Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid

Winter, Heinrich; Drouen, T.; Eck, M. van; Geertsema, B.; Cazemier, J.; Ridderbos-Hovingh, C.

pro facto

Onderzoek voor het WODC

Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid

Groningen, 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	Juni 2022
Status	**DEFINITIEF**

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.

Inhoud

Veelgebruikte afkortingen

ABRvS	Afdeling bestuursrechtspraak van de Raad van State
ACM	Autoriteit Consument & Markt
A-G	Advocaat-generaal
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Awb	Algemene wet bestuursrecht
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek
Cbp	College bescherming persoonsgegevens
EDPB	European Data Protection Board
EHRM	Europese Hof voor de Rechten van de Mens
FG	Functionaris voor Gegevensbescherming
HVJ-EU	Hof van Justitie van de Europese Unie
NGFG	Nederlands Genootschap van Functionarissen voor de Gegevensbescherming
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
Wbp	Wet bescherming persoonsgegevens
Wft	Wet op het financieel toezicht
WGBO	Wet geneeskundige behandelingsovereenkomst
Woo	Wet open overheid
WP29	Artikel 29-werkgroep (article 29 Working Party)
Wpr	Wet persoonsregistraties
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme

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:

I de werking van de UAVG; en
II 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 kome

Summary

Background

The General Data Protection Regulation Implementing Act (UAVG) entered into force on 25 May 2018. In accordance with Article 50 UAVG, within three years the Minister will send a report to the States General on the effects and the practical implementation of the UAVG. This evaluation consequently addresses both of these elements: how is the implementation proceeding and what are the effects of the law?

The UAVG and the General Data Protection Regulation (AVG) replace Directive 95/46/EC and the Personal Data Protection Act (Wbp). In the UAVG the Dutch legislator has chosen – where the regulation leaves room for national choices, or for a more detailed interpretation of rules – to build on the framework of standards from Directive 95/46/EC and the Personal Data Protection Act (Wbp). According to the explanatory memorandum, there was no time to develop a new framework. Another argument for minimising differences compared to the pre-AVG situation was the desire for a smooth transition from the old to the new situation.[5] The legislator therefore made provision for an evaluation (stipulated in Article 50 UAVG), the results of which can be used in a discussion about the need to amend the law. This is the scope of this evaluation.

Additionally, the research addresses the question of the extent to which the obligation to report data breaches is complied with and the extent to which the supervisory authority's power to impose fines contributes to an efficient and effective implementation and enforcement of the UAVG. On 1 January 2016 – while the AVG was about to be enacted – the Wbp was expanded to include the duty to report data breaches and the supervisory authority, from then on referred to as the Authority for the Protection of Personal Data (AP), was given the power to impose administrative fines. These components have been added to the evaluation in response to the 2015 motion by Members of Parliament Schouw and Segers requesting the government to evaluate the Dutch Data Breach Notification Act and the power to impose fines within four years of its entry into force.[6] The power to impose fines and the obligation to report data breaches were included in the AVG on 25 May 2016; the AVG applies from 25 May 2018.

[5] *Kamerstukken II,* 2017/18, 34851, no. 3, p. 4.
[6] *Kamerstukken II,* 2015/16, 33662, no. 20,

The UAVG is the organisational act that establishes the AP and lays down rules on its organisation (bodies, independence, etc.) and its tasks and powers. Otherwise, the UAVG follows the Wbp in respect of matters for which the AVG provides scope for the national legislature to make additions. It is important to note that the evaluation of the UAVG is emphatically not an evaluation of the AVG. Neither is it an evaluation of the AP. Insofar as the UAVG functions as an act establishing the AP, we have left these provisions out of consideration in our study. While this is an important starting point, it is unavoidable that the functioning of the UAVG will touch upon the AVG and that the effectiveness of administrative fines and the obligation to report data breaches will be influenced by how the AP exercises supervision and enforcement. In other words, it is unavoidable that our research will also touch upon the AVG and the AP.

This evaluation therefore covers:

the working of the UAVG; and

the compliance and effectiveness of the obligation to report data breaches and the application and effectiveness of administrative fines.

Research questions

The overarching question central to the study is:

How were the standards of the UAVG met in the period 2018 - 2020 and to what extent did the UAVG contribute to an efficient and effective implementation and enforcement of the AVG?

The research was conducted on the basis of the following sixteen research questions.

How do lawyers, the AP and processors of personal data judge the clarity and accessibility of the UAVG?

To what extent are the standards of the UAVG clarified by the AP and case law?

What information is given to the different target groups at what time and in what way? What role does the AP play in this?

How do lawyers, the AP and processors of personal data judge the practicability of the UAVG?

How do lawyers, the AP and processors of personal data judge the enforceability of the UAVG?

How do processors of personal data comply with the provisions of the UAVG?

To what extent is the obligation to report data breaches complied with by processors of personal data?

What is the role of the Data Protection Officer within organisations, including in ensuring compliance with the reporting obligation?

To what extent does case law have a preventive effect with regard to compliance with the provisions of the UAVG and the obligation to report data breaches, and how could this be increased?

What is the supervisory strategy of the AP?

What is the enforcement policy of the AP?

How does supervision and enforcement by the AP take place in practice?

How is the seriousness of the breach of standards, the degree of culpability and an appropriate course of action determined when the AP exercises its power to impose fines?

To what extent does the authority to impose fines and the application thereof by the AP contribute to an efficient and effective implementation and enforcement of the AVG?
Is there any reason to change the AP's application of its powers and, if so, how?
How do lawyers, the AP and processors of personal data judge the extent to which the UAVG has exploited the scope that the AVG leaves for national choices in the implementation of the AVG?

Method

Fact-finding mission
We started the study by gaining an orientation on the subject by studying relevant literature and documents, such as the legislative history of the UAVG, (legal) commentaries on the regulation, annual reports of the AP, the evaluation of the AVG by the European Commission of July 2020 and the consultation of the bill amending the UAVG.[7]

During this fact-finding mission, we also started the legal analysis and jurisprudence research that also served as input for the questionnaire survey and the other empirical research methods. In the first phase of the study, talks were held with (former) legislative lawyers and policy officers of the Ministry of Justice and Security with the UAVG in their portfolio, with some academic experts and with the chairman of the Dutch Association of Data Protection Officers (NGFG).[8]

In this phase of the study, we also wanted to have an informative discussion with the chairman of the board of the AP (Aleid Wolfsen). Due to objections raised by the Authority regarding the origins of the assignment, and the nature, set-up and scope of the research and the people involved, the AP decided, after several discussions between representatives of the ministry and the WODC and staff members of the AP, not to cooperate with the research at all. Later, however, we were able to submit a draft final text with questions. In response, the AP provided detailed comments and answers to questions asked. The researchers were able to benefit extensively from the AP's written response, which led to additions to the text in several places.

Following the refusal of the AP to cooperate with the research, the approach of the research was adjusted in consultation with the supervisory committee. This was done in two areas. As a result of the AP's refusal, the AP's Data Protection Officer register could not be used for the questionnaire survey of Data Protection Officers. The Privacy Law Association and the Dutch Association of Data Protection Officers (NGFG) were however willing to ask their members to participate in the digital survey. Neither could records of fines and notifications of data breaches at the AP be studied. For this reason, it was decided to carry out some case studies of decisions and notifications that have been publicised in the mainstream press. Otherwise, we discussed the application of the UAVG, the obligation to report data leaks and the power to impose fines with a large number of respondents.

Legal analysis and caselaw study
The legal sub-studies were given shape at the start of the project. In this way, the initial findings could also be used for the drafting of the questionnaire survey, on which the supervisory committee provided comments, and the preparation of the topics to be discussed in the interviews. Within the framework of the legal sub-studies, interviews were held with various

[7] Annex 2 contains a list of the sources we consulted.
[8] A list of all the people interviewed during the evaluation is included in Annex 2.

academic experts, lawyers specialising in data protection law and State Councillors of the Council of State.

Questionnaire survey
For the questionnaire survey, we wrote to a large number of data protection officers (an estimated two thousand who are members of the Privacy Law Association and the Dutch Association of Data Protection Officers (NGFG)), asking them to participate in the digital survey. In the end, we received responses from 190 data protection officers, working for administrative bodies (24%), social institutions (38%) and companies (37%). This spread of the respondents corresponds to the spread in the total population in our country.

More in-depth interviews
We conducted 33 in-depth interviews, including interviews with the management of a number of organisations (five), data protection officers (ten), lawyers (five), judges (three), some independent experts, such as academics (five) and (former) employees of ministries. We asked them about their views on how understandable the UAVG standards are and how applicable and enforceable they are.

Case studies
We conducted six case studies to form a picture, from start to finish, of a number of supervisory and enforcement processes involving the obligation to report data breaches and/or the instrument of an administrative fine. We studied a number of cases that have received publicity in the national press. Two cases were about the supervision and enforcement of a data breach: at Uber and the GGD GHOR. GGD GHOR Nederland is the umbrella organisation of the GGDs and GHOR agencies. GGD stands for Municipal or Community Health Service. GHOR stands for medical assistance organisation in the region. Three cases involved violations of other provisions of the AVG: Tax office/VAT number, Football TV and BKR (Financial Registration Office) Finally, research was carried out into the creation of the Code of Conduct for Health Care, given the importance of codes of conduct for the purpose of interpreting the open standards of the (U)AVG within sectors.

The findings and conclusions of the study are discussed below.

General: the system

The AVG Implementation Act (UAVG) is a Dutch law that supplements the European General Data Protection Regulation. It is clear from the study that in fact the UAVG has only limited significance. In any case, it is clear that the law does not offer any more clarification of the AVG standards. This is perhaps understandable in view of the background to the UAVG, the limited time available for its creation and the choice made at the time for a 'policy-neutral' transposition of the existing standards. But that merely serves to limit the added value of the UAVG.

However, in the systematics of data protection law, in the combination of the AVG, UAVG and sectoral codes of conduct, it was precisely from those codes of conduct that an operationalisation of the standards in data protection law was expected. Against this background, the finding that codes of conduct have not been developed is important. Codes of conduct have the potential to bolster compliance with the AVG standards by operationalising these in specific situations for a particular industry, or by providing options to choose between in a specific

case. There are various reasons why more codes of conduct have not been developed, but one key reason seems to be the requirement for an independent and effective monitoring mechanism, which must be part of any code of conduct.

How the UAVG works

Clarity and accessibility

The study shows that the clarity and accessibility of the UAVG are subject to criticism. The 'policy-neutral' interpretation of the law and the short time in which it had to be implemented were among the reasons for this. When examining to what extent the standards in the law have been further defined by the AP and in case law, the conclusion is that this has been done in part, but other parts still need further elaboration. Examples of this are given at various points in the research report. A clear example is the line taken by the Administrative Jurisdiction Division of the Council of State in its rulings of 1 April 2020 and 2 February 2022. In that case, the Division deemed itself competent to decide on a claim for compensation for damage arising from the processing of personal data pursuant to Article 8:88(1)(a) of the General Administrative Law Act (Awb) in conjunction with Article 34 of the UAVG. The survey conducted among data protection officers shows that they generally have a reasonable grasp of the standards. Bottlenecks do occur in some areas (such as the exceptions for processing special personal data and/or data of a criminal nature), but on the whole the data protection officers say they can work well with the standards.

Practicability of the UAVG

What has been said above about the clarity and accessibility of the UAVG has a direct relationship with the practicability of the UAVG. At various points, for example in chapter 6 of the report, comments are made on the provisions on automated decisions and on scientific research (see also section 7.2). In its supervision and enforcement, the AP focuses on the AVG, but also takes into account the standards of the UAVG. In the case studies, it emerged several times that parties under supervision need further clarification of the standards, and would like to discuss this with the AP. It appears from the case studies that the AP is not always prepared to conduct such a dialogue. On the other hand, the AP points out that prior to an intended processing operation, the AP can be asked for a so-called prior consultation, but so far little use has been made of this instrument. Also relevant to mention is that the AP says it regularly speaks with industry organisations (over 350 talks a year), in which a lot of attention is paid to the explanation of standards, including bankruptcies and the handling of transaction data by banks. The AP says it also has such discussions with legislative lawyers in ministries.

Compliance with the UAVG

The question regarding compliance with the provisions of the UAVG is difficult to answer. In general, the impression is that compliance with the AVG and UAVG is still an ongoing process of awareness-raising and implementation within organisations. Organisations are getting better at organising themselves with an eye to the risks involved in protecting personal data, but there is still room for improvement. The data protection officer plays an important role in many organisations when it comes to internal supervision of compliance with the provisions of data protection law. The majority of data protection officers say that they are involved in almost all data breaches in their organisation (60%). However, about one in six data protection officers think they are involved in less than half of the cases. The AP has set up a desk for questions from data protection officers, where, according to the AP, around 100 questions a month have been received in recent years, which are also dealt with directly by the AP. From

the questionnaire survey conducted among data protection officers, we see that most data protection officers serve as a contact point for the AP. But what is striking is that less than half of the respondents always feel free to approach the AP and a quarter never or only sometimes feel free to do so. It also emerges from the interviews that data protection officers are hampered by the fear that contact with the AP may lead to interventions or increased monitoring.

Authority to impose fines and obligation to report data breaches

The research findings with regard to the power to impose fines and the obligation to report data breaches suggest that both instruments are useful in ensuring that the data protection law system functions properly when it comes to monitoring compliance. Nevertheless, this does not detract from the fact that in both cases there are also comments to be made about how the supervisory authority applies these instruments.

Power to impose fines
What is striking about the enforcement by the AP is that there is no policy rule setting out the supervision and enforcement policy. As far as we could ascertain, there is no known policy on this. So exactly how the AP operates with an escalation strategy is not clear. In the cases studied, there seemed to be little or no escalation strategy. It is also noteworthy that in a number of cases, a dialogue between the party under supervision and the AP was entirely or almost entirely absent. Even if the offender ceases the infringement, in the cases studied, the AP still imposes the fine. There is a policy on the mitigation of fines, but how this is applied in practice is not clear; in any case, a comparison of the cases did not provide any guidance on this point.

The adoption of supervisory and enforcement policies in which the administrative fine is accorded a place in the escalation model of the AP would create a great deal of clarity about how the AP operates. The expectation is that the parties under supervision will be more accepting of how they are treated by the AP. This is because the AP's behaviour would be more predictable and therefore more likely to be understood.

Obligation to report data breaches
The AP’s efforts to ensure compliance with the obligation to report are largely focused on data breaches that have been reported. Non-reporters seem to have more or less free play, although the AP itself states that it works with a risk analysis. In the case studies, we find that the AP imposes heavy fines precisely in cases where reporting has taken place. It is not inconceivable that this method of working will make potential reporters more reluctant to report. Timely reporting does not lead to a reduction of fines imposed for security deficiencies that come to light as a result of timely reported data breaches.

1 Inleiding

1.1 Aanleiding

De Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) is op 25 mei 2018 in werking getreden. Volgens artikel 50 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 is de wens voor een soepele overgang van de oude naar de nieuwe situatie.[9] 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.

De UAVG is de organisatiewet die de toezichthouder, de Autoriteit Persoonsgegevens, 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. Dit betreft bijvoorbeeld:

- regeling van bijzondere categorieën persoonsgegevens (ras, politieke opvattingen, gegevens over gezondheid; artikel 22 tot en met 30 UAVG);
- algemene uitzonderingen voor persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 33 en 34 UAVG);
- uitzondering op het verbod op geautomatiseerde besluitvorming (artikel 40 UAVG);
- mogelijk maken van uitzonderingen voor de rechten van betrokkenen en de meldplicht bij een inbreuk, artikel 41 en 42 UAVG;
- in overeenstemming brengen van vrijheid van meningsuiting en informatie en bescherming van persoonsgegevens (artikel 43 UAVG);

[9] *Kamerstukken II*, 2017/18, 34851, nr. 3, p. 4.

- uitzondering op het verwerken van bijzondere persoonsgegevens voor wetenschappelijk of historisch onderzoek of onderzoek met een statistisch oogmerk (artikel 24 UAVG);
- uitzondering voor verwerking van persoonsgegevens die deel uitmaken van archief- bescheiden die berusten in een archiefbewaarplaats (artikel 45 UAVG);
- specifieke voorwaarden aan de verwerking van een nationaal identificatienummer (artikel 46 UAVG).

Deze evaluatie betreft niet de bepalingen in de UAVG over de Autoriteit Persoonsgegevens; evaluatie van de toezichthouder is dus niet aan de orde. Wel besteden we aandacht aan de materiële bepalingen van de UAVG. 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 ter hoogte van € 820.000, dan wel 10% van de jaaromzet. 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.[10] Aandachtspunten daarbij zouden zijn de naleving van de meldplicht, de toepassing en de effectiviteit van de boetebevoegdheid, de administratieve lasten en de nalevingskosten voor gegevensverwerkers en de aansluiting van de wet op Europese regels over gegevensbescherming. De boetebevoegdheid is op 25 mei 2016 in artikel 83 AVG opgenomen; de AVG is vanaf 25 mei 2018 van toepassing. De toezichthoudende autoriteit kan organisaties die de AVG overtreden een boete opleggen van maximaal twintig miljoen euro of 4% van de wereldwijde jaaromzet. De meldplicht datalekken is opgenomen in artikel 33, eerste lid AVG, waar melding binnen 72 uur bij de toezichthouder is voorgeschreven en in artikel 34, eerste lid AVG, waar onverwijlde mededeling aan de betrokkene is geregeld.

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.

1.2 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 een zestiental onderzoeksvragen die als kapstok dienden voor de hoofdstukken in het rapport waarin we verslag doen van de onderzoeksbevindingen en die in het concluderende hoofdstuk 7 van dit onderzoeksrapport van een antwoord worden voorzien:

[10] *Kamerstukken II* 2015/16, 33662, nr. 20.

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?

1.3 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.[11]

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).[12]

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

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). De gemaakte afspraak in april 2021 werd echter afgezegd, waarbij werd gewezen op de totstandkoming van de opdracht, en de aard, opzet en scope van het onderzoek en de betrokkenen daarbij. De bezwaren van de AP bleken in sterke mate samen te hangen met het feit dat de organisatie op geen enkele wijze bij het totstandkomingsproces en de gunning van het onderzoek betrokken was. Ook was de reikwijdte van het onderzoek in de ogen van de AP niet duidelijk; de toezichthouder vreesde dat het onderzoek zich zou uitstrekken tot een evaluatie van het functioneren van de AP. De AP stelde daarnaast vraagtekens bij de positie van de voorzitter van de begeleidingscommissie, die behalve hoogleraar ook advocaat is en in die functie partijen bijstaat in procedures over besluiten van de AP. En in de brief werden ook zorgen onder woorden gebracht over een van de medewerkers van het onderzoeksteam die eerder in een managementfunctie bij de AP heeft gewerkt en die later waarnemend hoofd was van de afdeling van het ministerie die de onderzoeksaanvraag aan het WODC heeft gedaan.

Over deze bezwaren is tussen vertegenwoordigers van het departement en het WODC en medewerkers van de AP meerdere keren gesproken. De onderzoekers hebben in een toelichtend memo de reikwijdte van het onderzoek voor de AP getracht te verduidelijken, waarbij ze aangaven dat het functioneren van de AP geen onderdeel van het onderzoek is. Vanuit het WODC is door het hoofd van de afdeling Externe Wetenschappelijke Betrekkingen een schriftelijke toelichting gestuurd aan de AP om dit punt verder te verhelderen. Van de zijde van de AP bleek dit niet voldoende en werd in een schrijven aan de minister voor Rechtsbescherming van 1 oktober 2021 aangedrongen op het maken van goede afspraken over een hernieuwde onderzoeksopzet en –uitvoering. In een schriftelijke reactie van 3 december 2021 schreef de minister voor Rechtsbescherming vervolgens niet te willen treden in de onafhankelijke positie van het WODC bij de keuze van het onderzoeksbureau en de samenstelling van de begeleidingscommissie.

Nadat bekend werd dat de AP medewerking weigerde aan het onderzoek, pasten de onderzoekers in afstemming met de begeleidingscommissie van het onderzoek de aanpak van het onderzoek aan. 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[13] bij de AP kon ook niet worden uitgevoerd. Daarom is gekozen voor het uitvoeren 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.

Uiteindelijk maakte de AP in een brief van 27 december kenbaar onder een aantal voorwaarden in beperkte mate medewerking te kunnen verlenen. Die medewerking betrof 'dat deel van de evaluatie dat zich richt op de nationale keuzes achter de UAVG en op de wetssystematiek van de UAVG'.

[13] Van een datalek is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).

De onderzoekers hebben dus geen interviews kunnen houden met medewerkers van de AP of met bestuursleden van de toezichthouder. Wel is in reactie op de toegezegde beperkte medewerking een concept-eindtekst met een belangrijk deel van de bevindingen van het onderzoek met een verzoek om commentaar voorgelegd. In die tekst hebben we op verschillende punten vragen gesteld aan de AP in de hoop dat antwoorden daarop een bijdrage zouden kunnen leveren aan een evenwichtige evaluatie. In reactie hierop heeft de AP uitvoerig commentaar geleverd op de gepresenteerde bevindingen en ook de in de tekst opgenomen vragen van antwoorden voorzien. De onderzoekers hebben in ruime mate hun voordeel kunnen doen met de schriftelijke reactie van de AP, die op verschillende plaatsen in de tekst tot aanvulling op de tekst heeft geleid.

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
Het vragenlijstonderzoek FG's liep enige vertraging op vanwege het gebrek aan medewerking van de AP. Daarom konden we geen gebruik maken van het bestand van FG's dat door de AP wordt beheerd. Door de bereidheid om aan het onderzoek mee te werken van NGFG en de Vereniging Privacyrecht, is alsnog een groot aantal FG's (naar schatting de tweeduizend FG's die lid zijn van beide verenigingen) 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. In bijlage 2 is een overzicht opgenomen van de gesprekspartners, voor zover met instemming van de geïnterviewde mogelijk, met naam en toenaam, in andere gevallen alleen met een functienaam.

Casestudy
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. De casus zijn geselecteerd in overleg met de begeleidingscommissie. 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.

1.4 Afbakening/begrenzing

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. Het is onvermijdelijk dat de weigering van de AP om ongeclausuleerd mee te werken aan het onderzoek van invloed is geweest op de onderzoeksbevindingen, in het bijzonder waar deze betrekking hebben op de bestuurlijke boete en de meldplicht datalekken.

1.5 Leeswijzer

Hierna gaan we in hoofdstuk 2 in op de tekst van het gegevensbeschermingsrecht. De hoofdlijnen van de AVG worden besproken, waarna de totstandkoming en inhoud van de UAVG aan de orde komen. Tevens gaan we in hoofdstuk 2 in op de meldplicht datalekken en het handhavingsinstrument van de bestuurlijke boete. Hoofdstuk 3 betreft het jurisprudentieonderzoek. In hoofdstuk 4 volgen de bevindingen van het vragenlijstonderzoek onder FG's. Hoofdstuk 5 beschrijft de zes casestudy's. Hoofdstuk 6 analyseert de belangrijkste bevindingen van het onderzoek. Tot slot volgen de belangrijkste conclusies en de beantwoording van de onderzoeksvragen in hoofdstuk 7.

2 Juridisch kader

2.1 Inleiding

In dit inleidende hoofdstuk wordt de relevante context van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) beschreven. De UAVG vult de ruimte die op Europees niveau in de Algemene verordening gegevensbescherming (AVG) wordt geboden verder in. In dat kader wordt allereerst in paragraaf 2.2 beschreven hoe de AVG op Europees niveau tot stand is gekomen. Dan volgt in paragraaf 2.3 een bespreking van de hoofdlijnen van de AVG en de verhouding tussen de AVG en de UAVG. In paragraaf 2.4 komen de hoofdlijnen van de UAVG aan bod. Vervolgens in gaan we in paragraaf 2.5 in op de stand van zaken van de Verzamelwet Gegevensbescherming die in voorbereiding is. Tot slot wordt in paragraaf 2.6 aandacht besteed aan de meldplicht datalekken en de boetebevoegdheid.

2.2 Totstandkoming AVG

Op 25 januari 2012 diende de Europese Commissie een voorstel in met betrekking tot hervorming van Europese wetgeving op het gebied van gegevensbescherming. Een nieuwe algemene verordening gegevensbescherming zou, in plaats van de tot op dat moment geldende Richtlijn 95/46/EG, in de toekomst meer bescherming bieden in een door technologie snel veranderende maatschappij.[14]

De Commissie overwoog dat de sinds 1995 geldende Richtlijn 95/46/EG (in Nederland onder andere geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp)) betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, na vijftien jaar – waarin de technologie een vlucht had genomen – knelpunten en problemen met zich meebracht.[15] Deze problemen deden zich bijvoorbeeld voor in het omgaan met de gevolgen van nieuwe technologieën, het omgaan met de globalisering en internationale gegevensdoorgifte, en de behoefte aan een samenhangend wettelijk kader voor gegevensbescherming.[16] Kortom, de ontwikkeling van de technologie stelde nieuwe eisen aan de bescherming van persoonsgegevens, aldus de Europese Commissie.

[14] Europese Commissie 2012, p. 20.
[15] Europese Commissie 2010, p. 2.
[16] Europese Commissie 2010, p. 3 en 4.

Bovenstaande gaf de Commissie aanleiding om op 4 november 2010 de aanpak voor een herziening van de Richtlijn 95/46/EG te schetsen. De hoofdlijnen en uitgangspunten van de Richtlijn 95/46/EG bleven ongewijzigd. Deze uitgangspunten betroffen ten eerste de bescherming van de fundamentele rechten op gegevensbescherming en ten tweede het vrije verkeer van persoonsgegevens in het kader van de verwezenlijking van de interne markt.[17]

Twee jaar na het schetsen van de kaders voor het herzien van de Richtlijn, koos de Commissie dus op 25 januari 2012 voor het indienen van een ontwerpverordening. Het was volgens de Commissie tijd voor een 'krachtiger en coherenter' kader en dit zou worden bewerkstelligd door een verordening. De doelstellingen en uitgangspunten van het bestaande rechtskader waren nog steeds valide, maar een richtlijn had niet kunnen realiseren dat persoonsgegevens op een uniforme manier zouden worden beschermd. Door de rechtstreekse toepasselijkheid zou een verordening de juridische fragmentatie verminderen en de rechtszekerheid bevorderen door een geharmoniseerd pakket basisregels in te voeren, de bescherming van de grondrechten van natuurlijke personen te verbeteren en bij te dragen aan de werking van de interne markt.[18]

Dit uitgangspunt kwam onder druk te staan toen een aanmerkelijk aantal lidstaten van de Unie zich op het standpunt stelde dat er ruimte voor nationale regelgeving moest blijven bestaan met betrekking tot de verwerking van persoonsgegevens door overheidsinstanties en op het gebied van arbeidsrechtelijke aspecten.[19] Detailregelingen zouden volgens de lidstaten resulteren in 'conflicterende afbakeningen voor regelgeving door de overheidsinstanties van de lidstaten op het gebied van gegevensverwerking.' Als deze lidstaten dit onderscheid in de verordening niet langer konden terugzien, dan wensten zij in elk geval te voorkomen dat aanvaarding van de verordening zou leiden tot een lager beschermingsniveau. Zij schaarden zich daarom achter de mogelijkheid tot het vaststellen van strengere voorschriften voor verwerkingen in de sfeer van de overheid. Samenhangend met het vraagstuk van de overheidsverwerkingen werd ook ruimte gezocht voor onderwerpen die sterk met de nationale rechtsorde zijn verbonden. Het betrof de gegevensverwerking in het kader van de vrijheid van meningsuiting, de gezondheidszorg, het arbeidsrecht, wetenschappelijke, statistische en historische doeleinden en archieven en de verwerking van persoonsgegevens door beroepen die een geheimhoudingsregime hebben.[20]

Na ruim vier jaar onderhandelen door 28 lidstaten is op 27 april 2016 door het Europees Parlement en de Raad de verordening 2016/679 (AVG) en intrekking van Richtlijn 95/46/EG vastgesteld. De verordening is op 4 mei 2016 in het Publicatieblad van de EU bekendgemaakt, trad op 24 mei 2016 in werking en is van toepassing sinds 25 mei 2018.[21] De verordening vertoont op onderdelen kenmerken van een richtlijn, in die zin dat lidstaten op onderdelen bevoegdheden en verplichtingen kregen om nadere regels te stellen. In Nederland is die ruimte onder meer ingevuld door de UAVG[22].

[17] Europese Commissie 2010, p. 2.
[18] Europese Commissie 2010, p. 20.
[19] Comité van de Regio's 2012.
[20] Comité van de Regio's 2012.
[21] De verordening geeft uitvoering aan artikel 16 VWEU waarin in het eerste lid is vastgelegd dat een ieder recht op de bescherming van de persoonsgegevens en in het tweede lid de Europese wetgever wordt opgedragen hierover regels op te stellen.
[22] Naast de UAVG is ook in sectorwetgeving nadere regelgeving tot stand gekomen. Daarnaast gelden specifieke uitvoeringsregimes voor de Wet basisregistratie personen, de Kieswet en de Tijdelijke Referendumwet.

