pro facto

Samenvatting

Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid

Groningen/Den Haag, 22 juni 2022

www.pro-facto.nl

rijksuniversiteit groningen

Colofon

Pro Facto
Ossenmarkt 5
9712 NZ Groningen
www.pro-facto.nl
info@pro-facto.nl
050-3139853

Auteurs	Heinrich Winter, Thijs Drouen, Marlies van Eck, Lisanne Kramer, Bieuwe Geertsema, Jeanne Cazemier, Chantal Ridderbos-Hovingh
Opdrachtgever	WODC
Datum	22 juni 2022

Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum – uitgevoerd door Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs en Hooghiemstra & Partners, strategisch en juridisch adviesbureau op het raakvlak van data en recht.

Begeleidingscommissie:
Prof.dr.mr. Gerrit-Jan Zwenne (voorzitter; Universiteit Leiden)
Dr. Jef Ausloos (UvA)
Mr. Paul Breitbarth (Catawiki)
Mr. Taetske van der Reijt (DWJZ, JenV)
Dr. Leontien van der Knaap (WODC)

Voor de inhoud van het rapport zijn de onderzoekers verantwoordelijk. Het leveren van een bijdrage (als medewerker van een organisatie of als lid van de begeleidingscommissie) betekent niet automatisch dat de betrokkene instemt met de gehele inhoud van het rapport. Dat geldt eveneens voor het ministerie van Justitie en Veiligheid en zijn minister.

Samenvatting

Inleiding

De Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is op 25 mei 2018 in werking getreden. Volgens artikel 50 UAVG zendt de minister binnen drie jaar een verslag aan de Staten-Generaal over de effecten en de uitvoering in de praktijk van de UAVG. Deze evaluatie richt zich daarmee op beide elementen: hoe verloopt de uitvoering en wat zijn de effecten van de wet?

De UAVG en de Algemene verordening gegevensbescherming (AVG) vervangen Richtlijn 95/46/EG en de Wet bescherming persoonsgegevens (Wbp). De Nederlandse wetgever heeft ervoor gekozen in de UAVG – daar waar de verordening ruimte laat voor nationale keuzes, of met het oog op een nadere invulling van regels – voort te bouwen op het normenkader uit Richtlijn 95/46/EG en de Wbp. Voor het ontwikkelen van een nieuw kader zou volgens de memorie van toelichting de tijd ontbreken. Een ander argument voor zo klein mogelijke verschillen met de situatie van voor de AVG was de wens voor een soepele overgang van de oude naar de nieuwe situatie.[1] De wetgever voorzag daarom in een evaluatie (neergelegd in artikel 50 UAVG) waarvan de uitkomsten gebruikt kunnen worden in een gesprek over de noodzaak van wijziging van de wet. Daarmee is de reikwijdte van deze evaluatie gegeven.

Daarnaast betreft het onderzoek de vraag in welke mate de meldplicht datalekken wordt nageleefd en in hoeverre de boetebevoegdheid van de toezichthouder bijdraagt aan een doelmatige en doeltreffende uitvoering en handhaving van de UAVG. Op 1 januari 2016 – terwijl de AVG op het punt stond te worden vastgesteld – werd de Wbp uitgebreid met de meldplicht datalekken en kreeg de toezichthouder, vanaf dat moment aangeduid als Autoriteit Persoonsgegevens (AP), een bevoegdheid tot het opleggen van een bestuurlijke boete. Deze onderdelen zijn aan de evaluatie toegevoegd naar aanleiding van de motie van de Kamerleden Schouw en Segers uit 2015 waarin de regering wordt verzocht de Wet meldplicht datalekken en boetebevoegdheid binnen vier jaar na inwerkingtreding te evalueren.[2] De boetebevoegdheid en de meldplicht datalekken zijn op 25 mei 2016 in de AVG opgenomen; de AVG is vanaf 25 mei 2018 van toepassing.

[1] *Kamerstukken II*, 2017/18, 34851, nr. 3, p. 4.
[2] *Kamerstukken II* 2015/16, 33662, nr. 20.

