

aan DT DRI

van 5.1.2.e

onderwerp borging privacy binnen DRI vanuit CBS brede aanpak risicomanagement

datum 21 september 2023

Situatie – waar staan we nu

- De CQO actualiseert het managementsysteem handboek dat de basis vormt voor hoe we binnen het CBS invulling geven aan de normen vanuit ISO9001, ISO27001 en het Norea privacy framework. De directiebeoordeling beoordeelt jaarlijks of het managementsysteem nog afdoende functioneert, zodat het management in control is en compliant met het ISO normen kader (cf. managementsysteem handboek). Risicomanagement is een van de onderwerpen in het normenkader.
- Het risicomanagementproces is binnen het CBS in ontwikkeling. Strategische CBS risico's zijn in beeld en worden periodiek heroverwogen en vanuit Informatiebeveiliging worden IB risico's in kaart gebracht, met behandelplannen om deze te mitigeren. Om in dat proces de PDCA cyclus helemaal rond te maken, moet ook aandacht komen voor de beoordeling van het effect van de maatregelen en moet het beheer van benoemde risico's worden toegevoegd aan het risicomanagementproces (advies IB auditor). Het risicobeheer regelt dat risico's en mitigerende maatregelen periodiek worden heroverwogen, bijgesteld en aangevuld afhankelijk van ontwikkelingen in de context van het CBS. Voor de IB risico's is inmiddels een risicoregister opgesteld.
- Niet voldoen aan de AVG is een cruciaal risico voor het CBS. Het CBS privacy beleid is nu beschikbaar als het formele kader voor hoe het CBS invulling geeft aan de AVG en de CBS wet. Het CBS privacy beleid omvat verschillende onderwerpen, die onder meer worden toegelicht vanuit adviezen van de FG. Bijvoorbeeld m.b.t. privacy by design en dataminimalisatie. Van de hoofddirecties wordt verwacht dat zij een vervolg geven aan het FG advies over dataminimalisatie.
- De CQO, de CPO (en FG) en de CISO werken samen in bovenstaande ontwikkelingen, met ondersteuning van de coördinatoren vanuit de verschillende hoofddirecties. De ambitie is komen tot een uniforme effectieve en efficiënte aanpak die kan worden toegepast binnen de verschillende hoofddirecties.

Vraag

We zijn dus al enige tijd binnen het CBS bezig met maatregelen om risico's te mitigeren. Vooral de privacy borging krijgt veel aandacht omdat we daarin willen excelleren.

Hoe kunnen we vanuit de geschetste situatie goede vervolgstappen zetten, op een uniforme wijze, met in acht neming van het privacy beleid, de FG adviezen (m.n. dataminimalisatie) en wat er al gebeurt of is uitgevoerd aan mitigerende maatregelen? Hoe zouden we dat dan kunnen aanvlagen?

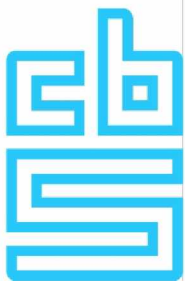
Advies

- Pak het risicomanagementproces zoals dat binnen het CBS vanuit CISO uniform wordt opgezet voor de IB risico's als basis voor een uniform risicomanagementproces op CBS niveau.
- Werk het risicomanagementproces dat voor IB risico's is ontwikkeld verder uit zodat de PDCA cyclus volledig is ingevuld. Houdt daarbij rekening met de verbeterpunten vanuit de IB audits. Naast het



benoemen van risico's, het vorm geven van behandelplannen en afspraken maken over de uitvoering van deze behandelplannen, wordt ook invulling gegeven aan:

