PROVINCIE UTRECHT

PROVINCIAAL BLAD

Officiële uitgave van de provincie Utrecht

Nr. 5115

18 juli

2019

Besluit van Gedeputeerde Staten van Utrecht van 2 juli 2019, nr. 81F20568, tot vaststelling van een statuut gegevensbescherming

Gedeputeerde Staten van Utrecht;

Gelet op artikel 13b van het Organisatiebesluit provincie Utrecht 2004 en de Algemene verordening gegevensbescherming;

Besluiten:
tot vaststelling van het Statuut Gegevensbescherming

Artikel 1: Inleiding

1. De aanwijzing van een Functionaris Gegevensbescherming is een wettelijke verplichting die is opgenomen in artikel 37 van de Algemene Verordening Gegevensbescherming. De Functionaris Gegevensbescherming dient te worden aangemeld bij de Autoriteit Persoonsgegevens. Het college van Gedeputeerde Staten benoemt en ontslaat de Functionaris Gegevensbescherming en draagt zorg voor een formele melding aan de Autoriteit Persoonsgegevens (AP).
2. Het Organisatiebesluit bepaalt dat de inrichting en werkwijze met betrekking tot persoonsgegevens in een statuut verder worden uitgewerkt. Dit statuut voorziet hierin. De taken, verantwoordelijkheden en bevoegdheden van de Functionaris Gegevensbescherming in relatie tot andere actoren worden in dit statuut vastgelegd.

Artikel 2: Definities

In dit statuut wordt verstaan onder:

a. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
b. Verwerken: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via (geautomatiseerde) processen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen; raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
c. Betrokkenen: de natuurlijke persoon die geïdentificeerd of identificeerbaar is, op wie de gegevens betrekking hebben;
d. Gegevenseffectenbeoordeling/Data Protection Impact Assessment (DPIA): een instrument om van voorgenomen verwerkingsprocessen met persoonsgegevens, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen en maatregelen voor te stellen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of te verkleinen;
e. Autoriteit Persoonsgegevens: de toezichthoudende autoriteit die toezicht houdt op de naleving van de Algemene Verordening Gegevensbescherming.

Artikel 3: Taken van de Functionaris Gegevensbescherming

1. Op grond van artikel 39 Algemene Verordening Gegevensbescherming heeft de Functionaris Gegevensbescherming een aantal wettelijke taken die hieronder worden genoemd.
2. De Functionaris Gegevensbescherming informeert en adviseert desgevraagd en/of op eigen initiatief de provinciale organisatie over de verplichtingen op grond van de Algemene Verordening Gegevensbescherming.
3. De Functionaris Gegevensbescherming ziet als toezichthouder toe op de naleving van de Algemene Verordening Gegevensbescherming en het privacybeleid van de provinciale organisatie.
4. De Functionaris Gegevensbescherming ziet erop toe dat medewerkers worden bewust gemaakt en opgeleid conform de Algemene Verordening Gegevensbescherming en het privacybeleid van de provinciale organisatie.
5. De Functionaris Gegevensbescherming ziet erop toe dat audits met betrekking tot de naleving van de Algemene Verordening Gegevensbescherming en het privacybeleid van de provinciale organisatie worden uitgevoerd.
6. De Functionaris Gegevensbescherming ziet toe op het uitvoeren van gegevensbescherming effectbeoordelingen (DPIA's) en adviseert, namelijk:

a. of er een DPIA moet worden uitgevoerd,
b. op welke wijze de beoordeling wordt gedaan,
c. of de beoordeling intern wordt gedaan of wordt uitbesteed aan een externe partij,
d. welke waarborgen er moeten worden getroffen om de in de beoordeling gebleken risico's te beperken,
e. of de DPIA goed is gedaan, en
f. of de uitkomsten ervan voldoen aan de Algemene Verordening Gegevensbescherming.