De UAVG is de organisatiewet die de toezichthouder, de AP, instelt en die regels stelt over haar inrichting (organen, onafhankelijkheid etc.) en haar taken en bevoegdheden. Verder sluit de UAVG aan bij de Wbp op punten waarvoor de AVG ruimte biedt voor de nationale wetgever om aan te vullen. Het is van belang vast te stellen dat het onderzoek naar de UAVG met nadruk geen onderzoek is naar de AVG. Ook is het geen evaluatie van de toezichthouder. Voorzover de UAVG fungeert als instellingswet voor de AP hebben we die bepalingen buiten beschouwing gelaten in het onderzoek. Dat is een belangrijk uitgangspunt, maar tegelijkertijd valt niet te vermijden dat het functioneren van de UAVG raakt aan de AVG en dat de effectiviteit van de bestuurlijke boete en van de meldplicht datalekken beïnvloed wordt door de manier waarop de AP het toezicht en de handhaving uitoefent. Helemaal is dus niet te vermijden dat het onderzoek daarmee ook de AVG en de AP raakt.

Deze evaluatie betreft daarmee:

— de werking van de UAVG; en
— de naleving en effectiviteit van de meldplicht datalekken en de toepassing en effectiviteit van de bestuurlijke boete.

Vraagstelling

De overkoepelende vraag die in het onderzoek centraal staat luidt als volgt:

Hoe werden in de periode 2018 - 2020 de normen van de UAVG nageleefd en in hoeverre heeft de UAVG bijgedragen aan een doelmatige en doeltreffende uitvoering en handhaving van de AVG?

Het onderzoek is uitgevoerd langs de lijnen van de volgende zestiental onderzoeksvragen.

1. Hoe beoordelen juristen, de AP en verwerkers van persoonsgegevens de duidelijkheid en toegankelijkheid van de UAVG?
2. In hoeverre worden de normen van de UAVG verduidelijkt door de AP en de jurisprudentie?
3. Welke informatie wordt op welk moment aan de verschillende doelgroepen gegeven en op welke manier? Wat is de rol van de AP hierbij?
4. Hoe beoordelen juristen, de AP en verwerkers van persoonsgegevens de uitvoerbaarheid van de UAVG?
5. Hoe beoordelen juristen, de AP en verwerkers van persoonsgegevens de handhaafbaarheid van de UAVG?
6. Hoe leven verwerkers van persoonsgegevens de bepalingen van de UAVG na?
7. In welke mate wordt de meldplicht datalekken nageleefd door verwerkers van persoonsgegevens?
8. Wat is de rol van de Functionaris voor Gegevensbescherming binnen organisaties, onder meer bij de naleving van de meldplicht?
9. In hoeverre heeft de jurisprudentie preventieve werking voor de naleving van de bepalingen van de UAVG en de meldplicht datalekken en hoe zou deze kunnen worden vergroot?
10. Hoe ziet de toezichtstrategie van de AP er uit?
11. Hoe luidt het handhavingsbeleid van de AP?
12. Op welke wijze vinden toezicht en handhaving door de AP in de praktijk plaats?

13. Hoe worden bij het uitoefenen van de boetebevoegdheid door de AP de ernst van de normschending, de mate van verwijtbaarheid en een passende wijze van optreden bepaald?
14. In hoeverre draagt de boetebevoegdheid en het toepassen daarvan door de AP bij aan een doelmatige en doeltreffende uitvoering en handhaving van de AVG?
15. Is er aanleiding tot een wijziging van de toepassing van de bevoegdheden door de AP en zo ja, in welk opzicht?
16. Hoe beoordelen juristen, de AP en verwerkers van persoonsgegevens de mate waarin de UAVG de ruimte heeft benut die de AVG laat voor nationale keuzes bij de uitvoering van de AVG?

Aanpak

Vooronderzoek
We zijn het onderzoek gestart met een oriëntatie op het onderwerp door het bestuderen van relevante literatuur en documenten, zoals de wetsgeschiedenis van de UAVG, (juridische) commentaren op de regeling, jaarverslagen van de AP, de evaluatie van de AVG door de Europese Commissie van juli 2020 en de consultatie van het wetsvoorstel tot wijziging van de UAVG.[3]

Tijdens het vooronderzoek zijn we ook gestart met de juridische analyse en het jurisprudentieonderzoek dat mede als input diende voor het vragenlijstonderzoek en de andere empirische onderzoeksmethoden. In de eerste fase van het onderzoek is gesproken met (oud-)wetgevingsjuristen en beleidsmedewerkers van het ministerie van JenV met de UAVG in portefeuille, met enkele academisch experts en met de voorzitter van het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG).[4]

