

**College van Gedeputeerde Staten
statenbrief**

Aan Provinciale Staten

DATUM	16-2-2021	NUMMER PS	Voegt de griffie toe
DOMEIN	BDV	COMMISSIE	BEM
STELLER	Remco ter Heijne	TELEFOONNUMMER	06 5326 5024
DOCUMENTUM NUMMER	821F4A3D	PORTEFEUILLEHOUDER	Strijk

Onderwerp Statenbrief:

Voortgang Programma Informatieveiligheid en Privacy (IV&P), tweede helft 2020

Voorgestelde behandeling:

Ter informatie

Geachte dames en heren,

Essentie / samenvatting

Met deze Statenbrief informeren wij u over de ontwikkelingen en vorderingen van het programma Informatieveiligheid en Privacy (IV&P) gedurende de tweede helft van 2020.

In de tweede helft van 2020 is vooruitgang zichtbaar, met name op het vlak van de AVG en de bewustwording in de organisatie. Het is helaas niet gelukt om op alle onderdelen van informatieveiligheid & privacy voortgang te boeken of te versnellen. Dit is te verklaren doordat door Corona de prioriteiten in de organisatie tijdelijk naar de continuïteit van de bedrijfsvoering werden verlegd en door de krapte op de arbeidsmarkt voor IV&P-professionals.

In 2021 kan het programma verder versnellen omdat het onlangs gelukt is om extra gekwalificeerde mensen aan te nemen in het programmateam.

Het aantoonbaar voldoen van de organisatie aan alle geldende richtlijnen op het gebied van informatieveiligheid & privacy is een proces dat nog een aantal jaren vergt. De provincie Utrecht onderscheidt zich wat dit betreft niet van veel andere vergelijkbare overheidsorganisaties.

Voorgeschiedenis

Informatieveiligheid en privacy vormen een maatschappelijke verantwoordelijkheid die vanzelfsprekend moet zijn voor elke overheidsinstantie.

Op 25 mei 2018 trad de Algemene Verordening Gegevensbescherming (AVG) in werking, die hoge eisen stelt aan de bescherming van persoonsgegevens door organisaties. De commissie BEM is op 25 juni en 29 oktober 2018 over de voortgang geïnformeerd. Het programma Informatieveiligheid en Privacy (IV&P) pakt het onderwerp sinds 2019 op met als doel de organisatie aantoonbaar te laten voldoen aan de geldende voorschriften en vereisten.

In 2019 is conform afspraak door de eenheid Concern Control een tweejaarlijks onderzoek verricht naar de voortgang rondom informatieveiligheid en privacy. U bent over de resultaten van dit onderzoek middels een statenbrief op 21 april 2020 geïnformeerd. Bij de Statenbrief met kenmerk 2020BEM49 was het rapport bijgevoegd. De conclusie van het rapport was kritisch en luidde kort samengevat dat het verbetertraject op het gebied van Informatieveiligheid & privacy in 2019 was gestagneerd.

Op 27 mei jl. stuurde het college u een reactie (kenmerk 2020BEM71) op dit onderzoek en rapporteerde zij over de gepleegde interventie op het programma waardoor de verantwoordelijkheid voor de aansturing en voortgang van het programma belegd is binnen de lijnorganisatie.

In de Statenbrief van 10 november jl. bent u geïnformeerd over de voortgang in het eerste halfjaar van 2020.

Toelichting

Hieronder is beschreven op welke onderdelen in de tweede helft van 2020 vooruitgang is geboekt.

Het onderdeel AVG is verbeterd

Op grond van de AVG dient elke organisatie een register bij te houden van de verwerkingen van persoonsgegevens. Dit register is aangevuld en geactualiseerd en de organisatie is ingericht om het op orde te houden. Daarnaast is het noodzakelijk dat met elke externe partij die voor de provincie persoonsgegevens verwerkt een verwerkersovereenkomst wordt afgesloten. Hierin worden afspraken opgenomen over de manier waarop dit gebeurt. Op dit moment zijn nog niet alle benodigde verwerkersovereenkomsten aanwezig. Het is een verantwoordelijkheid van de lijnorganisatie om de benodigde verwerkersovereenkomsten op te stellen, het programmteam IV&P kan hierbij ondersteunen.

De provincie heeft een Functionaris Gegevensbescherming (FG) die toezicht houdt op de naleving van de AVG. Op basis van haar jaarrapportage 2020 is voor 2021 een plan met verdere verbeteracties opgesteld. Met deze verbeteracties zorgen we ervoor dat de organisatie eind 2021 voldoet aan de belangrijkste onderdelen van de AVG.