Verschuiving van bevoegdheden
Sinds 1983 bevat artikel 10 van de Grondwet een opdracht aan de formele wetgever om ter bescherming van de persoonlijke levenssfeer regels te stellen over de bescherming van persoonsgegevens. Deze bepaling was in de Grondwet opgenomen, omdat de bescherming van persoonsgegevens in de eerste instantie een nationale aangelegenheid was.[23]

In de loop der jaren heeft er een steeds verdergaande Europese integratie wat betreft bescherming van persoonsgegevens plaatsgevonden. In dat kader is het Verdrag van Lissabon uit 2009 een belangrijke mijlpaal. Ter bescherming van persoonsgegevens werd een zelfstandige algemene rechtsgrondslag opgenomen in artikel 16 van het Verdrag betreffende de Werking van de Europese Unie (VWEU). Op grond van artikel 16 VWEU stelt de Europese wetgever voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens. Naast artikel 16 VWEU heeft het Handvest van de grondrechten van de Europese Unie en het daarin in artikel 8 vastgelegde recht op bescherming van persoonsgegevens juridisch bindende werking gekregen.[24] De bescherming van het grondrecht op de bescherming van persoonsgegevens is inmiddels dus ook een EU-aangelegenheid.

Het gevolg van de hierboven beschreven ontwikkeling en de komst van de AVG, heeft ertoe geleid dat de rol van nationale wetgevers beperkter is geworden. Als gezegd biedt de AVG wel op expliciete plaatsen ruimte aan nationale wetgevers om bepalingen uit de AVG verder in te vullen (zie paragraaf 2.3).

2.3 Hoofdlijnen AVG en verhouding AVG en UAVG

2.3.1 Hoofdlijnen AVG

Met de AVG is gekozen voor een eenvormige en gelijkwaardige bescherming van persoonsgegevens en daarmee voor het harmoniseren van het gegevensbeschermingsrecht binnen de Europese Unie. De AVG bevat elf hoofdstukken met in totaal 99 artikelen en 173 overwegingen.

De voornaamste verschillen van de AVG ten opzichte van de Richtlijn 95/46/EG zagen op een versterking van de rechten van betrokkenen en in verband daarmee de uitbreiding van verplichtingen van verwerkingsverantwoordelijken. De betrokkene kwam met de komst van de verordening bijvoorbeeld het recht op overdraagbaarheid en het recht op gegevenswissing toe. Voor verwerkingsverantwoordelijken bracht de AVG met zich mee, dat bijvoorbeeld voorafgaand bij de bouw van een verwerkingssysteem, passende en organisatorische maatregelen dienen worden getroffen met als doel gegevensbeschermingsbeginselen te waarborgen (recht op gegevensbescherming door ontwerp en door standaardinstellingen).[25] Ook werd in meer gevallen de aanstelling van een Functionaris voor Gegevensbescherming verplicht.[26]

De rol van de toezichthoudende autoriteiten op de naleving van gegevensbescherming onderging door de komst van de AVG ook een transformatie. De toezichthoudende autoriteiten kregen een meer onafhankelijke positie ten opzichte van de lidstaat en gingen deelnemen aan een vernieuwde en met vergaande bevoegdheden ingestelde Europese overlegstructuur van

[23] *Strct.* 2014, 34523, p. 5.
[24] *Strct.* 2014, 34523, p. 6.
[25] Artikel 25 AVG.
[26] Artikel 37 AVG.

toezichthouders, de European Data Protection Board (EDPB).[27] Dit om een zo eenduidig mogelijke uitleg van de verordening te bewerkstelligen.[28] Daarnaast werd de sanctiebevoegdheid van de toezichthoudende autoriteit uitgebreid met het opleggen van administratieve geldboetes tot twintig miljoen euro of 4% van de totale wereldwijde omzet in het voorgaande boekjaar, indien dat hoger is.[29] Deze bevoegdheid werd toegekend met het oog op een krachtiger handhaving van de regels en de administratieve inbreuken op de verordening te harmoniseren.[30]

2.3.2 Verhouding AVG en UAVG

Het stelsel van het gegevensbeschermingsrecht, zoals neergelegd in de AVG en eerder in de Wbp kenmerkt zich als omnibuswetgeving doordat de AVG regels bevat die (in principe) gelden ongeacht door wie en binnen welke sector de persoonsgegevens worden verwerkt. Door de brede toepasselijkheid van deze regelgeving is gebruik gemaakt van open begripsbepalingen en normen, waarbij de invulling van open begripsbepalingen in de concrete situatie bepaalt welke verplichtingen gelden. Het gaat hierbij om sleutelbegrippen zoals persoonsgegevens, verwerking, pseudonimisering, verwerkingsverantwoordelijke, verwerker en hoofdvestiging. Tevens dient in veel gevallen de concrete invulling van de beginselen, zoals doelbinding en verenigbaarheid, gegevensminimalisatie, juistheid, opslagbeperking en integriteit door de verwerkingsverantwoordelijke zelf te worden gegeven.

Omdat door de rechtstreekse werking van de verordening de AVG niet behoeft te worden omgezet in nationaal recht, leidt dit in principe tot verdergaande harmonisatie dan een richtlijn. De richtlijnachtige kenmerken van de AVG vloeien dan ook voort uit het feit dat de verordening op verschillende plekken aan nationale wetgevers de ruimte laat (of verplicht) om uitzonderingen of andere elementen verder in te vullen. Een voorbeeld hiervan is de invulling van de uitzonderingen op het verwerkingsverbod van bijzondere persoonsgegevens in de artikelen 22 tot en met 30 UAVG.

In Nederland is de invulling van de AVG tot uiting gekomen in de intrekking van de Wbp en de vaststelling van de UAVG die sinds 25 mei 2018 van toepassing is. De nationale wetgever heeft er uitdrukkelijk voor gekozen om in de UAVG voort te bouwen op het normenkader uit Richtlijn 95/46/EG en de Wbp. Dit houdt in dat bij onderdelen uit de verordening die vragen om een nadere invulling in nationaal recht, zoveel mogelijk is aangesloten bij het voorheen bestaande nationaal recht en de bestaande nationale beleidskeuzes. Waar dat niet mogelijk was is gekozen om zo dicht mogelijk bij het nationale recht te blijven.[31] Dit is gedaan ‘enerzijds omdat gelet op de inwerkingtreding van AVG de tijd ontbrak om een geheel nieuw kader te ontwikkelen. Anderzijds om de overgang van de oude naar de nieuwe situatie zo soepel mogelijk te laten verlopen. Hoe kleiner die verschillen zijn, des te vloeiender de overgang naar het nieuwe regime.’ Bovendien achtte de wetgever het zinvol om eerst een aantal jaren ervaring op te doen met de verordening alvorens ook op die punten waar nog keuzevrijheid bestaat, af te wijken van het bestaande kader.[32] Mede daarom is in artikel 50 UAVG ook een artikel opgenomen dat voorziet in het uitvoeren van een evaluatie van de uitvoeringswet.

[27] In het Nederlands aangeduid als het Europees Comité voor gegevensbescherming.
[28] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 11.
[29] Artikel 83, zesde lid AVG.
[30] Overweging 148 en 150 AVG.
[31] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 17.
[32] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 4.

2.4 Hoofdlijnen UAVG

Zoals hierboven aangegeven biedt de AVG op verschillende punten de ruimte voor de nationale wetgever om in- en aan te vullen. Hoe deze ruimte in bepaalde gevallen wordt benut is uitgewerkt in de UAVG. De UAVG is onderverdeeld in de volgende hoofdstukken.

1. Algemene bepalingen (art. 1-5)
2. De Autoriteit persoonsgegevens (art. 6 -21a)
3. Bepalingen ter uitvoering van de verordening (art. 22-39)
4. Uitzonderingen en beperkingen (art. 40-47)
5. Overgangs- en slotbepalingen (art. 48-54)

De oprichting en inrichting van de nationale toezichthouder
Met het oog op een uniforme normtoepassing is in de AVG voorzien van een gelaagde toezichtstructuur tussen de EDPB en nationale toezichthoudende autoriteiten. De verordening formuleert daartoe verplichtingen tot onderlinge samenwerking en afstemming tussen toezichthouders.[33] Om dit te bewerkstelligen nemen de toezichthouders zitting in de EDPB dat net als de voorganger – de Article 29 Working Party (WP29) – opinies formuleert. Het gebruik van deze (interpretatieve) soft law door de EDPB in de vorm van richtsnoeren zou daarmee een bijdrage leveren aan een grotere transparantie en adequate en uniforme toepassing van de normen uit de AVG in de lidstaten. Bovendien functioneert de EDPB als geschilbeslechter tussen de toezichthouders door middel van een coherentiemechanisme. Dit ter vergroting van de eenduidigheid van onder meer de uitleg van de open normen die de AVG kent.

Een van de kernwaarden van de toezichthoudende autoriteiten binnen de AVG is onafhankelijkheid. Een aantal zorgplichten die de nationale lidstaten in dit kader worden opgedragen zijn in paragraaf 2.1 UAVG uitgewerkt. Het gaat daarbij om zaken als de aanwijzing en samenstelling van de Autoriteit Persoonsgegevens.

Taken en bevoegdheden van de toezichthoudende autoriteit
De taken en bevoegdheden die de toezichthoudende autoriteit toekomen zijn met name bepaald in de AVG.[34] Grotendeels betreffen dit handhavingstaken, maar daarnaast betreffen dit ook de taken als het verstrekken van advies, het samenwerken met andere toezichthoudende autoriteiten en het behandelen van klachten van betrokkenen die menen dat er bij de verwerking van persoonsgegevens inbreuk is gemaakt op de bescherming van persoonsgegevens. Op welke wijze de nationale toezichthoudende autoriteiten de taken prioriteren in de uitvoering is aan henzelf. De autoriteit heeft daarin, binnen de grenzen van de verordening, beleidsvrijheid die met beleidsregels kan worden ingevuld. Deze beleidsvrijheid is er in het kader van het op een doelmatige manier uitvoering te kunnen geven aan de handhavingstaak. De beleidsvrijheid geldt niet ten aanzien van het behandelen van klachten.[35]

In de verordening zijn in artikel 58 bevoegdheden toegekend aan de toezichthoudende autoriteiten met betrekking tot het doen van onderzoek, het nemen van corrigerende maatregelen en het geven van advies die verband houden met de bescherming van persoonsgegevens. Met betrekking tot de bevoegdheden van de toezichthoudende autoriteit wordt lidstaten de mogelijkheid geboden aanvullende bevoegdheden toe te kennen.[36] Hiervan is in de UAVG gebruik

[33] Artikelen 60 tot en met 76 AVG.
[34] Artikel 57 AVG.
[35] Artikelen 77 en 78 AVG.
[36] Artikel 58, zesde lid AVG.

gemaakt met het toekennen van de bevoegdheid tot het opleggen van een last onder dwangsom en een last onder bestuursdwang. Deze bevoegdheden zijn aan de Autoriteit Persoonsgegevens toegekend, omdat de onder toezicht gestelden en de Autoriteit Persoonsgegevens bekend waren met deze instrumenten en omdat dit een meer laagdrempelige manier voor de toezichthouder zou zijn om handhaving te bewerkstelligen, 'zonder dat er onmiddellijk een boete hoeft te worden opgelegd.'[37] Verder is in artikel 15, vijfde lid UAVG een bepaling opgenomen op grond waarvan de Autoriteit Persoonsgegevens ook bevoegdheden toekomt voor het uitvoeren van de taken in het kader van hoofdstuk 7 van de AVG (samenwerking en coherentie).

Zoals eerder gezegd komt de toezichthoudende autoriteit op grond van de verordening ook de bevoegdheid toe tot het opleggen van administratieve boetes.[38] Er is wel een maximale maar geen minimale hoogte voor de boete in de verordening opgenomen. De boete zal proportioneel moeten zijn in het licht van de geconstateerde overtreding.[39] De meeste bepalingen van de verordening kunnen op grond van artikel 83 AVG worden gesanctioneerd. Het sanctioneren van overtredingen in het kader van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (opgenomen in artikel 10 AVG) kan echter niet op artikel 83 AVG worden gebaseerd. In de artikel 17 UAVG is daarom opgenomen dat een bestuurlijke boete ook kan worden opgelegd bij overtreding van artikel 10 AVG.[40]

Bijzondere categorieën van persoonsgegevens

Bijzondere persoonsgegevens betreffen volgens de verordening acht categorieën persoonsgegevens. Deze gegevens worden in artikel 9, eerste lid AVG als volgt beschreven: 'persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.'[41]

Het verwerken van bijzondere categorieën van persoonsgegevens is op grond van artikel 9 van de verordening verboden, tenzij een van de limitatief opgenomen uitzonderingen zich voordoet. Een aantal van die uitzonderingen uit de verordening is rechtstreeks toepasselijk (bijvoorbeeld wanneer betrokkene toestemming geeft).[42] In andere gevallen moet een uitzondering in het lidstatelijk recht zijn opgenomen.[43]

In artikel 23 en 24 UAVG wordt invulling gegeven aan de ruimte die de verordening biedt voor het opnemen van een uitzondering op het verbod om bijzondere categorieën van persoonsgegevens te verwerken wanneer deze verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, of wanneer verwerking noodzakelijk is met het oog op historisch of wetenschappelijk onderzoek of statistische doeleinden. Andere mogelijkheden die de AVG biedt om in lidstatelijk recht invulling te geven aan uitzonderingen of nadere regels op te nemen, zijn in de UAVG in de volgende artikelen benut:

[37] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 29.
[38] Artikel 83 AVG.
[39] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 30.
[40] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 31.
[41] Artikel 9, eerste lid AVG.
[42] Artikel 9, a, c, d, e, f AVG en artikel 22, tweede lid, onder a t/m e UAVG.
[43] Het gaat hier om de uitzonderingen van artikel 9, b, g, h, i, j AVG.

- In artikel 25 UAVG is een uitzondering opgenomen die het mogelijk maakt om redenen van zwaarwegend algemeen belang af te wijken van het verbod om persoonsgegevens te verwerken waaruit iemands ras of etnische afkomst blijkt.
- In artikel 26 UAVG is een uitzondering gemaakt op het verbod om persoonsgegevens waaruit politieke opvattingen blijken te verwerken voor vervulling openbare functies. Deze gegevens spelen bijvoorbeeld een rol bij burgemeestersbenoemingen.[44]
- In artikel 27 UAVG is een uitzondering opgenomen inzake de verwerking van persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken ten behoeve van geestelijke verzorging.
- Artikel 28 UAVG biedt invulling aan de mogelijkheid om aanvullende voorwaarden of beperkingen op te nemen in lidstatelijk recht wanneer het gaat om de verwerking van genetische gegevens.[45]
- In artikel 29 UAVG is een uitzondering opgenomen op het verbod om biometrische gegevens te verwerken. Verwerking van biometrische gegevens, met het oog op identificatie, is in dit artikel mogelijk gemaakt, indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De reden voor het opnemen van deze uitzondering lag in het feit dat afzien van een nationale uitzondering voor biometrische gegevens dit zou 'betekenen dat de bestaande ontwikkelingen in het gebruik van biometrie als identificatiemiddel sterk gehinderd zouden worden'. Bij die ontwikkelingen werd gedacht aan toepassing van biometrische gegevens voor 'bijvoorbeeld het reguleren van de toegang tot bepaalde plaatsen en gebouwen, maar ook toegang tot informatiesystemen.'[46]
- In artikel 30 UAVG is bepaald dat het verbod om gezondheidsgegevens te verwerken niet van toepassing is wanneer dit noodzakelijk is 'op het terrein van arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht, om redenen van zwaarwegend algemeen belang en voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten.'[47]
- Paragraaf 3.2 van de UAVG ziet op het verwerken van persoonsgegevens van strafrechtelijke aard en geeft algemene (artikel 32) en overige (artikel 33) uitzonderingsgronden op grond waarvan dergelijke persoonsgegevens mogen worden verwerkt.

Geautomatiseerde individuele besluitvorming, waaronder profilering

Op grond van artikel 22, eerste lid AVG heeft een betrokkene het recht niet worden onderworpen 'aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.' Het eerste lid geldt niet wanneer het besluit: (1) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke, (2) in een lidstatelijke of unierechtelijke bepaling is toegestaan en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van betrokkene, (3) berust op de uitdrukkelijke toestemming van betrokkene.

[44] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 106.
[45] Artikel 9, vierde lid AVG.
[46] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 108.
[47] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 109.

Het begrip 'besluit' uit de verordening moet ruimer worden geïnterpreteerd dan het besluitbegrip in de Algemene wet bestuursrecht (Awb): 'ook private partijen vallen onder de reikwijdte van deze bepaling wanneer ze gebruik maken van geautomatiseerde besluitvorming.'[48]

De gedachte achter artikel 22 AVG was dat niemand mag worden 'onderworpen aan de gevolgen van een besluit enkel en alleen op basis van kenmerken van een bepaalde groep waartoe hij of zij behoort.'[49]

Omdat er ook sprake kan zijn van geautomatiseerde besluitvorming op basis van strikt individuele kenmerken (bijvoorbeeld bij toeslagen), is geautomatiseerde besluitvorming toegestaan op grond van artikel 40 UAVG 'indien de geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.' [50]

De verwerkingsverantwoordelijke moet in dat geval passende maatregelen treffen die strekken tot bescherming van de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene. Wanneer de verwerkingsverantwoordelijke geen bestuursorgaan is gelden nog een aantal aanvullende eisen voor het gebruik maken van geautomatiseerde besluitvorming.[51] De verwerkingsverantwoordelijke dient passende maatregelen te treffen die strekken tot bescherming van de rechten van betrokkene. Dit is in ieder geval gedaan indien er sprake is van menselijke tussenkomst, betrokkene zijn standpunt kenbaar kan maken en het recht heeft zijn besluit aan te vechten.

Beperkingen van de rechten van betrokkenen en de meldplicht bij inbreuk
In de verordening is het mogelijk gemaakt voor lidstaten om de rechten van betrokkenen en verplichtingen van een verwerkingsverantwoordelijke te beperken.[52] Hierbij geldt als voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele rechten onverlet laat en een noodzakelijke en evenredige maatregel is ter waarborging van een aantal zaken (zoals de nationale veiligheid, landsverdediging, de openbare veiligheid etc.). Ook is vastgelegd dat de beperkingen die kunnen gemaakt, bepalingen dienen te bevatten met betrekking tot genoemde elementen (zoals de categorieën persoonsgegevens, het toepassingsgebied van de ingevoerde beperkingen).

In artikel 41 UAVG is een algemene bepaling opgenomen die een belangenafweging met betrekking tot het beperken van de rechten van betrokkene overlaat aan de verwerkingsverantwoordelijke. Het gaat daarbij om situaties die niet altijd op voorhand te voorzien zijn voor de nationale wetgever en waarvoor in de praktijk daadwerkelijk een noodzaak tot inperken van de reikwijdte van bepaalde rechten van betrokkene bestaat. De in dit artikel geboden generieke mogelijkheid voor een verwerkingsverantwoordelijke om bepaalde rechten van betrokkenen in te perken, is inroepbaar in uitzonderlijke individuele situaties waarin aan de ene kant de wetgever (nog) niet heeft voorzien in een oplossing, terwijl er aan de andere kant dermate grote in het artikel opgesomde belangen op het spel staan voor de verwerkingsverantwoordelijke dat die het (deels) beperken van voornoemde rechten rechtvaardigen.[53]

[48] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 46.
[49] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 46.
[50] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 120.
[51] Artikel 40, derde lid UAVG.
[52] Artikel 23 AVG.
[53] Ministerie van Justitie en Veiligheid 2020, p. 21 en 22.

In het conceptwetsvoorstel Verzamelwet gegevensbescherming wordt voorgesteld artikel 41 te wijzigen door deze bepaling meer in lijn te laten zijn met artikel 23 AVG, waarmee artikel 41, eerste lid, aanhef, als volgt luidt:

'De verwerkingsverantwoordelijke kan de reikwijdte van de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de verordening, *alsmede in artikel 5, voor zover de bepalingen van dat artikel overeenkomen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 21*, beperken voor zover zulks noodzakelijk en evenredig is ter waarborging van:'

Vrijheid van meningsuiting en van informatie
In artikel 85, tweede lid AVG worden lidstaten ertoe verplicht uitzonderingen vast te stellen met betrekking tot de vrijheid van meningsuiting en informatie met daaronder begrepen de verwerking voor journalistieke doeleinden en academische, artistieke of literaire uitdrukkingsvormen, en de hoofdstukken 2 tot en met 7 en 9 AVG. In de UAVG is deze verplichting in artikel 43 UAVG ingevuld.

In lijn met de beleidsneutrale implementatie is ervoor gekozen om het systeem onder de Wbp grotendeels voort te zetten. Er zijn wel enkele veranderingen aangebracht daar waar de praktijk of jurisprudentie daartoe noodzaakten. Zo is het recht van betrokkene om toestemming voor het verwerken van persoonsgegevens te allen tijde in te kunnen trekken, uitgezonderd. Ook is in verband met nieuw opgenomen bepalingen in de AVG een aantal uitzonderingen gemaakt, zoals de verplichting tot het voorleggen van een gedragscode.[54]

Verwerkingen ten behoeve van wetenschappelijk, historisch of statistisch onderzoek
Het verwerken van bijzondere categorieën van persoonsgegevens ten behoeve van wetenschappelijk, historisch of statistisch onderzoek is toegestaan wanneer de betrokkene toestemming heeft verleend.[55] Wanneer toestemming niet kan worden verkregen of dit een onevenredige inspanning kost, kan de verwerking zijn toegestaan op grond van artikel 24 UAVG. Overigens zijn in dat artikel wel een drietal aanvullende voorwaarden opgenomen: (1) het onderzoek moet een algemeen belang dienen, (2) de verwerking moet noodzakelijk zijn voor het wetenschappelijk of historisch onderzoek of het statistisch doel en, (3) er moet bij de uitvoering worden voorzien in waarborgen die verzekeren dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

Met betrekking tot de rechten van betrokkenen inzake de verwerking van persoonsgegevens voor wetenschappelijk onderzoek en statistiek is in artikel 44 UAVG een aantal uitzonderingen opgenomen. Deze uitzonderingen geven invulling aan artikel 89, tweede lid AVG, waar lidstaten op dit onderwerp ruimte is geboden voor nadere afwijkingen. Het recht op inzage, rectificatie en beperking van de verwerking zijn net zoals in de Wbp uitgesloten.[56]

Uit de consultatie van het wetsvoorstel bleek dat er onduidelijkheid bestond over de reikwijdte van de definitie 'ten behoeve van wetenschappelijk, historisch of statistisch onderzoek'. Kijkend naar overweging 159 AVG, zou het uitgesloten zijn 'dat het louter en alleen om publiek gefinancierd onderzoek zou gaan.'[57] Ook niet met publiek geld gefinancierd onderzoek zou gebruik kunnen maken van deze uitzondering.[58]

[54] Artikelen 41 t/m 43 UAVG.
[55] Artikel 9, tweede lid, sub a AVG.
[56] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 125 en 126.
[57] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 51.
[58] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 51.

Archivering in het algemeen belang
Artikel 89 AVG bevat een specifieke regeling voor de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang. In het derde lid van voornoemd artikel wordt lidstaten de mogelijkheid geboden af te wijken van voorschriften met betrekking tot wat in de verordening is bepaald inzake de rechten van betrokkene. In verband met de 'eigen aard van archiefwerkzaamheden', zijn de bepalingen met betrekking tot het recht op inzage, het recht op rectificatie, en het recht op beperking van verwerking, en het recht op overdraagbaarheid van gegevens,[59] niet van toepassen maar hebben deze een speciale betekenis. Zo is er bijvoorbeeld wel een specifiek recht op inzage in archiefstukken in een archiefbewaarplaats.[60]

Verwerking van het nationaal identificatienummer
In artikel 87 AVG wordt lidstaten de mogelijkheid geboden specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer. In artikel 46 UAVG is daar invulling aangegeven door te bepalen dat 'een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.' In sectorale wetgeving kunnen dus bepalingen worden opgenomen over het gebruik van het burgerservicenummer (BSN). Voor de overheid is dit geregeld in de Wet algemene bepalingen Burgerservicenummer (Wabb), en voor de zorg in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.[61] Met de hiervoor genoemde bepaling uit de UAVG is door de nationale wetgever invulling gegeven aan de mogelijkheid om voorwaarden te stellen aan de verwerking van een nationaal identificatienummer, zoals in artikel 87 van de verordening mogelijk is gemaakt.

Voorwaarden voor toestemming van kinderen
Een element van de verordening waar de nationale wetgever geen verdere invulling aan heeft gegeven, betreft artikel 8 AVG. Op basis van die bepaling geldt dat kinderen onder de zestien jaar toestemming moeten hebben om op het aanbod van diensten van de informatiemaatschappij in te gaan. Vervolgens wordt lidstaten de mogelijkheid geboden om deze grens te verlagen naar maximaal dertien jaar. De nationale wetgever heeft geen reden gezien om de grens van zestien jaar, die in de Wbp was opgenomen, aan te passen en heeft die in de UAVG overgenomen.[62]

2.5 Verzamelwet Gegevensbescherming

Om de UAVG zo soepel mogelijk en gelijktijdig met de inwerkingtreding van de AVG in werking te laten treden, is in Nederland gekozen om niet bovenop de veranderingen die de AVG meebracht nieuwe nationaalrechtelijke regels te introduceren. Wel is tijdens de behandeling van het wetsvoorstel voorgesteld direct na de afronding van het wetsvoorstel te verkennen of er mogelijkheden zijn tot verbetering en verdere modernisering van het gegevensbeschermingsrecht.[63] Naar aanleiding van de behandeling en de constatering dat er binnen de Tweede Kamer nog diverse vragen en wensen leefden, is de motie-Koopmans ingediend en overgenomen. In deze motie werd de regering verzocht de ervaringen met de nieuwe wetgeving binnen

[59] Artikelen 15, 16, 18, eerste lid, sub a en 20 AVG.
[60] Artikel 45, tweede lid UAVG.
[61] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 51.
[62] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 52.
[63] *Handelingen II* 2017/18, 59, item 4, p. 18.

een half jaar na inwerkingtreding met de Tweede Kamer te delen, en zo nodig maatregelen te treffen.[64]

De Tweede kamer is vervolgens op 1 april 2019 geïnformeerd over de resultaten van de inventarisatie, waarbij vooral uit de punten uit de motie-Koopmans werd ingegaan.[65] Uit de inventarisatie kwam naar voren dat er over de uitleg van de AVG en UAVG veel vragen leefden en er behoefte was aan voorlichting. Ook kwam naar voren dat er zorgen bestonden over de ruimte voor gegevensverwerking. Daarnaast waren er klachten over de toename van administratieve lasten, was er behoefte aan duidelijkheid of men in specifieke gevallen de (U)AVG goed naleefde, en bestond er een knelpunt op het element van de leeftijdsgrens. Verder werd aangegeven dat de Kamer geïnformeerd zou worden over punten die onder de aandacht waren gebracht en op welke punten een wijziging van de UAVG zal worden voorbereid.[66]

De Tweede Kamer is een half jaar later op 31 oktober 2019 geïnformeerd over de punten waarop de UAVG zou moeten worden gewijzigd. Met betrekking tot de onderdelen waarvoor een wijziging in de UAVG wenselijk was, gaf de minister aan dat een wetsvoorstel zou worden opgesteld. Dit wetsvoorstel is op 5 mei 2020 gepubliceerd, lag tot 14 juni 2020 voor ter consultatie en is aan de AP voor advies voorgelegd. In het wetsvoorstel worden, naast wijzigingen van meer technische en verduidelijkende aard, ook inhoudelijke wijzigingen voorgesteld, zoals onder meer de voorwaarden waaraan het gebruik van biometrische gegevens dient te voldoen en een uitzonderingsgrond voor de verwerking van bijzondere categorieën persoonsgegevens bij verplichte accountantscontroles. Ook houdt het conceptwetsvoorstel een wijziging van de Faillissementswet in waardoor persoonsgegevens (inclusief BSN), voor zover dit noodzakelijk is voor bijvoorbeeld het beheer en vereffening van de boedel, verwerkt mogen worden door curatoren en (Wsnp-)bewindvoerders.[67]

De AP heeft al op 11 november 2020 een schriftelijk advies over het wetsvoorstel uitgebracht.[68] Het advies van de Raad van State over het wetsvoorstel is op 22 mei 2022 gepubliceerd.[69] De Raad van State maakt onder andere opmerkingen over de invulling die wordt gegeven aan open AVG-normen zoals ‘zwaarwegend algemeen belang’ en ‘passende en specifieke maatregelen en waarborgen’. De Raad vindt dat de Nederlandse regels waarmee de AVG wordt uitgevoerd nog meer kunnen verhelderen hoe dit soort open normen moet worden ingevuld, zodat duidelijker is wat daarmee wordt bedoeld. De Raad stelt vast dat het met het oog op de overzichtelijkheid en toegankelijkheid van de AVG en het daarop gebaseerde nationale gegevensbeschermingsrecht van belang is dat duidelijkheid bestaat over wat in de UAVG en wat in sectorale wetten is geregeld. In de toelichting bij het eerdere wetsvoorstel UAVG is met het oog daarop als uitgangspunt geformuleerd dat uitzonderingen, en rechtsgrondslagen voor de verwerking van (bijzondere) persoonsgegevens voor het vervullen van een publieke taak of wettelijke verplichting doorgaans worden gegeven in sectorspecifieke wetgeving. Dit uitgangspunt leidt ertoe dat in de UAVG met name regelingen zijn te vinden die het belang van een specifieke sector overstijgen. De Raad acht het wenselijk dat dit uitgangspunt ook gehanteerd wordt bij de wijzigingen die in de Verzamelwet worden voorgesteld en vraagt zich af of dat voldoende consequent is gedaan.

