provincie Zuid-Holland

JAARVERSLAG 2023

Op weg naar een krachtige bescherming van persoonsgegevens

Niels Bons
Functionaris voor Gegevensbescherming
Provincie Zuid-Holland

maart 2024

Krachtig Zuid-Holland

Inhoud

Voorwoord

Het jaarverslag van de Functionaris Gegevensbescherming (FG) van de provincie Zuid-Holland voor 2023 heeft tot doel verantwoording af te leggen over de wijze waarop de FG diens taken zoals vastgelegd in artikel 39 van de Algemene Verordening Gegevensbescherming (AVG) heeft uitgeoefend. Kort gezegd omvat deze taak het informeren en adviseren van het provinciebestuur over hun verplichtingen, het toezicht houden op de naleving van de AVG, het adviseren met betrekking tot de uitvoering van gegevensbeschermingseffectbeoordelingen (Data Protection Impact Assessment, DPIA) en het onderhouden van contacten met de Autoriteit Persoonsgegevens (AP).

Daarnaast belicht dit jaarverslag het algemene nalevingsbeeld op privacygebied, de uitgevoerde activiteiten en opgeleverde resultaten, de bevindingen over 2023 en de aandachtspunten voor 2024.

Dit verslag wordt uitgebracht aan het College van Gedeputeerde Staten, aangezien dit college eindverantwoordelijk is voor het merendeel van de verwerkingen van persoonsgegevens binnen de provincie Zuid-Holland. Het college kan de adviezen uit het jaarverslag gebruiken als sturingsinstrument in het verbeteren van de naleving van de AVG.

Inleiding

Op grond van de AVG dienen overheidsinstanties een Functionaris voor Gegevensbescherming (FG) aan te wijzen. Deze FG fungeert als een onafhankelijke interne toezichthouder, met als hoofddoel het waarborgen van naleving van wet- en regelgeving met betrekking tot de bescherming van persoonsgegevens. De wettelijke basis voor het toezicht door de FG omvat de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), en de Wet politiegegevens (Wpg). Binnen de provincie Zuid-Holland houdt de FG toezicht op de naleving van zowel de AVG als de Wpg.

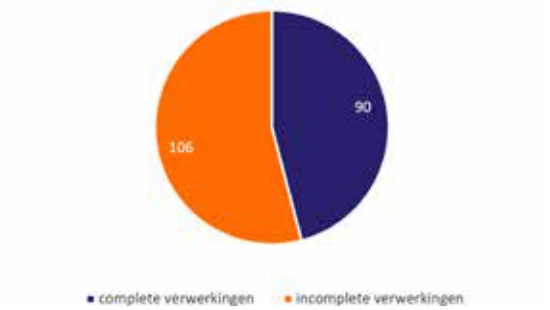
De FG heeft ingevolge de AVG de rechtens aan hem opgedragen taak om de verwerkingsverantwoordelijke te informeren, adviseren en controleren of de verwerking van persoonsgegevens binnen de provincie Zuid-Holland rechtmatig, behoorlijk en transparant plaatsvindt.
De provincie Zuid-Holland heeft drie bestuursorganen die als verwerkingsverantwoordelijke kunnen worden aangemerkt. Het leeuwendeel van de verwerkingen vindt plaats onder verantwoordelijkheid van het College van Gedeputeerde Staten (GS). De FG heeft voor alle drie bestuursorganen een aanwijzingsbesluit. Dit jaarverslag ziet op de verwerkingen onder verantwoordelijkheid van Gedeputeerde Staten.

Tevens controleert de FG of zowel interne als externe betrokkenen van de provincie Zuid-Holland hun privacyrechten kunnen uitoefenen, en ziet hij toe op een correcte afhandeling van datalekken en verzoeken en klachten met betrekking tot de verwerking van persoonsgegevens. Daarnaast wordt vanuit de AVG van de FG verwacht dat hij nauw samenwerkt met de externe toezichthouder, de Autoriteit Persoonsgegevens (AP). Naast het handhaven op naleving van wet- en regelgeving, heeft de FG ook ingezet op het stimuleren van het verbeteren van de privacyorganisatie binnen de provincie Zuid-Holland.

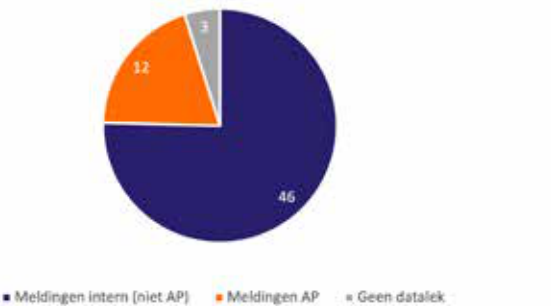
In 2023 hield de FG toezicht op de manieren waarop persoonsgegevens binnen de provincie Zuid-Holland worden verwerkt, voerde onderzoek uit, en verstrekte zowel gevraagd als ongevraagd advies. Tevens besteedde de FG specifieke aandacht aan verwerkingen van persoonsgegevens die een hoog risico vormen voor de rechten en vrijheden van personen, zoals die voortvloeien uit het gebruik van (nieuwe) technologieën.