In deze fase van het onderzoek wilden we ook een oriënterend gesprek voeren met de voorzitter van het college van de Autoriteit Persoonsgegevens (mr. Aleid Wolfsen). Wegens bezwaren van de Autoriteit Persoonsgegevens met betrekking tot de totstandkoming van de opdracht, en de aard, opzet en scope van het onderzoek en de betrokkenen daarbij, besloot de AP na meerdere gesprekken tussen vertegenwoordigers van het departement en het WODC en medewerkers van de AP aanvankelijk in het geheel niet mee te willen werken aan het onderzoek. Later werd het alsnog mogelijk een concepteindtekst met vragen voor te leggen. In reactie daarop leverde de AP uitvoerig commentaar en werden antwoorden op gestelde vragen gegeven. De onderzoekers hebben in ruime mate hun voordeel kunnen doen met de schriftelijke reactie van de AP, die op verschillende plaatsen tot aanvulling op de tekst heeft geleid.

Na de weigering de AP medewerking te verlenen aan het onderzoek werd de aanpak van het onderzoek in afstemming met de begeleidingscommissie aangepast. Dat is gebeurd op twee punten. Als gevolg van de weigering van de AP kon geen gebruik gemaakt worden van het FG-register van de AP voor het vragenlijstonderzoek onder Functionarissen voor Gegevensbescherming (FG's). De Vereniging Privacyrecht en het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG) bleken bereid hun aangesloten leden te vragen aan de digitale enquête deel te nemen. Dossieronderzoek naar boetebesluiten en meldingen datalekken bij de AP kon ook niet worden uitgevoerd. Daarom is gekozen voor het uitvoeren

[3] Bijlage 2 geeft een overzicht van geraadpleegde bronnen.
[4] Een overzicht met alle gesprekspartners gedurende de evaluatie is opgenomen in bijlage 2.

van enkele casestudy's naar besluiten en meldingen waaraan via de algemene pers bekendheid is gegeven. Verder is met veel respondenten gesproken over de toepassing van de UAVG en van de meldplicht datalekken en de boetebevoegdheid.

Juridische analyse en jurisprudentieonderzoek
De juridische deelonderzoeken zijn vanaf het begin van het project vormgegeven. Op die manier konden de eerste bevindingen ook worden benut voor de opzet van het vragenlijstonderzoek, waarop de begeleidingscommissie commentaar heeft geleverd, en de samenstelling van de itemlijsten voor de interviews. In het kader van de juridische deelonderzoeken zijn gesprekken gevoerd met verschillende academische experts, in het gegevensbeschermingsrecht gespecialiseerde advocaten en met Staatsraden van de Raad van State.

Vragenlijstonderzoek
In het vragenlijstonderzoek is een groot aantal FG's (naar schatting de tweeduizend FG's die aangesloten zijn bij de Vereniging Privacyrecht en het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG)) aangeschreven met het verzoek aan het digitale surveyonderzoek mee te werken. Uiteindelijk is een reactie ontvangen van 190 FG's, die werkzaam zijn voor bestuursorganen (24%), maatschappelijke instellingen (38%) en bedrijven (37%). Deze verdeling van de respondenten komt overeen met de verdeling in de totale populatie in ons land.

Verdiepende interviews
We voerden 33 verdiepende interviews, waaronder interviews met het management van een aantal organisaties (vijf), en verder met FG's (tien), advocaten (vijf), rechters (drie), enkele onafhankelijke experts, zoals academici (vijf) en (oud-)medewerkers van ministeries. Hen bevroegen we op hun opvattingen over de begrijpelijkheid van de normen van de UAVG en de toepasbaarheid en handhaafbaarheid daarvan.

Casestudy's
We voerden een zestal casestudy's uit om ons van begin tot eind een beeld te vormen van een aantal toezichts- en handhavingstrajecten waarbij de meldplicht datalekken en/of het instrument van de bestuurlijke boete aan de orde waren. We bestudeerden een aantal casus die in de landelijke pers publiciteit kregen. Twee casus betroffen het toezicht en de handhaving van een datalek: bij Uber en de GGD GHOR. In drie gevallen ging het om overtreding van andere bepalingen van de AVG: Belastingdienst/BTW-nummer, VoetbalTV en BKR. Tot slot is onderzoek gedaan naar de totstandkoming van de Gedragscode Gezondheidszorg, gelet op het belang van gedragscodes voor de invulling van de open normen uit de (U)AVG binnen sectoren.

Hieronder wordt op de bevindingen en conclusies van het onderzoek ingegaan.