[64] *Kamerstukken II* 2017/18, 34851, nr. 19.
[65] *Kamerstukken II* 2018/19, 32761, nr. 132.
[66] *Kamerstukken II* 2018/19, 32761, nr. 132, p.2.
[67] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 1. De inhoudelijke voorgestelde wijzigingen zijn opgenomen in bijlage x.
[68] Autoriteit Persoonsgegevens 2020-2.
[69] Raad van State 2022.

2.6 Wijziging Wbp: meldplicht datalekken en bestuurlijke boete

In 2005 werd de regering in het kader van de wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (Computercriminaliteit II) in de motie van de leden Gerkens en Van Dam[70] reeds verzocht in kaart te brengen wat de positieve en negatieve gevolgen zouden kunnen zijn van het instellen van een verplichting voor bedrijven, overheden en organisaties om burgers en bedrijven op de hoogte te brengen wanneer hun gegevens ontvreemd dan wel hun systemen gehackt zijn.

Naar aanleiding van een groot aantal en soms ook ernstige incidenten, waarbij door een inbreuk op de beveiliging van, onder meer, websites persoonsgegevens vrijkwamen met nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen, werd in het regeerakkoord van het kabinet-Rutte I 'Vrijheid en verantwoordelijkheid' van 30 september 2010 over de noodzaak van een meldplicht datalekken gesproken. Het toezicht op de naleving en de handhaving van de meldplicht zou aan het College bescherming persoonsgegevens (Cbp) worden opgedragen.

In het regeerakkoord van het kabinet-Rutte II 'Bruggen slaan' van 29 oktober 2012 was opgenomen dat het Cbp meer bevoegdheden zou krijgen, waaronder de bevoegdheid om in meer gevallen bestuurlijke boetes op te leggen.[71] [72] Dit hield verband met een breed ervaren nalevingstekort van de Wbp, zoals dat uit de tweede evaluatie van de Wbp naar voren kwam. Tevens was er bij de regering het besef dat het opleggen van reparatoire sancties of het dreigen daarmee een generaal preventieve werking ontbeerde en het gemis van de dreigende en afschrikwekkende werking van een forse bestuurlijke boete. De verwachting was dat dit de effectiviteit en efficiëntie van het optreden van het Cbp ten goede zou komen.[73] Dit correspondeerde met een beroep dat het Cbp in 2009 op de wetgever deed om onder meer een plicht tot het melden van datalekken op te nemen in de wet en een versterking van het sanctiestelsel in de Wbp.[74] Het voorstel voor uitbreiding van de boetebevoegdheid[75] sloot tevens aan bij de doelstelling van de verordening om de handhaving te versterken. Ook de concept-verordening algemene gegevensbescherming voorzag in de bevoegdheid voor de nationale toezichthouders om bestuurlijke boetes op te leggen bij overtreding van de verordening.

Op 17 juni 2013 werd het wetsvoorstel om te komen tot een meldplicht datalekken aangeboden aan de Tweede Kamer. Na drie nota's van wijziging, waarbij in de tweede nota van wijziging het voorstel werd opgenomen om de materiële normen van de Wbp bestuurlijk beboetbaar te maken, trad op 1 januari 2016 de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp in werking.[76]

2.6.1 Meldplicht datalekken

Ingevolge de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp die onder meer haar beslag kreeg in artikel 34a Wbp diende de verwerkingsverantwoordelijke het Cbp onverwijld in kennis te stellen van een inbreuk op de beveiliging als bedoeld in artikel

[70] *Kamerstukken II* 2005-2006, 26671, nr. 20.
[71] *Kamerstukken II* 2012/13, 33662, nr. 3.
[72] Zie ook motie Recourt, Elissen en Berndsen, *Kamerstukken II 2011/12*, 32761, nr. 40.
[73] *Kamerstukken II* 2014/15, 33 662, nr. 9.
[74] College bescherming persoonsgegevens 2010.
[75] Het CBP had reeds een beperkte bevoegdheid om overtreding van administratieve verplichtingen bestuurlijk te beboeten. Het CBP kon aan de verwerkingsverantwoordelijke een bestuurlijke boete opleggen van ten hoogste € 4.500.
[76] *Stb.* 2015, 281.

13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Daarnaast diende de verwerkingsverantwoordelijke de betrokkene onverwijld in kennis te stellen van de hiervoor genoemde inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Bij de totstandkoming van de meldplicht datalekken heeft de wetgever bewust niet volledig aangesloten bij de meldplicht datalekken zoals deze in de conceptverordening algemene gegevensbescherming was opgenomen. De reden daarvoor was dat de regeling van de meldplicht in de concept-verordening, die destijds nog niet was vastgesteld, te veel aanleiding gaf tot vragen over de reikwijdte van de daarin opgenomen verplichtingen en de invulling van de daarbij in acht te nemen voorwaarden en het was nog prematuur om ervan uit te gaan dat de Europese wetgever met een redelijke mate van zekerheid regeling overeenkomstig het voorstel zal vaststellen.[77]

Hoewel de in artikel 34a Wbp opgenomen meldplicht datalekken qua reikwijdte aansloot bij de meldplicht datalekken in de conceptverordening, was deze bepaling minder verstrekkend omdat de meldplicht uit de Wbp een clausulering bevatte waarmee werd beoogd[78] bagatelzaken van de meldplicht uit te sluiten door de plicht uitsluitend betrekking te laten hebben op de doorbrekingen van maatregelen voor de beveiliging van persoonsgegevens. De conceptverordening (en uiteindelijk ook de AVG) kende een dergelijke clausulering niet, waardoor volgens de wetgever elk denkbaar datalek aan de toezichthouder zou moeten worden gemeld. Een dergelijke clausulering was volgens de Wbp-wetgever nodig, omdat anders de effectiviteit van de meldplicht voor datalekken snel aan betekenis zou verliezen wanneer elk denkbaar datalek in aanmerking komt om te worden gemeld. Een meldplicht zonder enige beperking leidt bovendien tot een nodeloze belasting van bedrijfsleven en overheid, aldus de wetgever.[79]

Overigens stelde de Afdeling advisering van de Raad van State in haar eerste advies vraagtekens bij de effectiviteit van de meldplicht en bij de lasten die deze mee zou brengen. De onbepaaldheid van de meldplicht in combinatie met de forse boete die op het niet naleven stond, zou ertoe kunnen leiden dat vaker onnodig zou worden gemeld met alle gevolgen van dien.[80] Dit standpunt werd door de regering niet gedeeld. Met de gekozen formulering werd aangesloten bij de normstelling in de Wbp, die naar zijn aard als algemeen-abstract werd gekenschetst. Dit werd verklaard door de grote diversiteit aan verwerkingen van persoonsgegevens in de private en publieke sector. De regering meende dat de gekozen formulering voldoende duidelijk was en in de praktijk ook goed hanteerbaar; een nadere precisering zou ontegenzeggelijk leiden tot een beperktere meldplicht dan wenselijk was. Daarnaast meende de regering dat de noodzaak om meldingen van datalekken te doen vooral ook zou afhangen van de naleving van de verplichting om zorg te dragen voor een adequate beveiliging van persoonsgegevens, zodat deze niet zouden worden blootgesteld aan onrechtmatige verwerking of verlies. Daarbij werd verwezen naar de in februari 2013 door het Cbp gepubliceerde richtsnoeren, waarin het aangeeft wat het van de beveiliging van persoonsgegevens verwacht. Ondanks dat de regering het moeilijk vond om te voorspellen wat de effecten daarvan zouden zijn, werd in zijn algemeenheid verwacht dat deze richtsnoeren eraan zouden bijdragen dat de verwerkingsverantwoordelijken investeren in een goede en op de specifieke kenmerken en risico's van de verwerking van toegesneden beveiliging, zodat het lekken van persoonsgegevens

[77] *Kamerstukken II* 2012/13, 33662, nr. 3.
[78] *Kamerstukken II* 2012/13, 33662, nr. 4.
[79] *Kamerstukken II* 2012/13, 33662, nr. 3.
[80] *Kamerstukken II 2012/13*, 33662, nr. 4.

wordt voorkomen of beperkt. Op 16 december 2015 publiceerde het Cbp de Beleidsregels meldplicht datalekken[81] met als doel om bedrijven, overheden en andere organisaties tot wie de meldplicht datalekken zich richt te ondersteunen bij de afweging of een concreet datalek dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Ook dienden de beleidsregels als uitgangspunt voor de toezichthouder bij het toepassen van handhavende maatregelen.

Na het van toepassing worden van de AVG op 25 mei 2018 werd de Wbp ingetrokken en gold de in de AVG opgenomen meldplicht datalekken. Ingevolge artikel 33 was sprake van een te melden datalek, indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Daarmee kent de AVG in tegenstelling tot de Wbp een algemene uitzondering op de meldplicht. De European Data Protection Board (EDPB) en haar voorganger de WP29 publiceerde een tweetal guidelines. WP29 publiceerde in oktober 2017 een guideline met een meer algemene toelichting en uitleg over datalekken.[82] Nu deze eerste guideline niet alle praktische problemen voldoende adresseerde, heeft de EDPB op 21 januari 2021 een guideline gepubliceerd met praktijkgerichte guidance.[83]

2.6.2 Bestuurlijke boete

Op 1 januari 2016 kreeg de AP de bevoegdheid tot het opleggen van een bestuurlijke boete ter hoogte van € 820.000 dan wel 10% van de jaaromzet.

Gevolg gevend aan het advies van de Afdeling advisering van de Raad van State voorzag de aanpassing van de Wbp daarnaast in een tweetal voorzieningen die tegemoet moesten komen aan de behoefte om meer checks and balances in het systeem in te bouwen en om de waarborgen voor de verantwoordelijken te versterken. De behoefte aan meer checks and balances hing samen met het feit dat een sterkere concentratie van uiteenlopende taken bij de toezichthouder zou komen te liggen. Een deel van de normstelling kwam te liggen bij het orgaan dat vervolgens werd geacht om dezelfde normen door middel van punitieve sancties te handhaven, waarmee de normstelling en handhaving in belangrijke mate in één hand kwamen te liggen. Dit resulteert in een bepaling die inhoudt dat beleidsregels van de AP die uitleg geven aan de materiële normen van de Wbp waarvan overtreding door de AP met een bestuurlijke boete kan worden bestraft, aan ministeriële goedkeuring zijn onderworpen. Tevens wordt, in verband met het algemeen-abstracte karakter van de normen van de Wbp en het lex certa-beginsel[84], een bepaling opgenomen die inhoudt dat de AP bij een vermoeden van overtreding van deze open normen in de regel niet zonder meer een bestuurlijke boete kan opleggen, maar dat het eerst een bindende aanwijzing moet geven. In de bindende aanwijzing zal de toezichthouder ter concretisering van de wettelijke norm moeten aangeven welke gedraging op grond van de Wbp van de verantwoordelijke wordt verwacht en hem zo mogelijk moeten

[81] *Stcrt.* 2015, 46128.
[82] Data Protection Working Party 2018.
[83] European Data Protection Board 2021.
[84] Het betreft een subbeginsel van het legaliteitsbeginsel en houdt kort in dat voor iedereen duidelijk moet zijn welk handelen en nalaten leidt tot strafrechtelijke aansprakelijkheid, alsmede welke sancties daar op kunnen volgen. Deze duidelijkheid moet in de wet besloten zijn. Maar daarbij doet zich een tegenstrijdigheid voor omdat de wetgever soms met een zekere vaagheid, door het gebruik van algemene termen, delicten omschrijft om te voorkomen dat gedragingen die strafwaardig zijn buiten het bereik van de delictsomschrijving vallen. Die vaagheid kan onvermijdelijk zijn, omdat niet altijd te voorzien is op welke wijze de te beschermen belangen in de toekomst zullen worden geschonden en omdat, indien dit wel is te voorzien, delictsomschrijvingen anders te verfijnd worden met als gevolg dat de overzichtelijkheid wegvalt en daarmee het belang van de algemene duidelijkheid van de wetgeving schade lijdt. Uit EHRM 11 november 1996, nr. 17862/91, ECLI:CE:ECHR:1996:1115JUD001786291 volgt dat artikel 7 EVRM mede het lex certa-beginsel inhoudt

opdragen om de overtreding geheel of gedeeltelijk te herstellen.[85][86] Het direct opleggen van een bestuurlijke boete is mogelijk, indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid. Volgens de kamerstukken is daarvan sprake, in het geval het een gevolg is van grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen of indien meerdere malen eenzelfde type overtreding heeft plaatsgevonden. Ook het niet-nakomen van een opgelegde bindende aanwijzing is afzonderlijk bestuurlijk beboetbaar, waarmee wordt aangesloten bij vergelijkbare constructies in andere wetten en de Algemene wet bestuursrecht.[87]

Een bindende aanwijzing noch een bestuurlijke boete zou na deze wijziging van de Wbp worden opgelegd. Ook in de periode na 1 januari 2016 tot het van toepassing worden van de AVG geeft de toezichthouder blijk van een voorkeur om gebruik te maken van de bevoegdheid tot het opleggen van een last onder dwangsom.[88] Waar echter onder de Wbp een bindende aanwijzing gekoppeld was aan de bevoegdheid om een bestuurlijke boete op te leggen, komt dit voorportaal tot boeteoplegging niet terug in de UAVG. De reden daarvoor is dat toezichthouders op grond van de AVG beschikken over een scala aan bevoegdheden om toezicht te houden op de naleving daarvan en om zo nodig handhavend op te treden. Binnen deze systematiek ziet de wetgever geen ruimte om de toezichthouder te verplichten tot het geven van een bindende aanwijzing voorafgaand aan het opleggen van een bestuurlijke boete.[89]

Met oog op de toepassing van die bevoegdheid heeft de Autoriteit Persoonsgegevens beleidsregels vastgesteld, zijnde de 'Boetebeleidsregels Autoriteit Persoonsgegevens 2016'.[90]

Met deze uitbreiding van de boetebevoegdheid van de Autoriteit Persoonsgegevens onder de Wbp, heeft de Autoriteit Persoonsgegevens de gelegenheid gekregen toe te groeien naar het handhavingssysteem van de per 25 mei 2018 van toepassing geworden AVG. De AVG voorziet in een uitgebreide bevoegdheid voor de nationale toezichthouders om boetes op te leggen bij overtreding van deze verordening. De toezichthoudende autoriteit kan ingevolge artikel 83 organisaties die de AVG overtreden een boete opleggen van maximaal twintig miljoen euro of 4% van de wereldwijde jaaromzet. Op grond van artikel 14, derde lid UAVG is deze bevoegdheid toebedeeld aan de Autoriteit Persoonsgegevens. Op grond van de artikelen 17 en 18 UAVG kan de Autoriteit Persoonsgegevens ook boetes opleggen aan een overheidsinstantie of een overheidsorgaan wegens overtredingen van de AVG en de UAVG.

Op 3 oktober 2017 heeft de WP29 'Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten in de zin van Verordening (EU) 2016/679'[91] goedgekeurd. Op 25 mei 2018 heeft 'de EDPB deze richtsnoeren bekrachtigd. Hierin zijn regels en uitgangspunten opgenomen met het oog op een consistente aanwending van de boetebevoegdheid onder de AVG.

Het opleggen van een administratieve geldboete wordt in deze opinie gezien als een belangrijk instrument dat de toezichthoudende autoriteiten in passende omstandigheden moeten gebruiken. Deze autoriteiten worden aangemoedigd om bij het gebruik van corrigerende

[85] *Kamerstukken II* 2014/15, 33662, nr. 9 in samenhang bezien met het advies van de Afdeling advisering van de Raad van State van 19 februari 2014 (*Strct*. 2014, 34523; W03.13.0464/II).
[86] *Kamerstukken II* 2014/15, 33662, nr. 19.
[87] *Kamerstukken II* 2014/15, 33662, nr. 16.
[88] Jaarverslagen 2016, 2017 en 2018 Autoriteit Persoonsgegevens.
[89] *Kamerstukken II* 2017/18, 34 851, nr. 4.
[90] Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015 (*Stcrt*. 2016, 2043), zoals laatstelijk gewijzigd op 6 juli 2016 (*Stcrt.* 2016, 34960), met betrekking tot het opleggen van bestuurlijke boetes.
[91] WP29-opinie WP 253.

maatregelen een weloverwogen en evenwichtige aanpak te hanteren teneinde zowel een doeltreffende en afschrikkende als een evenredige reactie op de inbreuk te bewerkstelligen. Het gaat er niet om de geldboete als laatste redmiddel aan te merken, noch om ervoor terug te deinzen een geldboete op te leggen, maar wel om deze niet zodanig te gebruiken dat de doeltreffendheid als instrument wordt aangetast. Bij het bepalen of een administratieve geldboete wordt opgelegd dienen toezichthoudende autoriteiten alle feiten van het geval op een consistente en objectief gerechtvaardigde wijze te beoordelen.[92]

Of de toezichthoudende autoriteiten de eerdergenoemde beoordeling op consistente en objectief gerechtvaardigde wijze uitvoeren, kan in het kader van de geschilbeslechting tussen de autoriteiten achteraf door de EDPB worden beoordeeld en uiteindelijk door het Europese Hof van Justitie (HvJ-EU) in de daar voorliggende situatie.

Aangezien de EDPB op dat moment nog geen gezamenlijke uitgangspunten voor de berekening van boetehoogte had vastgesteld, heeft de AP aanleiding gezien om beleid vast te stellen inzake de invulling van de bevoegdheid tot het opleggen van een boete onder de AVG en UAVG. Meer specifiek heeft dit beleid – Boetebeleidsregels Autoriteit Persoonsgegevens 2019 – betrekking op het bepalen van de hoogte van een boete, omwille van de rechtsgelijkheid en rechtszekerheid.[93]

De EDPB heeft op het moment van schrijven van dit rapport de Guidelines ‘on the calculation of administrative fines under the GDPR’[94] in consultatie gedaan, waarmee de EDPB invulling heeft aan de gemeenschappelijke uitgangspunten voor de berekening van de boetehoogtes.

[92] WP29, WP253, p. 6-8.
[93] Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (*Stcrt.* 2019, 14586).
[94] European Data Protection Board 2022, par. 1.2. De consultatie van deze richtsnoeren loopt tot en met 27 juni 2022.

3 Jurisprudentieonderzoek

3.1 Inleiding

In dit deel van het evaluatieonderzoek hebben we met behulp van de zoekfunctionaliteit van het uitsprakenregister op www.rechtspraak.nl gezocht op de termen 'UAVG' en 'Uitvoeringswet AVG'. De hypothese is dat we daarmee de uitspraken zouden vinden waarin partijen een op de UAVG gebaseerde stelling naar voren hebben gebracht, alsmede de uitspraken waarin het ging om een besluit van de AP. We realiseren ons evenwel dat de beschermende werking van de AVG en UAVG nog niet altijd gemeengoed is onder procederende partijen en de rechterlijke macht. En we moeten dus accepteren dat we niet de uitspraken hebben gevonden waarin de AVG en UAVG geen betekenis hebben gehad, waar dat mogelijk wel had gekund.

Dit hoofdstuk geeft een antwoord op deelvraag 2 die gaat over de mate waarin de jurisprudentie de normen van de UAVG verduidelijkt en de deelvragen 9 en 16 die de preventieve werking van de jurisprudentie op de naleving van de UAVG en de meldplicht datalekken betreffen.

3.2 Toetsing aan de UAVG

Uit de analyse van de jurisprudentie volgt dat de UAVG door de rechter expliciet en ook ambtshalve wordt betrokken bij de beoordeling van vraagstukken die raken aan het procesrecht. Het gaat daarbij over de toepasselijkheid van de Awb bij de beoordeling van een schriftelijke beslissing op een verzoek als bedoeld in artikel 15 tot en met 22 UAVG (artikel 34 UAVG), de toepasselijkheid en reikwijdte van de verzoekschriftprocedure als bedoeld in artikel 35 UAVG, de ontvankelijkheid van het verzoekschrift en de vraag of de procedure van artikel 34 of die

van artikel 35 UAVG moet worden gevolgd. [95, 96] In dit verband is de 1 april-jurisprudentie van de Afdeling bestuursrechtspraak van de Raad van State van belang. Daarin heeft de Afdeling zich op grond van artikel 8:88, eerste lid, aanhef en onder a Awb in samenhang met artikel 34 UAVG, bevoegd geacht om te beslissen op een verzoek om schadevergoeding vanwege schade ontstaan uit een verwerking van persoonsgegevens in verband met een besluit van een bestuursorgaan op een verzoek op grond van de artikelen 15-22 AVG.[97] In het verlengde van de 1 april-jurisprudentie heeft de Afdeling in haar uitspraak van 2 februari 2022 overwogen dat degene die op grond van artikel 82 AVG aanspraak stelt te maken op vergoeding van schade die het gevolg is van het onrechtmatig verwerken van persoonsgegevens door een bestuursorgaan, overeenkomstig artikel 8:88 Awb, keuzevrijheid heeft om zijn verzoek aan de bestuursrechter voor te leggen dan wel zijn aanspraak op schadevergoeding via de civielrechtelijke weg te realiseren. Voor indiening van een dergelijk verzoek is het niet nodig dat de betrokkene eerst een beroep heeft gedaan op zijn rechten genoemd in hoofdstuk III van de AVG.[98]

Materieelrechtelijk vormt zich het beeld dat alleen aan de UAVG wordt getoetst wanneer partijen zelf de UAVG bij hun betoog betrekken of wanneer het gaat om een besluit van de AP. Ambtshalve lijkt er geen (zichtbare) materiële toetsing plaats te vinden aan de UAVG (bijvoorbeeld door het ambtshalve aanvullen van rechtsgronden), in zaken waarin de feiten daartoe wel aanleiding hadden kunnen geven. In die gevallen wordt of aan hoger recht getoetst (het EVRM en het Handvest) of toetst de rechter direct aan sectorale wetgeving, zonder daarbij ook expliciet te toetsen of de UAVG een voorwaarde schept om het verwerkingsverbod op bijzondere persoonsgegevens te doorbreken. In een enkel geval geeft de rechter ervan blijk dat de UAVG een rol speelt in het geschil, zonder ook daadwerkelijk aan de UAVG te toetsen.[99] De wetgever heeft destijds uit vrees dat de verbrokkeling van regelgeving in ernstige mate afbreuk zou doen aan de samenhang, de begrijpelijkheid en het verkrijgen van een volledig en juist beeld van het regime van de bijzondere categorieën van persoonsgegevens gebruik gemaakt van de ruimte die overweging 8 van de AVG biedt om in weerwil van het overschrijfverbod artikel 9 AVG over te nemen in artikel 22 UAVG.[100] De wetgever heeft daarom getracht om artikel 22 UAVG als schakelbepaling te laten functioneren tussen de AVG enerzijds en sectorale wetgeving en de specifieke bepaling uit de UAVG anderzijds. In de praktijk wordt echter direct getoetst aan de uitzonderingsgronden in de artikelen 23 tot en met 30 UAVG dan wel

[95] Rb. Zeeland-West-Brabant 13 augustus 2020, ECLI:NL:RBZWB:2020:3789; Rb. Midden-Nederland (vzr.) 23 juni 2020, ECLI:NL:RBMNE:2020:2424; ABRvS 1 april 2020, ECLI:NL:RVS:2020:898; Rb. Den Haag (vzr.) 13 november 2019, ECLI:NL:RBDHA:2019:12031; Rb. Amsterdam 25 september 2019, ECLI:NL:RBAMS:2019:8329; Rb. Midden-Nederland 29 mei 2019, ECLI:NL:RBMNE:2019:2434; Rb. Amsterdam 14 maart 2019, ECLI:NL:RBAMS:2019:2001; Rb. Amsterdam (vzr.) 15 februari 2021, ECLI:NL:RBAMS:2021:619; Hof Amsterdam 2 februari 2021, ECLI:NL:GHAMS:2021:312; Rb. Amsterdam (vrz.) 21 januari 2021, ECLI:NL:RBAMS:2021:174; HR 3 december 2021, ECL:NL:HR:2021:1814; Rb. Limburg 4 september 2020, ECLI:NL:RBLIM:2020:6702; Rb. Amsterdam 3 december 2020, ECLI:NL:RBAMS:2020:7536; Rb. Amsterdam 23 december 2019, ECLI:NL:RBAMS:2019:9887; Rb. Noord-Nederland 4 december 2019, ECLI:NL:RBNNE:2019:5063; Rb. Overijssel 9 oktober 2019, ECLI:NL:RBOVE:2019:3754; Rb. Amsterdam 18 juli 2019, ECLI:NL:RBAMS:2019:5182; Rb. Midden-Nederland 29 mei 2019, ECLI:NL:RBMNE:2019:2434; Rb. Amsterdam 20 juni 2019, ECLI:NL:RBAMS:2019:4418; Rb. Noord-Holland 23 mei 2019, ECLI:NL:RBNHO:2019:4283; Rb. Amsterdam 21 maart 2019, ECLI:NL:RBAMS:2019:2166; Rb 's-Gravenhage 7 maart 2019, ECLI:NL:RBDHA:2019:4324; HR 14 december 2018, ECLI:NL:HR:2018:2311; Rb. Midden-Nederland 3 oktober 2018, ECLI:NL:RBMNE:2018:5020; Rb. Zeeland-West-Brabant 24 mei 2019, C/02/353094/HA RK 18-244, *JBP* 2019/124; Hof Amsterdam 5 november 2019, ECLI:NL:GHAMS:2019:3966; Hof Arnhem-Leeuwarden 7 januari 2020, ECLI:NL:GHARL:2020:126.

[96] Verondersteld kan worden dat de vraag of de betrokken entiteit verwerkingsverantwoordelijke is, gelet op de strekking van de artikelen 34 en 35 UAVG (zie onder meer Rb. Noord-Nederland 1 maart 2021 ECLI:NL:RBNNE:2021:738 en Hof Arnhem-Leeuwarden 22 februari 2022 ECLI:NL:GHARL:2022:1322) eveneens ambtshalve dient te worden beoordeeld.

[97] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, r.o. 22; ABRvS 1 april 2020, ECLI:NL:RVS:2020:899, r.o. 19; ABRvS 1 april 2020, ECLI:NL:RVS:2020:900, r.o. 21; ABRvS 1 april 2020, ECLI:NL:RVS:2020:901, r.o. 27.

[98] ABRvS 2 februari 2022, ECLI:NL:RVS:2022:319, r.o. 14.1.

[99] Vgl. Rb. Den Haag 15 mei 2020, ECLI:NL:RBDHA:2020:4789.

[100] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 44

de in sectorale wetgeving opgenomen uitzonderingsgronden. Daarmee heeft artikel 22 UAVG niet de schakelfunctie die de wetgever voor ogen had.

Bij de beoordeling of een verwerkingsverantwoordelijke terecht de verplichtingen en rechten uit de artikelen 12 tot en met 21 en 34 AVG buiten toepassing heeft gelaten, toetst de rechter in het overgrote deel van de gevallen expliciet aan artikel 41 UAVG, waarin uitzonderingen op de plichten van verwerkingsverantwoordelijken en de rechten van betrokkenen zijn opgenomen.[101] In een enkel geval gebeurt dit niet en toetst de rechter rechtstreeks aan sectorale wetgeving, waarin een vergelijkbare uitzondering is opgenomen.[102]

3.3 Rechtsbescherming

Wanneer een betrokkene zijn rechten uitoefent op grond van de artikelen 15 tot en met 22 AVG en daarbij niet het gewenste resultaat behaalt, kent de UAVG twee sporen waarlangs de betrokkene rechtsbescherming kan verkrijgen, namelijk het bestuursrechtelijke spoor (artikel 34 UAVG) en het civielrechtelijke spoor (artikel 35 UAVG). Deze procedures zijn gelijk aan die in de Wbp.