7. Indien het advies van de Functionaris Gegevensbescherming met betrekking tot de DPIA, zoals bedoeld in voorgaand lid, niet wordt overgenomen, dient in de documentatie van de DPIA specifiek schriftelijk te worden aangegeven waarom het advies niet is overgenomen.
8. De Functionaris Gegevensbescherming treedt op als contactpunt voor de Autoriteit Persoonsgegevens en werkt samen met de Autoriteit Persoonsgegevens.
9. De Functionaris Gegevensbescherming kan andere taken en plichten vervullen. De concern controller zorgt ervoor dat deze taken of plichten niet tot een belangenconflict leiden.

Artikel 4: Lines of Defense

De verdeling van verantwoordelijkheden binnen het 'privacydomein' in de gehele organisatie is in 3 Lines of Defense onderverdeeld, met als doel het bevorderen van een effectieve samenhang van werkzaamheden door een efficiënte samenwerking. De Lines of Defense bestaan uit:

a. De eerste Line of Defense: De teamleiders en opgavemanagers van de provinciale organisatie. Zij zijn verantwoordelijk voor hun eigen verwerkingsprocessen (het verwerken van persoonsgegevens binnen hun expertteam of opgaveteam);
b. De tweede Line of Defense: De Privacy Officer. De Privacy Officer stelt privacykaders, richtlijnen en procedures op. Daarnaast ondersteunt de Privacy Officer de eerste lijn en adviseert, signaleert en rapporteert hij over de wijze waarop persoonsgegevens worden verwerkt door het management;
c. De derde Line of Defense: De Functionaris Gegevensbescherming. De Functionaris Gegevensbescherming is belast met het toezicht en adviseert de Algemeen Directeur, de teamleiders, de opgavemanagers en Gedeputeerde Staten, zoals beschreven onder artikel 3 van dit statuut.

Artikel 5: Verantwoordelijkheid teamleiders en opgavemanagers

1. De Teamleiders en Opgavemanagers zijn verantwoordelijk voor de uitvoering van de verplichtingen op grond van de Algemene Verordening Gegevensbescherming. Zij zijn proces- en data-eigenaar en verantwoordelijk voor de verwerkingsprocessen binnen hun team, zoals vastgelegd in het verwerkingsregister. Zij zijn ervoor verantwoordelijk dat:
   a. nieuwe of gewijzigde verwerkingsprocessen vooraf worden gemeld door middel van het meldingsformulier nieuwe verwerkingsactiviteiten bij de Privacy Officer voor het verwerkingsregister;
   b. verwerkersovereenkomsten met verwerkers worden gesloten;
   c. DPIA's worden uitgevoerd;
   d. datalekken worden gemeld;
   e. er niet meer persoonsgegevens worden verwerkt dan noodzakelijk;
   f. de bewaartermijnen niet worden overschreden;
   g. de persoonsgegevens passend zijn beveiligd;
   h. de juiste autorisatie van toepassing is op het gebruik en de inzage in persoonsgegevens.

2. Voor een nadere uitwerking van de taken van de Teamleiders en Opgavemanagers wordt verwezen naar de bijlage bij dit statuut.

Artikel 6: Privacy Officer

1. De Privacy Officer is een rol die binnen de provinciale organisatie functioneert onder verantwoordelijkheid van de teamleider Inkoop, Juridische zaken en Subsidies.
2. De Privacy Officer informeert de Functionaris Gegevensbescherming over aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens. De Functionaris Gegevensbescherming geeft de Privacy Officer zonodig desgevraagd of op eigen initiatief advies.
3. De Privacy Officer stelt in het kader van de bescherming van persoonsgegevens privacybeleid, richtlijnen, procedures en instructies op ter vaststelling door Gedeputeerde Staten.
4. De Privacy Officer is belast met het adviseren aan de eerste Line of Defense over het opstellen van verwerkersovereenkomsten, het adviseren over het aanleveren van informatie voor het bijhouden van het verwerkingsregister, het uitvoeren van een DPIA en overige advisering in het kader van de toepassing van de AVG en aanverwante regelgeving.
5. De Functionaris Gegevensbescherming geeft functionele sturing aan de Privacy Officer en kan functionele aanwijzingen geven aan de Privacy Officer.
6. Voor een nadere uitwerking van de taken van de Privacy Officers wordt verwezen naar de bijlage.

