Auteurs: Aaf Stuijt LLM en Roswitha Talen LLM zijn beiden ervaren privacy juristen en trainers met een praktische inslag. Ze geven Wpg-trainingen aan boa's, hun beleidsmakers en toezichthouders. Ze begeleiden Wpg-audits en adviseren vaak met succes over complexe samenwerkingsvraagstukken. Voor contact met Aaf en Roswitha mail naar contact@aafstuijt.nl en info@talenjuridischadvies.nl.

Van BIO naar boa (en weer terug)

De bescherming van persoonsgegevens gaat over technische en organisatorische beveiligingsmaatregelen die deze gegevens moeten beschermen tegen onbevoegde, onbedoelde en onnodige verwerking. Andere beschermings-maatregelen zijn van juridische aard en gaan over het hebben van de juiste rechtsgronden, doelbinding en wettelijke basis.

Als we spreken van informatiebeveiliging bij de overheid, komen we al snel uit bij de Baseline Informatiebeveiliging Overheid (BIO). De BIO is de opvolger van zowel de Baseline Informatiebeveiliging Rijk (BIR) als de Baseline Informatiebeveiliging Gemeenten (BIG). De informatiebeveiligers van zowel het rijk als de gemeenten hebben de handen ineengeslagen om gezamenlijk tot één baseline te komen. Hulde voor dit staaltje samenwerken waarmee het bewijs is geleverd dat de weg kan worden gevonden, als de wil er maar is. Alles wat je wil weten over de BIO staat op de website (1).

Hoewel de BIO steeds meer aan bekendheid wint, komt het nog weleens voor dat medewerkers bij de overheid glazig kijken wanneer privacy-adviseurs naar de BIO verwijzen. Wat voor de BIO geldt, geldt ook een beetje voor de Algemene Verordening Gegevensbescherming (AVG). De AVG krijgt steeds meer bekendheid, maar er zijn nog steeds veel mensen die slechts de klok hebben horen luiden, maar nog op zoek zijn naar de klepel. Daarom toch een heel korte introductie.

Pakket uit 2016

Op 25 mei 2016 is er een Europees pakket aan wetgevingsinstrumenten vastgesteld. Dit pakket beoogt uniformering van de bescherming van personen bij de verwerking van gegevens die indirect of direct naar hen herleidbaar zijn. Het pakket bestaat voor zover hier relevant uit de AVG en de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad (2). Deze wetgevingsinstrumenten samen worden wel aangeduid als het Europese gegevensbeschermingspakket uit 2016. Het is niet toevallig dat ze samen het licht zagen omdat ze eenzelfde doel hebben: ze beogen een uniform beschermingsniveau te bieden aan de betrokkenen van wie de persoonsgegevens worden verwerkt. Hoewel het doel hetzelfde is hebben deze verschillende wetgevingsinstrumenten wel een andere reikwijdte.

AVG reikwijdte

De AVG is een Europese wet die rechtstreeks werkt in de Europese lidstaten maar verrassend genoeg ook daarbuiten. Dat is geregeld in artikel 3 van de AVG waar de territoriale reikwijdte van de AVG wordt bepaald. Zo is de AVG ook van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een organisatie met een vestiging in de Europese Unie, ongeacht of de verwerking in de Unie plaatsvindt. Dat betekent dat alle organisaties die een al dan niet substantiële vestiging hebben ergens in Europa (denk aan de Amsterdamse Zuidas) onder de werking van de AVG zijn gebracht (3).

De tweede uitbreiding van de territoriale reikwijdte is de verwerking van persoonsgegevens van betrokkenen die zich in de Europese Unie bevinden, door een niet in de Europese Unie gevestigde organisatie. Deze uitbreiding is beperkt tot twee situaties. Het moet gaan om verwerkingen van persoonsgegevens die verband houden met het aanbieden van goederen of diensten aan deze betrokkenen al dan niet tegen betaling. Of het moet gaan om het monitoren van hun gedrag, voor zover dit gedrag in de Europese Unie plaatsvindt (4).