3.3.1 Bestuursrecht

Voor zover de verwerkingsverantwoordelijke een bestuursorgaan in de zin van de Awb is, is ingevolge artikel 34 UAVG de Awb van toepassing op beslissingen naar aanleiding van de uitoefening van rechten van betrokkenen. De beslissing van het bestuursorgaan, waarbij gevolg wordt gegeven aan het verzoek als het verzoek geheel of gedeeltelijk wordt geweigerd, is dan een besluit als bedoeld in artikel 1:3, eerste lid Awb, waartegen bezwaar kan worden gemaakt en beroep kan worden ingesteld.[103] Op grond van artikel 12, derde lid AVG moet een verwerkingsverantwoordelijke onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek informeren over het gevolg dat aan het verzoek is gegeven. Wanneer het om een complex verzoek gaat, kan de beslistermijn met twee maanden wordt verlengd. Dit betekent dat verzoeker binnen een maand in ieder geval een eerste reactie dient te krijgen op zijn verzoek. Indien deze reactie uitblijft is er op grond van artikel 6:2 aanhef en onderdeel b Awb derhalve sprake van een besluit en is artikel 6:12 Awb van toepassing. Dit betekent dat beroep kan worden ingesteld tegen het niet tijdig nemen van het besluit op voorwaarde dat het bestuursorgaan in gebreke is gesteld en twee weken de tijd heeft gekregen om alsnog te besluiten.[104] De mogelijkheid die artikel 6:12 Awb biedt, geldt eveneens indien het bestuursorgaan nog geen beslissing heeft genomen binnen twee maanden na de kennisgeving dat de termijn met twee maanden is verlengd.[105]

De UAVG kent geen mogelijkheid om door middel van het bestuursrecht het achterliggend bestuurlijk handelen met betrekking tot de verwerking van persoonsgegevens zelf aan de rechter voor te leggen. Wel heeft de Afdeling bestuursrechtspraak in navolging van haar eerdere zogenoemde 1 april-jurisprudentie met haar uitspraak van 2 februari 2022 ruimte geboden om een verzoek als bedoeld in artikel 82 AVG overeenkomstig 88 AVG aan de bestuurs-

[101] Rb. Amsterdam 20 juni 2019, ECLI:NL:RBAMS:2019:4418; Rb. Amsterdam 25 september 2019, ECLI:NL:RBAMS:2019:8329; Rb. Den Haag 10 oktober 2019, ECLI:NL:RBDHA:2019:13029.
[102] Zie ook Rb. Amsterdam 25 september 2019, ECLI:NL:RBAMS:2019:8329, *JBP* 2020/24 m.nt. K. Konings.
[103] Rb. Den Haag (vzr.) 13 november 2019, ECLI:NL:RBDHA:2019:12031, r.o. 4.2; Rb Amsterdam 25 september 2019, ECLI:NL:RBAMS:2019:8329.
[104] Rb. Zeeland-West-Brabant 13 augustus 2020, ECLI:NL:RBZWB:2020:3789, r.o. 2.
[105] *Kamerstukken II* 2017/18, 34 851-2, nr 3.

rechter voor te leggen zonder dat betrokkene eerst een beroep heeft gedaan op zijn rechten genoemd in de artikelen 15 tot en met 22 AVG.[106]

3.3.2 Civiel recht

Indien de verwerkingsverantwoordelijke geen bestuursorgaan is, schrijft artikel 35 UAVG voor dat betrokkene of een andere belanghebbende door middel van een verzoekschriftprocedure als bedoeld in artikel 261 van het Wetboek van Burgerlijke Rechtsvordering (Rv) zich tot de civiele rechter wenden om op te komen tegen een beslissing van een verwerkingsverantwoordelijke op een verzoek op grond van de artikelen 15 tot en met 22 AVG. Indien de verwerkingsverantwoordelijke heeft gereageerd binnen de termijn ingevolge artikel 12, derde lid AVG dient binnen zes weken na ontvangst van het antwoord het verzoekschrift te zijn ingediend. Antwoord de verwerkingsverantwoordelijke niet binnen die termijn, dan geldt er geen termijn voor het indienen van een verzoekschrift.[107] Op deze wijze gelden voor de bestuursrechtelijke en civielrechtelijke dezelfde termijnen.[108]

Het hiervoor beschreven stelsel berust op de gedachte dat partijen eerst onderling tot overeenstemming proberen te komen, de belanghebbende daarna als uitgangspunt kort de tijd heeft om bij de rechter een vordering in te dienen. De strekking van de genoemde termijn is mede om te voorkomen dat de verwerkingsverantwoordelijke lange tijd nadat hij het verzoek heeft afgewezen, nog in rechte kan worden betrokken.[109]-[110] Uit de rechtspraak volgt dat het voor betrokkene niet zonder meer duidelijk is wanneer een verzoek is geweigerd en daarmee wanneer de termijn van zes weken verlopen is.[111]

De wetgever lijkt voor de verzoekschriftprocedure boven de procedure ingeleid bij dagvaarding ingevolge artikel 78 in samenhang bezien met artikel 261 Wetboek van Burgerlijke Rechtsvordering (Rv) te hebben gekozen, omdat de verzoekschriftprocedure in het algemeen als laagdrempeliger, eenvoudiger, informeler en korter wordt beschouwd en waarbij bovendien een uitzondering is gemaakt op de anders bij de rechtbank verplichte procesvertegenwoordiging. Dit om op snelle en eenvoudige wijze vast te stellen of en zo ja welke, en op welke wijze, persoonsgegevens worden verwerkt en waarbij het eventueel te geven bevel aan de verwerkingsverantwoordelijke om het verzoek om inzage, rectificatie, wissing of beperking alsnog toegewezen kan worden al dan niet versterkt met een dwangsom.[112] [113]

De rechtsingang door middel van een verzoekschriftprocedure beperkt zich tot het bevel om een verzoek als bedoeld in de artikelen 15 tot en met 22 toe of af te wijzen. Indien aanvullend wordt verzocht om bijvoorbeeld vernietiging van bepaalde genomen besluiten of een verklaring voor recht dat een verwerkingsverantwoordelijke onrechtmatig gehandeld heeft of een

[106] ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, *JBP* 2020/56, m.nt. J.A.N. Baas, p. 427.
[107] Rb Midden-Nederland 29 mei 2019, ECLI:NL:RBMNE:2019:2434, r.o. 3.2.
[108] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 118.
[109] Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1020, r.o. 4.8.
[110] Hof Den Haag 5 oktober 2021, ECLI:NL:GHDHA:2021:1924 ro. 5.4.
[111] Zie onder meer Hof Den Haag 5 oktober 2021, ECLI:NL:GHDHA:2021:1924 ro. 5.6, Rb. Rotterdam 14 januari 2020, ECLI:NL:RBROT:2020:293, ro. 4.2, Rb. Amsterdam 17 september 2019, ECLI:NL:RBAMS:2019:6817.
[112] Rechtbank Amsterdam 3 december 2020, ECLI:NL:RBAMS:2020:7536, r.o. 2.6.
[113] In de praktijk worden geschillen over de verwerking van persoonsgegevens in kort geding voorgelegd. Volgens vaste jurisprudentie staat de bijzondere rechtsingang van artikel 35 UAVG hieraan niet in de weg (Rb. Amsterdam 21 januari 2021, ECLI:NL:RBAMS:2021:174). Wel oordelen de meeste rechters in kort geding dat de eiser niet-ontvankelijk moet worden verklaard, indien de gevraagde voorziening strekt tot staking van de verwerking van persoonsgegevens en de dagvaarding is uitgebracht ná het verstrijken van de in artikel 35, tweede lid UAVG genoemde termijn (zie Hof Amsterdam 5 november 2019, ECLI:NL:GHAMS:2019:3966, r.o. 3.4.5; Hof Arnhem-Leeuwarden 7 januari 2020, ECLI:NL:GHARL:2020:126, r.o. 5.8; Hof Amsterdam 2 februari 2021, ECLI:NL:GHAMS:2021:312, r.o. 4.8.).

ongedaanmaking van een deactivering van een account, zoals in de Uber-profileringszaak[114], gaat dat het bestek van de verzoekschriftprocedure als bedoeld in artikel 35 UAVG te buiten. Dit betekent dat dergelijke verzoeken ingeleid dienen te worden door een dagvaardingsprocedure. Ondanks het feit dat artikel 82 AVG niet is genoemd in artikel 35 UAVG moet het volgens de hiervoor genoemde uitspraak niet uitgesloten worden geacht dat (materiële en immateriële) schadevergoeding in de zin van artikel 82 AVG – die blijkens punt 146 van de considerans bij de AVG volledig en daadwerkelijk moet zijn –, indien deze wordt gevraagd bij hetzelfde verzoekschrift dat het verzoek als bedoeld in artikel 35 UAVG bevat, in die procedure ook behandeld en toegekend kan worden, tenzij de aard van de zaak zich hiertegen verzet.[115] De Rechtbank Oost-Brabant oordeelt in de tussenbeschikking van 2 maart 2022 dat informatieverplichtingen als bedoeld in de artikelen 12 tot en met 14 en artikel 26, tweede lid AVG in beginsel eveneens kunnen worden meegenomen in een procedure op de voet van artikel 35 UAVG.[116] Het gaat naar het oordeel van de rechtbank om het nakomen van relatief eenvoudige, maar in het licht van de AVG essentiële informatieverplichtingen die op grond van de AVG op de verwerkingsverantwoordelijke rusten. Er is door de onderzoekers geen andere jurisprudentie aangetroffen in lijn met deze tussenbeschikking.

3.4 Laagdrempelige rechtsbescherming?

3.4.1 Bestuursrecht

Artikel 34 UAVG beperkt zich tot de bestuursrechtelijke rechtsbescherming in relatie tot verzoeken van betrokkene als bedoeld in de artikelen 15 tot en met 22 in die zin dat een beslissing op een dergelijk verzoek wordt aangemerkt als een besluit in de zin van artikel 1:3, eerste lid Awb. De UAVG voorziet niet in bestuursrechtelijke rechtsbescherming tegen feitelijk bestuurshandelingen op grond van de (U)AVG. Evenmin bevat de UAVG een bevoegdheid voor de bestuursrechter om te veroordelen tot het vergoeden van schade als gevolg van een onrechtmatige gegevensverwerking door een bestuursorgaan.

Dit laatste komt voort uit het fundamentele verschil tussen de bestuursrechtelijke systematiek en het gegevensbeschermingsrecht. In het gegevensbeschermingsrecht gaat het om feitelijke bestuurshandelingen. In het bestuursrecht gaat het om besluiten van bestuursorganen waarmee een eenzijdige rechtshandeling wordt bewerkstelligd. In de uitspraak van 2 februari 2022 heeft de Afdeling bestuursrechtspraak door het hanteren van een ruime connexiteitseis[117] ruimte geboden om een verzoek als bedoeld in artikel 82 AVG overeenkomstig artikel 8:88 Awb aan de bestuursrechter voor te leggen zonder dat betrokkene eerst een beroep heeft gedaan op zijn rechten genoemd in de artikelen 15 tot en met 22 AVG.

Het zou de rechtsbescherming van betrokkenen tegen feitelijke bestuurshandelingen op grond van de (U)AVG ten goede komen, indien de wetgever een brug weet te slaan eendachtig de hiervoor aangehaalde uitspraak tussen deze bestuurshandelingen en de rechtsbescher-

[114] Rb. Amsterdam 3 december 2020, ECLI:NL:RBAMS:2020:7536, r.o. 2.7.
[115] Rb. Amsterdam 3 december 2020, ECLI:NL:RBAMS:2020:7536, ro. 2.9.
[116] Rb. Oost-Brabant 2 maart 2022, ECLI:NL:RBOBR:2022:787, r.o. 5.18-5.20.
[117] Zie in dat kader de eerder zogenoemde 1-april jurisprudentie. De Afdeling bestuursrechtspraak kiest ervoor om artikel 8:88 Awb ruim uit te leggen in die zin dat er voor de bevoegdheid van de bestuursrechter 'minder strikt' wordt vastgehouden aan de eis van een onrechtmatig besluit, omdat wel een verband moet zijn met een besluit als bedoeld in artikel 34 UAVG, maar dit besluit (bijvoorbeeld een verzoek om inzage) niet onrechtmatig hoeft te zijn (ABRvS 1 april 2020, ECLI:NL:RVS:2020:957, r.o. 22). Hoewel dit in strijd is met de letter van de wet (dat wil zeggen de Awb), is dit in de context van de AVG-aansprakelijkheid en de UAVG alleszins verdedigbaar. Sterker, het leidt tot een beter stelsel van rechtsbescherming dat recht doet aan de intentie van de wetgever. Ter zijde dient te worden opgemerkt dat de verruiming van artikel 8:88 Awb ziet op de specifieke materie en context en dat de bestuursrechter hier in de regel toch zeer strikt is, aldus R.J.N. Schlössels, JB 2020/104.

ming op grond van de Awb. Daartoe zou een eerste stap kunnen worden gezet door in het verlengde van de eerder aangehaalde uitspraken van de Afdeling bestuursrechtspraak van de Raad van State artikel 8:88, eerste lid, aanhef en onder b Awb aan te passen in die zin dat de connexiteitseis tussen de onrechtmatige handeling van een bestuursorgaan en het daaropvolgende onrechtmatige besluit wordt losgelaten. Een andere mogelijkheid zou kunnen zijn om in de UAVG een bepaling op te nemen die – in afwijking van artikel 8:88, eerste lid, aanhef en onder b Awb – beroep bij de bestuursrechter openstelt voor degene die op grond van artikel 82 AVG aanspraak stelt te maken op vergoeding van schade die het gevolg is van het onrechtmatig verwerken van persoonsgegevens en daarmee het onrechtmatig bestuurlijke handelen door een bestuursorgaan, zonder dat reeds een (onrechtmatig) besluit door dat bestuursorgaan is genomen. Door dit te doen ontstaat voor de betrokkene de mogelijkheid om vroegtijdig, in ieder geval voordat een besluit in de zin van artikel 1:3, eerste lid Awb is genomen, de juistheid van zo'n verwerking te betwisten zonder een voor hem nadelig besluit of een keten van besluiten te moeten afwachten. Dit voorkomt tevens dat de betrokkene op de civiele rechter als restrechter is aangewezen, waarbij procesvertegenwoordiging verplicht is.

3.4.2 Civiel recht

Zoals hiervoor reeds is weergegeven beperkt de verzoekschriftprocedure zich tot het bevel om een verzoek als bedoeld in de artikelen 15 tot en met 22 AVG af of toe te wijzen. Indien om aanvullende acties wordt verzocht om de onrechtmatige handeling ongedaan te maken, gaat dit de in artikel 35 UAVG weergegeven reikwijdte van de verzoekschriftprocedure te buiten en zal een dagvaardingsprocedure dienen te worden geïnitieerd.[118] Hierbij dient in aanmerking te worden genomen dat de verzoekschriftprocedure laagdrempeliger is dan een dagvaardingsprocedure. Zo draagt de griffier zorg voor de oproeping van partijen en andere belanghebbenden en geldt er geen verplichte procesvertegenwoordiging. Een verzoekschriftprocedure kan daarnaast zowel partijen als de rechter meer flexibiliteit bieden. De verzoekschriftprocedure wordt dan ook sneller, doeltreffender en minder kostbaar geacht dan de dagvaardingsprocedure.[119]

Waar voor de uitoefening van de rechten van betrokkenen een laagdrempelige toegang tot de rechter geregeld is, dient voor het wegnemen van de (andere) gevolgen van de onrechtmatige verwerking een dagvaardingsprocedure te worden gestart. Het is denkbaar dat artikel 35 UAVG wordt verbreed zodat ook voor het wegnemen van (andere) gevolgen de verzoekschriftprocedure kan worden gevolgd. Dit draagt niet alleen bij tot een vereenvoudiging voor de betrokkene om zijn recht te halen, maar draagt ook bij tot een effectievere bescherming van betrokkene in verband met de verwerking van persoonsgegevens.

Om als betrokkene te weten wie, voor welk doel, op welke wijze zijn of haar persoonsgegevens verwerkt, geeft de AVG – naast in de artikelen 12 tot en met 14 opgenomen transparantiebepalingen – de betrokkene op grond van artikel 15 AVG het recht op inzage. Dit houdt in dat de betrokkene het recht heeft om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen in die persoonsgegevens, Daarnaast moet aanvullende informatie over de verwerking worden gegeven, zoals voor welke doeleinden de gegevens worden gebruikt en wat de bewaartermijn is, en of sprake is van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, eerste en vierde lid, bedoelde profilering. Indien dit aan de orde is moet ook aan de betrokkene nuttige informatie worden verstrekt over de onderliggen-

[118] Rb Amsterdam 3 december 2020, ECLI:NL:RBAMS:2020:7536, r.o. 2.7 en 2.9.
[119] Hoboken e.a. 2020, p. 60-63.

de logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Artikel 22, eerste lid AVG geeft de betrokkene het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming kent daarmee drie cumulatieve voorwaarden: 1. Het moet gaan om een beslissing, 2. Die uitsluitend is gebaseerd op een geautomatiseerde verwerking, en 3. met rechtsgevolgen voor de betrokkene, of de beslissing treft hem anderszins in aanmerkelijke mate.

Tot dusver wordt in de schaarse jurisprudentie die voorhanden is een beperkte interpretatie gehanteerd van de informatieverplichtingen[120] die ingevolge de AVG gelden bij geautomatiseerde besluitvorming.[121] Op basis van deze jurisprudentie heeft de betrokkene namelijk alleen recht op informatie over geautomatiseerde besluitvorming (al dan niet in het kader van een inzageverzoek), indien aan alle drie voormelde cumulatieve voorwaarden is voldaan. Een grammaticale interpretatie van de bedoelde informatieverplichtingen zou echter leiden tot een bredere interpretatie: alleen al het feit dat sprake is van geautomatiseerde besluitvorming zou dan voldoende moeten zijn voor de betrokkene om informatie te verkrijgen over de verwerking van zijn persoonsgegevens in dat kader. De strikte interpretatie in vorenbedoelde jurisprudentie is problematisch, omdat deze leidt tot een vicieuze cirkel waarin de betrokkene geen informatie kan krijgen over de geautomatiseerde besluitvorming, ténzij hij kan bewijzen dat de geautomatiseerde besluitvorming rechtsgevolgen voor hem heeft of hem anderszins in aanmerkelijke mate treft. Dit bewijs zal hij doorgaans niet gemakkelijk kunnen leveren, juist dóór het gebrek aan informatie over de geautomatiseerde besluitvorming en de onderliggende logica, het belang ervan en de te verwachten gevolgen voor betrokkene kan de betrokkene. Uiteindelijk is het voor de betrokkene dan ook moeilijk om een beroep te doen op zijn recht om niet aan geautomatiseerde besluitvorming te worden onderworpen.[122]

Artikel 150 Rv bepaalt dat de partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, de bewijslast draagt van die feiten of rechten, tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling van de bewijslast voortvloeit.

De UAVG kent geen bepaling, waarin in afwijking van de hoofdregel een andere verdeling van de bewijslast is neergelegd. Dit betekent dat als uitgangspunt geldt dat het bewijsrisico bij betrokkene ligt om bewijs naar voren te brengen waaruit blijkt dat aan de drie cumulatieve eisen wordt voldaan.[123] In de onderzochte jurisprudentie wordt conform de hoofdregel uit artikel 150 Rv de bewijslast bij de betrokkene neergelegd. Dit terwijl de facto alleen de verwerkingsverantwoordelijke inzicht kan geven of zich een besluit voordoet dat uitsluitend is gebaseerd op een geautomatiseerde verwerking en of dat een aanmerkelijk effect heeft op

[120] Artikel 13, tweede lid, aanhef en onder f AVG (recht op informatie over geautomatiseerde besluitvorming wanneer persoonsgegevens bij de betrokkene worden verzameld); artikel 14, tweede lid, aanhef onder g AVG (recht op informatie over geautomatiseerde besluitvorming wanneer persoonsgegevens niet bij de betrokkene worden verzameld) en artikel 15, eerste lid, aanhef en onder h AVG (de in het kader van het inzagerecht geldende verplichting tot het geven van aanvullende informatie over geautomatiseerde besluitvorming).

[121] Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018, Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1019 en Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1020.

[122] Zie ook mr. N.W. Groenhart, *Tijdschrift voor Internetrecht*, 2021/5, p.204.

[123] Voor de verwerkingsverantwoordelijke betekent de hoofdregel dat de stelplicht in beginsel op hem rust als hij zich beroept op een uitzonderingsbepaling (Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018, r.o. 4.15). Dit doet niets af aan de bewijslast van de betrokkene.

betrokkene. Bovendien is de verwerkingsverantwoordelijke reeds op basis van artikel 13, tweede lid, aanhef en onder f, dan wel artikel 14, tweede lid, aanhef en onder g AVG in beginsel gehouden om eigener beweging informatie daarover aan betrokkene te verstrekken om ten overstaan van betrokkene een behoorlijke en transparante verwerking te waarborgen. Een omkering van de bewijslast ligt, gezien de eisen van redelijkheid en billijkheid daarmee meer voor de hand. Dit mede gezien de structurele onevenwichtigheid die anders de rechtsbescherming voor betrokkene frustreert. Het toevoegen van een bepaling aan de UAVG, waarin in afwijking van de hoofdregel de bewijslast anders wordt verdeeld, is op dit moment prematuur, nu de jurisprudentie zich op dit punt nog nader moet uitkristalliseren.

3.5 Conclusie

Wanneer een betrokkene zijn rechten uitoefent op grond van de artikelen 15 tot en met 22 AVG en daarbij niet het gewenste resultaat behaalt, kan volgens de UAVG zowel langs bestuursrechtelijke (artikel 34 UAVG) als civielrechtelijke (artikel 35 UAVG) weg rechtsbescherming worden gezocht. Is de verwerkingsverantwoordelijke een bestuursorgaan, dan geldt de standaard-rechtsgang van bezwaar bij het verwerkingsverantwoordelijke bestuursorgaan, beroep bij de sector bestuursrecht van de bevoegde rechtbank en hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Uit het jurisprudentieonderzoek blijkt dat het aantal gepubliceerde uitspraken waarin de UAVG een materiële rol speelt, beperkt is. De rechtsbescherming kan worden ingeroepen tegen het besluit van de verwerkingsverantwoordelijke in gevolge een verzoek van een betrokkene over de uitoefening van zijn rechten uit hoofde van artikel 15 tot en met 22 AVG, of tegen het uitblijven van zo'n besluit. Is de verwerkingsverantwoordelijke geen bestuursorgaan dan geldt volgens artikel 35 UAVG dat de betrokkene of een andere belanghebbende door middel van een verzoekschriftprocedure als bedoeld in artikel 261 Wetboek van Burgerlijke Rechtsvordering (Rv) zich tot de civiele rechter wendt om op te komen tegen een beslissing van een verwerkingsverantwoordelijke op een verzoek op grond van de artikelen 15 tot en met 22 AVG.

De effectiviteit van de bestuursrechtelijke rechtsbescherming op grond van artikel 34 UAVG is beperkt. De UAVG voorziet namelijk niet in bestuursrechtelijke rechtsbescherming tegen feitelijk bestuurshandelingen op grond van de (U)AVG. Evenmin bevat de UAVG een bevoegdheid voor de bestuursrechter om een bestuursorgaan te veroordelen tot een schadevergoeding als gevolg van een onrechtmatige gegevensverwerking door dat bestuursorgaan. Het zou de rechtsbescherming van betrokkenen tegen feitelijke bestuurshandelingen op grond van de (U)AVG ten goede komen, indien de wetgever een brug weet te slaan eendachtig de hiervoor aangehaalde uitspraak van de Afdeling bestuursrechtspraak van de Raad van State tussen deze bestuurshandelingen en de rechtsbescherming op grond van de Awb. Door dit te doen ontstaat voor de betrokkene de mogelijkheid om vroegtijdig, in ieder geval voordat een besluit in de zin van artikel 1:3, eerste lid Awb is genomen, de juistheid van zo'n verwerking te betwisten zonder een voor hem nadelig besluit of een keten van besluiten te moeten afwachten. Dit voorkomt tevens dat de betrokkene op de civiele rechter als restrechter is aangewezen, waarbij procesvertegenwoordiging verplicht is. Daartoe zou een eerste stap kunnen worden gezet door in het verlengde van de eerder aangehaalde uitspraken van de Afdeling bestuursrechtspraak van de Raad van State artikel 8:88, eerste lid, aanhef en onder b Awb aan te passen in die zin dat de connexiteit tussen de onrechtmatige handeling van een bestuursorgaan en het daaropvolgende onrechtmatige besluit wordt losgelaten. Een andere mogelijkheid zou kunnen zijn om in de UAVG een bepaling op te nemen die in afwijking van artikel 8:88, eerste lid, aanhef en onder b Awb beroep bij de bestuursrechter openstelt voor degene die op grond van

artikel 82 AVG aanspraak stelt te maken op vergoeding van schade die het gevolg is van het onrechtmatig verwerken van persoonsgegevens en daarmee het onrechtmatig bestuurlijke handelen door een bestuursorgaan zonder dat reeds een (onrechtmatig) besluit doordat bestuursorgaan is genomen.

Ook de effectiviteit van de civiele rechtsbescherming staat ter discussie. Zoals hiervoor reeds is weergegeven beperkt de verzoekschriftprocedure zich tot het bevel om een verzoek als bedoeld in de artikelen 15 tot en met 22 af of toe te wijzen. Indien om aanvullende acties wordt verzocht om de onrechtmatige handeling ongedaan te maken, gaat dit de in artikel 35 UAVG weergegeven reikwijdte van de verzoekschriftprocedure te buiten en zal een dagvaardingsprocedure dienen te worden geïnitieerd. Waar de voor de uitoefening van de rechten van betrokkene dus een laagdrempelige toegang tot de rechter geregeld is, dient voor het wegnemen van de (andere) gevolgen van de onrechtmatige verwerking een meer belastende dagvaardingsprocedure te worden gestart. De effectiviteit van de civielrechtelijke rechtsbescherming zou gediend zijn met een verbreding van de reikwijdte van artikel 35 UAVG in lijn met het vorenstaande.

De beperkte rechtspraak ten aanzien van de positie van de betrokkene bij geautomatiseerde gegevensverwerking laat zien dat door de daarin gehanteerde interpretatie van het begrip geautomatiseerde besluitvorming de betrokkene in een lastige bewijspositie terecht komt. Deze moet namelijk bewijzen dat de geautomatiseerde besluitvorming een aanmerkelijk effect heeft voor de betrokkene. En een dergelijk effect wordt vooralsnog niet snel door de rechtbank aangenomen. Uit het oogpunt van effectiviteit van de rechtsbescherming is dat opmerkelijk. Het is immers bij uitstek de verwerkingsverantwoordelijke die inzicht kan geven of zich een besluit voordoet dat uitsluitend is gebaseerd op een geautomatiseerde verwerking en of dat een aanmerkelijk effect heeft op betrokkene. Een omkering van het bewijsrisico ligt, gezien de eisen van redelijkheid en billijkheid mogelijk meer in de reden. Dit mede gezien de structurele onevenwichtigheid die anders de rechtsbescherming voor betrokkene frustreert. Om een bepaling aan de UAVG toe te voegen, waarin in afwijking van de hoofdregel de bewijslast anders wordt verdeeld, lijkt echter nog wat prematuur, nu de jurisprudentie zich op dit punt nog nader moet uit kristalliseren.

4 Vragenlijstonderzoek en interviews: FG's aan het woord

4.1 Inleiding

In het kader van de evaluatie van de UAVG is een vragenlijst uitgezet, bedoeld voor Functionarissen voor Gegevensbescherming (FG's) in Nederland. Omdat we niet konden beschikken over de gegevens van de FG's in de bestanden van de AP en we de vragenlijst ook niet via de AP konden versturen, zijn drie alternatieve routes gekozen:

— Het Nederlandse Genootschap van Functionarissen voor de Gegevensbescherming (NGFG) heeft een uitnodiging voor de vragenlijst rondgestuurd aan haar leden via de nieuwsbrief. Later is via dezelfde weg een herinnering rondgestuurd.
— De Vereniging Privacyrecht heeft in twee mailings een uitnodiging en herinnering rondgestuurd aan haar leden.
— Via social media hebben de onderzoekers hun netwerk ingezet om de vragenlijst verder te verspreiden. Daarbij zijn voor zover mogelijk FG's binnen het netwerk ook persoonlijk benaderd met het verzoek de vragenlijst in te vullen en hebben leden van de begeleidingscommissie ook hun netwerk ingezet om FG's te benaderen en zodoende de respons te verhogen.

Uiteindelijk heeft dit geleid tot een respons van 190 vragenlijsten, waarvan 125 volledig. De gedeeltelijke respons is voor zover mogelijk meegenomen in de analyse. Hoewel we geen volledig beeld hebben van het aantal FG's in Nederland, kunnen we bij een totale populatie van maximaal 11.000[124] FG's uitgaan van een foutmarge van 8%. De gegeven antwoorden zullen vooral indicatief worden geïnterpreteerd en in de eindanalyse worden gebruikt ter aanvulling en ondersteuning van de bevindingen gebaseerd op kwalitatieve onderzoeksmethoden. Ter verdieping van de bevindingen van het vragenlijstonderzoek zijn met een tiental FG's die in de vragenlijst aangaven daarvoor open te staan korte interviews gehouden.

[124] Volgens het meest recent gepubliceerde jaarverslag van de AP (2020; Autoriteit Persoonsgegevens 2021) zijn er bij de AP ruim 11.000 FG's aangemeld.

In dit hoofdstuk staan de deelvragen 1, 4 en 5 centraal die de duidelijkheid, toegankelijkheid, uitvoerbaarheid en handhaafbaarheid van de bepalingen van de UAVG betreffen. Daarnaast zijn ook deelvragen 3 en 8 van belang die gaan over de informatie die functionarissen krijgen die met de UAVG moeten werken en over de rol van de FG's binnen organisaties bij de naleving van de meldplicht datalekken.