- monitoren dat mitigerende maatregelen vanuit het behandelplan worden correct worden doorgevoerd.
 - voor alle risico's in het risicoregister uniform rapporteren over de voortgang in de behandelplannen.
 - vaststellen of mitigerende maatregelen vanuit de behandelplannen het gewenste effect hebben en zo niet bijsturen op de maatregelen (indien mogelijk en wenselijk).
 - periodiek evalueren in hoeverre risico's nog actueel zijn en of de mitigerende maatregelen (vanuit de behandelplannen) nog afdoende zijn of dat deze bijstelling behoeven omdat de context is veranderd.
- Pas het uniforme CBS risicomanagementproces toe op alle CBS risico's. Dat betekent dat de strategische CBS risico's en de privacy borging kunnen worden geïntegreerd in het uniforme risicomanagementproces en daarmee ook in het risicoregister.
 - De strategische CBS risico's, waarvoor behandelplannen worden toegepast en die inmiddels ook al een keer zijn geactualiseerd, kunnen aan het risico register worden toegevoegd.
 - Het privacy beleid en FG adviezen vormen (in termen van het risicomanagementproces) een belangrijk en uitgebreid behandelplan met mitigerende maatregelen. Deze worden binnen de (hoofd)directies verder uitgewerkt en toegepast voor de eigen disciplines. Voortgang in de toepassing van mitigerende maatregelen en monitoren van het effect van maatregelen voor dataminimalisatie en overige zaken zoals die in de privacy agenda worden benoemd lift mee in de uniforme rapportage over de voortgang in de behandelplannen van alle risico's in het risicoregister. Dat geldt dus ook voor de opvolging van FG adviezen m.b.t. Dataminimalisatie.
 - Daar waar voor processen binnen (hoofd)directies nog aanvullende risico's bestaan (bovenop strategische, IB of privacy risico's) kunnen die ook aan het risicoregister worden toegevoegd. Zodat ook die risico's in het uniforme risicomanagement proces kunnen worden meegenomen.
 - alle risico's, behandelplannen en beheeractiviteiten worden vastgelegd en gemonitord vanuit één centraal, volledig en overzichtelijk CBS risico register. Rapportages vanuit de PDCA cyclus binnen het risicomanagementproces kunnen daarmee op verschillende niveaus uniform worden opgeleverd.
- Het verbeterde risicomanagementproces kan door de CQO worden vastgelegd in een volgende update van het managementsysteem handboek. Zodat het ISO9001 kader met een geborgde en volledige PDCA cyclus op het gebied van risicomanagement nog beter is geborgd.
- Vanuit CSB zorgen CQO, CPO en CISO dat de beleidskaders op CBS niveau actueel blijven en de juiste kader bieden voor een optimaal risicomanagement binnen het CBS.



Praktische uitwerking

Risicomanagementproces: Algemeen

Het voorstel betekent concreet binnen de hoofddirecties dat zij binnen hun PDCA cyclus (in het bedrijfsvoeringproces) gaan opnemen dat risico's en maatregelen periodiek dienen te worden geëvalueerd en dat waar relevant aanpassing van risico's en mitigerende maatregelen plaats vindt. Mitigerende maatregelen die al vanuit privacy borging (of andere risico's) zijn ingevuld worden daarin meegenomen. Denk aan Baselinetoetsen, maatregelen rondom bewaartermijnen en autorisaties. Maar dat geldt ook voor opgestelde DPIA's, en voor meer aspecten die vanuit behandelplannen (o.a. privacy beleid en FG adviezen) worden benoemd.

Risicomanagementproces: behandelplan Privacy en Dataminimalisatie

Dataminimalisatie is een van mitigerende maatregelen vanuit de AVG en het CBS privacy beleid. Het CBS heeft een hoog privacy risiconiveau vanwege de grote hoeveelheid gegevens die een grotere kans biedt op identificatie van een individu en vervolgens op een potentieel veelomvattende beeld van dit individu. Dus zijn er veel technische en organisatorische maatregelen nodig om de verwerking van gegevens tot een minimum te beperken, zonder dat dit afbreuk doet aan een goede invulling van de rol van het CBS. Dit vraagt om een bewuste inspanning om elke verwerking van persoonsgegevens zo veel mogelijk te beperken, niet alleen (met terugwerkende kracht) binnen de gestandaardiseerde statistische processen bij het CBS, maar vooral ook bij de inrichting van nieuwe processen/verwerkingen (privacy by design). Het privacy beleid en het FG advies geven de kaders aan en welke dimensies van dataminimalisatie in processen bij het CBS kunnen worden onderscheiden. Dat is bepalend voor de inrichting, uitvoering en evaluatie van het proces (behandelplan) dat stuurt op privacy borging en dataminimalisatie.