Samenvatting in cijfers

Verwerkingsregister



Datalekmeldingen



Verwerkingsregister

complete verwerkingen	90
incomplete verwerkingen	106

Datalekmeldingen

Meldingen intern (niet AP)	46
Meldingen AP	12
Geen datalek	3

Privacy Impact Assessments

Rechten van betrokkenen

PIA's

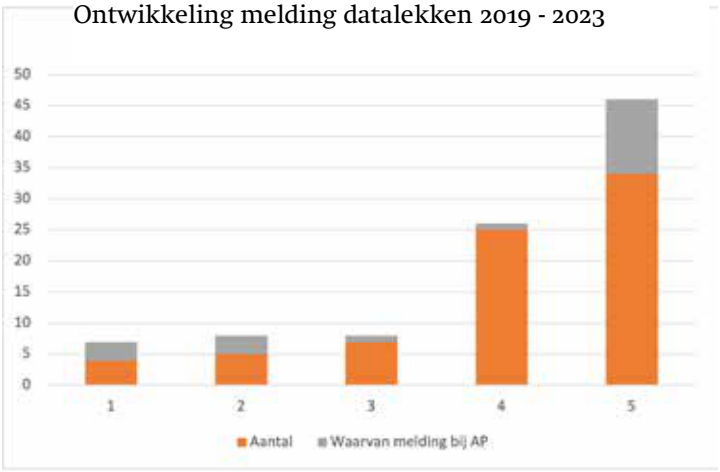
Afgeronde PIA's	1
Lopende PIA's	20
nog niet gestart	28
afgekeurd	0

Rechten van betrokkenen

Inzage	1
Gegevenswissing	0

Klachten

Ontwikkeling melding datalekken 2019 - 2023



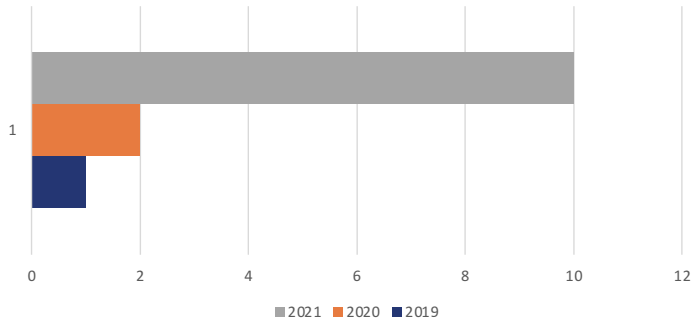
Klachten

Gegrond	0
Ongegrond	2

Ontwikkeling melding datalekken

2019	Aantal	4
	Gemeld AP	3
2020	Aantal	5
	Gemeld AP	3
2021	Aantal	7
	Gemeld AP	1
2022	Aantal	25
	Gemeld AP	1
2023	Aantal	34
	Gemeld AP	12

Verzoeken rechten betrokkenen



Ontwikkeling verzoeken rechten van betrokkenen

2019	1
2020	2
2021	10

AVG op onderdelen:

Binnen de AVG zijn verschillende kernonderdelen te identificeren die bij de naleving van de AVG met name van belang zijn en daarmee ook in het bijzonder de aandacht hebben in het kader van het toezicht van de FG en, achterliggend, de AP. Zonder compleet te zijn, kunnen de volgende onderwerpen worden genoemd:

- Register van verwerkingsactiviteiten
- Data protection impact assessment (DPIA)
- Datalekken
- Rechten van betrokkenen & verzoeken o.g.v. AVG

In het navolgende zal bij elk van deze onderwerpen worden ingegaan op de bevindingen die de FG gedurende de verslagperiode binnen de praktijk van de provincie Zuid-Holland heeft gedaan.

Register van verwerkingsactiviteiten

Op grond van artikel 30 van de AVG is de provincie Zuid-Holland verplicht een zogenoemd verwerkingsregister in te richten, waarin zij alle activiteiten en processen dient op te nemen waarin persoonsgegevens verwerkt worden. Dit register vormt enerzijds een belangrijk instrument binnen de verantwoordingsplicht die gegevensverwerkende organisaties hebben, en vormt anderzijds een cruciale basis voor diverse aspecten die vanuit de AVG moeten worden benaderd, waaronder de uitoefening van de rechten van betrokkenen.

De afgelopen jaren heeft de provincie Zuid-Holland veel effort gestoken in het completeren van het register van verwerkingsactiviteiten. In de verslagperiode is er door de verschillende domeinen, met ondersteuning van de eenheid Privacy (EP), gewerkt aan het verder vullen van het register. Daarnaast is door de EP gewerkt aan het opschonen van het register waarbij dubbelingen en verwerkingen die niet (meer) bestaan zijn verwijderd. Het vullen en bijhouden van het register van verwerkingsactiviteiten is echter geen eenmalige activiteit, maar een continu proces, waarvoor de verantwoordelijkheid bij de opdrachten ligt die eigenaar zijn van de systemen en (bedrijfs)processen waarin de te registreren verwerkingen plaatsvinden. De EP monitort hier weliswaar op, doch het vullen van het register en verder beheren van de registraties dient plaats te vinden door de betrokken opdrachten zelf. De EP kan daarbij waar nodig ondersteunen. Gedurende de verslagperiode is geconstateerd dat er nog steeds domeinen zijn die achterblijven met het vullen van het verwerkingsregister. Met name twee voormalige afdelingen binnen het domein Bedrijfsvoering springen daarbij in het oog. Hoewel zowel de EP als de FG hiervoor op verschillende momenten en wijzen aandacht hebben gevraagd, zijn er gedurende de verslagperiode vrijwel geen verwerkingen door deze geleding van de organisatie in het verwerkingsregister opgenomen. Het domein Bedrijfsvoering heeft geen privacy ambassadeurs aangewezen, daar waar dat in andere geledingen van de organisatie in de meeste gevallen wel heeft plaatsgevonden. Ten tijde van het schrijven van dit jaarverslag is bekend geworden dat er tijdelijke capaciteit is vrijgemaakt voor het aantrekken van een externe consultant, welke de opdracht heeft gekregen de verwerkingen binnen I&A binnen vijf maanden te inventariseren en aan het register toe te voegen.

Het is positief dat daarmee een inhaalslag gemaakt wordt voor de afgelopen tijd, maar het verdient aanbeveling ook voor de toekomst de continuïteit van het beheer van de registraties in het verwerkingsregister te regelen. Temeer omdat door inschakeling van tijdelijke aanvullende capaciteit mogelijk intern onvoldoende kennis en bewustzijn wordt opgebouwd op dit gebied.

Aanbeveling: privacy beter en duurzaam beleggen binnen delen van het domein Bedrijfsvoering.

Voor het overige kon worden geconstateerd dat eind 2023 in totaal 196 verwerkingen waren opgenomen in het register, waarvan 90 volledig waren goedgekeurd na de verschillende daarop uit te voeren controles.