4.2 Beeld van de respondenten

Voor het afnemen van de vragenlijst was het niet mogelijk een steekproef te nemen op basis van verschillende kenmerken. Daarom is het van belang om de aard en type van de respondenten goed in kaart te krijgen, zodat eventuele over- of ondervertegenwoordiging meegenomen kan worden in de analyse. In tabel 4.1 t/m 4.8c worden deze kenmerken gepresenteerd. We zien in tabel 4.1 dat bijna de helft van de respondenten bij meerdere organisaties tegelijk werkzaam is (geweest) als FG. De functie wordt dus vaak gecombineerd, wat ook logisch is gezien het feit dat de gemiddelde omvang van de functie iets meer dan een halve fte is (tabel 4.2). Overigens is de omvang van de functie sterk afhankelijk van de omvang van de organisatie. Bij organisaties met maximaal honderd fte aan werknemers is de gemiddelde omvang iets minder dan twaalf uur per week, bij organisaties tot duizend fte is de omvang ongeveer zeventien uur per week en daarboven is dit ruim 29 uur per week.

TABEL 4.1

Bent u bij meerdere organisaties tegelijk werkzaam (geweest) als FG?		
Ja	82	43%
Nee	108	57%
Totaal	**190**	

TABEL 4.2

Wat is bij uw organisatie de omvang van de FG-functie in uren per week?		
0 t/m 8	61	33%
8 t/m 16	27	15%
16 t/m 24	21	11%
24 t/m 32	20	11%
32 t/m 40	57	31%
Totaal	186	
Gemiddelde omvang functie	**20,8**	

Bij een ruime meerderheid van de respondenten is de instelling van een Functionaris voor Gegevensbescherming (FG) verplicht geweest voor de organisatie, bij 18% was dit een eigen overweging (tabel 4.3). Een even zo grote meerderheid van de respondenten werkt als FG op basis van een dienstverband bij de organisatie (intern), de rest werkt op basis van een overeenkomst als extern FG. We zien dat deze tweede groep vooral FG's betreft die gemiddeld veel minder tijd per organisatie besteden aan deze functie (tabel 4.4). Ongeveer de helft van de respondenten is alleen FG, de andere respondenten combineren de functie met een of meerdere andere functies (tabel 4.5). Opvallend is dat 5% van de respondenten ook actief is als chief information security officer, terwijl die combinatie in verband met de vereiste

onafhankelijkheid van de FG door de AP ontraden wordt.[125] Deze combinatie komt voornamelijk voor bij commerciële instellingen en zorginstellingen, en niet bij bestuursorganen. Bij de optie 'overige' wordt in veel gevallen compliance officer als tweede functie genoemd, maar ook vaak (bedrijfs)jurist of kwaliteitsmedewerker.

TABEL 4.3

Is uw organisatie wettelijk verplicht een FG aan te stellen?		
Ja	155	82%
Nee, daar heeft de organisatie zelf voor gekozen.	35	18%
Totaal	**190**	

TABEL 4.4

Heeft u een dienstverband bij deze organisatie of werkt u op basis van een overeenkomst?			
			Gemiddelde omvang FG-functie (uur per week)
Dienstverband	152	80%	24
Overeenkomst	37	20%	7
Totaal	**189**		

TABEL 4.5

Bent u naast FG ook nog in één van de onderstaande functies werkzaam bij uw organisatie? (Kiezen welke van toepassing is, meerdere antwoorden mogelijk)		
Nee, alleen als FG	90	46%
Ja, ook als privacy officer	30	15%
Ja, ook als chief information security officer (CISO)	9	5%
Overige	69	35%
Totaal	**197**	

In de tabellen 4.6 en 4.7 krijgen we een indruk van de omvang van de organisaties waar de respondenten werkzaam zijn. Dit lijkt een evenwichtige verdeling te betreffen, met ongeveer een zesde van de respondenten werkzaam bij een kleine organisatie en bijna 40% van de respondenten afkomstig van een bedrijf met meer dan duizend fte aan werknemers. We hebben ook gekeken naar het aantal personen waarvan gegevens worden verwerkt door deze organisaties; hier blijkt het zwaartepunt in de respons te liggen bij organisaties die regelmatig op grote schaal gegevens verwerken. Ongeveer een derde van de organisaties doet dit voor minimaal een half miljoen personen.

[125] Om belangenverstrengeling te voorkomen, mag de FG binnen de organisatie niet ook een functie hebben waarin hij het doel en de middelen van een gegevensverwerking bepaalt. Dit kan bijvoorbeeld zo zijn als de FG een managementpositie vervult. Zoals (…) chief information security officer (CISO); Informatie Autoriteit Persoonsgegevens.

TABEL 4.6

Hoeveel werknemers heeft uw organisatie, uitgedrukt in totaal aantal fte?		
0 t/m 50	29	16%
51 t/m 100	12	7%
101 t/m 500	45	25%
501 t/m 1.000	27	15%
1.001 t/m 10.000	61	34%
> 10000	8	4%
Totaal	**182**	

TABEL 4.7

Van hoeveel betrokkenen (bijv. klanten, burgers, aanvragers, leerlingen of patiënten) verwerkt uw organisatie persoonsgegevens?		
0 t/m 1.000	22	14%
1.001 t/m 5.000	18	11%
5.001 t/m 10.000	12	8%
10.001 t/m 50.000	27	17%
50.001 t/m 100.000	14	9%
100.001 t/m 500.000	19	12%
> 500.000	48	30%
Totaal	**160**	

In tabel 4.8 zien we de verdeling van de organisaties waarbij respondenten werkzaam zijn tussen verschillende typen organisaties, tabellen 4.8A t/m C geven een verdere toespitsing van deze categorieën. In deze subtabellen geven we twee percentages weer: het aandeel binnen de drie categorieën en het aandeel van de totale respons. Bijvoorbeeld (eerste rij tabel 4.8A): er zijn twee respondenten werkzaam bij een detailhandel bedrijf, wat 3% van het aantal bedrijven onder de respondenten vormt en 1% van het totaal aantal respondenten. Voor de analyse is van belang dat het om betrekkelijk kleine groepen van respondenten gaat. Daardoor zijn alleen zeer grote verschillen in de beantwoording (rond 25%) significant. De verdeling over de typen organisaties wijst waarschijnlijk op een oververtegenwoordiging van bestuursorganen in de respons, in de zin dat een relatief groot deel van het totaal aantal bestuursorganen heeft deelgenomen aan het vragenlijstonderzoek.[126] Bij de andere twee categorieën ligt dat aandeel veel lager; het aantal respondenten is nog niet twee keer zo hoog, terwijl het aantal bedrijven en maatschappelijke instellingen in Nederland veel groter is.

[126] In totaal 46 respondenten van circa vijfhonderd bestuursorganen (in 2021: 352 gemeenten, twaalf provincies, 21 waterschappen, twaalf ministeries en circa honderd zelfstandige bestuursorganen).

TABEL 4.8

Voor welk type organisatie werkt u?		
Een commercieel bedrijf	70	37%
Een maatschappelijke instelling	72	38%
Een bestuursorgaan	46	24%
Totaal	**188**	

TABEL 4.8A

In welke branche is uw bedrijf (hoofdzakelijk) werkzaam?			
			Van totaal
Detailhandel	2	3%	1%
Transport	2	3%	1%
ICT, media, communicatie	11	16%	6%
Industrie	4	6%	2%
Zakelijke dienstverlening	18	26%	10%
Financiële dienstverlening	18	26%	10%
Overige	15	21%	8%
Totaal	**70**		

TABEL 4.8B

Welk type maatschappelijke instelling gaat het om?			
			Van totaal
Onderwijs	18	25%	10%
Volkshuisvesting	2	3%	1%
Zorg	41	57%	22%
Belangenstichting/ -vereniging	4	6%	2%
Overige	7	10%	4%
Totaal	**72**		

TABEL 4.8C

Wat voor bestuursorgaan gaat het om?			
			Van totaal
Ministerie	4	9%	2%
Provincie	1	2%	1%
Gemeente	23	50%	12%
Uitvoeringsorganisatie	7	15%	4%
Overige	11	24%	6%
Totaal	**46**		

4.3 Rol van de FG als aanspreekpunt voor de AP

Om de rol van de FG als aanspreekpunt voor de AP in kaart te krijgen hebben we een aantal stellingen voorgelegd. In tabel 4.9 zien we de respons op deze stellingen. De eerste vier kolommen geven de totale respons volledig uitgesplitst weer, de vijfde is een optelling van de antwoorden ‘meestal’ en ‘altijd’. Deze optelling presenteren we vervolgens ook voor twee uitsplitsingen: op basis van het type organisatie (drie hoofdcategorieën) en op basis van de omvang van de organisatie (minder of meer dan vijfhonderd fte). We zien dat de FG’s in ruime

meerderheid van de gevallen als aanspreekpunt van de AP fungeren en betrokken zijn bij verdere contacten tussen de organisatie en de AP. Bij de derde stelling dient zich een enigszins zorgelijk beeld aan: minder dan de helft van de respondenten voelt zich altijd vrij om de AP te benaderen, een kwart voelt zich nooit of soms vrij. Dit duidt op een onwenselijke druk op de FG die in strijd is met de functie. In interviews met FG's is in een aantal gevallen aangegeven dat er vooral druk wordt ervaren, omdat contact met de AP mogelijk kan leiden tot interventies of versterkte controle: men wil geen slapende honden wakker maken. Overigens zien we dat de uitsplitsingen naar type of omvang van de organisaties geen significante resultaten opleveren: de verschillen vallen binnen de foutmarges.

TABEL 4.9

Stellingen (n=186)										
						Altijd of meestal				
	Alle respondenten					Type organisatie			Omvang organisatie (fte)	
	Nooit	Soms	Meestal	Altijd	Altijd of meestal	Commercieel	Maatschappelijk	Bestuursorgaan	tot 500	500+
Ik fungeer namens mijn organisatie als aanspreekpunt voor de AP voor alle zaken verband houdend met gegevensbescherming.	6%	8%	27%	59%	86%	87%	86%	85%	82%	89%
Ik word betrokken bij contacten tussen de AP en mijn organisatie.	8%	6%	20%	66%	86%	85%	90%	80%	82%	88%
Ondanks de geldende verplichtingen tot geheimhouding/vertrouwelijkheid, voel ik mij vrij om de AP te benaderen voor advies.	7%	20%	33%	41%	73%	68%	77%	76%	72%	76%

4.4 Duidelijkheid van normen in de UAVG

De UAVG regelt onder meer de uitzonderingsgronden bij verwerking van bijzondere persoonsgegevens en gegevens van strafrechtelijke aard. We hebben allereerst gevraagd welk type gegevens worden verwerkt door de organisaties waar onze respondenten werkzaam zijn. De resultaten worden gepresenteerd in tabel 4.10. We zien dat gegevens over de gezondheid door 80% van de door ons bestudeerde organisaties worden verwerkt en dat gegevens over ras en etniciteit en gegevens van strafrechtelijke aard relatief vaak worden verwerkt. Overigens komt verwerking van die derde categorie gegevens vooral veel voor bij bestuursorganen, die sowieso voor alle categorieën persoonsgegevens relatief vaak aangeven deze te verwerken. Slechts iets meer dan 10% van de respondenten geeft aan dat er geen bijzondere persoonsgegevens of gegevens van strafrechtelijke aard verwerkt, waarbij er een verschil lijkt te zijn tussen bedrijven (20%) en bestuursorganen (3%).

In deze cijfers lijkt sprake te zijn van overschatting. Het is mogelijk dat FG's bijvoorbeeld bij het opslaan van beeldmateriaal er (misschien voor de zekerheid) vanuit gaan dat dit persoonsgegevens zijn waaruit ras of etniciteit blijkt. Ook registraties van ziekmeldingen en dergelijke kunnen worden opgevat als gegevens over de gezondheid. Deze vermoedens zijn tijdens

interviews voorgelegd, maar daar werden ze niet bevestigd. Toch willen we de mogelijkheid niet onbenoemd laten dat in een grotere groep FG's dit effect toch kan hebben opgetreden.

TABEL 4.10

Welke categorieën van bijzondere persoonsgegevens en/of gegevens van strafrechtelijke aard worden binnen uw organisatie verwerkt?								
	Alle respondenten		Commercieel bedrijf		Maatschappelijke instelling		Bestuursorgaan	
Persoonsgegevens waaruit ras of etnische afkomst blijkt	69	43%	15	27%	26	43%	28	70%
Persoonsgegevens waaruit politieke opvattingen blijken	37	23%	7	13%	6	10%	24	60%
Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken	52	33%	9	16%	23	38%	20	50%
Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt	46	29%	11	20%	16	27%	19	48%
Gegevens over iemands gezondheid	128	80%	39	70%	53	88%	36	90%
Gegevens over iemands seksueel gedrag of seksuele gerichtheid	45	28%	5	9%	21	35%	19	48%
Genetische gegevens	25	16%	3	5%	19	32%	3	8%
Biometrische gegevens met het oog op de unieke identificatie van een persoon	31	19%	8	14%	9	15%	14	35%
Gegevens van strafrechtelijke aard	65	41%	16	29%	13	22%	36	90%
Binnen onze organisatie worden geen bijzondere- en/of gegevens van strafrechtelijke aard verwerkt	17	11%	11	20%	5	8%	1	3%
Aantal respondenten	**160**		**56**		**60**		**40**	

Vervolgens hebben we enkele stellingen voorgelegd over mate waarin specifieke elementen binnen de UAVG duidelijk zijn voor de FG's en de organisaties waarin zij actief zijn. We vatten de resultaten samen in tabel 4.11, waarbij we de resultaten vergelijken door te kijken naar het deel van de respondenten dat het enigszins of geheel eens is met de stellingen. Voor wat betreft algemene en specifieke uitzonderingsgronden is het beeld overwegend positief. Toch is er in aanzienlijke mate wel sprake van knelpunten bij deze uitzonderingsgronden: 53% ervaart geen knelpunten, maar ruim een kwart van de respondenten is het met deze stelling enigszins of helemaal oneens. Bij de eventuele verduidelijking vanuit jurisprudentie over de UAVG is het beeld relatief het minst positief. Slechts 21% onderschrijft deze stelling, 37% is het oneens met de stelling en ruim 40% is neutraal of heeft geen mening. Dit wijst er enerzijds op dat respondenten de jurisprudentie niet erg duidelijk vinden, maar zou er ook op zou kunnen duiden dat respondenten niet goed op de hoogte zijn van de jurisprudentie.

In aansluiting op deze stellingen is ook gevraagd of men bepaalde grondslagen of uitzonderingsgronden mist in de UAVG. Dit geldt in beperkte mate: 22% van de respondenten mist een grondslag voor verwerking van bepaalde gegevens die nu onder de UAVG vallen, 19% mist bepaalde uitzonderingsgronden.

TABEL 4.11

Stellingen (n=151)	Alle respondenten (in procenten)								Omvang organisatie (fte)		Positie FG	
	Helemaal oneens	Enigszins oneens	Neutraal	Enigszins eens	Helemaal eens	Weet niet	Geen mening	Totaal enigszins en helemaal mee eens	t/m 500	> 500	Intern	Extern
In onze organisatie is het duidelijk op grond van welke algemene uitzonderingsgronden bijzondere gegevens en/of gegevens van strafrechtelijke aard mogen worden verwerkt.	0	8	9	25	54	1	3	79	79	78	79	76
In onze organisatie is het duidelijk op grond van welke specifieke uitzonderingsgronden bijzondere gegevens en/of gegevens van strafrechtelijke aard mogen worden verwerkt.	1	13	6	29	45	1	5	75	77	71	76	69
In onze organisatie ervaren wij geen knelpunten bij de uitzonderingsgronden voor de verwerking van bijzondere gegevens en/of gegevens van strafrechtelijke aard.	8	19	14	27	26	1	5	53	56	51	53	50
Het is voor ons duidelijk welke uitzonderingen en beperkingen er zijn met betrekking tot de rechten van betrokkenen.	1	9	10	32	46	1	1	78	81	75	79	75
Het is voor ons duidelijk hoe de uitzonderingen en beperkingen met betrekking tot de rechten van betrokkenen geïnterpreteerd/toegepast moeten worden.	3	9	12	40	36	0	1	75	86	67	75	79
De normen uit de UAVG worden goed verduidelijkt door jurisprudentie.	11	26	27	19	2	8	7	21	23	1%	19	29

Voor ondersteuning bij de FG's (onder meer voor het verhelderen van eventuele onduidelijkheden) heeft de AP een helpdesk (telefonisch en e-mail) opgezet voor bij hen ingeschreven

FG's. 59% van de respondenten geeft aan daar wel eens gebruik van te hebben gemaakt. Van die respondenten hebben 84 een beoordeling van de hulp gegeven. Dit zijn tekstuele beoordelingen die moeilijk te categoriseren zijn, maar waar toch een aantal observaties bij te maken zijn: veertien beoordelingen waren ronduit positief over de advisering, maar de teneur uit de overige antwoorden is verder gematigd negatief. Een aantal respondenten geeft aan sterk wisselende ervaringen te hebben gehad, een aantal beklaagt zich over de zeer voorzichtige houding bij de AP waardoor van nuttige voorlichting niet echt sprake is, en een deel is ook ronduit negatief over de geboden hulp. Voor deze stellingen hebben we gekeken of de mate van verwachte expertise van invloed is op de beantwoording; bij grotere organisaties of organisaties met een externe (en vaak specialistische) FG zouden we kunnen verwachten dat deze minder moeite hebben met het interpreteren van deze elementen van de UAVG. Er blijken echter geen significante verschillen op te treden.

Ook in de gesprekken met FG's is gevraagd naar hun ervaring met de hulplijn van de AP. Een aantal gesprekspartners gaf aan wel eens gebruik te hebben gemaakt van de hulplijn, en een aantal van hen had hiermee geen goede ervaring. Een van de gesprekspartners gaf aan dat het antwoord dat wordt gegeven op een vraag afhankelijk is van de persoon die aan de telefoon komt. Een andere gesprekspartner gaf aan dat ook vaak niet werd opgenomen toen de FG de hulplijn probeerde te bellen.

TABEL 4.12

Heeft u als FG wel eens gebruik gemaakt van de hulplijnen van de AP?		
Ja	90	59%
Nee	58	38%
Weet ik niet (meer)	4	3%
Totaal	**152**	

4.5 Meldplicht datalekken

Met betrekking tot datalekken hebben we allereerst gekeken naar kennis en bewustwording onder de medewerkers binnen de organisaties. De respondenten zijn overwegend positief over dit kennisniveau: ongeveer 90% van hen onderschrijft de stelling dat medewerkers weten wat een datalek is of een idee daarvan hebben (tabel 4.13). Bijna 80% stelt ook dat er vaak of heel vaak wordt gewerkt aan bewustzijn om deze datalekken te voorkomen (tabel 4.14). In tabel 4.15 zien we vervolgens welke activiteiten in dit kader worden ondernomen. Het delen van informatie en nieuws via interne communicatiekanalen als intranet en e-mail staan hierbij voorop, maar bij veel organisaties worden ook trainingen gegeven. Alleen het inloopspreekuur lijkt een wat zeldzamere vorm van voorlichting (slechts 12% van de respondenten). In vrijwel alle organisaties (tabel 4.16) is een protocol, richtlijn of handleiding opgesteld om medewerkers te instrueren bij een eventueel datalek.

TABEL 4.13

Stelling: Medewerkers binnen onze organisatie weten wat onder een 'datalek' wordt verstaan.	Totaal		Commercieel bedrijf		Maatschappelijke instelling		Bestuursorgaan	
Helemaal oneens	1	1%	0	0%	0	0%	1	3%
Enigszins oneens	9	7%	1	2%	6	12%	2	6%
Neutraal	4	3%	1	2%	2	4%	1	3%
Enigszins eens	68	49%	21	41%	25	48%	22	63%
Helemaal eens	56	41%	28	55%	19	37%	9	26%
Weet niet	0	0%	0	0%	0	0%	0	0%
Geen mening	0	0%	0	0%	0	0%	0	0%
Totaal	**138**		**51**		**52**		**35**	

TABEL 4.14

Binnen onze organisatie werken wij aan bewustwording onder medewerkers om datalekken te voorkomen.	Totaal		Commercieel bedrijf		Maatschappelijke instelling		Bestuursorgaan	
Nooit	0	0%	0	0%	0	0%	0	0%
Zelden	1	1%	0	0%	1	2%	0	0%
Soms	30	22%	10	20%	9	17%	11	31%
Vaak	79	57%	28	55%	33	63%	18	50%
Heel vaak	29	21%	13	25%	9	17%	7	19%
Totaal	**139**		**51**		**52**		**36**	

TABEL 4.15

Wat wordt er binnen uw organisatie aan bewustwording onder medewerkers om datalekken te voorkomen gedaan?	Totaal		Commercieel bedrijf		Maatschappelijke instelling		Bestuursorgaan	
Het houden van presentaties tijdens introductiesessies voor nieuwe medewerkers	88	63%	36	71%	29	56%	23	64%
Het delen van informatie/nieuws via intranet/mail	124	89%	40	78%	48	92%	36	100%
Het aanbieden van trainingen aan alle medewerkers	98	71%	39	76%	32	62%	27	75%
Het beschikbaar hebben van algemeen voorlichtingsmateriaal beschikbaar (bijv. via intranet/folders)	92	66%	29	57%	40	77%	23	64%
Het organiseren van een inloopspreekuur voor medewerkers	16	12%	6	12%	4	8%	6	17%
Overige	30	22%	11	22%	14	27%	5	14%
Totaal	**139**		**51**		**52**		**36**	

TABEL 4.16

Is er binnen uw organisatie een protocol/richtlijn/handleiding over hoe medewerkers om dienen te gaan met een datalek?		
Ja	137	99%
Nee	1	1%
Totaal	**138**	

Voor de afgelopen twee jaar hebben we opgevraagd hoeveel datalekken zich hebben voorgedaan en hoeveel datalekken vervolgens ook zijn gemeld bij de AP. Door die twee cijfers te combineren hebben we een percentage berekend dat de meldingsbereidheid in kaart brengt. We zien de resultaten in tabel 4.17. Als leesvoorbeeld interpreteren we de eerste rij onder 2019: dit betekent dat van de respondenten (81 hebben cijfers opgegeven) 19% van de organisaties tussen 0 en 10% van hun datalekken in 2019 daadwerkelijk bij de AP heeft gemeld, 30% van de organisaties heeft tussen 10% en 25% gemeld en slechts 7% van de organisaties meldde minimaal 75% van de bij hun opgetreden datalekken. Van alle datalekken die zich in 2019 hebben voorgedaan bij de 81 organisaties waarvan we cijfers hebben, is 27% gemeld bij de AP. In 2020 lag dit percentage iets lager. We hebben de respons ook geanalyseerd met een uitsplitsing op basis van typen organisaties; daarbij zien we geen significante verschillen tussen commerciële organisaties, maatschappelijke organisaties en bestuursorganen. In tabel 4.18 zien we dat de datalekken ongeveer even vaak bij de betrokken personen (van wie gegevens mogelijk zijn gelekt) worden gemeld. Omdat door bijna drie kwart van de organisaties minder dan de helft van de datalekken wordt gemeld bij de personen van wie de gegevens mogelijk zijn gelekt – en in totaal slechts 30% van de datalekken wordt gemeld – wordt vaak niet volgens de wettelijke voorschriften gehandeld.

TABEL 4.17

Hoeveel datalekken heeft uw organisatie gemeld bij de AP?				
	2019		2020	
0% t/m 10%	15	19%	18	22%
10% t/m 25%	24	30%	27	33%
25% t/m 50%	25	31%	22	27%
50% t/m 75%	11	14%	9	11%
75% t/m 100%	6	7%	6	7%
Gemiddeld percentage		27%		24%
Totaal	**81**		**82**	

TABEL 4.18

Bij hoeveel datalekken heeft uw organisatie in onderstaande jaren betrokkenen ingelicht (klanten, burgers, aanvragers, leerlingen of patiënten etc.)?				
	2019		2020	
0% t/m 25%	35	44%	36	46%
25% t/m 50%	24	30%	22	28%
50% t/m 75%	7	9%	10	13%
75% t/m 100%	13	16%	10	13%
Gemiddeld percentage		30%		26%
Totaal	**79**		**78**	

We hebben de FG's ook gevraagd naar hun inschatting van het gedeelte van datalekken waar zij zelf binnen hun organisatie bij betrokken worden. Dat beeld is overwegend positief. 58%

van de FG's denkt dat ze bij vrijwel alle datalekken betrokken worden, nog eens 20% denkt dat ze bij minimaal driekwart van de datalekken op de hoogte worden gesteld. Toch vermoedt nog steeds ongeveer een op de zes FG's dat ze bij minder dan de helft van de gevallen betrokken worden.

TABEL 4.19

Bij welk percentage van de interne meldingen over datalekken denkt u dat u als FG betrokken wordt?		
0% t/m 25%	9	7%
25% t/m 50%	12	10%
50% t/m 75%	7	6%
75% t/m 95%	25	20%
95% t/m 100%	73	58%
Totaal	**126**	

Wanneer FG's gevraagd wordt naar de belangrijkste redenen voor het ontstaan van een datalek, is de menselijke fout verreweg de meest aangewezen reden. De andere redenen, zoals beveiligingsfouten of cyberaanvallen worden vrijwel nooit als belangrijkste reden aangewezen.

TABEL 4.20

Wat is de belangrijkste reden voor het ontstaan van een datalek binnen uw organisatie?		
Tijdsdruk	4	3%
Onvoldoende beveiligingsmaatregelen	3	2%
Cyberaanval: hacking/malware/phishing	3	2%
Onwetendheid	2	1%
Bewust voorrang geven aan andere belangen t.o.v. beveiliging	3	2%
'Menselijke fout'	105	78%
Weet niet	2	1%
Niet van toepassing	3	2%
Overige	9	7%
Aantal respondenten	**134**	

De lage meldingsbereidheid die we hierboven zien is mogelijk (in elk geval deels) te verklaren door het beeld wat we hebben gekregen van de reacties vanuit de AP op gedane meldingen. In tabel 4.21 is dit beeld gepresenteerd. Let op: de percentages tellen op tot meer dan 100% omdat er bij verschillende meldingen verschillende reacties kunnen zijn geweest. Een aantal respondenten heeft meerdere opties aangekruist. Meer dan de helft van de respondenten geeft aan dat het geregeld is voorgekomen dat men geen reactie kreeg van de AP na een melding, bijna de helft geeft daarnaast aan dat er doorgaans wel een ontvangstbevestiging is ontvangen maar dat het daar dan bij is gebleven. Slechts een op de drie respondenten verklaart dat er doorgaans een inhoudelijke reactie komt in de vorm van doorvragen, informatieverstrekking, advies op maat of een andere actie. Het is de vraag hoe motiverend deze reacties zijn voor het gedrag bij een volgend datalek; het is niet ondenkbaar dat de lage meldingsbereidheid daardoor verklaard kan worden.

TABEL 4.21

Wat is (doorgaans) de reactie geweest van de AP op de melding(en) die u deed?		
Ik kreeg geen reactie	50	56%
Ik kreeg alleen een ontvangstbevestiging, verder geen reactie	44	49%
De AP heeft standaard informatie opgestuurd over nader te volgen stappen	3	3%
De AP heeft contact opgenomen om meer informatie op te vragen	19	21%
De AP heeft advies op maat gegeven over nader te volgen stappen	3	3%
De AP heeft naar aanleiding van de melding de afhandeling begeleid op meerdere momenten	0	0%
Overige	5	6%
Aantal respondenten	**90**	

4.6 Toezicht van de AP op naleving van de UAVG

Bijna 40% van de respondenten heeft wel eens te maken gehad met onderzoek vanuit de AP, in lichte vorm (informatieverzoek) tot zware vorm (verscherpt toezicht), zoals te zien in tabel 4.22. De percentages in deze tabel komen in totaal op meer dan 100% omdat de eerste drie antwoorden elkaar niet uitsluiten.

TABEL 4.22

Heeft de AP wel eens op een van de onderstaande manieren onderzoek uitgevoerd binnen uw organisatie?		
Ja, de AP heeft een informatieverzoek gedaan	44	33%
Ja, de AP heeft een onderzoek gedaan	9	7%
Ja, onze organisatie staat/stond onder verscherpt toezicht	1	1%
Nee	83	63%
Weet ik niet	1	1%
Aantal respondenten	**132**	

Op basis van deze ervaringen hebben we de respondenten een aantal stellingen voorgelegd. De respons op deze stellingen is in tabel 4.23 gepresenteerd. Bij een aanzienlijk deel van de FG's die te maken kregen met een informatieverzoek liet de communicatie naar aanleiding van dit verzoek door de AP wat hen betreft te wensen over. Bij communicatie over uitgevoerd onderzoek zijn de FG's meer tevreden, maar dat betreft slechts negen respondenten. Twee derde van alle respondenten vindt wel dat de bevoegdheden die de AP ter beschikking staan passend zijn in verhouding met het takenpakket. Tegelijk schat steeds ongeveer een derde van de respondenten in dat de AP geen goed toezicht kan houden op toepassing van uitzonderingen bij verschillende vormen van verwerking van bijzondere categorieën persoonsgegevens, getuige de reacties op de laatste drie stellingen.