De bewustwording in de organisatie is toegenomen

In 2020 zijn veel teams door het programmteam bezocht. Er zijn gesprekken met teamleiders, domeinmanagers en MT's gevoerd over wat informatieveiligheid & privacy inhoudt en wat dit betekent voor hun werkzaamheden. In de tweede helft van 2020 is de Are You Secure Game gespeeld door de organisatie. Dit is een app die de kennis en het bewustzijn van de medewerkers meet en ontwikkelt. De Are You Secure Game is ook aan GS en PS beschikbaar gesteld. Tenslotte is er een simulatie-phishingmail gestuurd. Door deze activiteiten is de bewustwording vergroot en weten management en medewerkers het programmteam IV&P beter te vinden voor advies en ondersteuning.

Er is een opleidingsplan IV&P opgesteld

De organisatie is doordrongen van de noodzaak van informatieveiligheid en privacy. Men weet echter nog onvoldoende welk handelen daarbij hoort. Er is behoefte aan aanvullende kennis. Om deze reden is eind 2020 een opleidingsplan opgesteld. Deze is begin 2021 door het CMT vastgesteld. Momenteel wordt de uitrol van dit plan voorbereid. Naar verwachting zal deze de 2^e helft van 2021 plaatsvinden.

De implementatie van het Information Security Management System (ISMS) is gestart

Een ISMS is een kwaliteits- en sturingsmethodiek voor informatieveiligheid en privacy. Hiermee kan gestuurd worden op de implementatie van maatregelen die nodig zijn om risico's in de organisatie op het gebied van informatieveiligheid & privacy te mitigeren. In de tweede helft van 2020 is gestart met het vullen van dit systeem. Naarmate het systeem meer gevuld raakt met risico's en maatregelen, kan de provincie hier beter op sturen. Dit traject zal meerdere jaren duren en loopt naar verwachting door tot en met 2023.

Er is een penetratietest uitgevoerd

In de tweede helft van 2020 is een penetratietest op het netwerk uitgevoerd. Hierbij is het niet gelukt het netwerk binnen te dringen. Er waren wel een aantal aandachtspunten, deze zijn / worden zo spoedig mogelijk opgelost.

Hieronder worden de aandachtspunten beschreven zoals die zijn ervaren gedurende de tweede helft van 2020.

Inzichtelijk krijgen van de grootste risico's

Een belangrijk aandachtspunt is dat de risico's in de organisatie op het gebied van IV&P nog niet voldoende in beeld zijn.

Het risicobeeld compleet maken, is meer werk dan vooraf is ingeschat. Om dit te versnellen en risicoreductie te bereiken, is in de tweede helft van 2020 aan alle teamleiders gevraagd om hun hoog-risico-processen te benoemen. Aan deze oproep is goed gehoor gegeven. Dit betekent dat we begin 2021 starten met het uitvoeren van risicoanalyses en daarbij de nog benodigde tegenmaatregelen in beeld kunnen brengen.

Afspraken in Samenwerkingsverbanden

De provincie Utrecht is een netwerkorganisatie en heeft veel samenwerkingsverbanden. Er is echter nog geen centraal overzicht met alle samenwerkingsverbanden. Om te toetsen of hierin goede afspraken zijn opgenomen over de uitwisseling van gegevens is dit overzicht nodig. Er wordt nu gewerkt aan het compleet krijgen van het totaaloverzicht.

Leveranciersmanagement

Een groot deel van onze ICT-infrastructuur is uitbesteed aan hosting partners. Er is nog niet voldoende sturing op de nakoming van afspraken met leveranciers op het gebied van informatieveiligheid & privacy. De provincie is echter wel volledig verantwoordelijk voor de gegevensverwerkingen bij de (hosting)partners. In 2021 wordt dit verder opgepakt.

Structureel toezicht op projecten en programma's

Voor het inbedden van structureel toezicht op informatieveiligheid & privacy is inzicht nodig de activiteiten van de projecten en programma's in de organisatie. Door de verdere inrichting van portfoliomanagement door de lijnorganisatie verbetert dit inzicht, maar dit is nog niet volledig.

Kritische bedrijfsprocessen

In de tweede helft van 2020 was nog onvoldoende zicht op de borging en beschikbaarheid van de kritische bedrijfsprocessen ten aanzien van informatieveiligheid & privacy.

Een aantal van bovengenoemde aandachtspunten is ook benoemd in de voortgang van het programma in de eerste helft van 2020.

Vervolg

In 2021 werkt het programmateam verder aan het aantoonbaar op orde brengen van de organisatie op het gebied van informatieveiligheid & privacy. Er wordt extra capaciteit ingezet op de beschreven aandachtspunten zodat hier vooruitgang op geboekt kan gaan worden.

Met ingang van 2021 wordt per kwartaal gerapporteerd over de voortgang van het programma IV&P. Dit gebeurt gezamenlijk met de rapportages over de voortgang van de overige digitale agenda's en een aantal verbetertrajecten binnen het domein Bedrijfsvoering.

Gedeputeerde Staten van Utrecht,

Voorzitter,
mr. J.H. Oosters

Secretaris,
mr. drs. A.G. Knol-van Leeuwen