Een punt van zorg blijft het proces rond het signaleren en opnemen van nieuwe verwerkingen. Nieuwe verwerkingen en systemen moeten consequent worden opgenomen in het register, dat een integraal onderdeel moet worden van alle bedrijfsprocessen waarbij de provincie Zuid-Holland persoonsgegevens verwerkt.

Aanbeveling: borg het proces rondom nieuwe verwerkingen zodanig dat privacy daarbij altijd een rol speelt.

Zoals eerder door de FG in zijn jaarverslag over 2021 is gesteld, kan GS in het kader van transparantie en verantwoording, overwegen om het register, al dan niet in beperkte vorm, openbaar te maken op de website van de provincie.

Aanbeveling: publiceer een afgeslankte versie van het register van verwerkingsactiviteiten op de corporate website.

DPIA's

Volgens de AVG, Wpg en de Wet justitiële en strafvorderlijke gegevens (Wjsg), zijn organisaties in bepaalde gevallen verplicht om een DPIA uit te voeren. Dit instrument dient om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te nemen om deze risico's te verminderen, aldus de AP.

De (Europese) wetgever heeft een minimale drempel vastgesteld waarbij een DPIA verplicht is. Op verwerkingen die mogelijk een hoog risico in zich bergen op het gebied van de bescherming van persoonsgegevens dient de provincie Zuid-Holland een risicoanalyse uit te voeren. Om als betrouwbare overheid te fungeren, zouden overheidsorganisaties, inclusief de provincie, er overigens voor kunnen kiezen om niet strikt aan deze drempel te voldoen, maar eerder ruimer te handelen. Naast het verbeteren van het imago brengt dit ook andere voordelen met zich mee, zoals het verschaffen van meer inzicht in verwerkingen voor transparantie, het vergroten van bewustzijn binnen de organisatie over processen met persoonsgegevens, en het scherper kijken naar het AVG-principe van privacy-by-design.

Een belangrijke verplichting rondom DPIA's betreft het voorschrift in de AVG dat met verwerkingen waarop een DPIA wordt uitgevoerd niet eerder mag worden begonnen voordat de DPIA is afgerond en daarop een (zwaarwegend) advies van de FG is uitgebracht. De provincie Zuid-Holland heeft het afgelopen jaar veel aandacht besteed aan het in kaart brengen van welke DPIA's moeten worden uitgevoerd. Gedurende 2023 is binnen de provincie onderkend dat nog veel DPIA's moeten worden uitgevoerd en zijn daar inmiddels middelen voor vrijgemaakt. De EP ondersteunt bij veel van de uit te voeren DPIA's en daarnaast zijn ook enkele externe partijen ingeschakeld om te ondersteunen bij een aantal DPIA's.

Voor de toekomst zal er meer aandacht moeten komen voor het tijdstip waarop een DPIA dient te worden uitgevoerd, zoals hiervoor gememoreerd dat dit dient te geschieden voordat met de betreffende verwerking wordt begonnen. In enkele gevallen werden verwerkingen gestart, zonder dat een daarvoor verplichte DPIA werd uitgevoerd. De provincie Zuid-Holland loopt risico met deze wijze van omgaan met DPIA's en verwerkingen. In gevallen waarin de FG een afwijzend advies op een DPIA afgeeft terwijl de betreffende verwerking niettemin is of wordt gestart, begaat de provincie Zuid-Holland daarmee een boetewaardige overtreding van de AVG. Belangrijker is nog dat, daarmee mogelijk ook de rechten van burgers en medewerkers worden geschaad. Naast geldelijke en imago-schade voor de provincie Zuid-Holland en/of eventuele individuele schade voor betrokkenen brengt een en ander zodoende ook een afbreukrisico met zich mee. Het kan immers afbreuk doen aan het vertrouwen dat de burger in de overheid zou mogen hebben.

Aanbeveling: beleg privacy en het uitvoeren van een DPIA in een vroeg stadium in de opgaven, zodat een DPIA geen belemmering hoeft te zijn in de voortgang van een opgave.

Datalekken

Een van de elementen in de verantwoordingsplicht die organisaties op grond van de AVG hebben, is het verplicht vastleggen van alle inbreuken op persoonsgegevens, ook wel bekend als het bijhouden van een datalekregister. Het doel van deze verplichte registratie is het bevorderen van organisatorisch leren uit eerdere inbreuken en het nemen van maatregelen om de kans op toekomstige inbreuken te verminderen. De registratie van datalekken biedt daarmee ook een basis voor het aansnijden van discussies binnen de organisatie over bewustzijn met betrekking tot de AVG. Bovendien kan de AP als toezichthoudende autoriteit aan de hand van de vastgelegde gegevens controleren of organisaties voldoen aan de meldplicht voor datalekken. De registratie van datalekken wordt vooraf gegaan door een melding van een datalek. Veelal geschiedt de melding door een medewerker van de provincie Zuid-Holland, maar kan ook worden gedaan door de FG of door de EP. Het datalekregister wordt op een adequate wijze bijgehouden door de EP.

Naast registratie van datalekken door het verwerkende orgaan zelf, kan voor bepaalde datalekken de verplichting bestaan deze te melden bij de Autoriteit Persoonsgegevens. Een datalek dient in de meeste gevallen te worden gemeld bij de AP, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de betrokkene.