Artikel 7: Onafhankelijkheid Functionaris Gegevensbescherming

1. Gedeputeerde Staten stellen de Functionaris Gegevensbescherming aan.
2. De Functionaris Gegevensbescherming is binnen de provinciale organisatie geplaatst in de eenheid concerncontrol. De Functionaris Gegevensbescherming is voor zover het de uitvoering van zijn taken betreft niet hiërarchisch ondergeschikt aan de concerncontroller, noch aan de algemeen directeur/provinciesecretaris.
3. De Functionaris Gegevensbescherming heeft een onafhankelijke en onpartijdige positie binnen de provinciale organisatie conform art 38 Algemene Verordening Gegevensbescherming.
4. De Functionaris Gegevensbescherming ontvangt geen instructies met betrekking tot de uitvoering van zijn taken.
5. De Functionaris Gegevensbescherming wordt niet ontslagen of gestraft voor de uitvoering van zijn taken.
6. De Functionaris Gegevensbescherming brengt jaarlijks rechtstreeks verslag uit aan de algemeen directeur en Gedeputeerde Staten over de stand van zaken met betrekking tot de naleving van de Algemene Verordening Gegevensbescherming door de provinciale organisatie.
7. De Functionaris Gegevensbescherming brengt direct verslag uit aan de algemeen directeur en Gedeputeerde Staten, in geval van overtredingen van de Algemene Verordening Gegevensbescherming.
8. De algemeen directeur zorgt ervoor dat de Functionaris Gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
9. Voor een nadere uitwerking van de taken van de Functionaris Gegevensbescherming wordt verwezen naar de bijlage.

Artikel 8: Toegang

1. De Functionaris Gegevensbescherming moet kunnen beschikken over de voor de uitoefening van zijn taak noodzakelijke faciliteiten en middelen.
2. De Functionaris Gegevensbescherming heeft de bevoegdheid om ongevraagd alle ruimtes in de provinciale organisatie te betreden voor zover dit noodzakelijk is voor de uitoefening van zijn taak.
3. De Functionaris Gegevensbescherming heeft in relatie tot zijn taken de bevoegdheid om inlichtingen en inzage te krijgen en om zaken te onderzoeken.

Artikel 9: Klachten, bezwaar en rechten van betrokkenen

1. Betrokkenen kunnen, als zij van mening zijn dat de verwerking van hen betreffende persoonsgegevens inbreuk maakt op de Algemene verordening gegevensbescherming, een klacht indienen bij de Functionaris Gegevensbescherming, alvorens hierover de Autoriteit Persoonsgegevens te benaderen. De Functionaris Gegevensbescherming ziet er op toe dat de klacht van de betrokkenen wordt behandeld conform artikel 77 van de Algemene verordening gegevensbescherming alsmede de procedurebeschrijving van de provinciale organisatie inzake klacht en bezwaar over de niet naleving van de Algemene verordening gegevensbescherming.
2. Betrokkenen hebben een aantal rechten op grond van artikel 15 tot en met 22 Algemene Verordening Gegevensbescherming. Een verzoek tot het behandelen van deze rechten kunnen worden ingediend bij de Functionaris Gegevensbescherming. De Functionaris Gegevensbescherming ziet er op toe dat het verzoek van de betrokkenen wordt behandeld conform de procedurebeschrijving inzake de rechten van betrokkenen van de provinciale organisatie.

Artikel 10: Geheimhouding en integriteit

De Functionaris Gegevensbescherming is met betrekking tot de uitvoering van zijn taken tot geheimhouding gehouden.

Aldus vastgesteld in de vergadering van Gedeputeerde Staten van Utrecht van 2 juli 2019.