In onderstaande tabel staan per dimensie de praktische toepassingen (mitigerende maatregelen):

Dimensie	Minimalisatie bij verzamelen en verwerken van persoons- en bedrijfsgegevens door
Tijd	<ul style="list-style-type: none">• Verkorten leverings- en verwerkingsperiode• Verlagen periodiciteit levering• Beperken toegang in de tijd• Beperken bewaren
Variabelen	<ul style="list-style-type: none">• Alleen variabelen verzamelen/gebruiken nodig voor statistische doel• Minder bijzondere persoonsgegevens verzamelen/gebruiken• Aggregeren, anonimiseren, (effectief) pseudonimiseren van direct identificerende gegevens (waar mogelijk en in die volgorde)• Grootteklassen/categorieën van variabelen gebruiken• Beschikbare variabelen hergebruiken• Statistisch beveiligen van output
Opslag	<ul style="list-style-type: none">• Verminderen aantal rustpuntbestanden/versies• Verwijderen niet-noodzakelijke duplicaten op verschillende locaties• Beperken/uitbannen fysieke verstrekking
Toegang	<ul style="list-style-type: none">• Beperken wie, waar, hoe en hoe lang toegang krijgt tot persoonsgegevens (lees-/wijzigrechten, verdere verwerkingsmogelijkheden)• Compartimenteren toegang gebruikers (van verschillende functiegroepen) in variabelen en records



Dat levert de volgende aanbevelingen m.b.t. dataminimalisatie:

Governance

- Pas beleid en maatregelen, waar relevant, uniform op alle processen toe binnen het CBS en maak dit aantoonbaar met bijvoorbeeld stuurinformatie en/of rapportages.
- Evalueer periodiek, en herzie waar nodig, het beleid voor dataminimalisatie en de implementatie in de processen (procesinrichting), inclusief logging, monitoring van gegevenstoegang (toegangsrechten) en procesbeschrijvingen (inclusief bedrijfsvoering en ondersteuning) en inclusief controle en allocatie van verantwoordelijkheden bij de verstrekking van gegevens binnen en buiten het CBS en via RA.

Door privacy en dataminimalisatie te integreren in het uniforme risicomanagementproces wordt voldaan aan bovenstaande aanbevelingen.

Mitigerende maatregelen

Centralisatie

- Ban het fenomeen van 'schaduwadministraties' (eigen kopieën) van microdatabestanden uit.
- Stimuleer centrale bestanden en voorzieningen als het DSC en maak het eenvoudiger om het dataminimalisatie beleid te handhaven.
- Mitigeer risico's die (juist) voortvloeien uit centralisatie d.m.v. compartimentering en andere technische en organisatorische maatregelen.

Vereenvoudiging

- Automatiseer en beperk het aantal processtappen om menselijke fouten te voorkomen.
- Reduceer verschillende werk omgevingen en geef duidelijke richtlijnen per omgeving.
- Beperk uitzonderingen op staand beleid (softwaregebruik, omgevingsgebruik, BSN-gebruik etc).
- Beperk datatoegangsrechten en evalueer deze periodiek (varonis).

Bovenstaande wordt toegepast met inachtneming van de stand van de techniek, de uitvoeringskosten, aard, omvang, context, het doel van de verwerking en waarschijnlijkheid en ernst van de risico's voor betrokkenen.

Maatregelen binnen DRI (wat gebeurt er al)

Binnen DRI is in 2021 een inventarisatie gemaakt van aandachtspunten en maatregelen rondom privacy borging. O.a. om het beeld te bevestigen dat er binnen de verschillende waarde stromen al van alles speelt, waardoor de meeste medewerkers van DRI awareness hebben ontwikkeld voor privacy borging. Dus niet alleen vanuit de geheimhoudingsverklaring vanuit de eed van belofte. De zaken die daaraan bijdragen zijn uitgelegd in het document "20220214 overzicht issues awareness privacy DRI" (in bijlage 1). Hier zitten ook issues tussen die te maken hebben met dataminimalisatie.