De derde uitbreiding van de territoriale reikwijdte van de AVG is meer formeel van aard. De AVG is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de Europese Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lid-statelijke recht van toepassing is. Denk aan een schip dat onder de Nederlandse vlag vaart.

Naast genoemde territoriale uitbreidingen, wordt de materiële reikwijdte van de AVG tegelijkertijd beperkt. Die beperkingen vinden we in artikel 2 van de AVG. Daar staat voor zover hier relevant: 'Deze verordening is niet van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.' Dat betekent huiselijk gezegd dat de AVG in deze gevallen opzij wordt gezet.

Wpg reikwijdte

De 'verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten', is in Nederland geregeld in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). De Wpg en Wsjg zijn de Nederlandse implementatie van de genoemde Richtlijn (EU) 2016/680 uit het Europese wetgevingspakket

pakket uit 2016. Persoonsgegevens die worden verwerkt onder de Wpg noemen we politiegegevens, persoonsgegevens die worden verwerkt onder de Wjsg noemen we justitiële of strafvorderlijke gegevens. In dit artikel beperken we ons tot politiegegevens. Het verwerken van politiegegevens kan nooit dus plaatsvinden onder de AVG maar alleen onder de Wpg.

Verwerkingsverantwoordelijke AVG en Wpg

Het verwerken van persoonsgegevens onder de AVG mag alleen in opdracht van een verwerkingsverantwoordelijke. En dat kan volgens de AVG werkelijk iedereen zijn; 'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'. In de Wpg is de verwerkingsverantwoordelijke expliciet benoemd en beperkt tot een klein groepje. Voor de politie is het bijvoorbeeld de korpschef, voor de Rijksrecherche het College van procureurs-generaal (PG's) en voor de Koninklijke Marechaussee (KMar) de minister van Defensie.

Mandaat of bevoegdheid AVG

Je zult begrijpen dat een verwerkingsverantwoordelijke doorgaans niet zelf de persoonsgegevens verwerkt. Via mandaatbesluiten geeft de verwerkingsverantwoordelijke aan welke medewerkers bevoegd zijn om (welke) persoonsgegevens namens hem of haar te verwerken. De verwerkingsverantwoordelijke onder de AVG is helemaal vrij in het mandateren van de verwerkingen aan wie dan ook. Het mooie van mandaat is namelijk dat de bevoegdheden en de aansprakelijkheid altijd in handen blijven van de verwerkingsverantwoordelijke zelf. Anders gezegd: een verwerkingsverantwoordelijke kan de eigen verwerkingsverantwoordelijkheid en de aansprakelijkheid nooit delegeren. Dat is ook de kern van de privacybescherming: iemand is volgens wet verantwoordelijk voor het naleven van de wet en de regels en die kan deze verantwoordelijkheid nooit afschuiven, ontlopen of negeren. Denk aan aansprakelijkheid en boetes.

Houd ook in gedachten dat de AVG niet alleen geldt voor de overheid maar ook voor het bedrijfsleven, private organisaties en zelfs voor onszelf. Immers, elke natuurlijke persoon die persoonsgegevens verwerkt en die zich niet kan beroepen op een beperking van de materiële reikwijdte van de AVG zoals genoemd in artikel 2 AVG is een verwerkingsverantwoordelijke (5).

Mandaat of bevoegdheid Wpg

In de Wpg is dat heel anders geregeld. Bij opsporen en vervolgen mogen er om begrijpelijke redenen grotere inbreuken worden gemaakt op de persoonlijke levenssfeer. Deze ruimere bevoegdheden om inbreuk te maken op de persoonlijke levenssfeer gaan vergezeld van extra privacywaarborgen die expliciet zijn opgenomen in de wet. Een van deze waarborgen is dat deze ruimere bevoegdheden om inbreuk te maken zijn toegekend aan een afgebakende groep mensen. Het primaat van opsporing en vervolging is in Nederland huiselijk gezegd neergelegd bij politie en justitie. Eigenrichting wordt niet zo op prijs gesteld in ons democratische rechtsstelsel. Om die reden zijn de verwerkingsverantwoordelijken voor de Wpg limitatief opgesomd in de wet. Hetgeen hiervoor is opgemerkt over mandaat bij verwerkingsverantwoordelijken geldt ook voor deze limitatieve groep verwerkingsverantwoordelijken.