Gedeputeerde Staten van Utrecht,
Voorzitter,

Secretaris,

Nr	Uitgangspunten	Sturings- en verantwoordings-informatie	Taken teamleiders en opgavemanagers (1e line of defense)	Taken Privacy Officer , team IJS (2e line of defense)	Taken Functionaris Gegevens-bescherming, eenheid CCO (3e line of defense)
Algemeen					
P.1	De provincie streeft voor haar processen m.b.t. privacy naar een proces-volwassenheids-niveau van 3 met een minimum van 2.	- Aan CMT: 1x per 2 jaar wordt in het dashboard privacy de proces-volwassenheid gerapporteerd. - Indicator procesprestatie.			- rapporteren en adviseren over proces-volwassenheid privacy als resultaat van de audit (is samenwerking met CCO).
Privacybeleid & strategie					
P.2	De provincie onderhoudt strategie en beleid voor privacy dat beschrijft hoe werknemers in de gehele organisatie dienen om te gaan met het verzamelen, gebruiken, bewaren, verstrek-ken en verwijderen van persoonsgegevens, inclusief het verschaffen van informatie aan externe belanghebbenden.	- Vastgesteld document privacystrategie - Vastgesteld document privacybeleid - Vastgesteld document met richtlijnen omgang met persoonsgegevens incl. transport. - Vastgesteld document privacystatement	- kennis hebben van de strategie en het beleid op het gebied van privacy en het privacystatement. - informatie aanleveren over de verwerking t.b.v. het privacy statement	- opstellen en doen vaststellen privacystrategie - opstellen en doen vaststellen privacy-beleid - opstellen en doen vaststellen richtlijnen omgang persoonsgegevens - opstellen en doen vaststellen privacystatement	- gevraagd en ongevraagd adviseren over de strategie en het beleid op het gebied van privacy en het privacystatement.
Privacy Officer & Overlegstructuur					
P.3	De provincie heeft een organisatiestructuur, rollen en verantwoordelijk-heden voor het beheersen van de verzameling, het gebruik, het bewaren, het verstrekken en het verwijderen van persoonsgegevens, en voor de operationele afstemming daarover.	- Vastgestelde documenten organisatie-structuur, processen, rollen, verantwoordelijk-heden m.b.t. privacy - Vastgesteld document toewijzing rollen m.b.t. privacy aan personen.	- doen toewijzen van rollen van lijnmanagement naar medewerkers. - vastleggen van rollen en bijhouden veranderingen.	- opstellen en doen vaststellen organisatiestructuur, rollen en verantwoordelijk-heden.	- toezien, rapporteren en adviseren over verdeling van verantwoordelijk-heden
Training & Awareness					
P.4	De provincie houdt de privacykennis bij mede-werkers op adequaat niveau	- Aan CMT: 1x per jaar rapporteert de provincie de resultaten van de meting van bewustzijn en	- verstrekken van relevante informatie aan medewerkers op de werkvloer over het werken met persoonsgegevens	- monitoren bewustzijn en bekwaamheid van medewerkers mbt privacy - opstellen en doen vaststellen	- rapporteren en adviseren over bewustzijn en bekwaamheid mbt privacy - geven van trainingen en