Binnen DVZ worden in afstemming met de statistische afdelingen alleen die gegevens bij de primaire waarneming uitgevraagd die nodig zijn voor het maken van de statistiek. Bij de secundaire waarneming komen meer gegevens binnen dan nodig en is dataminimalisatie de verantwoordelijkheid van de statistiekafdeling waar de data direct naar worden doorgezet. In de toekomst is het streven dat al in de



rustpuntbestanden vanuit de secundaire waarneming wordt opgeschoond. Verder is het gehele proces van dataverzameling binnen Phoenix ingericht op dataminimalisatie, zowel wat betreft procesinrichting (baselinetoetsen), voor autorisaties als voor bewaartermijnen (inclusief geautomatiseerde vernietiging). En vanuit functioneel beheer wordt gestuurd op jaarlijkse pentesten. Dit is verder toegelicht in bijlage 1 en 2 van het document "20211130 Uitwerking privacy issues binnen DRI".

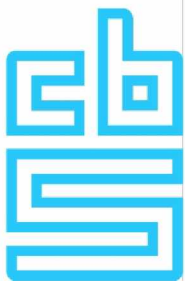
Binnen beleidsstatistiek en dataservices (RA) is veel aandacht voor privacybescherming en informatiebeveiliging en wordt invulling gegeven aan de aanbevelingen vanuit de commissie van de Berg, die specifiek onderzoek heeft gedaan naar de privacy borging en dataminimalisatie. Men werkt zo veel mogelijk in een SEC-omgeving waarbij data zijn verrind. Ook legt men contractueel vast wanneer data van externen wordt vernietigd en hoe met data wordt omgegaan. Voor het project 'kwaliteit stelsel basisregistraties' waarbij BSN tot op het laatst bewaard moet blijven, is een aparte werkomgeving ingericht waarvoor alleen specifieke projectmedewerkers rechten hebben. Aanvullende beheersmaatregelen, ook op het gebied van dataminimalisatie zijn toegelicht in bijlage 4 van het document "20211130 Uitwerking privacy issues binnen DRI". Het op een begrijpbare manier aan buitenstaanders (het publiek) uitleggen wat het beleid is van het CBS m.b.t. privacy en welke maatregelen m.n. vanuit dataservices worden genomen om gegevens te beschermen, is een belangrijk verbeterpunt.

Vanuit methodologie en procesontwikkeling draagt DRI bij aan innovatie binnen het CBS. DRD ziet daarbij ook toe dat vernieuwingen geen of minimale privacy risico's met zich mee brengen (privacy by Design), o.a. door te sturen op dataminimalisatie. DRD werkt in projectverband of voor een adviesopdracht met versleutelde (verrind) microdatasets. DRD streeft naar zo min mogelijk datasets in de eigen (tijdelijke) mappen van de afgeschermd SEC-omgeving, en maakt zo veel mogelijk gebruik van de data in de mappen die bij de statistische afdeling beschikbaar zijn. Slim combineren van microbestanden kan toch tot situaties leiden waarbij privacy in het geding komt. Maar dergelijke informatie is begrensd beschikbaar binnen het project bij een beperkte groep medewerkers, die zich bewust is van privacybescherming. DRD werkt inhoudelijk veel samen met universiteiten. Daar zijn veel PhD's of studenten bij betrokken. Die doorlopen vanuit een bijzondere constructie dezelfde aanstellingsprocedure als vaste CBS medewerkers binnen DRD, inclusief de toezegging om zorgvuldig om te gaan met informatie. Bij de samenwerking met hoogleraren is de awareness en privacy borging afgedekt via het samenwerkingscontract met de universiteit. Opschoning van de (rechten op) mappen en accounts op de SEC-omgeving is een aandachtspunt. Daarbij speelt ook dat vanuit methodologisch oogpunt lange tijdreeksen juist cruciaal zijn voor het onderzoeken van ontwikkelingen, maar ook om over langere periodes cijfermatige inzichten te kunnen opleveren. Aanvullende beheersmaatregelen, ook op het gebied van dataminimalisatie zijn toegelicht in bijlage 3 van 20211130 Uitwerking privacy issues binnen DRI.docx.

