



aan Erik Bruinsma

van 5.1.2.e

onderwerp Memo terugkoppeling Privacy audit 2022

datum 7 maart 2023

Constateringen privacy audit

De privacy audit loopt van 1 november 2021 tot en met 31 oktober 2022.

Er zijn 7 bevindingen gedaan (zie p.12 – 14 van de rapportage).

- 3 aanbevelingen stonden al op agenda voor de PC en CPO voor het eerste half jaar als actiepunt (het privacybeleid, proces DPIA's en implementatie en evaluatie bewaartermijnen).
- 3 aanbevelingen worden in samenhang met de CISO en CQO opgepakt (risicoanalyses, directiebeoordelingen en het verbeterregister);
- 1 aanbeveling zal door de FG en CPO ingepland worden.
- 2 observaties met aanbevelingen.

7 bevindingen relevante afwijking met aanbeveling

	Norm en Relevante afwijking	Verbeterpunt/ aanbeveling Actie	Planning en actiehouders
PPO01	Het (gedocumenteerde) privacybeleid wordt niet jaarlijks door het management geëvalueerd en goedgekeurd.	Het privacy-beleid dient jaarlijks (aantoonbaar) te worden geëvalueerd. - De CPO en PC zullen het privacy-beleid expliciet vastleggen in een document ter beoordeling DB. Dit beleid zal jaarlijks op de agenda gezet worden ter evaluatie.	CSB –Q2
RMA03	De uitgevoerde 'CBS brede' risicoanalyse voldoet niet aan daaraan te stellen kwaliteitseisen (zie ook het ISO27001 rapport). <u>Deze bevinding is vorig jaar ook gedaan.</u>	De risicoanalyse(methodiek) dient te worden aangepast aan best practices zoals (bijvoorbeeld) de ISO 31000 (Risicomanagement - Principes en richtlijnen). - In overleg met de CISO is besloten aan te sluiten op de risicoanalyse zoals voor de audit ISO 27001 wordt uitgewerkt. Hiervoor zal de CISO het voortouw nemen, naar verwachting is dat einde Q1 afgerond en zal de CPO aansluiten bij hetzelfde framework.	CSB (CIO) Q2 – Q3
RMA05	CBS brengt de beheersmaatregelen in kaart die nodig zijn om privacyrisico's te mitigeren en implementeert deze. De voortgang van de implementatie wordt gevolgd en beoordeeld. - Het opvolgingsproces t.a.v. de bevindingen van de FG is niet duidelijk geformaliseerd .	De bevindingen van de FG dienen procesmatig en procedureel te worden opgevolgd. Hiervoor zou gebruik kunnen worden gemaakt van het proces uit ISO 27001 10.1 ISMS waarin CBS een soortgelijk proces heeft beschreven en voor de tekortkomingen toepast (zie ook REV01). - De CPO zal in overleg met de FG hiervoor het initiatief nemen.	CSB Q2
PIA01	Er is geen vaste, eenduidige procedure rondom de uitvoering, toetsing en goedkeuring van DPIA's.	Een eenduidig proces voor de uitvoering, toetsing en goedkeuring van DPIA's dient te worden ingericht. De richtlijn van de AP (Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een	CSB Q1 – Q2