	met generieke en specifieke training toegepast op de verzameling, het gebruik, het bewaren, het verstrekken en het verwijderen van persoons-gegevens en awareness-activiteiten.	bekwaamheid m.b.t. privacy.		van concernbreed vormings- en opleidings-programma mbt privacy - zorgdragen voor trainingen en opleidingen	opleiding toegespitst op doelgroepen
Privacy Architectuur (Privacy by Design)					
P.5	De provincie heeft een proces om te borgen dat principes als gegevens-minimalisatie en doel-binding, privacy-by-default en gegevens ontdoen van persoonsinformatie (de-identificatie) vanaf het begin worden toegepast.	- In het dashboard privacy wordt de proces-volwassenheid gerapporteerd.		- beschrijven van de inrichting en werking van werkprocessen i.r.t. privacy. - invoeren van nieuwe verwerkingen obv PIA-light (door de lijn zelf uit te voeren) in het verwerkingsregister en privacytool - opstellen van procedures en instructies mbt gegevens-minimalisatie en doelbinding, privacy-by-default en de-identificatie van gegevens. - adviseren over toepassen principes gegevens-minimalisatie en doelbinding, privacy-by-default en de-identificatie van gegevens. - accorderen wijzigingen van domein in verwerkingen - adviseren over de (op te leveren) resultaten van projecten en programma's die van invloed zijn op de inrichting en werking van bestaande werkprocessen., alsmede inbedden in portfolio-management.	- toezien, rapporteren en adviseren over privacy aspecten mbt de (op te leveren) resultaten van projecten en programma's op concernniveau
Third Party Management					
P.6	De provincie heeft processen die de	- In het dashboard privacy wordt de	- verzamelen en aanleveren	- adviseren over het beschikbaar	- toezien, rapporteren en

	privacy risico's bij externe partijen beheersen.	proces-volwassenheid gerapporteerd - Het sluiten van verwerkers-overeenkomsten wordt geïntegreerd in het proces voor verwerving en contractvernieuwing. - Specificaties voor producten of diensten waarbij persoonsgegevens zullen worden verwerkt zijn voor de uitvraag geconfronteerd met het verwerkingsdoel vanuit het oogpunt van privacy principes waaronder gegevens-minimalisatie (zie ook IR.5). - Aan CMT: 1x per jaar rapportage externe verwerkers met per verwerker contractduur, aanwezigheid AVG-proof verwerkers-overeenkomst, wijze van toetsing, datum laatste toetsing.	actuele informatie verwerkingen	stellen van persoonsgegevens aan derden (incl. risico-inschatting) - adviseren over privacy principes bij vernieuwing/ verandering van decentrale I-systemen/ verwerkingen met persoonsgegevens - opstellen van en adviseren over standaard verwerkers-overeenkomsten - bijhouden register verwerkers-overeenkomsten - uitvoeren functioneel beheer verwerkingsregister - adviseren over verwerkers-overeenkomsten (door de lijn zelf op te stellen) - toetsen naleving verwerkers-overeenkomsten door derden.	adviseren over het gebruik persoonsgegevens door derden - rapporteren over privacy risico's bij externe verwerkers
Informatie Levenscyclus Management					
P.7	De provincie heeft processen en beheersings-maatregelen voor de hele informatielevens-cyclus van persoonsgegevens, gericht op het verzamelen tot en met het verwijderen van persoonsgegevens.	- Per verwerking wordt de aard en reikwijdte van toestemming(en) vastgelegd. Indien van toepassing worden verleningen en intrekkingen door betrokkenen ook vastgelegd. - Aan CMT: 4x per jaar KRI (key risk indicator) aantal verleningen en intrekkingen van toestemmingen, actueel en trend. - Verslagleggingen van vernietiging	- aanleveren informatie tbv verwerkingsregister - (doen) uitvoeren vernietiging persoonsgegevens	- opstellen van procedures en instructies mbt het gebruik van verwerkingsregister - instructies over registratie bewaartermijnen en bewaardoelen - adviseren over aard en reikwijdte van toestemmingen - adviseren over vastlegging verlengingen en intrekking toestemmingen - adviseren over vernietiging van persoonsgegevens	- toezien, rapporteren en adviseren over de werking van processen en beheersmaatregelen mbt de informatielevens-cyclus van persoonsgegevens.