In bovenstaande komen de benoemde dimensies van dataminimalisatie allemaal aan bod. In aanvulling hierop is vanaf 2022 vanuit verschillende initiatieven meer aandacht voor veilig data delen. Dat geldt ook voor vernietiging van gegevens, door periodiek actief en collectief vanuit opruimdagen of –weken per waarde stroom invulling te geven aan vernietiging van overbodige bestanden.

Vervolgaanpak binnen DRI

Als onderdeel van het risicomanagement proces dienen risico's en mitigerende maatregelen vanuit elke waarde stroom te worden beheerd en is het zaak periodiek te evalueren wat de status is. Dat vereist voldoende awareness voor de uitvoering en toegevoegde waarde van het risicomanagementproces. Ook



m.b.t. privacy borging en dataminimalisatie. Vanuit het risicomanagementproces wordt periodiek gekeken of dataminimalisatie voldoende is afgedekt of dat er nog verbeterpunten kunnen worden opgepakt. Enkele zijn reeds hiervoor benoemd. Zoals te veel data beschikbaar via bronbestanden, nog beter afschermen van projecten, opschoning van (rechten op) projecten, het beperken van de verstrekking van variabelen vanuit RA, het goed verwoorden van hoe het CBS de privacy borgt vanuit dataservices, betere registratie van vernietiging en het volledig uitsluiten van gegevensuitwisseling via email.

Binnen het uniforme risicomanagementproces is in onderstaande tabel een voorstel uitgewerkt voor een geborgde invulling van mitigerende maatregelen voor dataminimalisatie.

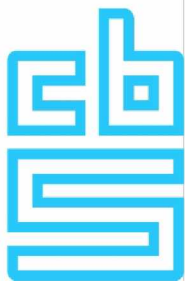
	Voorstel	Planning	Actiehouder
1	<i>Beoordeel jaarlijks per waarde stroom de uitvoering en de stand van zaken ten aanzien van dataminimalisatie en formuleer op basis hiervan verbetervoorstellen (als onderdeel van het risicomanagementproces)</i>	<i>Jaarlijks in april</i>	<i>Directeuren ondersteuning van Privacy coördinator (PC)</i>
2	<i>Terugdringen dubbele bestanden ('schaduwadministraties'), ook meenemen in de communicatie t.b.v. de opruimweek</i>	<i>Continu</i>	<i>Teammanagers</i>
3	<i>Nakomen van afspraken vanuit Veilig Data Delen</i>	<i>Continu</i>	<i>Teammanagers</i>
4	<i>Herbeoordeling van de inhoud van ontvangen data en intern verstrekte data (niet meer data ontvangen/geleverd dan nodig?)</i>	<i>Continu</i>	<i>Teammanagers</i>
5	<i>Uitwerken voorstel (en implementeren hiervan) van CBS-brede aanpak voor registratie van uitzondering op bewaartermijnen (is ook bevinding uit de externe privacy audit 2022)</i>	<i>Q1 2024</i>	<i>CPO met PC's divisies</i>

Excel "Dataminimalisatie in beeld" kan per waarde stroom worden afgevinkt om stand van zaken rondom dataminimalisatie per waarde stroom in beeld te brengen.



