Vragen en opwaardering m.b.t. SB Jaarrapportage 2022 - Functionaris Gegevensbescherming

Fractie	#	Vraag/input	Antwoord/reactie
D66	1	Opwaardeerverzoek: De maatregelen die door het college worden benoemd gaan niet 1-op-1 in op de door de FG genoemde onderdelen die nu lager dan een 2 op volwassenheid scoren. Graag ga ik het met college en de staten het debat aan over wat er voor nodig is om deze volwassenheid op deze punten (Geen gestructureerd risicomanagement, Informatiebeveiliging niet op het gewenste niveau en Geen gestructureerd intern toezicht) wel te behalen.	Zoals blijkt uit de Managementreactie op de jaarrapportage van de FG onderschrijft het CMT dat de organisatie nog niet voor alle onderdelen op het gewenste volwassenheidsniveau zit. Teneinde dit volwassenheidsniveau wel te behalen zijn er diverse acties uitgezet. Belangrijk zijn daarbij de verdere professionalisering van het risicomanagement, en de doorontwikkeling van de Baseline Informatiebeveiliging Overheid (BIO) waarvan hieronder een aantal concrete acties; Risicomanagement Privacy: - Door het CMT is besloten om voor de kolom Informatievoorziening over te gaan naar een nieuwe Governance. Hiertoe zijn drie gremia ingericht: 'IV-Raad', 'Portfolioboard' en het 'Voortbrengingsoverleg'. Het doel is om alle nieuwe initiatieven die raakvlakken hebben met informatievoorziening langs het voortbrengingsoverleg en de portfolioboard gaan en dus ook allemaal getoetst worden op Informatieveiligheid en privacy. Deze gremia zijn nu in de opstartfase. - Verder worden er, om privacy risico's bij nieuwe projecten of processen te inventariseren, Data Protection Impact Assessments (DPIA's) uitgevoerd. Inmiddels zijn er ruim 19 DPIA's uitgevoerd. Er is dus al sprake van een bepaalde mate van risicomanagement. Echter, om dit structureel te maken, is het noodzakelijk de uitgevoerde DPIA's periodiek te evalueren om zo te beoordelen of de geconstateerde risico's zijn veranderd. Dit jaar is een eerste start gemaakt met die evaluaties Risicomanagement voor informatieveiligheid Voor 2023 staan de volgende activiteiten gepland om invulling te geven aan IV-risicomanagement: • Beschrijven, vaststellen en implementeren van de aanpak voor risicomanagement, inclusief criteria voor het uitvoeren van risicoanalyses en acceptatiecriteria. • Selecteren van processen en/of applicaties waarvoor risicoanalyse moeten worden uitgevoerd (kroonjuwelen).

			• Uitvoeren van risico assessments voor de geselecteerde processen en/of applicaties. • Beleggen van eigenaarschap voor IV-risico's en uitvoeren van risicobehandeling. • Inrichten van een applicatie voor de provincie Utrecht voor de registratie van IV-risico's, maateregelen en statusinformatie. • Opzetten van monitoring en sturing ten aanzien van risicobeheersing. • Aansluiting op nieuwe processen, applicaties en grote wijzigingen in bestaande processen en applicaties (Security by Design). <u>Implementatie van de BIO (Baseline Informatiebeveiliging Overheid)</u> In 2023 ligt de focus op verdere implementatie van de BIO binnen de provincie. Middels een BIO Self-assessment is de BIO volwassenheid van de organisatie bepaald. Voor 2023 ligt de focus op de BIO-onderdelen waarvoor nog niet het minimale volwassenheidsniveau van 2.0 is bereikt. Het gaat om de volgende onderdelen: • Herijking van het Informatiebeveiligingsbeleid. In 2023 vindt een volledige herijking van het informatiebeveiligingsbeleid plaats. Een belangrijk aandachtspunten hierbij is de governance. • Incident Management (het beheersen van informatiebeveiligingsincidenten – o.a. oplossen, evalueren, verbeteren) • Toegangsbeveiliging (Logisch) (Het beheersen van de toegang tot informatie, IT-voorzieningen en bedrijfsprocessen op grond van bedrijfsbehoeften en beveiligingseisen) • Ontwikkelprocessen, testgegevens en te ontwikkelen informatiesystemen (informatieveiligheid bij ontwikkeling, acquisitie, uitbesteding etc. en testen van systemen/applicaties e.d.) • Leveranciers (informatieveiligheid in leveranciersrelaties) • Beheer van de operationele systemen (informatiebeveiliging bij het beheren van systemen) • Netwerk en informatietransport (informatiebeveiliging bij het