		van persoonsgegevens na verstrijken bewaartermijn of vervallen bewaardoel. - Aan CMT: 4x per jaar KRI aantal verslagleggingen van vernietiging.		- registreren vernietiging persoonsgegevens (op aangeven domeinen) - per kwartaal rapporteren over ontwikkelingen mbt verwerkers-overeenkomsten en vernietiging van persoonsgegevens	
Privacy Risico management					
P.8	De provincie heeft een proces om de privacyrisico's in kaart te brengen & houden en de beheersings-maatregelen te selecteren om deze risico's te managen en mitigeren.	- Organisator-ische, fysieke en technische beheersings-maatregelen voor privacy worden gedocumenteerd en periodiek getest en geëvalueerd - Aan CMT: 1x per jaar risicobeeld en risicobeheersings-beeld privacy voor concern en per domein.		- opstellen en bijhouden van overzicht van privacyrisico's en bijbehorende beheersings-maatregelen per werkproces - monitoren voortgang / status risicobeheersings-maatregelen - opstellen kaders risicobeheersings-beleid - opstellen procedures en instructies registratie risico's en beheersings-maatregelen - uitvoeren DPIA bij nieuwe verwerkingen met een hoog risicoprofiel	- toezien, rapporteren en adviseren over het risicobeeld privacy op domein- en concernniveau - adviseren over en (doen) uitvoeren van DPIA bij nieuwe verwerkingen met een hoog risicoprofiel
Privacy Processen					
P.9	De provincie heeft privacyspecifieke processen die borgen dat persoonsgegevens verwerkt conform de verplichtingen, waaronder: - het recht op inzage; - het recht op correctie; - het recht op verzet; - het recht op verwijdering / vergeten te worden; - het recht op dataportabiliteit.	- Rapporten van Privacy Impact Assessments wanneer vereist bij veranderingen in diensten, processen en/of systemen (zie IR.5). - Aan CMT: 4x per jaar KRI het aantal verzoeken plus percentage tijdig afgedaan per recht, actueel en trendmatig.		- het registreren , beoordelen, verwerken van verzoeken van personen mbt inzage, correctie, verzet en verwijdering van hun persoonsgegevens en het informeren van betrokkenen - opstellen van procedures, richtlijnen en instructies mbt verzoeken van personen omtrent inzage, correctie, verzet en verwijdering persoonsgegevens.	- toezien, rapporteren en adviseren over het afhandelen van verzoeken van personen omtrent hun persoonsgegevens.

				- uitvoeren en rapporteren van DPIA's van decentrale informatiesystemen en -verwerkingen	
Datalek Response Proces					
P.10	De provincie heeft een proces voor het identificeren en beoordelen van incidenten met persoonsgegevens en voor de respons daarop, zoals het melden bij de AP.	- Aan CMT: 4x per jaar KRI datalek meldingen aantal totaal, aantal afgedaan en aantal gemeld AP, actueel en trend	- het signaleren van datalekken in de werkprocessen of bij externe partijen. - melden datalek bij betrokkenen indien van toepassing (obv beoordeling FG hierover) - het verzamelen van informatie in het kader van onderzoek (door de PO) - het (doen) uitvoeren van beheersings-maatregelen m.b.t. datalekken - het informeren van de FG	- het opstellen van procedures en instructies inzake de melding en afhandeling van decentrale datalekken incl. lekken bij derden - het registeren van meldingen van datalekken in eigen register datalekken - het uitvoeren van onderzoek mbt gemelde datalekken - het adviseren over beheersings-maatregelen - melden van datalekken aan de autoriteit persoonsgegevens (op basis van beoordeling FG hierover)	- het coördineren van de afhandeling van datalekken. - het beoordelen van datalekken en zo nodig doen melden bij de Autoriteit Persoonsgegevens en beoordeling of datalek gemeld moet worden bij betrokkenen. - rapporteren en adviseren naar directie en bestuur inzake de melding en afhandeling van datalekken.
Juridische Processen					
P.11	De provincie heeft een proces voor het inzichtelijk maken en monitoren de huidige en toekomstige eisen in privacywetgeving en producten om zo de juiste processen en beheersings-maatregelen m.b.t. privacy in te richten.	- Vastgesteld document privacystatement		- het bijhouden van actuele (beleids) ontwikkelingen op het gebied van privacy en zo nodig bijstellen van kaders, richtlijnen, procedures en instructies en informeren van betrokkenen - opstellen en bijhouden privacystatements	- adviseren over actuele (beleids) ontwikkelingen op het gebied van privacy en de gevolgen voor de organisatie
Security Management					
P.12	De provincie vertaalt privacy-eisen naar noodzakelijke beveiligingseisen op het gebied van o.a. logische en fysieke toegangsbeveiliging,	- In het informatie beveiligingsbeleid zijn richtlijnen opgenomen voor het vertalen van privacy-eisen naar beveiligingseisen, op basis van classificatie van	- monitoren van (on)geautoriseerde toegang tot persoonsgegevens en zo nodig melden datalek. - inrichten van aanvullende maatregelen	- opstellen richtlijnen mbt vertalen privacy-eisen naar beveiligingseisen - adviseren over de inrichting van logische en fysieke	- toezien, rapporteren en adviseren over de inrichting en naleving van beveiligingseisen tav logische en fysieke toegang tot persoonsgegevens