Daar komt nog bovenop dat de feitelijke verwerking van politiegegevens is voorbehouden aan een selecte groep mensen die in artikel 1 van de Wpg worden aangeduid als 'ambtenaren van politie'. Deze ambtenaren van politie zijn anders dan wat je in het spraakgebruik zou verwachten: 'de ambtenaar, bedoeld in artikel 2 van de Politiewet 2012, alsmede de ambtenaar van de Koninklijke marechaussee voor zover werkzaam ter uitvoering van de politietaak, bedoeld in onderdeel a, en indien artikel 46 wordt toegepast, de ambtenaar, werkzaam bij de in dat artikel genoemde dienst en de ambtenaar, bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering'.

Uit bovenstaande volgt dat de Wpg ten opzichte van de AVG de groep verwerkingsverantwoordelijken limiteert en extra eisen stelt aan de personen die politiegegevens daadwerkelijk verwerken.

Mismatch

De oplettende lezer constateert nu een discrepantie. We

hebben hier vier verschillende soorten ambtenaren van politie (Politie, KMar, Bijzondere opsporingsdiensten en Bijzondere opsporingsambtenaren), terwijl we drie soorten verwerkingsverantwoordelijken hebben (korpschef, College van PG's, minister van Defensie). Hoe verhouden deze verwerkingsverantwoordelijken zich tot de genoemde ambtenaren van politie? Er lijkt sprake te zijn van een mismatch.

Deze ogenschijnlijke mismatch is veroorzaakt doordat in de eerdere versies van de Wpg niet alle groepen opsporingsambtenaren waren opgenomen. Opsporingsambtenaren werkzaam bij de bijzondere opsporingsdiensten (bod'en) en buitengewoon opsporingsambtenaren (boa's) zijn later toegevoegd aan het oorspronkelijke rijtje van politie, Rijksrecherche en KMar. In een van de slotbepalingen van de Wpg (artikel 46) is nu bepaald dat de opsporingsambtenaren die daar zijn genoemd ook politiegegevens verwerken. In twee algemene maatregelen van bestuur (dit noemen we een Besluit) is dit nader uitgewerkt. Een Besluit voor de opsporingsambtenaren van de bod'en en een Besluit voor de boa's.

Besluit politiegegevens bod'en

In het Besluit politiegegevens bod'en staat expliciet wie de verwerkingsverantwoordelijken zijn bij de vier Bijzondere opsporingsdiensten die Nederland rijk is:

1. Belastingdienst/Fiscale Inlichtingen- en Opsporingsdienst: onze minister van Financiën;
2. Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport: onze minister van Infrastructuur en Waterstaat;
3. Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit: onze minister van Landbouw, Natuur en Voedselkwaliteit;
4. Directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid: onze minister van Sociale Zaken en Werkgelegenheid.

Saillant detail: de ambtenaren van politie werkzaam bij een bod zijn geen bijzondere opsporingsambtenaren maar algemene opsporingsambtenaren in dienst bij een Bijzondere opsporingsdienst (6).

Besluit politiegegevens boa's

De ambtenaar bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering is de boa. Om erachter te komen wie de verwerkingsverantwoordelijken van de boa's zijn, moet je naar het Besluit politiegegevens boa's en het Besluit boa. Daarin staat dat de werkgever van de boa de verwerkingsverantwoordelijke is. Het is dus deze werkgever die aan de lat staat om de verplichtingen die voortvloeien uit de Wpg na te leven en niet de boa's zelf. De boa's roeien met de riemen die ze krijgen van hun werkgever. Naleven van de Wpg-verplichtingen door de werkgevers van de boa's heeft ongetwijfeld een positieve invloed op de kwaliteit van de werkzaamheden van de boa's. Dat positieve effect zal zich ook uitstrekken tot de bescherming van de persoonlijke levenssfeer van de betrokkenen van wie politiegegevens worden verwerkt.