TABEL 4.23

Stellingen	Helemaal oneens	Enigszins oneens	Neutraal	Enigszins eens	Helemaal eens	Weet niet	Geen mening	Aantal respondenten
De AP communiceerde actief over de bevindingen naar aanleiding van het informatieverzoek.	19%	21%	16%	16%	23%	2%	2%	**43**
De AP communiceerde actief over de bevindingen naar aanleiding van het onderzoek.	22%	0%	0%	22%	56%	0%	0%	**9**
De bevoegdheden die de AP ter beschikking staan voor het houden van toezicht zijn passend voor de taak van toezichthouder.	3%	5%	16%	19%	47%	5%	3%	**129**
Het is voor de AP goed mogelijk toezicht te houden op het juist toepassen van de algemene uitzonderingen voor het verwerken van bijzondere categorieën gegevens.	9%	23%	20%	19%	9%	11%	10%	**128**

Het is voor de AP goed mogelijk toezicht te houden op het juist toepassen van de nationaal-rechtelijke algemene uitzonderingen voor het verwerken van bijzondere categorieën gegevens.	7%	24%	20%	14%	9%	15%	11%	**128**
Het is voor de AP goed mogelijk toezicht te houden op het juist toepassen van de uitzonderingen voor het verwerken van bijzondere categorieën persoonsgegevens in het kader van wetenschappelijk of historisch onderzoek of statistische doeleinden.	13%	20%	19%	13%	7%	16%	12%	**128**

TABEL 4.24

Stelling: Het is voor de AP goed mogelijk toezicht te houden op het juist toepassen van de uitzonderingen voor het verwerken van bijzondere categorieën persoonsgegevens …								
	Helemaal oneens	Enigszins oneens	Neutraal	Enigszins eens	Helemaal eens	Weet niet	Geen mening	**Aantal respondenten**
… waar ras of etnische afkomst uit blijkt.	11%	25%	18%	20%	5%	14%	7%	**56**
… waaruit politieke opvattingen blijken voor de vervulling van openbare functies.	9%	18%	15%	30%	3%	12%	12%	**33**
… waaruit religieuze of levensbeschouwelijke overtuigingen blijken voor geestelijke verzorging.	8%	23%	13%	25%	3%	18%	13%	**40**
… inzake genetische gegevens.	21%	32%	16%	16%	0%	11%	5%	**19**
… inzake biometrische gegevens.	8%	31%	15%	27%	4%	8%	8%	**26**
… inzake gezondheidsgegevens.	10%	19%	16%	26%	9%	13%	8%	**104**

In tabel 4.24 zien we hoe FG's denken over de mate waarin de AP in staat is toezicht te houden op toepassing van uitzonderingen voor het verwerken van bijzondere persoonsgegevens. Hieruit komt een gemengd beeld naar voren, waarbij steeds ongeveer evenveel respondenten (gematigd) positief als (gematigd) negatief oordelen. Ook tussen de categorieën persoonsgegevens zijn geen grote verschillen te zien.

We hebben de mogelijkheden voor toezicht door de AP op de toepassing van algemene en bijzondere uitzonderingen voor verwerking van gegevens van strafrechtelijke aard ook laten beoordelen door de respondenten (tabel 4.25). Dat beeld lijkt iets minder negatief, maar hierbij valt ook op dat een zeer groot deel van de respondenten neutraal reageert of aangeeft onvoldoende van dit onderwerp te weten voor een goed oordeel ('weet niet', 'geen mening' en 'neutraal' bij elkaar opgeteld ongeveer 60%).

TABEL 4.25

Stellingen	Helemaal oneens	Enigszins oneens	Neutraal	Enigszins eens	Helemaal eens	Weet niet	Geen mening	Aantal respon-denten
Het is voor de AP goed mogelijk toezicht te houden op het juist toepassen van de algemene uitzonderingen voor het verwerken van gegevens van strafrechtelijke aard	6%	11%	13%	16%	10%	23%	21%	**128**
Het is voor de AP goed mogelijk toezicht te houden op het juist toepassen van de bijzondere uitzonderingen voor het verwerken van gegevens van strafrechtelijke aard	6%	10%	14%	15%	9%	24%	21%	**128**

4.7 Interventies door de AP

We hebben de respondenten gevraagd naar hun inschatting van de interventiemogelijkheden. Ruim twee derde van de respondenten kan zich vinden in de stelling dat deze mogelijkheden de naleving van normen uit AVG en UAVG bevorderen. Ze zijn wat minder positief als we vragen of de inzet van deze mogelijkheden ook het nemen van verantwoordelijkheid voor bescherming van persoonsgegevens bevordert. Daar is ruim de helft van de respondenten het nog mee eens.

TABEL 4.26

Stellingen	Helemaal oneens	Enigszins oneens	Neutraal	Enigszins eens	Helemaal eens	Weet niet	Geen mening	Aantal respondenten
De interventiemogelijkheden die de AP ter beschikking staan, bevorderen de naleving van de normen uit de AVG/UAVG	4%	10%	8%	36%	33%	6%	3%	**126**
De AP bevordert het nemen van verantwoordelijkheid voor de bescherming van persoonsgegevens door de manier waarop de AP de interventiemogelijkheden inzet	9%	20%	11%	35%	16%	6%	3%	**126**

Om een beeld te krijgen van de mate waarin interventies door de AP worden toegepast hebben we de respondenten gevraagd met welke interventies zij te maken hebben gehad. In tabel 4.27 is de beantwoording van die vraag te vinden. We presenteren het aantal keer dat een interventie is voorgekomen als percentage van het totaal aantal respondenten, maar ook als percentage van het aantal interventies dat is gemeld. Iets minder dan een derde van de respondenten heeft te maken gehad met een interventie. Van die interventies betreft ongeveer

een derde een normoverdragende brief vanuit de AP en bij een vijfde ging het om een waarschuwing. Bij een tiende van de interventies bij onze respondenten ging het om zwaardere interventies in de vorm van een last onder dwangsom, een boete of een tijdelijke gegevensverwerkingsbeperking. We moeten wel opmerken dat deze percentages berekend zijn op een totaal van 39 interventies, wat een te smalle basis voor verdiepende analyse vormt. Ten slotte zien we in tabel 4.28 dat respondenten gematigd kritisch zijn op de proportionaliteit van de toegepaste interventies. Ruim een derde vond deze interventie niet (helemaal) in verhouding staan met de overtreden norm(en), een iets groter deel van de respondenten kon zich wel vinden in de gekozen interventie.

TABEL 4.27

Binnen onze organisatie heeft de AP in de afgelopen drie jaar één van de onderstaande interventies toegepast:			
		% totaal	% van interventies
Er is een adviesgesprek gevoerd (AP heeft daarbij gewezen op de privacyregels)	9	7%	17%
De AP heeft een normoverdragende brief gestuurd	18	14%	33%
De AP heeft een normoverdragend gesprek op bestuursniveau gevoerd	4	3%	7%
De AP heeft een waarschuwing gegeven	11	9%	20%
De AP heeft een berisping gegeven	2	2%	4%
De AP heeft een last onder dwangsom opgelegd	1	1%	2%
De AP heeft een boete opgelegd	3	2%	6%
De AP heeft een tijdelijke of definitieve verwerkingsbeperking opgelegd (waaronder een verwerkingsverbod)	1	1%	2%
Overige	5	4%	9%
Er is geen interventie geweest	86	69%	
Aantal respondenten	**125**		

TABEL 4.28

Stelling: Deze interventie stond in verhouding tot de overtreden norm(en).		
Helemaal oneens	7	19%
Enigszins oneens	6	17%
Neutraal	8	22%
Enigszins eens	6	17%
Helemaal eens	9	25%
Weet ik niet	0	0%
Geen mening	0	0%
Totaal	**36**	

4.8 Conclusie: de belangrijkste bevindingen

We hebben geconstateerd dat FG's een centrale rol hebben binnen hun organisatie als het gaat om gegevensbescherming en contact met de AP. Ze zijn de aangewezen persoon om vragen op dit vlak aan te stellen en expertise van te verwachten. Toch blijkt dat deze rol vaak niet optimaal ingevuld kan worden. Zo zien we bij een deel van de respondenten weerstand om de AP te benaderen voor vragen, omdat het risico reëel wordt geacht dat er controles of

maatregelen volgen. Ook qua (vertrouwen in de eigen) kennis over verschillende aspecten zijn er mogelijk knelpunten. Een kwart van de respondenten ervaart knelpunten met betrekking tot uitzonderingsgronden (53% ervaart geen knelpunten) en ruim een derde van de respondenten vindt dat uit jurisprudentie geen of onvoldoende duidelijkheid volgt over de normen uit de UAVG.

De kennis en het bewustzijn over datalekken binnen de eigen organisatie wordt door de respondenten positief beoordeeld en er worden ook veel acties ondernomen om dit verder te vergroten. Toch is het percentage datalekken dat wordt gemeld bij de AP en bij de door de datalekken getroffen personen zeer laag: in beide gevallen gaat het om minder dan 30% van de datalekken. Dit terwijl de FG's wel bijna altijd op de hoogte zijn of worden gesteld wanneer er sprake is van een datalek (voor zover de FG's dat zelf kunnen overzien). Een mogelijke verklaring kan worden gevonden in het feit dat een inhoudelijke respons door de AP bij meldingen van datalekken vaak achterwege blijft of weinig informatieve waarde heeft.

De respondenten zijn over het algemeen niet uitgesproken positief over de mogelijkheden die de toezichthouder heeft om toezicht te houden op de juiste toepassing van algemene uitzonderingen voor het verwerken van bijzondere categorieën gegevens. Rond 25 tot dertig procent van de respondenten vindt dat het goed mogelijk is om hier toezicht op te houden. Ook bij de specifieke uitzonderingen (voor bepaalde categorieën gegevens) geldt dat rond de twintig tot dertig procent van de respondenten hier positief over is.

Ten aanzien van interventies is het belangrijk te vermelden dat een kleine meerderheid van de respondenten vindt dat de AP het nemen van verantwoordelijkheid voor de bescherming van persoonsgegevens bevordert door de manier waarop de toezichthouder haar interventiemogelijkheden inzet.

5 De meldplicht datalekken en de bestuurlijke boete in de praktijk

5.1 Inleiding

In dit hoofdstuk staan conform de opdracht de meldplicht datalekken en de bestuurlijke boete centraal. Beide instrumenten zijn per 1 januari 2016 in de Wbp gevoegd en in werking getreden. Met de evaluatie van deze instrumenten wordt invulling gegeven aan de motie Schouw en Segers uit 2015.[127] We bespreken beide instrumenten en het functioneren daarvan aan de hand van interviews en casestudy's. In het kader van elke casestudy zijn gesprekken gevoerd met betrokkenen vanuit de organisatie en in enkele casus ook met een rechtshulpverlener en andere betrokkenen.

In paragraaf 5.2 presenteren we vier casestudy's waarin de meldplicht en/of de boete aan de orde zijn. In 5.2.1 komt het aan Uber opgelegde boetebesluit aan de orde, opgelegd in verband met een datalek dat weliswaar door Uber werd gemeld, maar buiten de termijn van de AVG. Vervolgens komt het datalek van GGD GHOR NL aan de orde in paragraaf 5.2.2. In 5.2.3 bespreken we de casus Belastingdienst, waarin de AP geen boete oplegde maar wel een verwerkingsverbod in verband met het gebruik van het BSN. In paragraaf 5.2.4 staat de casus VoetbalTV centraal die gaat over het opleggen van een bestuurlijke boete aan VoetbalTV wegens het zonder wettelijke grondslag maken en verspreiden van beelden van voetbalwedstrijden. In paragraaf 5.2.5 komt de casus BKR aan de orde, waarin een bestuurlijke boete is opgelegd vanwege schending van artikel 12, tweede en vijfde lid AVG, het in rekening brengen van kosten voor de inzage in de in het register neergelegde persoonsgegevens. In paragraaf 5.3 en verder analyseren we de informatie uit de casestudy's en de interviews.

In dit hoofdstuk beantwoorden we daarmee de deelvragen 10 en 11 over de toezichtstrategie en het handhavingsbeleid van de AP. Verder komen vraag 12 en 13 aan de orde over de wijze waarop toezicht en handhaving in de praktijk gestalte krijgen en de mate waarin daarbij rekening wordt gehouden met de ernst van de normschending, de mate van verwijtbaarheid en een passende wijze van optreden. Daarnaast staat in dit hoofdstuk vraag 7 over de naleving van de meldplicht datalekken en vraag 14 over de bijdrage van de boetebevoegdheid aan de uitvoering en handhaving van de AVG centraal.

[127] *Kamerstukken II* 2015/16, 33662, nr. 20.

5.2 Casestudy's

De vijf casestudy's die hieronder worden besproken zijn uitgevoerd zodat van begin tot eind een beeld kon worden gevormd van een aantal toezichts- en handhavingstrajecten waarbij de meldplicht datalekken en/of het instrument van de bestuurlijke boete aan de orde waren. De casus zijn geselecteerd aan de hand van een aantal criteria. Ten eerste is gekeken naar de fase waarin de casus zich bevonden. Om een zo goed mogelijk beeld te kunnen krijgen van het toezichts- en handhavingstraject, zijn (bijna) afgeronde dossiers geselecteerd.[128] Ten tweede is gekeken naar de variëteit van onderwerpen van de casus (bijzondere persoonsgegevens, boetes en meldplicht datalekken).[129] Verder is er gestreefd naar een spreiding over domeinen en over de organisaties die daarin centraal staan (overheid, semi-overheid en markt).

5.2.1 Uber

Schets van de situatie en de kern van het geschil
Het Uber-concern – onder meer bestaande uit Uber B.V. (UBV) en Uber Technologies Inc. (UTI) – biedt een dienst aan die het voor gebruikers mogelijk maakt om door middel van de Uber app personenvervoer af te nemen. Gebruikers worden gekoppeld aan een chauffeur (driver) die via een andere app (Uber driver app) klanten kunnen aannemen. Van 13 oktober 2016 tot 15 november 2016 was sprake van een datalek waarbij onbevoegde personen van buiten het Uber-concern toegang kregen tot de gegevensopslag van Uber. Daarin zijn onder meer namen, e-mailadressen en telefoonnummers opgeslagen van wereldwijd 57 miljoen klanten en chauffeurs, waaronder destijds 174.000 Nederlanders. Op 14 november 2016 ontvangt UTI een e-mail van een melder waarin zij op de hoogte worden gesteld van een kwetsbaarheid in haar gegevensbeveiliging. Op 15 november 2016 verhelpt UTI het datalek. UTI besluit vervolgens om $100.000,00 aan beloning aan de melder te betalen, zodat de melder de gelekte data verwijdert. Ook bedingt het Uber-concern een geheimhoudingsclausule. Hieruit volgt dat het Uber-concern het datalek geheim heeft willen houden. De geheimhouding heeft standgehouden totdat een nieuw bestuur is aangetreden bij UTI en is geconfronteerd met het datalek.

Van 13 oktober 2016 tot 15 november 2016 waren de persoonsgegevens van Uber opgeslagen in de opslag die werd beheerd door UTI. Als gevolg van een hack waren die persoonsgegevens in die periode toegankelijk voor onbevoegde personen buiten het Uber-concern. Er was sprake van onrechtmatige verwerking en dus inbreuk op de beveiliging. Ingevolge de toen geldende Wbp heeft het Uber-concern binnen 72 uur na ontdekking van de inbreuk de AP in kennis moeten stellen van het datalek en onverwijld aan betrokken gebruikers. Op grond van 34a Wbp (thans artikel 33, eerste en tweede lid en artikel 34 AVG) heeft de verantwoordelijke een wettelijke meldplicht aan de AP en de betrokkenen als een inbreuk op de beveiliging zich heeft voorgedaan die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De melding van het datalek aan de AP bleef echter uit tot 21 november 2017. Ook werd op diezelfde dag het publiek ingelicht over het datalek door middel van een nieuwsbericht op de website van Uber. Naar aanleiding van de melding op 21 november 2017 is de AP een onderzoek gestart.

[128] Bij de casus van VoetbalTV en BKR loopt ten tijde van dit onderzoek nog een beroepsprocedure.
[129] We hebben ook 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. De beschrijving van deze casestudy is te vinden in paragraaf 6.3.

UBV en UTI hebben onder de Wbp een bewerkersovereenkomst (onder de AVG: verwerkersovereenkomst) gesloten voor de verwerking van persoonsgegevens. Daarmee is bewerkstelligd dat UTI als bewerker (onder de AVG: verwerker) optreedt en UBV als verantwoordelijke. Naar het oordeel van de AP zijn UBV en UTI, gelet op de feitelijke situatie, als gezamenlijke verantwoordelijken aangemerkt. Daarbij neemt de AP in aanmerking dat UTI autonoom en onafhankelijk van UBV optrad bij de afhandeling van het datalek en de feitelijke beslissing over de afhandeling van het datalek (de betaling van de beloning en het sluiten van de overeenkomst met de melder) geheel zelfstandig door UTI is genomen, zonder UBV daarbij te betrekken. Uit deze feitelijke situatie leidt de AP af dat UTI zelfstandig besluiten neemt en feitelijk de zeggenschap heeft over de manier waarop een datalek wordt afgehandeld. De AP verwijt Uber-concern ernstig verwijtbare nalatigheid door het datalek niet onverwijld te melden aan de AP en aan de betrokkenen. Onder artikel 66, vierde lid Wbp is de AP bevoegd om direct een boete op te leggen in geval van een ernstig verwijtbare nalatigheid. Dat heeft de AP ook gedaan door het Uber-concern een bestuurlijke boete op te leggen van € 600.000.

Als gevolg van de impact van deze inbreuk op de beveiliging zijn de toezichthoudende autoriteiten van meerdere landen, waaronder de VS, Duitsland en het VK, onderzoeken gestart naar het datalek en hebben zij boetes opgelegd aan het Uber-concern. In het licht van deze evaluatie wordt alleen het onderzoek in Nederland behandeld.

Procesverloop van het toezichts- en handhavingstraject
Naar aanleiding van de melding van Uber op 21 november 2017 is de AP een onderzoek gestart naar de naleving van artikel 34a Wbp. Daarbij is bij brief van 23 november 2017 aan UBV verzocht om aanvullende informatie over het datalek. Daarna zijn nog diverse informatieverzoeken gevolgd, waaraan Uber gevolg heeft gegeven.

De bevindingen van het onderzoek naar de melding van het datalek zijn opgenomen in een rapport van 1 juni 2018.

Op 15 juni 2018 heeft de AP aan Uber bekend gemaakt dat zij het voornemen heeft een bestuurlijke boete op te leggen wegens overtreding van artikel 34a, eerste lid en tweede lid Wbp. Uber heeft op 3 juli 2018 schriftelijk haar zienswijze gegeven op het voornemen tot het opleggen van een bestuurlijke boete en het rapport van 1 juni 2018.

Op 11 juli 2018 heeft een hoorzitting plaatsgevonden op het kantoor van de AP waarbij Uber haar zienswijze mondeling heeft toegelicht. Daarvan heeft de AP een verslag gemaakt en op 14 september 2018 toegestuurd aan Uber. Bij brief van 27 september 2018 heeft Uber haar opmerkingen op het verslag kenbaar gemaakt aan de AP. Op 22 oktober 2018 heeft de gemachtigde van Uber aan AP een nader stuk toegezonden.

Bij besluit van 6 november 2018 legde de AP het concern een bestuurlijke boete van € 600.000 wegens het schenden van de wettelijke meldplicht, zoals is bedoeld onder artikel 34a, eerste lid en tweede lid Wbp. Bij de vaststelling van de hoogte van deze boete hield de AP rekening met het feit dat het datalek uiteindelijk wel openbaar is geworden en dat de afdoening daarvan de nodige media-aandacht heeft gehad, zodat betrokkenen er kennis van hebben kunnen nemen. Op 27 november 2018 maakte de AP door middel van een persbericht het boetebesluit openbaar.

Analyse

Dit datalek vond plaats van 13 oktober 2016 tot 15 november 2016 en daarmee voor het van toepassing worden van de AVG. Op 21 november 2017 heeft Uber BV een melding gedaan van een datalek aan de Autoriteit Persoonsgegevens. Naar aanleiding daarvan startte de AP een ambtshalve onderzoek. Zowel onder het regime van de Wbp als dat van de AVG is het niet melden van een datalek een overtreding die beboetbaar was en is. Gelet daarop doet de AP een beroep op het leerstuk van de ononderbroken rechtsorde.[130] Dit betekent dat, ter waarborging van de continuïteit van de rechtsorde, voor gedragingen die plaatsvonden onder het regime van Richtlijn 95/46/EG en de Wbp, de naleving moet worden verzekerd van de rechten en plichten zoals die golden onder dat regime. De AP verwijst daarbij naar de Europeesrechtelijke jurisprudentie op dit vlak.[131] Gezien het bepaalde in artikel 5:46, vierde lid Awb in samenhang bezien met artikel 1, tweede lid Wetboek van Strafrecht[132] wordt het meest gunstige boeteregime toegepast, zijnde artikel 66, tweede lid Wbp. De AP gaat ook nog voor een tweede anker liggen. De AP verwijst naar artikel 48, achtste lid UAVG.[133] Op grond van die bepaling is op wettelijke procedures en rechtsgedingen waar het Cbp voorafgaand aan de inwerkingtreding van de UAVG is betrokken, het recht van toepassing zoals dit gold voorafgaand aan de inwerkingtreding van de UAVG. Voor zover het doen van onderzoek een wettelijke procedure is als bedoeld in artikel 48, achtste lid UAVG, dan ontleent de AP de bevoegdheid om een bestuurlijke boete op te leggen ook aan de Wbp. Het gaat dan om een wettelijke procedure waarbij de AP voorafgaand aan de inwerkingtreding van de UAVG – dus vóór 25 mei 2018 – betrokken is geraakt. Deze wettelijke procedure loopt door na intrekking van de Wbp en het van toepassing worden van de AVG en de inwerkingtreding van de UAVG. Dat betekent volgens de AP dat op grond van het overgangsrecht in de UAVG de Wbp in dit geval van toepassing is en de AP ter zake van de overtreding van artikel 34a, eerste lid Wbp – het niet onverwijld melden aan de AP van een datalek – bevoegd is op grond van artikel 48, achtste lid UAVG in samenhang met artikel 66, tweede lid Wbp een bestuurlijke boete op te leggen. Ter invulling van de boetebevoegdheid maakt de AP gebruik van de Boetebeleidsregels Autoriteit Persoonsgegevens 2016.

De bestuurlijke boete voor het schenden van de meldplicht onder de Wbp bedroeg ten hoogste € 820.000.[134] Onder de AVG zou Uber voor dezelfde overtreding beboet kunnen met een bedrag oplopend tot € 10 miljoen, of indien dit hoger is, tot 2% van de totale wereldwijde jaaromzet.[135] Desalniettemin is onder de AVG het één-loketmechanisme (de onestopshop) geïntroduceerd, hetgeen inhoudt dat in geval van grensoverschrijdende verwerkingen in beginsel door één toezichthoudende autoriteit (de leidende toezichthouder) onderzocht en beboet kan worden. De andere toezichthoudende autoriteiten moeten medewerking verlenen aan de leidende toezichthouder onder dezelfde overtreding.[136] De Wbp kende het één-loketmechanisme niet. Dit betekent dat het mogelijk is dat toezichthoudende autoriteiten van verschillende landen ieder afzonderlijk een onderzoek starten en afzonderlijk boetes opleggen voor hetzelfde datalek. In dit geval heeft Uber – naast de bestuurlijke boete van € 600.000 van de

[130] Paragraaf 3.1.2 van het boetebesluit.
[131] Vgl. HvJ-EU 29 maart 2011 inzake ThyssenKrupp (C-352/09 P), punt 79 en Gerecht van eerste aanleg van de EG van 12 september 2007 inzake González y Díez, SA, SA (T-25/04), punt 59.
[132] Deze bepaling geeft uitdrukking aan de erkenning van het legaliteitsbeginsel voor het (materieel) strafrecht. Ook op veranderingen van wetgeving met betrekking tot de strafbedreiging geldt dat op basis van het zogenoemde Scoppola-arrest van het EHRM (EHRM 17 september 2009, ECLI:CE:ECHR:2009:0917JUD001024903) en het Arrest van de Hoge Raad van 12 juli 2011 (ECLI:NL:HR:2011:BP6878, NJ 2012/78) de meest gunstige bepaling moet worden toegepast.)
[133] Paragraaf 3.1.3 van het boetebesluit.
[134] Artikel 66, tweede lid Wbp.
[135] Artikel 83, vierde lid AVG.
[136] Overweging 124 en 127 AVG.

AP – in Duitsland een boete van € 20.000 opgelegd gekregen. Ook in het VK heeft Uber een boete van £ 385.000 gekregen.[137]

Het doel van de meldplicht is om datalekken te voorkomen en, als deze zich voordoen, de gevolgen voor de betrokkenen zoveel mogelijk te beperken. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Transparantie over de aard van het datalek, de vermoedelijke omvang ervan en de aard van de mogelijke schade, de inspanningen die gepleegd worden om de schade te herstellen en raadgevingen aan publiek en klanten om zichzelf zo goed mogelijk in staat te stellen de consequenties voor de eigen belangen te overzien zijn noodzakelijke maatregelen voor behoud en herstel van dat vertrouwen. Daarnaast wordt de AP in staat gesteld zich een eigen beeld te vormen van de feiten, een oordeel te kunnen geven over de genomen maatregelen, onder omstandigheden met de verantwoordelijke te kunnen overleggen en zo nodig te kunnen interveniëren.[138] Niet alleen is Uber de meldplicht niet nagekomen, Uber heeft ook bewust geheimhouding bedongen met de melders om zich ervan te verzekeren dat het datalek niet kenbaar zou worden gemaakt.

Bijzonder aan deze casus is dat Uber in eerste instantie het datalek in de doofpot heeft willen stoppen, maar na een jaar toch heeft besloten de melding bij de AP te doen en het datalek kenbaar te maken via de website van Uber. Uber heeft ervoor gekozen om het aanzienlijk bedrag van $ 100.000 te betalen aan de melder als 'beloning voor het melden van de kwetsbaarheden in de informatiebeveiliging'. De hoogte van dit bedrag is buiten het normale wat aan dergelijke melders wordt betaald. De AP verwijt Uber ernstig verwijtbare nalatigheid vanwege het te laat melden van het datalek en het ontnemen van de mogelijkheden aan de betrokkenen te reageren op de nadelige gevolgen van het datalek.

De AP heeft Uber beboet voor het niet tijdig melden van het datalek aan de AP (artikel 34a, eerste lid Wbp) en het nalaten om betrokkenen onverwijld in kennis te stellen van het datalek (artikel 34a, tweede lid Wbp).

De AP heeft bij de evenredigheidstoets van de hoogte van de bestuurlijke boete rekening gehouden met het feit dat de huidige CEO van UTI de beslissing heeft genomen om het datalek alsnog na één jaar kenbaar te maken aan betrokkenen en te melden aan de AP. Hiermee geeft de AP het signaal af dat melden van het datalek loont, zelfs wanneer de termijn van 72 uur is verstreken. Dit moedigt verwerkingsverantwoordelijken aan om datalekken te melden. Bij de bepaling van de boetehoogte heeft de AP gebruik gemaakt van de Beleidsregels Autoriteit Persoonsgegevens 2016. Zo is gekeken naar de ernst van de overtreding, de duur en de impact van de overtreding op betrokkenen en/of de maatschappij.[139] Daarbij heeft de AP ook artikel 83, tweede lid AVG als basis genomen.[140] In het bijzonder lijkt artikel 83, tweede lid onder h AVG, 'de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld'. Hoewel de AP dit niet met zoveel woorden heeft gezegd is het goed mogelijk dat de AP de verlaging van de boete heeft gebaseerd op het in dit artikel vastgelegde omstandigheden.

[137] Buiten de Eurozone trof Uber met de Federal Trade Commission in de VS een schikking van $148 miljoen.
[138] *Kamerstukken II* 2012/13, 33662, nr. 3, p. 1 en 4.
[139] Artikel 6 Boetebeleidsregels Autoriteit Persoonsgegevens 2016 (oud).
[140] Zie voetnoten 129 en 132 van het Boetebesluit Uber.

In 2019 zijn de Boetebeleidsregels Autoriteit Persoonsgegevens 2016 vernieuwd. Sindsdien zijn de criteria van artikel 83, tweede lid AVG overgenomen in artikel 7 Boetebeleidsregels Autoriteit Persoonsgegevens 2019 en worden de omstandigheden die spelen bij de overtreding getoetst aan die criteria. Zo ook in de volgende twee uitgewerkte, tot op zekere hoogte vergelijkbare casus, waarin een datalek niet of niet tijdig is gemeld.