	versleuteling en logging.	persoonsgegevens en daaraan gerelateerde beveiligingsniveaus. - De logische en fysieke toegangsbeveiliging voor verwerkingen van persoonsgegevens worden ingericht conform beveiligingseisen. De werking ervan wordt gemonitord en gerapporteerd in het risicobeheersings-beeld IB of privacy. - Toegangsautorisaties voor verwerkingen van persoonsgegevens worden uitsluitend voor noodzakelijke toegang in verband met het verwerkingsdoel vrijgegeven en herzien bij in-, door- en uitstroom. - Toegang tot persoonsgegevens wordt gelogd en gemonitord op ongeautoriseerd (pogingen tot) toegang en zo nodig opgevolgd met een interne datalek melding. - Bij transport of op mobiele apparatuur worden persoonsgegevens versleuteld.	- monitoren van aanvullende maatregelen	toegangsbeveiliging van persoonsgegevens (incl versleuteling en logging). - inrichten en monitoren van de werking van centrale beveiligings-maatregelen	
Data Infrastructuur					
P.13	De provincie onderhoudt een overzicht van de datastromen en persoonsgegevens die binnen de organisatie worden verwerkt inclusief de verschillende doeleinden en de	- Actueel overzicht van datastromen en verwerkingen van persoonsgegevens met doeleinden, classificatie en PIA-status (verwerkingen-register). - Aan CMT: 4x per jaar KRI aantal	- informatie over nieuwe verwerkingen aanleveren aan PO	- opstellen standaard overzicht en bijbehorende instructie mbt datastromen en persoonsgegevens -Nieuwe aangemelde verwerkingen uit	- toezien, rapporteren en adviseren over actualiteit overzicht datastromen en persoonsgegevens

	classificatie van persoonsgegevens.	verwerkingen en aantal met status AVG-compliant.		domein accorderen en PIA light checken en zelf nieuwe geconstateerde verwerkingen vastleggen in het verwerkingsregister in de privacy tool - bijhouden overzicht datastromen - bijhouden van een overzicht van datastromen binnen de onderscheiden werkprocessen	
Verantwoording & Auditing (Accountability)					
P.14	De provincie heeft een continu proces waarin de interne en externe beheersings-maatregelen worden getoetst op effectiviteit, via rapportages, zelfevaluaties en audits.	- Aan het 2-jaarlijkse dashboard privacy ligt een onafhankelijke audit/review van privacyprocessen en –beheersings-maatregelen ten grondslag.		- uitvoeren van zelfevaluaties	- toezien, rapporteren en adviseren over het bestaan en de werking van een systeem van continue (zelf)evaluatie en bijsturing mbt interne en externe beheersings-maatregelen door de organisatie. - opstellen van een overzicht van geplande en uitgevoerde Data Protection Impact Analyses (DPIA), zelfevaluaties en audits door de organisatie.