Algemeen: de systematiek

De Uitvoeringswet AVG, is een Nederlandse wet die de Europese Algemene Verordening Gegevensbescherming aanvult. Het onderzoek maakt duidelijk dat de UAVG eigenlijk maar een beperkte betekenis heeft. Duidelijk is in ieder geval dat de wet geen nadere invulling biedt aan de AVG normen. Dat is wellicht begrijpelijk gelet op de ontstaansgeschiedenis van de UAVG, de beperkte tijd die voor de totstandkoming beschikbaar was en de keuze voor een 'beleidsneutrale' omzetting van de bestaande normen die destijds is gemaakt. Maar daarmee is de toegevoegde waarde van de UAVG slechts beperkt.

In de systematiek van het gegevensbeschermingsrecht werd in het samenstel AVG, UAVG en sectorale gedragscodes juist van die gedragscodes wel een operationalisering van de normen in het gegevensbeschermingsrecht verwacht. Tegen die achtergrond is de constatering dat de ontwikkeling van gedragscodes niet van de grond is gekomen van belang. Gedragscodes hebben de potentie de naleving van de AVG-normen te verstevigen door die in concrete situaties voor een bepaalde branche te operationaliseren dan wel door het bieden van keuzeopties waartussen in een concreet geval kan worden gekozen. Er zijn verschillende redenen waarom er niet nog meer gedragscodes zijn gekomen, maar een belangrijke reden lijkt de eis van een onafhankelijk en effectief toezichtsmechanisme te zijn, dat onderdeel moet zijn van een gedragscode.

De werking van de UAVG

Duidelijkheid en toegankelijkheid

Het onderzoek laat zien dat de duidelijkheid en toegankelijkheid van de UAVG kritisch wordt beoordeeld. Mede de 'beleidsneutrale' invulling van de wet en de korte tijd waarin deze tot stand moest komen hebben daartoe geleid. Wanneer wordt bezien hoe AP en de jurisprudentie nader invulling hebben gegeven aan de normen in de wet is de conclusie dat dit deels is gebeurd, maar voor een ander deel ook nog verder dient te worden uitgewerkt. In het onderzoeksrapport worden daarvan op verschillende plaatsen voorbeelden gegeven. Een duidelijk voorbeeld is de lijn die de Afdeling bestuursrechtspraak van de Raad van State met haar uitspraken van 1 april 2020 en de uitspraak van 2 februari 2022 heeft uitgezet. Daarin achtte de Afdeling zich op grond van artikel 8:88, eerste lid, aanhef en onder a Awb in samenhang met artikel 34 UAVG, bevoegd om te beslissen op een verzoek om schadevergoeding vanwege schade ontstaan uit een verwerking van persoonsgegevens. Uit het onderzoek onder FG's komt naar voren dat zij over het algemeen redelijk hun weg weten te vinden binnen de normstelling. Er doen zich op onderdelen wel knelpunten voor (zoals bij de uitzonderingen op verwerking van bijzondere persoonsgegevens en/of gegevens van strafrechtelijke aard), maar over het geheel genomen stellen de FG's zich goed te kunnen redden met de normen.

Uitvoerbaarheid van de UAVG

Wat hiervoor is gezegd over de duidelijkheid en toegankelijkheid van de UAVG heeft een directe relatie met de uitvoerbaarheid van de UAVG. Op verschillende onderdelen, onder meer in hoofdstuk 6 van het rapport, worden daarover opmerkingen gemaakt, bijvoorbeeld over de bepalingen over geautomatiseerde besluiten en over wetenschappelijk onderzoek (zie ook paragraaf 7.2). De Autoriteit Persoonsgegevens baseert zich in haar toezicht en bij de handhaving op de AVG, maar betrekt ook de normen van de UAVG daarbij. In de casestudy's blijkt verschillende keren dat onder toezicht gestelden behoefte hebben aan nadere duiding van de normen, waarover ze graag in gesprek willen met de AP. Uit de casus komt naar voren dat de AP niet altijd bereid lijkt te zijn zo'n dialoog te voeren. Daarentegen geeft de AP wel aan dat voorafgaand aan een voorgenomen verwerking de AP gevraagd kan worden om een zogenoemde voorafgaande raadpleging, maar van dit instrument wordt vooralsnog weinig gebruik gemaakt. Ook relevant om te melden is dat de AP aangeeft regelmatig te spreken met brancheorganisaties (ruim 350 gesprekken per jaar), waarin veel aandacht wordt besteed aan normuitleg, onder andere over faillissementen en de omgang met transactiedata door banken. Dergelijke gesprekken zegt de AP ook te voeren met wetgevingsjuristen bij departementen.