Vergelijkbare casus: Booking.com en PVV Overijssel
In de casus Booking.com heeft de AP voor een soortgelijke overtreding een boete opgelegd van € 475.000 voor het 22 dagen te laat melden van het datalek. Het ging om een datalek waarbij onbevoegden persoonsgegevens van meer dan 4.000 klanten hebben bemachtigd. Ook hebben zij de creditcardgegevens van bijna 300 klanten kunnen inzien. Ingevolge Bijlage I van Boetebeleidsregels Autoriteit Persoonsgegeven 2019 is schending van de meldplicht een categorie III-overtreding waar een basisboete van € 525.000 op staat.[141] Omdat Booking.com maatregelen heeft getroffen om de schade voor betrokkenen te beperken werd de basisboete door de AP verlaagd met € 50.000.[142]

In de boetezaak van PVV Overijssel is in het geheel niet overgegaan tot het melden van het datalek aan de AP. Het datalek betrof een e-mail die door PVV Overijssel was verzonden waarin de gehele lijst met mailadressen zichtbaar was voor alle geadresseerden. Volgens de AP is het geheel niet melden van het datalek door PVV Overijssel verwijtbaar. Initieel heeft de AP aan PVV Overijssel een boete van € 525.000 willen opleggen. Het boetebedrag is uiteindelijk verlaagd naar € 7.500, omdat PVV Overijssel het boetebedrag van € 525.000 niet kon dragen.[143]

Deze laatste casus geeft in relatie tot de Uber-case aanleiding tot de hiernavolgende bespiegeling. Nu PVV Overijssel het datalek nooit heeft gemeld en uit de gedraging ook opgemaakt kan worden dat PVV Overijssel niet de intentie heeft gehad het datalek te melden, zou dit – in lijn met de hiervoor besproken casus – een verzwarende factor moeten zijn voor verhoging van de basisboete. De AP heeft de gedraging veroordeeld en merkt dit aan als een verwijtbare gedraging en een ernstige overtreding. Toch heeft de AP in deze zaak geen aanleiding gezien om de basisboete te verhogen. Dit lijkt niet goed te rijmen met het door de AP gehanteerde boetebeleid en het bepaalde in artikel 83, tweede lid, onder h AVG. Het verhogen van de basisboete zou in deze zaak een duidelijk signaal afgeven over de ernst van de gedraging (geheel niet melden aan de AP). Dit zou de voorspelbaarheid van het boetebeleid van de AP ook ten goede komen. Ook blijft daarmee het afgegeven signaal van de AP vooralsnog intact, zelfs wanneer de boete verlaagd moet worden vanwege de financiële draagkracht van de overtreder.

5.2.2 GGD GHOR NL

Schets van de situatie en de kern van het geschil
RTL Nieuws signaleerde eind januari 2021 een datalek bij GGD GHOR NL, de koepelorganisatie van GGD'en. In het kader van de coronapandemie verwerken zij persoonsgegevens in de systemen CoronIT, HPZone en HPZone Lite. Medewerkers van de GGD hebben uit deze systemen persoonsgegevens gedownload. Het ging om adressen, telefoonnummers, burgerservicenummers en testresultaten. Een deel daarvan is te koop aangeboden op internet. RTL Nieuws meldde het datalek aan GGD GHOR NL en heeft het nieuws na twee dagen gepubliceerd.

[141] Bijlage I Boetebeleidsregels Autoriteit Persoonsgegevens 2019.
[142] Boete Booking.com.
[143] Boete PVV Overijssel.

De GGD GHOR NL deed binnen 72 uur na kennisneming een voorlopige melding van het datalek bij de AP. De AP startte daarna een onderzoek naar de beveiliging van persoonsgegevens in voormelde systemen. Deze systemen worden door alle 25 GGD'en gebruikt. In het kader van het onderzoek heeft de AP controles uitgevoerd bij GGD GHOR en steekproefsgewijs bij twee regionale GGD'en en een van de landelijke partners die capaciteit leveren voor het uitvoeren van bron- en contactonderzoek. De AP heeft in het bijzonder onderzocht of voldoende verbetermaatregelen zijn getroffen met het oog op toegangsbeveiliging, verleende autorisaties en autorisatiebeheer, logging van de gebruikte systemen, controle op deze logging en om het ongeoorloofd exporteren/printen van persoonsgegevens uit de systemen te voorkomen. Ook heeft de AP gecontroleerd of de aangekondigde maatregelen met betrekking tot beperking van de zoekfuncties van gebruikers in de systemen ook daadwerkelijk zijn getroffen. Daarnaast is onderzocht of de betrokkenen die geraakt zijn door het datalek in overeenstemming met de AVG zijn geïnformeerd over de inbreuk in verband met hun persoonsgegevens. Tenslotte heeft de AP naar aanleiding van berichtgeving in de media in februari 2021 onderzocht of de website www.coronatest.nl aan de beveiligingseisen voldoet die gelden voor aansluiting op DigiD.

De AP constateert in haar eindbrief[144] dat een aantal aangekondigde verbetermaatregelen is getroffen waardoor het risico op datalekken is verminderd. Wel ziet de AP nog wezenlijke risico's voor de beveiliging van persoonsgegevens die aanvullende verbetermaatregelen vereisen. Het gaat hier in het bijzonder om risico's die verband houden met het grote aantal partijen dat betrokken is bij de verwerkingen van persoonsgegevens in verband met het testen, vaccineren en bron- en contactonderzoek. In ieder geval zijn dit de 25 regionale GGD'en, de landelijke koepelorganisatie GGD GHOR NL, zes landelijke partnerorganisaties (callcenters en alarmcentrales), diverse uitzendbureaus en IT-leveranciers.

In haar eindbrief draagt de AP GGD GHOR NL en de GGD'en op om 'onderling en met de overige betrokken partijen per direct duidelijke afspraken op het vlak van informatiebeveiliging te maken, vast te leggen en actueel te houden. Voor partijen dient duidelijk te zijn wie voor welke technische en/of organisatorische maatregelen verantwoordelijk is. Dat is nu onvoldoende geregeld.' De AP geeft tot slot aan uiterlijk op 1 maart 2022 in een voortgangsrapportage hierop een reactie te verwachten en een overzicht van de verbetermaatregelen die in dit verband zijn of worden getroffen.

GGD GHOR NL geeft aan zelf tussentijds aan de AP te hebben laten zien welke maatregelen zij gedurende het onderzoek had getroffen, maar de eindbrief gaat uit van de feiten zoals die in het begin van het onderzoek zijn vastgesteld. De tussentijds genomen maatregelen zijn hierin niet meegenomen. Hierover is gedurende het onderzoek ook geen voortgangsgesprek geweest.

De AP heeft de eindbrief óók verstuurd naar de 23 GGD'en waarnaar zij geen onderzoek heeft gedaan en spreekt de verwachting uit dat alle GGD'en de in de eindbrief genoemde noodzakelijke verbetermaatregelen treffen om een passend niveau van beveiliging van persoonsgegevens te waarborgen.

[144] Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en.

Procesverloop van het toezichts- en handhavingstraject
GGD GHOR NL heeft op 22 januari 2021 (binnen 72 uur na kennisneming) een voorlopige melding van het datalek gedaan bij de AP. De AP startte vervolgens een onderzoek bij GGD GHOR en twee GGD'en. Onderzocht werd of passende technische en organisatorische maatregelen zijn getroffen om de persoonsgegevens die worden verwerkt in het kader van het testen, vaccineren en bron- en contactonderzoek in verband met de coronapandemie passend te beveiligen. In haar 'eindbrief' van 8 november 2021 heeft de AP GGD GHOR NL verzocht om uiterlijk op 1 maart 2022 een voortgangsrapportage te sturen, waarin zij ingaat op de beveiligingsmaatregelen die zij heeft getroffen naar aanleiding van alle in de eindbrief genoemde punten.

Analyse
Het door RTL Nieuws gesignaleerde datalek heeft binnen GGD GHOR NL het belang van goede gegevensbescherming onder de aandacht gebracht, zo stellen gesprekspartners binnen GGD GHOR NL. Het daaropvolgende onderzoek van de AP had impact op de relatie tussen GGD GHOR NL en de 25 GGD'en (waarvan er dus twee bij wijze van steekproef door de AP zijn onderzocht). De AVG-rol van GGD GHOR NL en de verhouding die zij heeft tot de 25 GGD'en is niet helder gedefinieerd in relevante wetgeving. Dit zorgde wel voor onrust omtrent het datalek, in het bijzonder in relatie tot het onderzoek daarnaar door de AP.

Gedurende het onderzoek heeft GGD GHOR NL vragen gesteld aan de AP, maar die werden volgens GGD GHOR NL niet beantwoord. De AP deed tussentijds geen handreikingen over hoe de (mogelijke) overtredingen op het gebied van beveiliging volgens haar konden worden beëindigd. GGD GHOR NL stelt dat zij de AP al vóór het onderzoek heeft gevraagd om mee te kijken bij een DPIA op het desbetreffende IT-systeem. De AP is hier niet op ingegaan. De AP kijkt wel mee in geval van een voorafgaande raadpleging, die door de verwerkingsverantwoordelijke moet worden aangevraagd bij een DPIA met hoge restrisico's.

GGD GHOR NL heeft lopende het onderzoek naar eigen zeggen gedeeltelijk aan de AP laten zien welke maatregelen zij had getroffen, maar volgens haar is er geen voortgangsgesprek geweest. Wel heeft GGD GHOR NL uitleg kunnen geven over het Security Operations Center (SOC) en de tooling die zij zou gaan gebruiken voor logging en controle daarop. De uiteindelijke eindbrief van begin november 2021 gaat uit van de feiten zoals die in het begin van het onderzoek zijn vastgesteld. De eindbrief verraste GGD GHOR NL, omdat zij een onderzoeksrapport had verwacht. In plaats daarvan staan de bevindingen in een eindbrief, waarin de AP een voortgangsrapportage eist van GGD GHOR NL. Er is vooralsnog geen boete opgelegd.

Vergelijkbare casus: HagaZiekenhuis, OLVG en Transavia
In soortgelijke gevallen waarin beveiligingsgebreken aan het licht komen na een datalek, hanteert de AP het stramien van een formeel onderzoeksrapport met een daaropvolgende handhavingsprocedure. Die handhaving bestaat doorgaans in het opleggen van een boete. Zo heeft de AP een boete opgelegd aan het HagaZiekenhuis naar aanleiding van een datalek dat eruit bestond dat medewerkers onrechtmatig het medisch dossier van een bekende Nederlander hadden ingezien. Naar aanleiding hiervan deed de AP onderzoek naar de beveiliging van medische dossiers. Die bleek tekort te schieten. De AP is uitgekomen op een boetebedrag van in totaal € 460.000. De boete is uiteindelijk door Rechtbank Den Haag gematigd naar € 350.000, omdat rekening moest worden gehouden met het feit dat het ziekenhuis in de tussentijd passende maatregelen heeft genomen om de overtreding te beëindigen.[145] Mede naar aanleiding van twee datalekmeldingen heeft de AP ook bij het ziekenhuis OLVG een onderzoek ingesteld

[145] Rb. Den Haag 31 maart 2021, ECLI:NL:RBDHA:2021:3090, r.o. 20.

naar de beveiliging van medische dossiers. De AP stelde vast dat het OLVG tussen 2018 en 2020 onvoldoende beveiligingsmaatregelen heeft genomen om toegang tot medische dossiers door onbevoegde medewerkers te voorkomen. Dit resulteerde eind 2020 in een boete van € 440.000. In 2021 heeft de AP een boete opgelegd aan Transavia. In die zaak heeft een hacker zich in 2019 toegang verschaft tot de systemen van Transavia en konden de persoonsgegevens van 25 miljoen personen worden ingezien. Vastgesteld is dat de persoonsgegevens van 83.000 personen en de gezondheidsgegevens van 367 personen zijn gedownload door de hacker. De AP legde een boete op van in totaal € 400.000. Bij de bepaling van de boetehoogte heeft de AP hier wel rekening gehouden met het feit dat Transavia tussentijds maatregelen heeft getroffen om de overtreding te beëindigen. Echter, niet als verlagende factor is meegewogen dat Transavia het datalek – dat als gevolg van de overtreden norm kon ontstaan – tijdig heeft gemeld. Volgens de AP heeft Transavia hiermee slechts voldaan aan haar wettelijke meldplicht aan de AP en betrokkenen.[146]

Gelet op deze vergelijkbare casus waarin de AP een boete oplegde in verband met tekortschietende beveiligingsmaatregelen die het ontstaan van een datalek mogelijk maakten (HagaZiekenhuis, OLVG en Transavia), is het opvallend dat de AP bij GGD GHOR is afgeweken van deze lijn door een eindbrief te sturen met de verplichting tot aanlevering van een voortgangsrapportage, in plaats van (direct) een formeel onderzoek te verrichten gevolgd door een handhavingsprocedure. Het is daarmee niet altijd duidelijk wat een verwerkingsverantwoordelijke van een onderzoeks- en handhavingstraject kan verwachten. Om dit inzichtelijker te maken zou het helpen als de AP steeds publiekelijk kenbaar maakt waarom zij voor een bepaalde insteek kiest (wel/geen formele onderzoeksprocedure, en toelichting op waarom wel/geen formele handhaving met een bepaald type instrument plaatsvindt).

5.2.3 Belastingdienst

Schets van de situatie en de kern van het geschil

Deze casestudy ziet op een kwestie die al een tijd bekend was[147] maar onder de UAVG tot een einde is gebracht. Het gaat om het BTW-nummer dat ondernemers gebruiken in hun contacten met de belastingdienst. Voor zzp'ers, als ondernemer verplicht tot het afdragen van omzetbelasting, werd dit nummer gebaseerd op het burgerservicenummer (BSN), de opvolger van het Sociaal Fiscaal nummer (Sofinummer). Europese regelgeving verplicht de ondernemer het BTW-nummer bekend te maken en te publiceren op facturen en op de website. Hierdoor wordt het BSN veel breder bekend gemaakt. Deze casestudy gaat dus niet over een datalek. De door de AP geconstateerde overtredingen zijn gelegen in artikel 6, eerste lid AVG en artikel 46 UAVG. Het BSN is een identificerend nummer als bedoeld in artikel 46 UAVG en mag alleen gebruikt worden ter uitvoering van de Wet algemene bepalingen burgerservicenummer of andere wetgeving.

Bij de casus zijn betrokken een zelfstandige zonder personeel (ZZP'er) die een ander BTW-nummer wil zonder haar BSN, de staatssecretaris van Financiën, de belastingdienst, de AP, de Tweede Kamer en de rechtbank Amsterdam. Op een later moment vraagt de staatssecretaris een commissie van deskundigen advies over de te kiezen uitvoeringsmaatregelen.

Grofweg waren er twee standpunten in deze kwestie: het standpunt dat door het gebruik van het BSN als BTW-nummer voor natuurlijke personen die een onderneming hebben in de zin van de Wet op de omzetbelasting, de regels van artikel 46 UAVG worden overschreden, en het

[146] Boete Transavia, par. 4.3.
[147] Zie Kamervragen van Omtzigt, mei 2011: Kamerstukken II, 2010/11, 2011Z09316.

standpunt dat het BTW-nummer mag bestaan uit het BSN omdat er een wettelijke grondslag is.

Procesverloop van het toezichts- en handhavingstraject

Deze casus is bijzonder omdat het illustreert hoe verschillende factoren een rol spelen bij het uiteindelijk naleven van de UAVG door een overheidsorganisatie. Het toont ook hoe een jarenlang lopende discussie ineens wel beslecht wordt, waarbij het niet zonder meer is vast te stellen of dit een causaal verband heeft met de UAVG of de interventie van de toezichthouder.

Dat het BSN onderdeel is van het BTW-nummer en zich daardoor mogelijk slecht verhoudt met de bescherming van persoonsgegevens was al langer bekend. In 2011 antwoordt de staatssecretaris van Financiën op vragen van Omtzigt dat het bij zelfstandige ondernemers niet mogelijk is om een nummer toe te kennen dat niet aan een persoon is gekoppeld. De staatssecretaris geeft aan dat als er voor een persoon twee verschillende registratienummers moeten worden gehanteerd, dit de overheid en de ondernemer tijd en geld kost. Ook wordt geconcludeerd dat 'het parallelle gebruik van twee registratienummers' minder efficiënt zal zijn en de overheid zal 'hinderen in de dienstverlening en handhavingsactiviteiten'.[148] De link tussen het openbaar maken van het BSN met het risico op identiteitsfraude wordt ook al meerdere malen gelegd.[149] Door de Tweede Kamer wordt in 2014 een motie-Van der Linden/Oosenbrug aangenomen om het BTW-nummer te ontkoppelen van het BSN. Namens de regering wordt aangegeven dat deze niet zal worden uitgevoerd.[150] In oktober 2015 verschijnt een artikel in het vakblad Privacy & Informatie van Wárlám getiteld 'De Belastingdienst mag het BSN niet omdopen tot BTW-nummer'.[151]

In 2016 worden opnieuw Kamervragen gesteld, dit keer door Oosenbrug en Vos. In de antwoorden van de regering wordt aangegeven dat het BTW-identificatienummer voldoet aan de eisen in artikel 24 Wbp, in de zin dat het een nummer is dat bij de Wet op de omzetbelasting is voorgeschreven en door de Belastingdienst voor bij die wet voorgeschreven doeleinden wordt gebruikt. De regering ziet geen 'omvangrijk privacyprobleem'. Volgens de regering weegt de 'praktische onmogelijkheid van het vervangen van het BTW-nummer van zelfstandigen' op tegen 'hun belangen uit oogpunt van gegevensbescherming'. Wel wordt toegezegd dat als mensen aantoonbaar schade leiden als direct gevolg van de koppeling tussen BSN en BTW-nummer én de verplichting om het BTW-nummer te vermelden op documenten, wordt onderzocht of eventueel geleden nadeel kan worden gecompenseerd.[152]

Ondertussen kaartte een zelfstandige ondernemer, hierna mevrouw X, de kwestie zelf aan bij de staatssecretaris van Financiën. In 2016 diende zij een verzoek in ter verbetering van haar persoonsgegevens op grond van artikel 36 Wbp. Ze wil dat haar BTW-nummer wordt vervangen door een ander nummer, want ze wil haar BSN privé houden. Dit verzoek werd afgewezen in augustus 2016. Haar bezwaar tegen dit verzoek is door de staatssecretaris ongegrond verklaard bij besluit van 21 december 2016. Zij gaat in beroep tegen dit besluit en ze verzoekt de AP om te bemiddelen. De AP laat haar weten niet te bemiddelen maar start wel, onder andere vanwege haar verzoek, een ambtshalve onderzoek naar de werkwijze van de Belastingdienst.

[148] *Kamerstukken II* 2010/11, Aanhangsel 2648.
[149] Bijvoorbeeld in de Kamervragen van Schouten, *Kamerstukken II* 2011/12, Aanhangsel 1219.
[150] *Kamerstukken II* 2013/14, 31066 nr. 210.
[151] Wárlám 2015.
[152] *Kamerstukken II* 2015/16, Aanhangsel 3113.

In april 2018 stelt de regering naar aanleiding van Kamervragen van Van der Molen, Omtzigt en Lodders, voor het eerst 'open te staan' voor een BTW-identificatienummer dat niet meer het BSN bevat. Er wordt gerefereerd aan het lopende onderzoek door de AP. Op voorhand stelt de regering dat er juridisch niets wijzigt en dat het gebruik van het BSN in het BTW-nummer een wettelijke grondslag heeft.[153]

Nadat de AP op basis van onderzoek heeft vastgesteld dat de verwerking geen wettelijke grondslag heeft, legt de AP een verwerkingsverbod op ingevolge artikel 58, tweede lid, onder f AVG. In het besluit wordt aangegeven dat de staatssecretaris de tijd krijgt de onrechtmatige situatie te herstellen, uiterlijk tot 1 januari 2020, de ingangsdatum van het verbod. Het niet naleven van het verbod kan worden beboet. Na het besluit verschijnt het rapport van de commissie van deskundigen waarin de staatssecretaris wordt geadviseerd hoe de transformatie binnen de gestelde tijd vorm zou kunnen krijgen. Tot een boete hoeft het niet te komen, de belastingdienst zorgt voor een tijdige wijziging in de uitvoering.

In deze zaak werd, soms gelijktijdig, op verschillende borden geschaakt. In een individuele rechtszaak bij de rechtbank Amsterdam door een betrokkene tegen de staatssecretaris van Financiën, in het parlement en de staatssecretaris en tussen de belastingdienst en de AP.

Uiteindelijk stelt de AP eerst de normschending vast om een half jaar later het handhavingsbesluit bekend te maken: een verwerkingsverbod met ingang van een jaar later, per 1 januari 2020. De AP legt aan dit besluit ten grondslag dat gelet op de duur, omvang en ernst van de overtredingen, waaronder het groot aantal betrokkenen, de overtredingen zo spoedig mogelijk ongedaan moet worden gemaakt, uiterlijk 1 januari 2020. De AP heeft bij de bepaling van deze termijn rekening gehouden met de inschatting van de belastingdienst dat de invoering vijf jaar in beslag zal nemen, maar versneld kan worden als er meer budget voor wordt vrijgemaakt. De AP noemt dit 'onmiskenbaar een kwestie van politieke prioriteit'.

Door het verloop van de tijd gaan vervolgens een aantal zaken door elkaar lopen. Voor de bespreking van de rechtszaak is belangrijk dat de rechtbank Amsterdam uitspraak doet op 28 maart 2019. De hiervoor beschreven gebeurtenissen worden door de rechtbank uitvoerig in de uitspraak besproken.

Opvallend is de opstelling van de staatssecretaris in deze rechtszaak. Er wordt om meer tijd gevraagd om zich uit te kunnen laten over het geschil nu er nieuwe wetgeving van toepassing is, de AVG en de UAVG. Vervolgens wordt namens de staatssecretaris onder andere aangevoerd dat eiseres geen procesbelang heeft omdat al in de Tweede Kamer was toegezegd dat er een vernummering zou plaatsvinden. Ook stelt de staatssecretaris dat de gegevensverwerking niet onrechtmatig was. Het zou pas onrechtmatig worden op het moment van het ingaan van het verwerkingsverbod op 1 januari 2020. Tot slot wordt gesteld dat het verzoek van eiseres de reikwijdte van artikel 17 AVG te buiten valt en dat er veel andere belangen zijn zodat er geen onredelijke vertraging is als bedoeld in artikel 17 AVG. Uit de gesprekken bleek dat deze opstelling een bewuste beleidsmatige keuze was vanuit het ministerie van Financiën.

De rechtbank is van oordeel dat de motivering van de staatssecretaris, namelijk dat er een wettelijk grondslag is voor de gegevensverwerking, niet deugdelijk is. Het bestreden besluit wordt vernietigd. Vervolgens toetst de rechtbank ex nunc om te bepalen of de rechtsgevolgen in stand blijven. Dat kan niet zodat de rechtbank zelf in de zaak voorziet. De rechtbank

[153] *Kamerstukken II* 2017/18, Aanhangsel 1841.

overweegt dat er geen wettelijke grondslag is voor het verwerken van het BSN in het BTW-nummer en dat de verwerking in strijd is met artikel 46 UAVG en artikelen 5, eerste lid, onder a en 6 eerste lid, onder e AVG. De rechtbank sluit zich voor de motivering hiervan aan bij het rapport van de AP.

De rechtbank vernietigt het besluit op bezwaar, herroept het primaire besluit en bepaalt dat verweerder uiterlijk 1 januari 2020 het BSN uit het BTW-nummer van eiseres dient te verwijderen en aan haar een nieuw BTW-nummer moet toekennen. Haar verzoek om het per direct toe te wijzen wordt niet gehonoreerd en de rechtbank baseert zich hiervoor op het rapport van de commissie van deskundigen van 10 december 2018.

Analyse
In deze zaak is interessant dat de staatssecretaris al voordat de AP het onderzoek heeft afgerond, en dus voor de vaststelling dat de verwerking niet rechtmatig was, aan de Tweede Kamer laat weten bereid te zijn om te kijken naar mogelijkheden om het BSN uit het BTW-nummer te halen. Hij loopt hiermee niet alleen vooruit op een eventuele conclusie maar hij verlaat hiermee ook een stelling die jarenlang verdedigd was. Het is lastig vast te stellen wat dit heeft veroorzaakt, maar de respondenten wijten de bereidheid van de regering en belastingdienst aan het inzicht dat de maatschappelijke opvatting over privacy en bescherming van persoonsgegevens veranderd is. Zij zagen niet direct een oorzakelijk verband tussen de UAVG en de koerswijziging.

De sanctie van de AP werd als passend ervaren omdat het een erkenning inhield van de ingewikkeldheid van de aanpassing en een extra stimulans vormde om de termijn te halen. We hebben echter niet kunnen vaststellen waarom in de latere rechtszaak door het bestuursorgaan over hetzelfde onderwerp niet dezelfde souplesse is getoond. Het was voorstelbaar geweest dat ter zitting namens de staatssecretaris het standpunt was ingenomen dat het verzoek van betrokkene per 1 januari 2020 zou worden gehonoreerd. Dit was immers al door de staatssecretaris aan de Tweede Kamer bericht. Integendeel, het beroep van betrokkene werd zwaar bestreden alsof er geen onderzoeksrapport of handhavingsbesluit van de AP en toezeggingen aan de Tweede Kamer waren gedaan.

5.2.4 VoetbalTV

Schets van de situatie en de kern van het geschil
In 2018 gaat VoetbalTV, een initiatief van de KNVB en Talpa Network, van start met een platform voor het live uitzenden of terugkijken van amateurvoetbalwedstrijden. Om dit mogelijk te maken hangt VoetbalTV slimme camera's op bij deelnemende voetbalclubs en verspreidt het initiatief de beelden onder publiek via een app. Deze beelden van de amateurvoetballers zijn als persoonsgegevens aan te merken en vallen daarmee onder het bereik van de (U)AVG. De spelers hoeven van VoetbalTV geen toestemming te verlenen voor het maken van de beelden door VoetbalTV, maar teams en individuele leden hebben wel de mogelijkheid kenbaar te maken dat zij niet willen dat er beelden van hen worden uitgezonden.

De AVG verlangt dat voor iedere verwerking van persoonsgegevens een verwerkingsgrondslag bestaat. Zo'n verwerkingsgrondslag is die van het gerechtvaardigd belang.[154] Over de invulling van het begrip gerechtvaardigd, als bedoeld in artikel 6, eerste lid, onderdeel f AVG, belang publiceert de AP ruim een jaar na de lancering van VoetbalTV, op 1 november 2019, een zgn.

[154] Artikel 6, eerste lid, sub f AVG.

normuitleg.[155] De Autoriteit geeft aan dat in de ogen van de toezichthouder een verwerking van persoonsgegevens ten behoeve van een commerciële activiteit niet als een gerecht-vaardigd belang kan worden aangemerkt. Deze uitleg voor het commercieel gebruik is strikter dan onder andere de opinie van de WP29 over het begrip uit 2014.[156] De WP29 stelde dat een gerechtvaardigd belang in (1) overeenstemming moet zijn met EU- en nationaal recht, (2) voldoende concreet moet zijn, en (3) niet speculatief, moet zijn. Ook verhoudt de normuitleg zich niet goed met de rechtspraak van het Hof van Justitie van de EU en de conclusies van de A-G. [157]

Vervolgens legt de Autoriteit Persoonsgegevens, nadat VoetbalTV een procedure wegens niet tijdig besluiten was begonnen, op 16 juli 2020 een boete op van € 575.000.[158] Deze boete ziet (mede) op gedragingen van vóór de publicatie van voormelde normuitleg.

VoetbalTV heeft volgens de toezichthouder zonder rechtmatige grondslag video-opnamen gemaakt van een groot aantal voetbalwedstrijden en deze beelden verder verspreid onder een groot publiek via de VoetbalTV-app. Daarmee heeft VoetbalTV volgens de AP in strijd gehandeld met het beginsel dat persoonsgegevens rechtmatig moeten worden verwerkt.[159] De verwerking zou volgens de AP niet noodzakelijk zijn voor de behartiging van gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde. VoetbalTV heeft volgens de AP een 'louter commercieel belang,' waarbij zij de persoonsgegevens van anderen 'te gelde maakt.' Dit is volgens de AP een ernstige overtreding en rechtvaardigt een hoge boete van € 575.000.[160]

In de rechtszaak die op de boete volgt, stelt VoetbalTV dat het opnemen en uitzenden van de wedstrijden valt onder de journalistieke exceptie,[161] maar hier gaat de rechtbank niet in mee.[162] Verder stelt VoetbalTV dat er sprake is van een gerechtvaardigd belang om persoonsgegevens te verwerken zoals bedoeld in de AVG.[163] In dit kader is interessant dat VoetbalTV in de beroepsprocedure aanvoert dat de normuitleg van de AP over het gerechtvaardigd belang in strijd is met de uitleg die de toezichthouder hier eerder aan gaf.[164] De rechter behandelt dit punt echter niet en gaat in plaats daarvan direct over op de behandeling van de vraag of zij de normuitleg van de AP inhoudelijk wel of niet volgt. Om te beoordelen of gebruik gemaakt kan worden van de grondslag van een gerechtvaardigd belang toetst de rechtbank aan de hand van artikel 6, eerste lid, onder f AVG aan de volgende punten:

1. Er is sprake van een gerechtvaardigd belang.
2. De verwerking van de persoonsgegevens zijn noodzakelijk voor de behartiging van dat gerechtvaardigde belang. Hierbij moet ook worden getoetst aan de proportionaliteit en subsidiariteit.
3. Er is een afweging gemaakt tussen de belangen van de verantwoordelijke en de betrokkenen.

[155] Autoriteit Persoonsgegevens 2020.
[156] Groep Gegevensbescherming artikel 29 2014.
[157] Zie bijv. arrest van het HvJ-EU, inzake ASNEF, 24 november 2011, nrs. C-468/10 en C-469/10, ECLI:EU:C:2011:777 Conclusie A-G HvJ-EU, 19 december 2018, nr.C-40/17, ECLI:EU:C:2018:1039 en Conclusie A-G HvJ-EU, 27 januari 2017, nr. C-13/16, ECLI:EU:C:2017:43.
[158] Dit boetebesluit is niet gepubliceerd.
[159] Artikel 5, eerste lid, sub d, aanhef en sub a in samenhang met artikel 6, eerste lid AVG.
[160] Rechtbank Midden-Nederland, 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 6 en 19.
[161] Artikel 85 AVG in samenhang met artikel 43 UAVG.
[162] Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 7 t/m 10.
[163] Artikel 6, eerste lid, aanhef en onder f AVG.
[164] Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 12.

