



aan CPO
van Staf DRI

onderwerp Privacy Governance DRI
datum 23 juni 2022

DRI is recentelijk ontstaan door het samenvoegen van Dataverzamelen (DVZ), Beleidsstatistieken en Data services (DBD) en Research en Development (DRD).

Dit betreft 4 verschillende disciplines met eigen specifieke kenmerken. Dat heeft zijn weerslag op hoe wordt omgegaan met privacy en daarmee ook op de privacy governance.

Op hoofdlijnen sturen de teamhoofden op afdoende privacy borging binnen de processen waar zij verantwoordelijk voor zijn. Het lijnmanagement van DRI pakt die verantwoordelijkheid op. Voor advies en ondersteuning kan men terecht bij de privacy coördinator binnen de centrale Staf van DRI. Binnen DRI is privacy borging opgenomen in het raamwerk kwaliteitszorg, waarmee ISO9001 en ISO27001 aspecten zijn belegd.

Binnen de centrale Staf zijn de functies van PC en kwaliteitscoördinator ondergebracht bij één beleidsadviseur, die daarnaast nog enkele andere portefeuilles heeft binnen de bedrijfsvoering. Deze beleidsadviseur adviseert en ondersteunt bij de uitwerking van kwaliteitszorg en privacy borging binnen DRI. Dat is inclusief de voorbereiding en afstemming van audits, o.a. met CAD.

Binnen **DVZ (1)** is de procescoördinator betrokken bij kwaliteitszorgzaken (incl privacy borging), vooral op het gebied van procesborging en daaraan gekoppeld T baselinetoetsen, bewaartermijnen en autorisatieprocedures. Daarnaast is binnen het Phoenixproject aandacht besteed aan privacybeschermende maatregelen. Dat betekent dat het waarneemsysteem, naast de juiste attitude bij medewerkers, een belangrijke ondersteuning biedt bij het voorkomen van datalekken. Dit is uitgewerkt in documenten hoe DVZ op basis van de AVG stuurt op privacy borging. De team managers (proceseigenaren) sturen op de juiste toepassing hiervan.

Binnen **DBD Beleidsstatistiek (2)** heeft één van de 3 teammanagers privacy borging in portefeuille (één proces dat door 3 teams wordt toegepast) en ziet met ondersteuning van een medewerker toe op voldoende borging van privacy en dat de Pls van de specifieke projecten binnen Beleidsstatistieken hier voldoende aandacht aan geven.

Voor **Dataservices (3)** binnen DBD is het proces van het delen van microdata zowel met externe onderzoekers (microdata services) als met interne onderzoekers (DSC) zeer strikt afgeschermd. Instructies, werkwijzen en systemen zijn nauwgezet ingericht op het voorkomen van datalekken of misbruik. Daartoe zijn specifieke technische processen ingericht. Vanwege die gevoeligheid zijn aanvullende audits geweest om dit proces maximaal te borgen. Doorlopend wordt bekeken of de beveiliging verder kan worden aangescherpt op basis van nieuwe technieken en nieuwe inzichten. Daarvoor werkt DRI nauw samen met BIT, CSB-J en SES (SSB). Dat toont aan dat het lijnmanagement hier uitdrukkelijk verantwoordelijkheid neemt voor privacy borging.



Binnen **DRD (4)** werken de methodologen en procesontwikkelaars die binnen ontwikkeltrajecten in de gehele CBS organisatie (vanuit privacy by design) toe moeten zien op privacy borging. Dat gebeurt vanuit Privacy Preserving Technieken, dataminimalisatie en afscherming van gegevens via beperkte toegang en het beperkt bewaren van gegevens. De DRD medewerkers werken in een eigen afgeschermd omgeving of maken gebruik van werkomgevingen van statistiekafdelingen, waar de statistiekafdeling zelf verantwoordelijk is voor de privacy borging. Voor innovatieve onderzoeksprojecten maakt DRD soms wel gebruik van echte data met persoonsgegevens, maar dat gebeurt dan in de afgeschermd werkomgeving. Daar waar dat aan de orde is, wordt dat bijgehouden in een inventarisatielijst. DRD beschikt over een eigen AVG document van waaruit noodzakelijke acties worden uitgezet en dat als kader dient voor privacy borging door DRD medewerkers. DRD management wijst medewerkers hier periodiek op.

Voor meer details over specifieke zaken die spelen rondom privacy borging binnen DRI wordt verwezen naar het document met een inventarisatie van privacy issues binnen DRI, dat eind 2021 is opgesteld.

Aandacht geven aan privacy awareness borgt binnen de organisatie dat persoonsgegevens zodanig worden afgeschermd en geminimaliseerd, dat deze niet in het bezit komen van anderen die daar misbruik van kunnen maken. De hierboven beschreven governance en de inventarisatie van wat er al speelt rondom privacy borging binnen DRI, maakt duidelijk dat in alle benoemde disciplines privacy de noodzakelijke aandacht krijgt. DRI heeft een pragmatische keuze gemaakt om, gezien hoge werkdruk door andere innovaties boven op het reguliere werk, geen aanvullende awareness sessie te doen.

Op het moment dat vanuit de centrale privacy sturing informatie beschikbaar komt, o.a. via Intranet, over privacy borging zal hier vanuit DRI extra aandacht aan worden besteed. Met name aan de hand van fact-sheets die beschikbaar komen worden medewerkers gewezen op een juiste attitude bij meer facetten van privacy borging, zoals waar je op moet letten bij thuis werken, of elders buiten kantoor, waar je op moet letten bij contractuele afspraken met externe partijen, enz.