In 2021 zijn er 8 datalekken gemeld. In het jaar 2022 zijn er 26 datalekken gemeld en geregistreerd, waarvan er 1 gemeld is bij de AP. In 2023 werden er bij de provincie 46 datalekken geregistreerd. Van de 46 geregistreerde datalekken zijn er 12 gemeld bij de Autoriteit Persoonsgegevens. De invloed van de EP is hier duidelijk merkbaar. Na de oprichting van de EP in mei 2022 is het aantal gemelde datalekken significant gestegen. Dat is een positieve ontwikkeling.
In vergelijking met de cijfers voor organisaties van dezelfde aard en omvang als de provincie Zuid-Holland is het aantal geregistreerde datalekken van de provincie Zuid-Holland echter nog relatief laag. De FG constateert dat er nog te weinig datalekken worden gemeld en dat deze meldingen soms ook erg laat worden gedaan. Mogelijk worden datalekken niet herkend of niet intern gemeld. Om deze reden zou het aanbeveling verdienen dat de provincie zich de komende jaren inspant om het bewustzijn van medewerkers rondom datalekken te vergroten en eventuele belemmeringen voor het melden ervan, zo aanwezig, weg te nemen. Positief daarbij is wel dat, zodra de datalekken zijn gemeld, het proces van het afdoen van datalekken uitstekend verloopt en dat alle datalekken binnen de wettelijk vereiste termijn zijn opgepakt en zo nodig gemeld bij de AP.

Aanbeveling: besteed in de bewustwording meer aandacht aan het (tijdig) melden van datalekken.

De aard van de datalekken die de afgelopen twee jaar zijn gemeld loopt uiteen van het verlies van devices tot heftige inbreuken op verwerkingen in de systemen van de provincie Zuid-Holland. De meest impactvolle inbreuk heeft plaatsgevonden in het iDMS, het document management systeem van de provincie Zuid-Holland. Het is niet voor het eerst dat er datalekken zijn geconstateerd en gemeld in iDMS en zowel de provinciearchivaris als de FG hebben in hun eerdere jaarverslagen aandacht gevraagd voor de risico's die het werken met dit document management systeem met zich meebrengt. De impact van het datalek in iDMS dat in het najaar van 2023 is gemeld is echter zeer groot te noemen. Zowel het dichten van dit lek als de maatregelen die genomen moeten worden om herhaling in de toekomst te voorkomen nemen nog geruime tijd in beslag.

Rechten van betrokkenen & verzoeken o.g.v. AVG

De AVG kent verschillende rechten toe aan betrokkenen, met name het recht op inzage, rectificatie en het wissen van persoonsgegevens. Volgens de AVG-termijnen heeft de verwerkingsverantwoordelijke, in dit geval het college van Gedeputeerde Staten, één maand om een verzoek af te handelen, met de mogelijkheid van een verlenging van 2 maanden in complexe gevallen. De provincie heeft alle verzoeken van het afgelopen jaar binnen de gestelde termijnen afgehandeld.

Het eerder genoemde register van verwerkingsactiviteiten draagt niet alleen bij aan een snellere en betere afhandeling van verzoeken, zeker wanneer dit compleet en volledig up to date is. Het elimineert ook vraagstukken over het eigenaarschap van gegevens en systemen, die momenteel nogal eens voorkomen. In het verwerkingsregister is vastgelegd wie verantwoordelijk is voor welke processen.

In 2023 is er slechts een verzoek om inzage op grond van artikel 15 AVG ingediend bij de provincie Zuid-Holland.

Privacybeleid

In 2023 is er een begin gemaakt met het opstellen van privacybeleid door de EP. Dit beleid is echter nog niet vastgesteld. Het vaststellen en naleven van een provinciaal privacybeleid heeft een positieve invloed op de betrouwbaarheid van de organisatie, vooral in de communicatie met betrokkenen. De praktijk heeft laten zien dat bepaalde keuzes met betrekking tot (de afhandeling van) een verzoek zich soms moeilijk laten uitleggen aan betrokkenen, omdat nog niet verwezen kan worden naar vastgestelde beleidsregels. De andere klacht ging over dat de provincie niet naleeft wat zij zegt over persoonsgegevens in haar eigen privacyverklaring. Beide klachten bleken ongegrond.

Bezwaar

Er zijn in 2023 geen bezwaarschriften ingediend inzake de AVG.

Organisatie

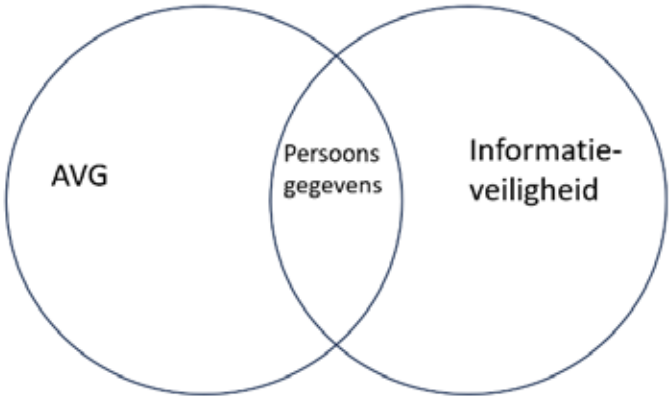
Voor de privacy organisatie binnen de provincie Zuid-Holland was 2022 een memorabel jaar. Mede dankzij inzet van de directie is in mei van dat jaar is de EP opgericht en in de maanden daarop werden ook alle functies ingevuld. De EP ondersteunt de organisatie bij het groeien in privacy-volwassenheid en bij het voldoen aan de vereisten van de AVG. De EP is zich terdege bewust van haar rol en positie en heeft daarbij het juiste perspectief voor ogen. Dat laat onverlet dat het vooral de organisatie zelf is, die het bewust omgaan met persoonsgegevens tot een automatisme moet aanleren.

In 2023 is de provincie in organisatorisch opzicht overgegaan van een hiërarchisch model met afdelingen naar een zogenoemde opgavegerichte organisatie (OGO). Dit nieuwe organisatiemodel heeft gevolgen voor de wijze waarop de verantwoordelijkheden op het gebied van privacyregelgeving belegd zijn en beheerst kunnen worden.

In het oude organisatiemodel hadden de afdelingen in principe allemaal een of meerdere privacy-ambassadeurs, die als eerste lijn fungeerden in een “3 Lines of defence” model. Het nieuwe organisatiemodel bestaat uit enkele domeinen en veelheid aan individuele opdrachten. Met het indelen van de organisatie in een veel groter aantal op zichzelf staande eenheden dan voorheen, is het een opgave voor de organisatie om privacy op eenduidige en uniforme wijze te borgen door al deze eenheden heen (domeinen/opgaven/opdrachten).

