2. Minimale gegevensverwerking (data minimalisatie)

- 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.

Checklist medewerkers 4

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;
 - Is gecheckt of dit onder de standaard CBS DPIA valt. Zo niet, aanvullende DPIA maken.

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.



Gedragsregels

- integer handelen en data vertrouwelijk behandelen
 - vergrendel de computer van een collega als die niet wordt gebruikt
 - verwijder een mail die niet voor jou bedoeld is en meld dit bij de afzender
 - help collega's als ze niet weten hoe ze iets moeten doen
 - gooi onbeheerde prints in de papierversnipperaar, als de eigenaar niet bekend is.
 - spreek collega's aan op correct gedrag werkt beter, of klop aan bij leidinggevende of vertrouwenspersoon
 - berg papieren op in een gesloten lade, locker of kast (thuis en op het werk)
 - werkapparatuur thuislaten op vakantie
 - privégebruik van CBS ICT-voorzieningen beperken en privégegevens (mail en documenten) opslaan in aparte map Privé
 - blijf weg van riskante, malafide of niet toegestane websites vanwege risico's op malware en schending van auteursrechten, voorkom opslag en verspreiding van downloadbestanden en respecteer het intellectueel eigendom
 - toegangspas niet uitlenen
- in beveiligde omgeving werken
 - gebruik stevige wachtwoorden want jij bent verantwoordelijk voor de veiligheid van jouw account
- gebruik zakelijke ICT-voorzieningen en vergrendel altijd jouw computer, laptop, tablet of telefoon als je wegloopt van je (thuis)werkplek
- geen documenten direct of indirect gerelateerd aan CBS beleid of werkzaamheden sturen buiten CBS netwerk om of naar je eigen privé emailadres. Je eigen salarisstroomkjes mag je bijvoorbeeld wel naar jezelf sturen. Check een extern emailadres vooraf en versleutel informatie zo nodig (kan via encrypted mail).
- Volg de CBS instructies m.b.t. apparatuur downloaden waarmee je werkt
- blijf voorzichtig met geanonimiseerde/gepseudonimiseerde/verrind data. Geen microdata naar buiten sturen!
- wat wel en wat niet bewust en onbewust verbaal delen (thuis, op feestjes, werken in trein, etc)
- voorkom meekijken op telefoon, laptop buiten kantoor (bijv. trein). Gebruik een voorzetscherm om meekijken te voorkomen. Af te halen bij de ICT-balie.
- Voorkom verlies van je telefoon, laptop of andere gegevensdrager met werk gerelateerde data
- stuur op dataminimalisatie (beperkte toegang, vernietigen en alleen gebruiken wat nodig)
- beducht zijn voor fishing mails, openbare wifi of andere manieren waarmee onbevoegden oneigenlijk toegang zouden kunnen krijgen tot data
- instructies volgen voor informatiebeveiliging