Wpg-verplichtingen

De materiële verplichtingen die voortvloeien uit de Wpg zijn grotendeels vergelijkbaar met de verplichtingen die we kennen uit de AVG. Een aantal zaken zijn explicieter geregeld en een aantal zaken zijn echt anders. Naast de materiële verplichtingen kent de Wpg in § 5 en § 7 nog enkele expliciete toezichtbepalingen. In 2019 is het verwerken van persoonsgegevens door boa's onder de Wpg gebracht. Tot die tijd verwerkten boa's persoonsgegevens onder de AVG. Dat betekent ook dat de werkgevers van de boa's vanaf dat moment de Wpg moeten naleven. En dat brengt extra verplichtingen met zich mee. Zoals een auditverplichting waarbij de audit moet worden uitgevoerd door een externe onafhankelijke en ter zake deskundige IT-auditor. De eerste audit moet in 2021 worden uitgevoerd.

Hierna gaan we kort in op enkele van deze verplichtingen met verwijzing naar het normenkader zoals NOREA dat hanteert (7).

Registerplicht

De registerplicht uit de Wpg komt grotendeels overeen met de registerplicht uit de AVG. Zie onderstaande overzicht voor de verplichtingen van de verwerkingsverantwoordelijke ten aanzien van een registerplicht waarbij de relevante wetteksten naast elkaar zijn gezet. Zoek de verschillen:

WPG	AVG	Conform
de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;	de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;	Ja
de doelen van de verwerking;	de verwerkingsdoeleinden;	Ja
de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;	de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;	Ja
een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;	een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;	Ja
in voorkomend geval, het gebruik van profilering;		Nee
in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie;	indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;	Ja
een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van		Nee
doorgiften, waarvoor de politiegegevens bedoeld zijn;		
zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;	indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;	Ja
zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a	indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.	Ja
de toekenning van de autorisaties, bedoeld in artikel 6		Nee

Figuur 1 – Registerplicht.

Artikel 32	WPG
1	De verwerkingsverantwoordelijke draagt zorg voor de schriftelijke vastlegging van:
a	de doelen van de onderzoeken, bedoeld in artikel 9, tweede lid;
b	de verstrekking of doorgifte van politiegegevens op grond van paragraaf 3, met uitzondering van de verstrekking, bedoeld in artikel 17 en artikel 24, eerste en tweede lid, indien dit zich niet verdraagt met het belang van de veiligheid van de staat;
c	de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid;
d	een inbreuk op de beveiliging van persoonsgegevens, bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.
2	Bij de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie, bedoeld in artikel 17a, tweede lid, onderdeel b, en derde lid, omvat de schriftelijke vastlegging de datum en tijd van doorgifte, informatie over de ontvangende bevoegde autoriteit, de reden van doorgifte en de doorgegeven gegevens zelf.
3	De verantwoordelijke draagt zorg voor de schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de Autoriteit persoonsgegevens.
4	De politiegegevens, bedoeld in het eerste lid, worden bewaard tenminste tot de datum waarop de laatste controle, bedoeld in artikel 33, is verricht.
5	Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de wijze van vastlegging.

Figuur 2 - Documentatieplicht.

Documentatieplicht

De documentatieplicht ontbreekt expliciet in de AVG. Impliciet is die er natuurlijk wel. Hoe kan de verwerkingsverantwoordelijke anders voldoen aan de verantwoordingsverplichtingen uit artikel 5 tweede lid en artikel 24 van de AVG?

In de Wpg is de documentatieplicht opgenomen in artikel 32 en bestaat uit de volgende onderdelen:

Loggingsplicht

Daar kunnen we kort over zijn. Deze expliciete verplichting is in Nederland nog niet in werking getreden maar dat zal niet altijd zo blijven. Voor nu laten we het daarom buiten beschouwing. Het is wel goed om je te realiseren dat het niet volledig implementeren van Europese richtlijnen niet geheel vrijblijvend is. De burger die hier last van heeft kan dan bij de rechter een rechtstreeks beroep doen op de richtlijn.