Naleving van de UAVG

De vraag naar de naleving van de bepalingen van de UAVG is lastig te beantwoorden. In algemene zin is de indruk dat bij de naleving van de AVG en de UAVG sprake is van een nog voortgaand proces van bewustwording en implementatie binnen organisaties. De inrichting van organisaties met het oog op risico's rond de bescherming van persoonsgegevens komt steeds beter op orde, maar er is ook nog steeds ruimte voor verbetering. De FG speelt binnen veel organisaties een belangrijke rol als het gaat om het interne toezicht op de naleving van de bepalingen van het gegevensbeschermingsrecht. De FG's geven in ruime mate (60%) aan dat ze bij vrijwel alle datalekken in hun organisatie worden betrokken. Daar staat tegenover dat ongeveer een op de zes FG's denkt bij minder dan de helft van de gevallen betrokken te worden. De AP heeft een loket ingericht voor vragen van FG's, waar volgens de toezichthouder de afgelopen jaren circa 100 vragen per maand zijn ingekomen, die ook direct worden afgehandeld door de AP. Uit het vragenlijstonderzoek onder FGs zien we dat de meeste FG's aanspreekpunt zijn voor de AP. Maar opvallend is wel dat minder dan de helft van de respondenten zich altijd vrij voelt om de AP te benaderen en dat een kwart zich nooit of soms vrij voelt. Ook uit de interviews blijkt dat FG's worden gehinderd door de vrees dat contact met de AP kan leiden tot interventies of versterkte controle.

Boetebevoegdheid en meldplicht datalekken

De onderzoeksbevindingen met betrekking tot de boetebevoegdheid en de meldplicht datalekken wijzen erop dat beide instrumenten nuttig zijn om het stelsel van het gegevensbeschermingsrecht als het gaat om het toezicht op de naleving goed te laten functioneren. Dat neemt niet weg dat op beide onderdelen ook kanttekeningen te plaatsen zijn bij de wijze waarop de toezichthouder ze hanteert.

Boetebevoegdheid

Wat opvalt bij de handhaving door de AP is dat een beleidsregel waarin het toezichts- en handhavingsbeleid is vastgelegd ontbreekt. Voor zover wij konden nagaan is geen sprake van kenbaar beleid op dit punt. Op welke wijze de toezichthouder in zijn handelen een escalatiestrategie toepast is daardoor niet duidelijk. In de bestudeerde casus leek niet of nauwelijks sprake te zijn van een escalatiestrategie. Daarbij valt op dat een dialoog tussen de onder toezicht gestelde en de toezichthouder in een aantal gevallen geheel of vrijwel geheel ontbrak. Ook als de overtreder de overtreding beëindigt houdt de AP in de bestudeerde casus vast aan de opgelegde boete. Er is beleid over de matiging van boetes, maar hoe dat in de praktijk wordt toegepast is niet inzichtelijk; een vergelijking van de casus gaf op dat punt in ieder geval niet meer houvast.

Het vaststellen van toezichts- en handhavingsbeleid waarin de bestuurlijke boete een plaats krijgt in het escalatiemodel van de AP zou veel duidelijkheid scheppen over de wijze van opereren van de toezichthouder. Daarvan is een grotere acceptatie door de onder toezicht gestelden te verwachten van de wijze waarop zij door de toezichthouder worden bejegend. Dat maakt het gedrag van de toezichthouder immers beter voorspelbaar en zorgt daarmee voor meer begrip.

Meldplicht datalekken

De inzet van de toezichthouder op de naleving van de meldplicht is grotendeels gericht op wel gemelde datalekken. Niet-melders lijken min of meer vrij spel te hebben, hoewel de AP zelf stelt te werken met een risicoanalyse. We constateren in de casestudy's dat de AP forse boetes

oplegt juist in gevallen waarin wel is gemeld. Het is niet ondenkbaar dat die werkwijze ertoe leidt dat potentiële melders eerder terughoudend worden om te melden. Wel tijdig melden leidt ook niet tot verlaging van opgelegde boetes in verband met beveiligingsgebreken die naar aanleiding van tijdig gemelde datalekken aan het licht komen.


pro facto