Bijlage 1:

Privacy binnen DRI			awareness en ontwikkelingen	
			DRI geeft voorkeur aan ontwikkeling van privacy awareness vanuit de verschillende initiatieven die in dit overzicht zijn benoemd. Veel medewerkers van DRI zijn direct of indirect betrokken bij deze initiatieven, hetgeen bijdraagt aan de ontwikkeling van de privacy awareness. Aanvullende sessies in sectoren en/of teams kosten tijd, die DRI dan liever in de voortgang van de benoemde trajecten investeert. Daarnaast worden medewerkers verwezen naar centraal beschikbare informatie (intranet of e-learning) over waar men zoal op moet letten indien men buiten kantoor werkt (thuis of in de trein of elders, o.a. procedure verlies toegangspas), indien men op kantoor werkzaam is, bij de inrichting en uitvoering van processen (o.a. datalek procedure) en indien men bezig is met nieuwe ontwikkelingen en innovatie. (nog verder uit te werken vanuit PC overleg, of via factsheets ipv hier benoemde 4 indeling).	
Nr	Onderwerp	Trigger	Toelichting	Bijdrage aan
0	Privacy audit 2021	Interne en externe audits	DRI	processen voldoende afschermen tegen misbruik van data
1	Geheimhoudingsclausule	arbeidscontract	DRI	voorkomen van misbruik van informatie
2	Privacy audit 2022	Interne en externe audits	DRI	processen voldoende afschermen tegen misbruik van data
3	T baseline toets	ISO 27001 audit	DRI	inzicht in privacy risico's per proces
4	Actualisatie autorisaties	ISO 27001 audit	DRI	toegangsrechten periodiek bijstellen
5	Actualisatie autorisaties	Varonis	DRI	toegangsrechten periodiek bijstellen
6	Nakomen bewaartermijnen - CBS breed proces via proces verbalen	ISO 27001 audit - Phoenix	DRI	toetsen op toepassing van bewaartermijnen
6a	Bewaartermijnen en archivering (primaire waarneming)	Phoenix (bewaartermijnen en vernietigen binnen teams)	DVZ	beleid rondom vernietiging van data binnen data verzamelen
6b	Bewaartermijnen en archivering (secundaire waarneming)	Phoenix (bewaartermijnen en vernietigen binnen teams)	DVZ	beleid rondom vernietiging van data bij secundaire bronnen
7	Automatisering nakomen bewaartermijnen	Phoenix (geautomatiseerd vernietigen)	DVZ	geautomatiseerd opruimen van bestanden
8	BSN toegang	actiepunt DB	DRI	minimaliseren van gebruik van BSN
9	CBS procesmonitor 2.0 inclusief privacygevoeligheid niet- primaire processen	werkgroep	DRI	inzicht in processen met P-gegevens
9a	Awareness sessie management	DG/CPO		awareness
10	Overzicht verwerkersovereenkomsten	ISO27001 audit	DRI	inzicht in verwerkersovereenkomsten
11	Veilig Data delen (Remote Access)	taak DBD	DBD	beveiligd beschikbaar stellen van data
12	Privacy Preserving Technieken	Methodologie DRD	DRD	beveiligd beschikbaar stellen van data
13	Dataminimalisatie secundaire bronnen	ABC (Bronnencatalogus)	DVZ/DRD	minimaliseren van benodigde data
14	Dataminimalisatie structureel beter borgen	DB	DRI	dataminimalisatie in de genen
15	Toekomst telefoonnummers CATI	AP standpunt	DVZ	alleen benaderinformatie die voldoet aan proportionaliteit en subsidiariteit
16	PIA W2C tooling interviewers	Nieuwe tooling	DVZ	DPIA proces geautomatiseerde verwerking verreden kms bij interviewer
17	Onderscheidende achtergrondkenmerken	Aandachtspunt DVZ	DVZ	DPIA (indien niet afgedekt door CBS PIA) proces doelgroep benadering
18	Binnenhalen van waarnemgegevens (beveiligde up en downloadportals)	Taak DVZ	DVZ	beveiligd delen van data - minimaliseren van processen, werkomgevingen en rustpunten
19	Waarneming via CATI en CAPI	Taak DVZ	DVZ	voorkomen van misbruik van informatie via procedures/instructies/opleiding
20	WOB verzoeken	aanvraag WOB	DRI	
21	Beleid onthullingsgevaar statistische informatie (Via CMO)	DB	DRI	beveiliging van statistische informatie binnen (werk)omgevingen
22	Inlogbeleid vragenlijsten - wachtwoord beleid respondenten	Taak DVZ	DVZ	(werk)omgevingen via eenduidige richtlijnen beveiligd - actueel dataminimalisatiebeleid - in control op dataminimalisatie
23	Privacy vanuit methodologisch kader (rol DRD)	Taak DRD	DRD	actueel en in control op dataminimalisatie
24	Werken binnen afgesloten "SEC-omgeving"	Taak DRD	DRD	toegang tot data beperken
25	Bestandsverwerking Beleidsstatistieken	Taak DBD	DBD	toegang tot en beschikbaarheid van data beperken