Artikel 33	Audit
1	De verwerkingsverantwoordelijke doet de uitvoering van de bij of krachtens deze wet gegeven regels controleren door middel van het periodiek doen verrichten van privacy audits.
2	De verwerkingsverantwoordelijke zendt een afschrift van de controleresultaten van de privacy audits aan de Autoriteit persoonsgegevens.
3	Indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens deze wet bepaalde, laat de verwerkingsverantwoordelijke binnen een jaar een hercontrole uitvoeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. Het tweede lid is van overeenkomstige toepassing.
4	Eenieder die betrokken is bij een controle als bedoeld in het eerste of derde lid is verplicht tot geheimhouding van de persoonsgegevens waarover hij de beschikking heeft gekregen, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of zijn taak daartoe noodzaakt.
5	Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld betreffende de inhoud en wijze van uitvoering van de controles, bedoeld in het eerste en derde lid.

Figuur 3 - Auditplicht.

Auditplicht

De expliciete auditverplichting in de Wpg is een groot verschil ten opzichte van de AVG. Waar de AVG volstaat met het sec noemen van de verplichting om verantwoording af te leggen en transparant te zijn gaat de Wpg een stuk verder. De Wpg vult het voldoen aan die verplichting in artikel 33 verder in. Let ook op de actieve rol van de AP bij deze Wpg-audits.

Uitvoering Wpg-audit

Hoe de Wpg-audits precies moeten worden uitgevoerd en door wie, is uitgewerkt in lagere regelgeving. Zie artikel 6:5 van het Besluit politiegegevens en de Regeling periodieke audit politiegegevens. In deze regeling worden de regels voor het uitvoeren van een externe en interne audit vastgesteld. De Wpg-audit is bijvoorbeeld altijd een IT-audit die moet worden uitgevoerd door een daartoe geautoriseerde en gekwalificeerde IT-auditor (Registered EDP Auditors). Kortheidshalve wordt volstaan met de verwijzing naar deze regels.

NOREA

De beroepsorganisatie van IT-auditors (edp-ers of RE's) NOREA heeft enige tijd geleden een normenkader ontwikkeld waarbij invulling kan worden gegeven aan de toets op de naleving van de AVG. NOREA heeft nu ook ingespeeld op de Wpg-auditverplichting voor werkgevers van boa's. In juni 2021 is een NOREA Handreiking Privacy audit Wpg voor boa's gepubliceerd. Deze Wpg handreiking is niet geënt op de al bestaande NOREA Handreiking Privacy Control Framework voor de AVG en kan dus zelfstandig worden gebruikt. Het enige dat nu nog rest is een fit-gap analyse tussen de BIO en de Wpg. Daar wordt al ergens in het netwerk aan gewerkt. Wederom hulde!

De auditverplichting uit de Wpg voor werkgevers van boa's is mogelijk een verrassing voor veel werkgevers. Wanneer het een overheidswerkgever betreft, zal hij moeten voldoen aan de BIO. Dat helpt omdat daarmee de naleving van veel verplichtingen uit de Wpg zullen worden getoetst. De naleving van de extra verplichtingen uit de Wpg kunnen worden getoetst met behulp van de NOREA-handreiking. IT-auditors met kennis van de BIO en de Wpg zullen schaars zijn. Haast is geboden omdat het einde van 2021 snel in zicht komt.

Referenties

(1) https://bio-overheid.nl

(2) De Wet justitiële en strafvorderlijke gegevens (Wjsg) laten we hier buiten beschouwing.

(3) We gaan hier niet in op de precieze afbakening van het Europese territoir in juridische zin.

(4) Je kunt je afvragen in hoeverre deze uitbreiding ook van toepassing is op de overheid. Een interessante vraag die te ver strekt voor het doel van dit artikel.

(5) Er staat in artikel 2 AVG nog een beperking van de reikwijdte: door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.

(6) https://www.justis.nl/producten/boa/BOD/bod.aspx

(7) www.norea.nl