		<p>Gegevensbeschermingseffectbeoordeling (DPIA) verplicht is: Staatscourant 64418) is wel bekend maar niet verwerkt in een gedocumenteerd proces.</p> <ul style="list-style-type: none"> - Deze actie stond al op de agenda van de CPO en PC. Er zal een procedure DPIA's opgesteld worden, een nieuw sjabloon (op verzoek van SER en DRI) en mogelijk wordt de standaard DPIA weer herzien. 	
DRE01	Het CBS brede beleid t.a.v. bewaartermijnen is niet eenduidig binnen alle directies geïmplementeerd. Binnen de directies bestaan verschillende vormen van 'procedures bewaartermijnen'. Uitzonderingen worden in sommige gevallen wel gedocumenteerd, maar dat is niet gestandaardiseerd. De eenmaal geaccordeerde uitzonderingen (structureel) worden niet (structureel) herbeoordeeld.	<p>Een omspannende, eenduidige en CBS brede procedure bewaartermijnen dient te worden geïmplementeerd binnen alle directies waarbij verplicht wordt gesteld op eensluidende en eenduidige wijze de uitzonderingen t.a.v. de bewaartermijnen vast te leggen en periodiek te herbeoordelen.</p> <ul style="list-style-type: none"> - In 2022 is het beleid geëvalueerd waaruit blijkt dat het beleid generiek is. Dit jaar komt de implementatie en evaluatie aan bod. 	<p>Q2 – Q3</p> <p>Alle directies, coördinatie CSB.</p>
REV01	Gerapporteerde bijzonderheden, afwijkingen e.d. uit zelfevaluatie, interne- en externe audits en interne controles worden niet in alle gevallen uitgezet en/of adequaat opgevolgd.	<p>Een eenduidig proces dient te worden ingericht om bijzonderheden uit zelfevaluatie, interne- en externe audits en interne controles op te volgen. Hiervoor zou gebruik kunnen worden gemaakt van het proces uit ISO 27001 10.1 ISMS waarin CBS een soortgelijk proces heeft beschreven en voor de tekortkomingen toepast (zie ook RMA05).</p> <ul style="list-style-type: none"> - De CPO zal in samenwerking met de CISO en CQO werken aan een verbeterregister. 	<p>Q2 – Q3</p> <p>Alle directies, coördinatie CSB.</p>
MON01, MON02 en MON03	De aansturing van het management ten aanzien van de onderdelen interne beoordelingen, in- en externe auditrapporten bereikt niet in alle gevallen het beoogde effect, nl. de juiste en tijdige opvolging van de bevindingen.	<p>De periodieke beoordeling van de operationele effectiviteit van privacymaatregelen dient te worden verbeterd. Verhoging van de frequentie van de directiebeoordeling en daarbij telkens een terugblik en vaststelling van de stand van zaken zou hierbij kunnen helpen (zie ook RMA05).</p> <ul style="list-style-type: none"> - De CPO zal in samenwerking met de CISO en CQO het framework directiebeoordelingen opstellen. 	<p>Q2 – Q3</p> <p>CSB</p>

2 Observaties met aanbevelingen

	Norm en Relevante afwijking	Verbeterpunt/ aanbeveling Actie	Planning en actiehouders
SCO01	CBS legt vast over welke competenties, met betrekking tot privacy, medewerkers die met persoonsgegevens werken moeten beschikken. De entiteit stelt legt daarnaast vast hoe deze competenties kunnen worden verworven (o.a. door trainingen).	<p>Aan het onderwerp privacy dient meer aandacht te worden gegeven in de e-learning. tevens bevelen wij aan een (meerjaren) bewustzijn programma op te stellen. Tevens bevelen wij aan om alle (niet alleen nieuwe) medewerkers regelmatig een e-learning over privacy te laten volgen.</p> <ul style="list-style-type: none"> - De E-learning IB wordt momenteel herzien en in een gesprek is geconstateerd dat deze vorm niet geschikt is voor alle privacy aspecten. We ontwikkelen momenteel een fysieke bijeenkomst voor nieuwe medewerkers voor een basistraining privacy. Ook 	<p>CSB</p> <p>Q2</p>



		gaan we dit jaar samen met IB de jaarlijkse IB en privacy bewustwordingsenquête uitvoeren. De jaarlijkse bewustwordingsprogramma's worden via de divisies sinds vorig jaar al opgepakt.	
IAM01	<p>Periodiek wordt een overzicht uit de applicatie Varonis gegenereerd ivm aanpassen rechten.</p> <p><u>Observatie:</u> managers/proceseigenaren zijn niet erg tevreden over de aangeleverde controlebestanden, tijdrovend en foutgevoelig doordat de (lange) lijsten door middel van visuele waarnemingen moeten worden onderzocht. Bij één van de directies is men gevraagd om door middel van een query de lijsten 'in te dikken' zodat deze minder werk opleveren en daardoor ook minder foutgevoelig zijn.</p>	<p>Wij adviseren CBS om een proces in te voeren zodat dergelijke initiatieven breed (breder) gedeeld gaan worden in de organisatie. Hierbij merken wij op dat de invoering van de rol privacy-coördinator en het periodieke overleg dat deze functionarissen hebben, hiervoor een geschikt gremium lijkt.</p> <p>Dit staat op de agenda van Informatiebeveiliging. Er zijn 2 acties ingezet:</p> <ul style="list-style-type: none"> - Werkgroep die rapporteert aan IV raad: onderzoek naar mappen- en rechtenstructuur; - CISO: opstellen kader voor integrale aanpak van het Identity & Access management. 	BIM