			verzenden/ontvangen e.d. van informatie) • Cryptografie (het versleutelen van informatie) • Inrichten van beoordelen en auditen van de informatiebeveiliging (audits, evalueren, naleving etc.) Het doel voor 2023 is om in eerste instantie voor de bovenstaande BIO-onderdelen volwassenheidsniveau 2 te halen. Vervolgens is het streven om voor de meest essentiële BIO-onderdelen volwassenheidsniveau 3 te halen. Een volwassenheidsniveau 3 is nodig om aan de BIO te voldoen. Bij de keuze voor het oppakken van onderdelen wordt behalve de score voor volwassenheid ook gekeken naar de weging van de verschillende onderdelen binnen het BIO Self-assessment. <u>Geen gestructureerd intern Toezicht:</u> Sinds de invoering van de Algemene Verordening Gegevensbescherming (AVG) is er door de provincie hard gewerkt om naleving van de AVG zo goed mogelijk te borgen in de organisatie. Hiervoor is onder meer beleid opgesteld, zijn procesbeschrijvingen opgesteld, modelcontracten gemaakt en is een verwerkingsregister opgesteld. Los van de controle die Functionaris Gegevensbescherming als toezichthouder uitvoert, is het noodzakelijk om intern bepaalde kwaliteitscontroles uit te voeren ten aanzien van de gemaakte afspraken. Op dit moment zijn die kwaliteitscontroles er nog niet. Er wordt gewerkt aan een Interne Toezichtsplannen, voor zowel Privacy als Infotmatieveiligheid waarin een dergelijke kwaliteitscontroles verder worden uitgewerkt.
SGP	2	<u>Opwaardeerverzoek</u>: De privacy volwassenheid beweegt zich langzaam richting het door de organisatie gewenste niveau van 3. Waarbij de belangrijke kanttekening wordt gemaakt, dat de laatste stapjes weerbarstig te zijn. Verder wordt aangegeven dat de ontwikkelingen in de techniek onverminderd snel gaan. Daarom zouden we graag met GS in gesprek gaan hoe zij ervoor gaan zorgen dat we in de toekomst gaan voldoen aan de wet- en regelgeving op dit terrein met daarbij de aantekening dat we nu nog niet op ons eigen gewenste niveau zitten.	

GroenLinks	3	Dank voor de heldere jaarrapportage 2022 van de Functionaris gegevens bescherming. GroenLinks constateerde In de zomernota is een reeks van aanvullingen op investeringen in/ aanbesteding van nieuwe digitale systemen. Daarnaast vindt GroenLinks de volgende 2 punten in de jaarrapportage 2022 van de Functionaris gegevensbescherming van belang: het nog te nemen besluit over waar/hoe de (eind)verantwoordelijkheid voor de informatievoorziening in de organisatie wordt belegd. het verbeteren van de 'gevoeligheid' voor informatieveiligheid en privacy in het totale personeelsbestand. Met het oog op deze punten heeft GroenLinks de volgende vragen. Hoe worden PS meegenomen in de ontwikkelingen in de provinciale organisatie op gebied van informatievoorziening, informatieveiligheid en privacy ?	Op dit moment worden PS door middel van de jaarrapportage van de FG jaarlijks geïnformeerd over de stand van zaken met betrekking tot de privacyvolwassenheid in de organisatie. Voor wat betreft informatiebeveiliging wordt PS periodiek over de staat van informatiebeveiliging naar aanleiding van uitgevoerde onderzoeken zoals het onderzoek dat dit najaar door CCO wordt uitgevoerd naar de implementatie van normen voortvloeiend uit de nieuwe Europese Richtijn inzake NIS2 (NetwerkInformatieSysteem. Hierover kunnen de Staten 1e kwartaal 2024 worden geïnformeerd. Verder wordt op deze onderwerpen ook verslag gedaan in de jaarrekening. De ontwikkelingen op het gebied van informatievoorziening (in brede zin) hebben hier een samenhang mee, maar staan ook deels op zichzelf. Onlangs is het nieuwe interne programma Informatievoorziening op Orde gestart. Hierover zullen PS separaat geïnformeerd worden.
	4	Informatieveiligheid en privacy zijn ook elementen van het Statenwerk. Hoe wordt daaraan aandacht geschonken en waar/hoe is dat belegd?	Bij besluit van 14 april 2021 is door Provinciale Staten besloten om voor de PS werkzaamheden aan te sluiten bij de uitgangspunten van het privacybeleid 2021 - 2025, zoals dat door GS is vastgesteld. PS heeft daarmee besloten geen eigen privacybeleid op te stellen, maar heeft wel aantoonbaar uitgangspunten vastgesteld voor de uitvoering van de eigen werkzaamheden in lijn met de AVG. In dit besluit is opgenomen dat met de griffie zal worden afgestemd hoe het bijpraten van de statenleden over de verplichtingen die voortvloeien uit de AVG en relevant zijn voor hun dagelijkse werkzaamheden vorm krijgt. Uiteraard zijn de onze functionarissen voor de informatieveiligheid en privacy graag bereid om, in afstemming met de griffie, een kennissessie te verzorgen voor Statenleden. Verder zijn de processen van de griffie getoetst aan de regels voor informatieveiligheid (BIO), privacy (AVG) en archivering (Archiefwet). Daarnaast zijn deze verwerkingen ook opgenomen in het verwerkingsregister en worden mogelijke datalekken van de Griffie ook opgenomen in het datalekregister van de Provincie Utrecht..