Privacy binnen DRI		awareness en ontwikkelingen			
		DRI geeft voorkeur aan ontwikkeling van privacy awareness vanuit de verschillende initiatieven die in dit overzicht zijn benoemd. Veel medewerkers van DRI zijn direct of indirect betrokken bij deze initiatieven, hetgeen bijraagt aan de ontwikkeling van de privacy awareness. Aanvullende sessies in sectoren en/of teams kost en tijd, die DRI dan liever in de voortgang van de benoemde traject en investeert. Daarnaast worden medewerkers verwezen naar centraal beschikbare informatie (intranet of e-leranings) over waar men zoal op moet letten indien men buiten kantoor werkt (thuis of in de trein of elders, o.a. procedure verlies toegangspas), indien men op kantoor werkzaam is, bij de inrichting en uitvoering van processen (o.a. datalek procedure) en indien men bezig is met nieuwe ontwikkelingen en innovatie, (nog verder uit te werken vanuit PC overleg, of via factsheets ipv hier benoemde 4 indeling).			
Nr	Onderwerp	Trigger	Toelichting	Bijdrage aan	
26	Kwaliteit stelsel basisregistraties	taak DBD	DBD	werkomgeving vanuit eenduidige richtlijnen beveiligd - uitzondering op staand beleid	
27	Privacy risico gegevens PhDs en studenten	HR taak DRD	DRD	toegang tot data beperken - voorkomen misbruik van data	
27a	Privacy in Webinar	DG/CPO	Awareness via voortgang in bepaalde privacy initiatieven.	awareness	
28	Omgang met onverrind data binnen DBD	Taak DBD	DBD	werkomgeving vanuit eenduidige richtlijnen beveiligd - uitzondering op staand beleid	
29	Vergroten van awareness (1)	Initiatief DB naar HDs	DRI		
30	Vergroten van awareness (2)	Initiatief CPO/PC werkgroep	DRI	awareness - praktische invulling	
31	Advies uitwerking persoonsgegevens	FG	DRI	awareness - theoretische onderbouwing	
32	Advies Samenwerkingsverbanden	FG	DRI	verantwoordelijkheden voor privacy borging	
33	Advies DPIA (Data Protection Impact Assessment)	FG	DRI	theoretische onderbouwing en praktische invulling	
	AVG gadget - datablockers	CPO	DRI		
34	Advies Dataminimalisatie	FG	DRI	dataminimalisatie in de genen	
35	DPIA Physical Activity pilot (Activity trackers = pre-pilot bewegsmeters) (3-2023)	DRD- DVZ (uitwerking - 5.1.2.e)	DRI		
36	DPIA 5.1.2.f (11-2022)	DRD-extern (uitwerking - A. Mitraeva)			
37	PDIA ODIN (11-2022)	DVZ - (afgerond A. Buis)			
38	DPIA OSSC (4-2023)	DRD-extern (uitwerking - 5.1.2.e Oirschot)			
39	DPIA SAVE-HEM (okt 2022)	DRD-extern			
40	DPIA seks onder 25e	SER(-DVZ)-extern (uitwerking 5.1.2.e)			
41	DPIA Smart Perceptions (SSI perceptions)	DRD (uitwerking B. 5.1.2.e)			
42	DPIA Userlab (mei 2022)	DRD (uitwerking D. Giessen)			
43	PDIA uploaden slimme meters	DRD (uitwerking M. Kompier - stopgezet)			