Aanbeveling: leg de borging van privacy vast in beleid en (bedrijfsvoerings)instructies voor de opdrachten en opgaven.

In de AVG wordt ook aandacht besteed aan de technische en organisatorische maatregelen die een organisatie dient te treffen voor de bescherming van persoonsgegevens.



Hierin zit een overlap met het werk van het team Informatieveiligheid van de provincie Zuid-Holland. In organisatorisch en procesmatig opzicht is de afstemming tussen beide teams naar de mening van de FG nog niet voldoende geborgd. Ook met betrekking tot het accepteren van het toezicht van de FG op de technische maatregelen kan de provincie Zuid-Holland nog wel wat stappen zetten.

Aanbeveling: stimuleer en borg de afstemming in de samenwerking tussen de EP en het team Informatieveiligheid

Bewustwording en compliancy

Een terugkerend thema in het jaarverslag van de FG is de bewustwording en houding en gedrag van de organisatie ten opzichte van privacy en de wet- en regelgeving die ziet op de bescherming van persoonsgegevens.

In 2021 eindigde het organisatiebrede bewustwordingsprogramma dat ziet op informatieverwerking in brede zin inclusief privacy. De afgelopen twee jaren zijn besteed aan het formuleren van een nieuwe opdracht voor bewustwording en het op poten zetten van een nieuwe campagne. Dit betekende wel dat er, afgezien van enkele kleine bewustwordingsmomenten, er geen inzet is geweest op actieve bewustmaking binnen de provincie Zuid-Holland.
In zijn meest eenvoudige vorm, die effectief is en gemakkelijk een 100 procent bereik heeft, kan een e-learning worden ingezet. De provincie Zuid-Holland is al een aantal jaren bezig met het zoeken naar een Leer Management Systeem waarin ook de e-learning voor privacy een plaats kan krijgen en tevens e-learnings op andere gebieden. De selectie en aanschaf van een Leer Management Systeem is echter een uitgebreid en tijdrovend proces, daar waar de bewustwording op het gebied van privacy al lang gestart had moeten zijn en uitstel niet kan worden geduld.

Aanbeveling: voer met voorrang een verplichte e-learning voor privacy en informatieveiligheid in voor de gehele organisatie.

In het jaarverslag over 2021 omschreef de FG de houding van de organisatie ten opzichte van compliancy als cherry picking. Compliancy kan worden omschreven als het bevorderen van, en het (doen) toezien op de correcte naleving van externe en interne (rechts)regels. Regels en normen die de organisatie zelf stelt, horen daar uitdrukkelijk bij. De mate waarin een organisatie hieraan voldoet is mede relevant voor de integriteit van die organisatie. Juist als organisatie die graag als een betrouwbare overheid wil worden gezien is het voldoen aan deze externe en interne regels van groot belang. Ook gedurende de verslagperiode voor dit jaarverslag is het de FG opgevallen dat de provincie Zuid-Holland verbeterslagen kan maken met betrekking tot het naleven van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens. De noodzaak om dit te doen wordt nog te weinig gevoeld, getuige het nog onvoldoende naleven van vereisten uit de AVG door delen van de organisatie. Daarnaast raadt de FG de organisatie aan om meer aandacht te hebben voor de adviezen die er vanuit de EP worden gegeven.

Aanbeveling: stuur vanuit bestuur en (hoger) management op naleving van wet- en interne en externe regelgeving en geef daarbij zelf het goede voorbeeld.

Wet politiegegevens

In 2022 heeft de op grond van de Wpg verplichte externe audit plaats gevonden op de verwerkingen die vallen binnen deze wet. Het betreft daarbij de verwerkingen die de Buitengewone opsporingsambtenaren van de provincie Zuid-Holland verrichten in het kader van hun handhavingstaken. De toezichtstaken van de Boa's vallen onder het regime van de AVG.

De eerste externe audit leverde een afkeurend oordeel op van de auditors, hetgeen de provincie Zuid-Holland noopte tot het opstellen van een verbeterplan gevolgd door een heraudit in 2023. De uitkomsten van deze audit zijn op dit moment nog niet bekend bij de FG. Wel heeft de FG, bij zowel schriftelijke als fysieke controles, geconstateerd dat veel van de zaken die in het verbeterplan zijn genoemd ook daadwerkelijk zijn uitgevoerd.

Vooruitblik

Veranderende wijze van toezichthouden door de FG

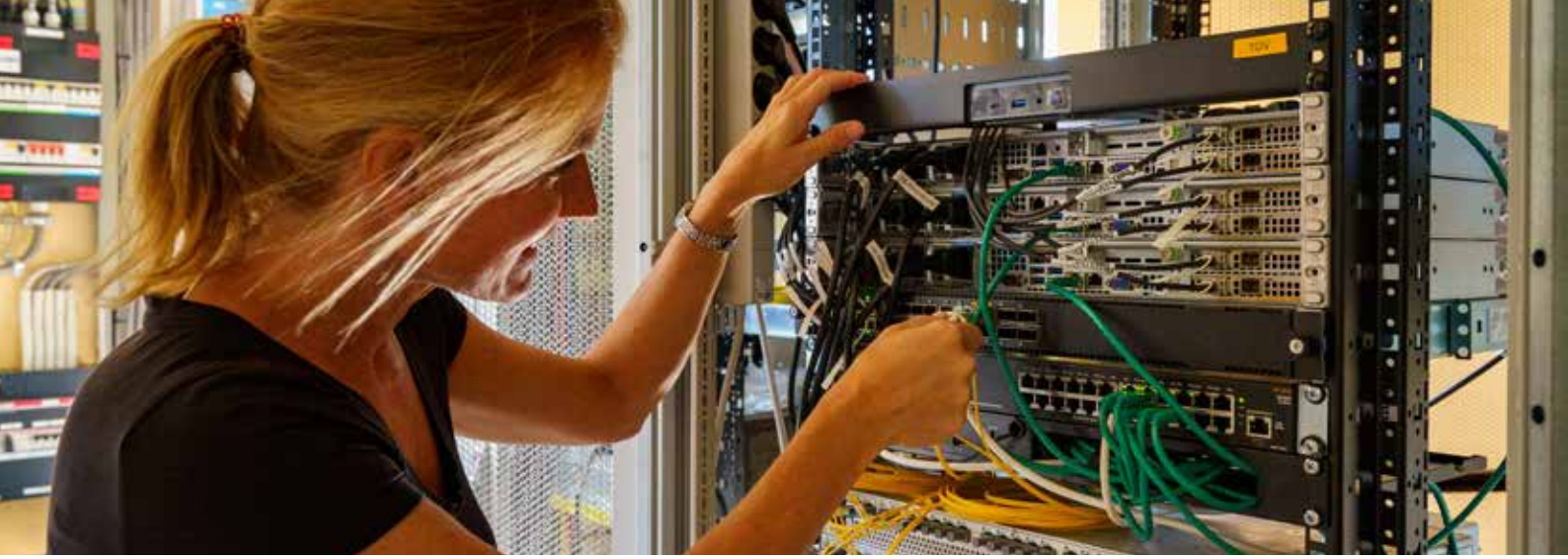
Met de komst van de EP kan de FG zich meer en meer gaan richten op zijn toezichthoudende taken. De FG voert onderzoeken uit op de naleving bij de provincie Zuid-Holland en, waar van toepassing, bij verwerkers en subverwerkers. Ook voor gegevensverwerking bij (sub)verwerkers is en blijft de provincie Zuid-Holland verantwoordelijk en valt de verwerking onder het nalevingstoezicht van de FG. In 2024 start de FG met het uitvoeren of doen uitvoeren van enkele audits op verwerkingen bij de provincie Zuid-Holland en enkele van haar (sub)verwerkers.

De FG voert systeemgericht toezicht uit op de processen/systemen rond, onder andere, de verantwoordingsplicht. De kwaliteit en borging van de verantwoordingsplicht is van belang voor een verdere inrichting van systeemgericht toezicht. Als een organisatieonderdeel over een goed werkend intern borgingssysteem (compliance management) beschikt, dan is het waarschijnlijker dat de organisatie de doelstellingen behaalt op het terrein van kwaliteit en gegevensbescherming.

Op grond van de wettelijke verantwoordingsplicht moeten alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens worden vastgelegd in een register van verwerkingsactiviteiten, voordat met de verwerking ervan wordt aangevangen. Dit centrale register toont inzichtelijk en overzichtelijk welke processen en activiteiten er met persoonsgegevens plaatsvinden, inclusief de verwerkingsdoelen en wettelijke grondslagen. De FG houdt toezicht op de kwaliteit en de naleving van de verplichting tot het bijhouden van het register van verwerkingsactiviteiten door de verwerkingsverantwoordelijke en de beheerders.
De FG houdt daarnaast toezicht op de uitvoering van de Data Protection Impact Assessments (DPIA's). Bij het opstellen van de DPIA wordt verplicht het advies (consultatie) ingewonnen van de FG, waarbij uiteindelijk ook een oordeel (appreciatie) wordt gevormd over de kwaliteit van de DPIA en de acceptatie van eventuele restrisico's. In 2024 zal de FG nog gerichter toezien op het naleven van de verantwoordingsplicht van de provincie Zuid-Holland en gebruik maken van zijn bevoegheden om toe te zien op het aanwijzen van verantwoordelijken in het vullen van met name het verwerkingsregister en het uitvoeren van DPIA's.

Daarnaast selecteert de FG (innovatieve en technologische) thema's om te onderzoeken. Bij een themagericht onderzoek wordt onderzoek gedaan naar één of meer specifieke aspecten bij meerdere onderdelen. Voor 2024 staat het thema generatieve AI op de toezichtagenda van de FG.

Behalve gepland toezicht worden ook ad hoc-toezichtbezoeken uitgevoerd naar aanleiding van incidenten, onregelmatigheden of datalekken. Meldingen van datalekken die een hoog risico opleveren voor de privacy van de betrokkenen, worden in afstemming met de FG ook extern gemeld aan de AP. Een datalek kan aanleiding vormen voor een onderzoek.



AI en algoritmes

De opkomst van kunstmatige intelligentie (AI) en algoritmes is een centraal punt van discussie geworden in zowel politieke kringen als de bredere samenleving. Deze aandacht wordt gerechtvaardigd door de alomtegenwoordigheid van algoritmes, die in toenemende mate worden ingezet, vaak onder het label van AI. Wat eens begon als een initiatief van private bedrijven, heeft zich nu verspreid naar publieke organisaties op alle niveaus van overheid en bestuur.

Het gebruik van AI en algoritmes brengt hoge verwachtingen met zich mee. De belofte van geavanceerde besluitvormingssystemen en gepersonaliseerde diensten heeft de verbeelding van velen gevangen. Echter, deze ontwikkeling heeft ook een scherpe toename gezien in de oproep voor passend toezicht op de implementatie van deze systemen.

De noodzaak voor toezicht komt voort uit verschillende zorgen. Ten eerste bestaat er bezorgdheid over mogelijke discriminatie en vooroordelen die ingebed kunnen zijn in de algoritmes zelf, wat kan leiden tot onrechtvaardige behandeling van individuen of groepen. Ten tweede roept het gebruik van AI vragen op over privacy en gegevensbescherming, aangezien deze systemen vaak afhankelijk zijn van grote hoeveelheden persoonlijke gegevens. Daarnaast zijn er ook zorgen over de transparantie en verantwoording van AI-systemen, aangezien hun complexiteit vaak hun innerlijke werking voor niet-experts verborgen houdt.

Het is duidelijk dat terwijl de mogelijkheden van AI en algoritmes zich blijven uitbreiden, het essentieel is om mechanismen te ontwikkelen die ervoor zorgen dat deze technologieën op een verantwoorde en ethische manier worden toegepast. Dit omvat niet alleen strikte regelgeving en toezicht, maar ook een voortdurende dialoog tussen beleidsmakers, technologen, maatschappelijke organisaties en het bredere publiek om de implicaties van deze technologische vooruitgang ten volle te begrijpen en aan te pakken.

Nieuwe wetgeving

In 2023 zijn er op het gebied van privacy een aantal nieuwe verordeningen en richtlijnen van kracht geworden.

Digital Governance Act (DGA)
Deze recent ingevoerde verordening, die op 24 september van kracht werd, omvat richtlijnen voor het delen van gegevens en data. Het hoofddoel is om:

- Een klimaat te scheppen waarin gegevens veilig en met vertrouwen gedeeld kunnen worden.
- Het vergroten van de beschikbaarheid van gegevens.
- Het faciliteren van het gemakkelijke hergebruik van gegevens.

Met behulp van een gestructureerd kader wordt een veilige omgeving gecreëerd voor het delen van gegevens, wat de ontwikkeling van nieuwe zakelijke modellen mogelijk maakt. Bovendien zal er een nationaal register worden opgesteld van erkende “data-altruïsten”. Dit zijn organisaties die gegevens verzamelen met het algemeen belang voor ogen, zoals gegevens die cruciaal zijn voor medisch-wetenschappelijk onderzoek. Dit register biedt de garantie dat de gegevens in betrouwbare handen zijn.

Op het moment van het schrijven van dit jaarverslag is de regering bezig met de implementatie van deze verordening.

Digital Market Act (DMA)

Deze wet is met name van toepassing op grote online platformen en daarom minder interessant voor de provincie Zuid-Holland in het naleven van deze verordening.

Network and Information Security Act (NIS2)

De Network and Information Security Verordening, ook bekend als de NIS2-verordening, vervangt de eerdere NIS-richtlijn. Het hoofddoel van deze nieuwe regelgeving is om de cyberbeveiliging en veerkracht van essentiële diensten binnen de lidstaten van de Europese Unie te versterken. In vergelijking met zijn voorganger heeft de NIS2 een breder toepassingsgebied, waardoor meer sectoren onder zijn regelgeving vallen. Bovendien legt de NIS2 strengere normen voor beveiliging op en vereist het meer gedetailleerde meldingen van incidenten.

In 2024 zullen daarnaast de volgende verordeningen en richtlijnen van kracht worden.

Digital Service Act (DSA)

Deze verordening is het zusje van de DMA en daarom minder interessant voor de provincie Zuid-Holland.

Data Act

Verwacht wordt dat de Data Act tegen het midden van 2024 van kracht zal worden. Deze wetgeving bepaalt dat gebruikers gedeeltelijk mede-eigenaar worden van de gegevens die worden gegenereerd door het Internet of Things. Gebruikers moeten te allen tijde zonder formele aanvraag toegang hebben tot deze gegevens, zoals die worden gegenereerd door bijvoorbeeld smartphones, slimme deurbellen en verlichting.

Bovendien biedt de verordening de mogelijkheid om een derde partij toegang te geven tot de gegevens om er waarde aan toe te voegen.

Daarnaast moeten online diensten en services zo worden ontworpen dat ze gegevens efficiënt met elkaar kunnen delen, waardoor het bijvoorbeeld gemakkelijker wordt om over te stappen van de ene clouddienst naar de andere.

AI Act

De focus van de AI Act ligt voornamelijk op AI-systemen die als hoog risico worden beschouwd. Een AI-systeem wordt als 'hoog risico' bestempeld als het valt onder bepaalde 'toepassingen' of 'categorieën', zoals migratie- en asielsystemen, kritieke infrastructuur en opleidingen en trainingen.

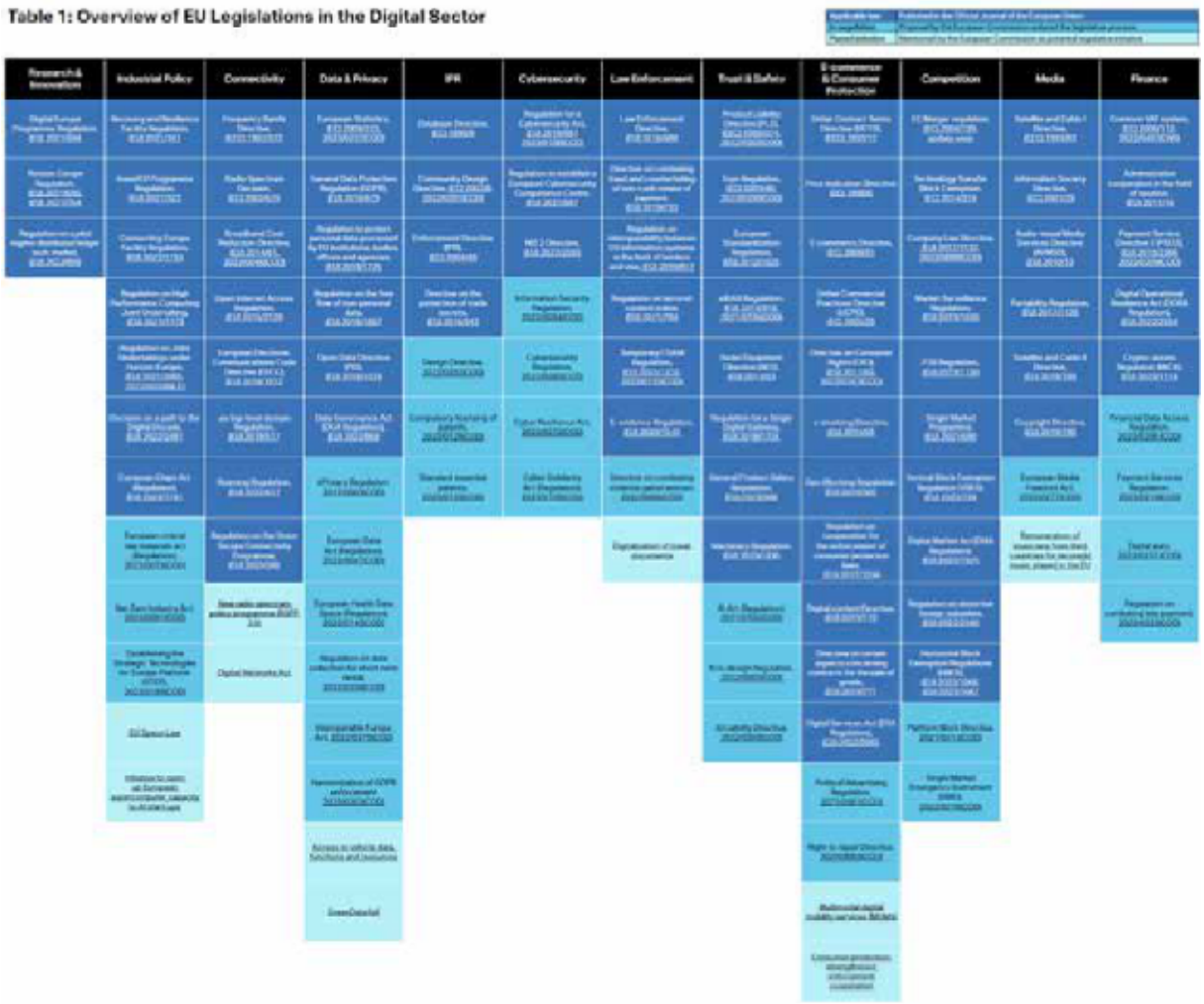
Er zijn twee soorten hoogrisico-toepassingen onderscheiden:
- AI-toepassingen met een hoog risico waarvoor zelfevaluatie verplicht is.
- AI-toepassingen met een hoog risico die door een externe instantie moeten worden getoetst op 'conformiteit'.

Voor 'biometrische systemen voor identificatie op afstand' is vastgesteld dat ze altijd door een externe instantie op conformiteit moeten worden getoetst (lijst 2). Voor andere hoogrisico-systemen is nog niet bepaald tot welke lijst ze behoren. De Autoriteit Persoonsgegevens (AP) adviseert dat alle AI-toepassingen die een hoog risico vormen, door een externe partij op conformiteit worden getoetst.

De AI Act verbiedt ook bepaalde toepassingen van AI-systemen die een onaanvaardbaar risico vormen voor de rechten en vrijheden van het individu, zoals social scoring en manipulatieve AI-systemen. Voor deze verboden, met name biometrische systemen, worden uitzonderingen geformuleerd in de AI Act. De AP benadrukt het belang van een volledig verbod op dergelijke toepassingen, zonder uitzonderingen, en pleit ervoor dat hier tijdens de onderhandelingen niet aan wordt getornd.

In de onderstaande tabel wordt een overzicht gegeven van het aantal wetten dat vanuit de EU voor ons van kracht zijn geworden (donkerblauw), binnenkort van kracht worden (blauw) of waarover nog wordt onderhandeld (lichtblauw). In de 4e kolom staan de wetten die op het terrein van privacy van toepassing zijn.

Table 1: Overview of EU Legislations in the Digital Sector



Conclusies

Zoals uit dit verslag zal spreken, waren de afgelopen jaren “zware jaren” voor de provincie Zuid-Holland op het gebied van naleving van wet- en regelgeving die zien op de bescherming van persoonsgegevens. De groei in de privacyvolwassenheid van de organisatie en haar medewerkers kan en moet worden versneld. De FG is echter hoopvol gestemd voor het jaar 2024. Met de uitgestoken hand van AP om de provincie Zuid-Holland te helpen in het verhogen van de privacyvolwassenheid kunnen in dit jaar goede stappen worden gezet in het voldoen aan de vereisten van de AVG. Ook de komst en vervolgens de inzet van de EP bieden perspectief tot een betere privacy huishouding van de provincie Zuid-Holland. Een voortdurende aandacht en inzet van (hoger) management en bestuur is daarbij van essentieel belang. Voldoende financiële middelen zijn daarbij ook een voorwaarde tot het kunnen bereiken van een minimale privacyvolwassenheid op niveau 3 cf. het model van het CIP.

Aanbeveling in dit verslag (samengevat)

Hieronder zijn de verschillende aanbevelingen die her en der verspreid zijn benoemd in dit jaarverslag nogmaals puntsgewijs weergegeven.

- Beleg privacy beter en duurzaam binnen het domein Bedrijfsvoering.
- Borg het proces rondom nieuwe verwerkingen zodanig dat privacy daarbij altijd een rol speelt.
- Publiceer een afgeslankte versie van het register van verwerkingsactiviteiten op de corporatewebsite.
- Beleg privacy en het uitvoeren van een DPIA in een vroeg stadium in de opgaven, zodat een DPIA geen belemmering hoeft te zijn in de voortgang van een opgave.
- Leg de borging van privacy vast in beleid en (bedrijfsvoerings)instructies voor de opdrachten en opgaven.
- Stimuleer en borg de afstemming in de samenwerking tussen de EP en het team Informatieveiligheid
- Voer met voorrang een verplichte e-learning voor privacy en informatieveiligheid in voor de gehele organisatie.
- Stuur vanuit bestuur en (hoger) management op naleving van wet- en interne en externe regelgeving en geef daarbij zelf het goede voorbeeld.

Lijst van afkortingen

AI	Artificiële Intelligentie
AP	Autoriteit Persoonsgegevens
CIP	Centrum voor Informatieveiligheid en Privacy Overheid
DPIA	Data Protection Impact Assessment
EP	Eenheid Privacy
FG	Functionaris voor Gegevensbescherming
GEB	Gegevensbeschermingseffectbeoordeling
GS	College van Gedeputeerde Staten
PS	Provinciale Staten
UAVG	Uitvoeringswet AVG
Wjsg	Wet justitiële en strafrechtelijke gegevens
Wpg	Wet politiegegevens

240300445