Bij de eerste vraag overweegt de rechtbank dat de vraag of een verwerker van persoonsgegevens een gerechtvaardigd belang heeft, aan de hand van een negatieve toets moet worden beoordeeld. Dit houdt in dat de verwerker geen belang mag nastreven dat in strijd is met de wet. Dat het gerechtvaardigd belang niet moet worden gezien als een min of meer wettelijk belang, zoals de AP stelt, maar veel meer als een legitiem belang, sluit volgens de rechtbank ook aan bij de buitenlandse vertalingen van het begrip gerechtvaardigd belang. Daarnaast heeft het HvJ-EU 'bij herhaling bevestigd dat het lidstaten niet vrijstaat om een beroep op het gerechtvaardigd belang voor bepaalde categorieën verwerkingen op voorhand of categorisch uit te sluiten', aldus de rechtbank.[165] De rechtbank volgt de AP dus niet in de normuitleg van gerechtvaardigd belang, onder verwijzing naar de jurisprudentie van het HvJ-EU.[166]

Verder stelt de rechtbank vast dat het uitgevoerde onderzoek door de AP geen betrekking heeft op de vraag of het noodzakelijk is dat VoetbalTV de persoonsgegevens voor de door haar gestelde doelen verwerkt. Ook is door de toezichthouder, in de fase van het onderzoek, geen belangenafweging gemaakt volgens de rechtbank. De AP is gestopt bij het vaststellen dat VoetbalTV geen gerechtvaardigd belang heeft, en heeft de verwerking van persoonsgegevens niet volledig onderzocht. De rechtbank oordeelt daarom dat het besluit niet zorgvuldig is genomen.[167]

Tegen dit besluit is door de AP hoger beroep ingediend bij de ABRvS. De zitting heeft plaatsgevonden op 23 mei 2022. Op moment van afronden van de onderhavige evaluatie is er nog geen uitspraak gedaan door de ABRvS.

Procesverloop van het toezichts- en handhavingstraject
Het proces van toezicht op VoetbalTV start nagenoeg tegelijkertijd met de lancering van het videoplatform voor amateurvoetbal. In de maand september 2018 reageert de AP via Twitter op het volgende bericht van een ouder over de beelden die door VoetbalTV worden gemaakt.

'Beste autoriteit, kijken jullie ook mee? Groepsdruk is zo groot om mee te doen, dat afwijken eigenlijk niet mag? Is dat toegestaan? Kun je nog voetballen als je niet gefilmd op internet wil?'

De reactie van de Autoriteit op 10 september 2019 op dat bericht luidt als volgt:

'Plannen voor @VoetbalTV roepen idd veel privacyvragen op. Mensen hebben zorgen over privacy. De AP gaat daarom met de @KNVB in gesprek. Het is een groot goed om je onbespied te mogen wanen, geldt zeker voor kinderen.'

Naar aanleiding van deze tweet vindt begin oktober 2018 een gesprek plaats tussen VoetbalTV, de KNVB, Talpa Network en de AP over het initiatief VoetbalTV.

Twee maanden later op 5 december 2018 deelt de AP VoetbalTV mee dat er een onderzoek wordt gestart naar de verwerking van persoonsgegevens. De AP vraagt documenten op en stelt een aantal vragen aan VoetbalTV. Het doel van dit onderzoek is om vast te stellen of VoetbalTV een wettelijke grondslag heeft voor het verwerken van de beelden van het

[165] Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 15.
[166] Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 13 t/m 21.
[167] Rechtbank Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 22.

amateurvoetbal. Ook heeft de Autoriteit Persoonsgegevens in die brief VoetbalTV in de gelegenheid gesteld op de brief te reageren.[168]

Naar aanleiding van het onderzoek van de AP stuurt de toezichthouder VoetbalTV het conceptrapport toe.

Op 6 november 2019 stuurt de AP het definitieve onderzoeksrapport naar VoetbalTV.[169] De conclusie van het definitieve rapport was dat VoetbalTV zonder verwerkingsgrond videobeelden van een groot aantal amateurvoetbalwedstrijden heeft gemaakt en deze beelden verder heeft verspreid onder een groot publiek via de VoetbalTV-app en via de analyse tools. Daarmee heeft VoetbalTV artikel 6, eerste lid AVG in samenhang met artikel 5, eerste lid, aanhef en onder a AVG, overtreden.'

In reactie op het definitieve rapport vraagt VoetbalTV de AP een besluit te nemen. Tevens vindt er op 5 december 2019 een zienswijzegesprek plaats bij de Autoriteit Persoonsgegevens.

Na het uitblijven van een beslissing stelt VoetbalTV op 20 mei 2020 beroep in wegens het niet-tijdig beslissen.[170]

Het besluit tot het opleggen van de bestuurlijke boete van € 575.000 aan VoetbalTV is gedateerd 16 juli 2020. De rechtbank verklaart op 23 november 2020 het beroep van VoetbalTV tegen het besluit van 16 juli 2020 gegrond.[171] Zoals gezegd heeft de AP hoger beroep ingesteld tegen de uitspraak van de rechtbank en heeft de ABRvS nog geen uitspraak gedaan ten tijde van het afronden van dit onderzoek.

Analyse
In het kader van toezicht en handhaving is het voor een verwerkingsverantwoordelijke van belang dat de invulling van een norm door de AP duidelijk, nauwkeurig en transparant is. Voorafgaand aan een beslissing tot handhavend optreden moet de AP op dat gebied een afweging maken. De vraag in de casus van VoetbalTV is of de invulling van de norm door de Autoriteit Persoonsgegevens van tevoren voldoende duidelijk was en of het handelen van de toezichthouder in die zin in voldoende mate voorspelbaar was. Wanneer een andere of nieuwe invulling aan een norm wordt gegeven, moeten verwerkingsverantwoordelijken tijd hebben om hun gegevensverwerking aan te passen. De vraag is of die tijd er voor VoetbalTV voldoende was, aangezien de boete voor VoetbalTV (mede) betrekking had op het handelen van VoetbalTV voor de gepubliceerde normuitleg in november 2019 en het definitieve rapport een aantal dagen na het definitieve rapport van de AP naar VoetbalTV werd verstuurd.

Het opleggen van een boete heeft naast het sanctioneren van een geconstateerde overtreding tot doel preventief te werken. Het is de vraag of in het geval van VoetbalTV ook een preventieve werking van het opleggen van de boete is uitgegaan, omdat het boetebesluit niet is gepubliceerd. Om bewustzijn te creëren over het feit dat een boete wordt opgelegd bij overtreding van de norm, en op die manier preventief te werken, had het voor de hand gelegen om

[168] Olsthoorn 2022.
[169] Olsthoorn 2022.
[170] Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.
[171] Het hoger beroep van de Autoriteit Persoonsgegevens tegen de uitspraak van 23 november 2020 loopt op dit moment nog.

het boetebesluit wel te publiceren. Het publiceren van de boete is wel het uitgangspunt van de 'Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens'.[172]

Verder kwam in de interviews naar voren dat er veel vergelijkbare initiatieven op de markt zijn en die ook na de boete aan VoetbalTV niet zijn gestopt. Ook buiten Nederland zijn er vergelijkbare initiatieven. De Nationaal rapporteur 'Twee jaar toepassing AVG' verwijst in een brief aan de vaste Kamercommissie voor Justitie en Veiligheid bijvoorbeeld naar een vergelijkbaar initiatief zoals het Duitse Soccerwatch.tv. Een diepgaande vergelijking heeft de rapporteur niet gemaakt, maar de rapporteur geeft aan dat hij van mening is dat 'de AVG ertoe zou moeten leiden dat binnen de EU vergelijkbare initiatieven vergelijkbare kansen hebben om tot ontwikkeling te komen. Uniforme regelgeving en een gelijk speelveld voor bedrijven zijn hierbij van groot belang.'[173] De boete die de AP VoetbalTV heeft opgelegd, heeft hier niet aan bijgedragen.

5.2.5 BKR

Schets van de situatie en de kern van het geschil
Stichting BKR (BKR) bestaat sinds 1965. De doelstelling van BKR is gelegen in het bevorderen van een maatschappelijk verantwoorde financiële dienstverlening. BKR wil consumenten behoeden voor overkreditering en andere financiële problemen. Ook wil BKR voor zijn zakelijke klanten een bijdrage leveren aan het beperken van de financiële risico's bij kredietverlening en aan het voorkomen en bestrijden van misbruik en fraude. Daartoe verzamelt BKR onder meer financiële gegevens van betrokkenen bij aangesloten kredietaanbieders. BKR beheert het Centraal Krediet Informatiesysteem (CKI). Het CKI is een systeem waarin betalingsachterstanden of andere onregelmatigheden die ontstaan tijdens de looptijd van een kredietovereenkomst met bijzonderheidscoderingen worden vermeld. BKR biedt verschillende digitale producten aan, waaronder de BKR Insolventie Toets, BKR Sanctie Toets, de Politically Exposed Person (PEP) en het BKR (VIS). In het kader van deze activiteiten verwerkt BKR persoonsgegevens van betrokkenen. De grondslag voor de verwerking van persoonsgegevens door BKR als verwerkingsverantwoordelijke is gelegen in artikel 6, eerste lid, aanhef en onder f AVG.[174]

Tot april 2019 bood BKR op haar website twee mogelijkheden aan om inzage te verkrijgen in de persoonsgegevens die BKR verwerkt. De eerste mogelijkheid tot inzage is een betaalde dienst, waarbij drie abonnementsvormen worden gehanteerd, die betrokkenen die inzage wensen in hun persoonsgegevens toegang verschaft tot een elektronische klantomgeving. De tweede mogelijkheid is dat betrokkenen via de website een inzageformulier downloaden, deze uitprinten, het formulier handmatig invullen en die per post in combinatie met een kopie van het identiteitsbewijs sturen naar een postbusnummer. BKR verlangt voor deze wijze van inzage geen betaling.

De AP legt op 30 juli 2019 aan BKR een bestuurlijke boete op van € 830.000. De AP is van oordeel dat BKR artikel 12, vijfde lid AVG vanaf 25 mei 2018 tot en met 28 april 2019 heeft overtreden, omdat BKR niet kosteloos op elektronische wijze inzage in persoonsgegevens heeft gegeven aan betrokkenen in het kader van het recht op inzage. Daarnaast is de AP tot de conclusie gekomen dat BKR tussen 25 mei 2018 tot en met 12 maart 2019 artikel 12, tweede

[172] De AP heeft in reactie op deze paragraaf aangegeven dat de AP ten aanzien van het openbaar maken van besluiten een openbaarmakingsbeleid hanteert. Dit beleid houdt in dat besluiten in beginsel openbaar worden gemaakt, tenzij uit een rechterlijk oordeel volgt dat dat (nog) niet is toegestaan. Hoe dat uitgangspunt in deze casus – waarin dus niet is gepubliceerd – is toegepast, is ook na deze reactie onduidelijk.
[173] Rapporteur 2021, p. 10.
[174] HR 3 december 2021, ECLI:NL:HR:2021:1814.

lid AVG heeft overtreden, doordat BKR het recht van inzage ingevolge artikel 15 AVG niet heeft gefaciliteerd. Op 6 juli 2020 heeft de AP over de boeteoplegging aan BKR een persbericht uitgebracht en het boetebesluit gepubliceerd.

De aanleiding voor de AP om onderzoek te doen en uiteindelijk een boetetraject te starten is gelegen in enkele klachten die de AP na 25 mei 2018 ontving over de wijze waarop BKR invulling gaf aan het recht op inzage. Volgens betrokkenen zou BKR drempels opwerpen voor het uitoefenen van het recht op inzage, dat is vastgelegd in artikel 15, eerste lid AVG.

Dit artikel bepaalt dat de betrokkene het recht heeft om van de verwerkingsverantwoordelijke inzage te verkrijgen in de hem betreffende persoonsgegevens die door de verwerkingsverantwoordelijke worden verwerkt. Een verwerkingsverantwoordelijke dient dit recht te faciliteren (artikel 12, tweede lid AVG) en de verstrekking van de desbetreffende informatie dient in beginsel kosteloos te geschieden (artikel 12, vijfde lid AVG).

Naar aanleiding van de klachten heeft de AP onderzoek gedaan en vastgesteld dat BKR artikel 12, vijfde lid AVG en artikel 12, tweede lid AVG heeft overtreden vanaf 25 mei 2018 tot en met 12 maart 2019. Daartoe heeft de AP overwogen dat BKR een financiële vergoeding vroeg aan betrokkenen die digitaal hun persoonsgegevens wilden inzien, terwijl dit niet mocht. Bovendien konden betrokkenen slechts één keer per jaar kosteloos per post inzage krijgen in hun persoonsgegevens bij BKR, terwijl dit eenvoudig en met redelijke tussenpozen mogelijk moet zijn. BKR had dit moeten faciliteren.

BKR heeft na het onderzoek van de AP de werkwijze aangepast. Sinds april 2019 kunnen mensen gratis hun gegevens bij BKR digitaal inzien. Ook heeft BKR vanaf maart 2019 het aantal keren dat mensen per post hun persoonsgegevens kunnen inzien, aangepast.[175]

BKR heeft bezwaar gemaakt tegen het boetebesluit en heeft vervolgens tegen het besluit op bezwaar beroep ingesteld bij de bestuursrechter. Deze beroepsprocedure liep nog ten tijde van het schrijven van het rapport. De AP heeft het besluit op bezwaar niet gepubliceerd, zodat voor de onderzoekers niet kenbaar is welke overwegingen aan dat besluit ten grondslag hebben gelegen.

Procesverloop van het toezichts- en handhavingstraject
De AP is op 6 juli 2018 een onderzoek gestart naar de naleving van de artikelen 12 en 15 AVG door BKR. Hierbij hebben toezichthouders van de AP in de periode van 6 juli 2018 tot en met 13 november 2018 op meerdere momenten de website van BKR bezocht en daar screenshots gemaakt en bestanden gedownload. De AP heeft ten slotte drie schriftelijke informatieverzoeken gestuurd waarop BKR naar eigen zeggen telkens op tijd en volledig heeft gereageerd.

Naar aanleiding van het artikel op NOS.nl ‘Juristen: BKR handelt in strijd met de privacywet’ en de verwijzing naar dit artikel op NU.nl twittert de AP op 12 december 2018 het bericht: ‘Wij hebben diverse klachten over BKR en recht op inzage in behandeling. Privacywet #AVG heeft duidelijke regels rond het recht op inzage en de vergoeding daarvoor. Meer weten over het recht op inzage? Zie autoriteitpersoonsgegevens.nl/nl/zelf-doen/p… … @BKR_TIEL’. In deze periode ligt er, zo stelt BKR, bij de voorzitter van de AP een schriftelijk

[175] Boete BKR.

verzoek van de voorzitter van BKR om in overleg te gaan. Op dit verzoekt ontvangt BKR geen reactie, aldus de voorzitter van BKR.[176]

De AP zendt BKR op 25 februari 2019 een conceptrapport. BKR geeft hierop op 12 maart 2019 per brief haar zienswijze. In haar zienswijze deelt BKR mede dat zij vanaf 29 april 2019 de elektronische inzage kosteloos aanbiedt. Hetgeen ook is gebeurd. Op 13 maart 2019 had BKR haar communicatie over het aantal maal dat inzage mocht worden gevraagd al aangepast.

Met inachtneming van deze zienswijze stelt de AP het definitieve rapport vast. Dit rapport is bij brief van 17 april 2019 aan BKR toegezonden. In dit rapport stelt de AP vast dat BKR artikel 12, tweede en vijfde lid AVG heeft overtreden vanaf 25 mei 2018 tot en met 12 maart 2019. Daartoe heeft de AP overwogen dat BKR een financiële vergoeding vroeg aan betrokkenen die digitaal hun persoonsgegevens wilden inzien, terwijl dit niet mocht. Bovendien konden betrokkenen slechts één keer per jaar kosteloos per post inzage te krijgen in hun persoonsgegevens bij BKR, terwijl dit eenvoudig en met redelijke tussenpozen mogelijk moet zijn. BKR had dit moeten faciliteren volgens de AP.

Bij brief van 15 mei 2019 zendt de AP aan BKR een voornemen tot handhaving. Daartoe tevens door de AP in de gelegenheid gesteld, heeft BKR bij brief van 4 juni 2019 schriftelijk haar zienswijze gegeven over dit voornemen en het daaraan ten grondslag gelegde definitieve rapport. Op 4 juni 2019 is BKR in de gelegenheid gesteld mondeling haar zienswijze toe te lichten.

Nadien heeft BKR desgevraagd nog nadere informatie toegezonden. Op 30 juli 2019 neemt de AP het besluit tot oplegging van een boete aan BKR van € 830.000. BKR ageert tegen openbaarmaking van het boetebesluit. Een verzoek om voorlopige voorziening gericht tegen het openbaarmakingsbesluit wordt door de voorzieningenrechter afgewezen.[177] Op 6 juli 2020 wordt de boete met een bijpassend persbericht gepubliceerd.

Analyse
Behoudens de informatieverzoeken ten behoeve van het onderzoek lijkt het erop dat de AP een overleg op bestuurlijk niveau afhoudt. Op een schriftelijk verzoek van de voorzitter van BKR aan de voorzitter van de AP wordt volgens BKR niet gereageerd. De houding van de AP past in de door de AP gehanteerde praktijk dat de AP in haar eigen woorden niet onderhandelt met verwerkingsverantwoordelijken voorafgaand of hangende een onderzoek- en/of handhavingstraject. De AP wijst er in dat kader op dat verwerkingsverantwoordelijken in contact willen treden met de toezichthouder vanuit de wens om door middel van onderhandeling met de AP een voor die verwerkingsverantwoordelijke gewenste uitkomst te realiseren. Wel wijst de AP verwerkingsverantwoordelijken op hun rechten in het kader van het onderzoeks- en handhavingstraject. Al lijkt de AP daarin niet consequent te handelen, gegeven andere sanctietrajecten (Belastingdienst en Voetbal TV) waar de AP zich toegankelijker heeft getoond ten opzichte van dergelijke verzoeken.

De keuze van de AP om het directe gesprek met de verwerkingsverantwoordelijken gedurende het onderzoeks- en handhavingstraject te mijden, afgezien van de momenten waarop een formele zienswijze gegeven kan worden, om zo niet in een voor haar ongewenste positie gebracht te worden, belemmert de toezichthouder niet om gedurende het onderzoek op Twitter te reageren op artikelen die op NOS.nl en NU.nl verschijnen over het recht op inzage bij BKR.

[176] Financieel Dagblad 2022.
[177] Vzr. Rb. Gelderland 29 juni 2020, ECLI:NL:RBGEL:2020:3159.

Ook op structurele basis vindt geen overleg meer plaats tussen BKR, als verwerkingsverantwoordelijke van grote hoeveelheden gevoelige data en als sleutelfiguur binnen het stelsel van kredietregistratie, en de AP. Dat is anders dan in het verleden toen wel dergelijk contact werd onderhouden tussen BKR en het CBP en diens voorganger de Registratiekamer.

Tijdens het onderzoek gaat BKR aan de slag met de manier waarop inzage wordt verschaft, zowel op papier als via elektronische weg. Dit ondanks de omstandigheid dat BKR zich niet kan vinden in de door de AP gestelde overtreding. BKR treft vooruitlopend op de onderzoeksresultaten in overleg met haar deelnemers maatregelen om binnen een tijdspad van twee maanden het systeem van elektronische inzage per 29 april 2019 kosteloos aan te bieden. Per 13 maart 2019 had BKR haar communicatie op de website aangepast om het beeld dat slechts eenmaal per inzage kon worden verkregen, weg te nemen. Aan deze inzet van de zijde van BKR wordt door de AP geen gewicht toegekend. De AP overweegt in het boetebesluit dat de medewerking van BKR niet verder is gegaan dan haar wettelijke plicht om te voldoen aan artikel 32, eerste lid AVG en uiteindelijk op 13 maart 2019 en 29 april 2019 aan artikel 12, tweede lid en artikel 12, vijfde lid AVG. BKR heeft daarmee niet op bijzondere wijze samengewerkt met de AP. BKR heeft bovendien na de aankondiging van het onderzoek door de AP op 5 september 2018 de overtredingen niet op korte termijn beëindigd, aldus de AP. De vraag is hoe dit zich verhoudt tot de uitspraak van de rechtbank Den Haag van 31 maart 2021 over de casus HagaZiekenhuis,[178] waarbij de rechtbank in artikel 7, aanhef en onder d Boetebeleidsregels 2019 reden lijkt te zien om aan het treffen van maatregelen ook nadat het onderzoek- en handhavingstraject is gestart gewicht toe te kennen bij het bepalen van de hoogte van het boetebedrag. Ook los van deze juridische insteek, kan gesteld worden dat door in het kader van het bepalen van de boetehoogte in de praktijk ook rekening te houden met de getroffen maatregelen – ook al gebeurt dit pas nadat de toezichthouder haar toezichts- en handhavingsbevoegdheden inzet – de toezichthouder de overtreder beweegt om gedurende het traject maatregelen te treffen die de overtreding beogen teniet te doen. Daarmee heeft de boete als punitief instrument een corrigerende werking en wordt voorkomen dat maatregelen pas getroffen worden wanneer over de boete is geprocedeerd dan wel in het geheel geen maatregelen worden getroffen, hetgeen niet in het voordeel van betrokkenen is.

Het boete-instrument heeft in de eerste plaats het doel om te straffen voor iets dat in het verleden heeft plaatsgevonden. Daarbij is het niet van belang of de overtreding voortduurt dan wel reeds teniet is gedaan. Vanuit dat perspectief is de boete effectief geweest. Ten tweede zou een boete een preventieve werking moeten hebben. Of daarvan in deze casus sprake is geweest is de vraag. De boete aan BKR was op dat moment de hoogst opgelegde boete door de AP. Gelet op de publiciteit die deze boete heeft genereerd, kan worden aangenomen dat het recht op inzage aandacht heeft gekregen bij organisaties. Onduidelijk is evenwel of de AP in navolging van deze boete actief met sectoren, bijvoorbeeld de financiële sector, in gesprek is gegaan over het recht op inzage en de voorwaarden waaraan dit dient te voldoen of dat andere toezichts- en handhavingstrajecten zijn gestart ten aanzien van organisaties die mogelijkerwijs in strijd handelen met artikel 15 AVG. De AP heeft in de ‘Beleidsregels openbaarmaking door de Autoriteit Persoonsgegevens’ vastgelegd dat het uitgangspunt is dat handhavingsbesluiten (waaronder boetebesluiten) openbaar worden gemaakt[179], maar de AP heeft geen beleid gepubliceerd waaruit volgt hoe opvolging wordt gegeven aan een boete om zo het effect van de preventieve werking van die boete te maximaliseren.

[178] ECLI:NL:RBDHA:2021:3090.
[179] *Stcrt*. 2016, 1380.

5.3 Kenbaarheid toezichts- en handhavingsbeleid

De reconstructie van de casus laat zien dat het lastig is duidelijke regelmatigheden te onderkennen in het toezichtsproces. Verwacht zou worden dat er normaliter sprake is van escalatie van het optreden van de toezichthouder, dat begint met een informeel contact en dat via verschillende stappen opbouwt naar formeel contact en een escalatie naar een handhavingsbesluit. Die escalatieladder ziet er in de onderzochte gevallen telkens anders uit. Dat kan te maken hebben met de verschillende ernst van de door de toezichthouder gepercipieerd nalevingsproblemen in de casus. Maar dat neemt niet weg dat het ook met inachtneming daarvan voor de hand had gelegen regelmatigheden in het toezichtsproces te ontdekken. We zien nu ook verschillen die moeilijk verklaarbaar zijn. Zo leidt een datalek bij Transavia tot de oplegging van een bestuurlijke boete, maar na het datalek bij GGD GHOR waarschuwt de toezichthouder dat verbeteracties moeten worden getroffen.

Dat het toezichtsproces een zeker onvoorspelbaar verloop kent in de casus zien we ook gereflecteerd in de reacties van de onder toezicht gestelden. Uiteraard, zou men zeggen, is een organisatie die wordt beboet voor een bepaalde gedraging niet gelukkig met die boete. Dat is niet uniek voor handhaving van het gegevensbeschermingsrecht, maar geldt ook voor andere toezichtsterreinen. Dat neemt niet weg dat wij op andere terreinen in sterkere mate overtreders zien waarbij een handhavingstraject een bijdrage levert aan de volwassenwording van het gedrag in een sector. Soms is er een verschil van inzicht over normuitleg, maar begrijpt men elkaars standpunten en lukt het daarover op een zakelijke wijze te communiceren. Uit veel onderzoek op dat terrein blijkt dat partijen het weliswaar over de inhoud oneens kunnen zijn, maar dat het niettemin toch mogelijk is daarover op een zodanige wijze te communiceren dat de uitkomst uiteindelijk toch geaccepteerd wordt.[180]

Op het terrein van het gegevensbeschermingsrecht valt evenwel op dat sprake is van veel onduidelijkheid over de normen en veel onbegrip, ergernis en frustratie en soms zelfs boosheid over het optreden van de toezichthouder. Dit kan erop duiden dat de toezichthouder er niet in slaagt om op te treden volgens de regels van *procedural justice*, die er op neerkomen dat contact wordt gelegd met de onder toezicht gestelde, die in de gelegenheid wordt gesteld te reageren en die het gevoel heeft dat er ook wordt geluisterd. De vaste bestuurspraktijk is er een waarbij de AP dergelijk overleg uit de weg gaat. De toezichthouder motiveert dat met het principe dat de toezichthouder niet onderhandelt. De vraag is of dat past bij de beweegredenen van de onder toezicht gestelden die vooral op zoek lijken te zijn naar uitleg en duiding.

De casus laten zien dat normuitleg op het terrein van het gegevensbeschermingsrecht en de communicatie daarover gebrekkig verlopen. Dat leidt ertoe dat organisaties soms in het ongewisse verkeren over de manier waarop de normen op hun terrein moeten worden toegepast. Veelal zouden organisaties geholpen zijn met een advies van de toezichthouder en zouden contacten, ook in handhavingszaken, tot veel verheldering kunnen leiden. Daar waar die contacten ontbreken (zoals in de BKR-casus en ook in de GGD GHOR-casus) constateren we dat toezichthouder en onder toezicht gestelde in een verscherpte verhouding tegenover elkaar komen te staan. En in een andere casus (zoals VoetbalTV) waren er wel contacten, maar verliepen die zeer moeizaam.

[180] K. van den Bos & L. van der Velden, Legitimiteit van de overheid, aanvaarding van overheidsbesluiten en ervaren procedurele rechtvaardigheid. *Prettig Contact met de Overheid 4*. Den Haag: 2013.

Het boete-instrument is een punitief handhavingsinstrument. Dit lijkt op het terrein van de gegevensbescherming de afgelopen jaren het belangrijkste interventie te zijn geworden. Naast de bestuurlijke boete hanteert de AP ook de last onder dwangsom en de berisping, maar in aantallen komen die maatregelen wat minder vaak voor en dat geldt zeker voor het verwerkingsverbod.[181] Waar het oogmerk van een toezichthouder gericht is op het bevorderen van normnaleving is het in stelling brengen van die andere interventies, zoals de last onder dwangsom, eigenlijk een zeer voor de hand liggende actie. In het handhavingsbeleid van de AP ontbreekt duidelijk zicht op deze instrumentenmix en de onderbouwing van de keuze die de afgelopen jaren wat vaker lijkt te wordt gemaakt voor de bestuurlijke boete. Dit punt sluit ook aan bij een aanbeveling uit de evaluatie van de AVG door de Europese Commissie uit 2020, waarin wordt gepleit voor het gebruik van het hele arsenaal aan handhavingsinstrumenten.[182] Het lijkt verstandig dat hiertoe beleid wordt ontwikkeld, zogenoemd toezichtbeleid, dat in beleidsregels wordt opgenomen en dat op die manier kenbaar is voor onder toezicht gestelden. Het zou denkbaar zijn dat in de UAVG wordt voorgeschreven dat de toezichthouder beleidsregels bekendmaakt, waarbij in een voorafgaande consultatieprocedure van belanghebbenden voorzien zou kunnen worden.

5.4 De werking van de meldplicht datalekken en de boetebevoegdheid

5.4.1 Meldplicht datalekken

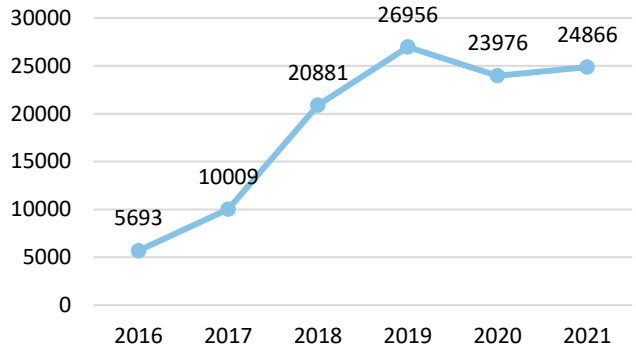
Op grond van artikel 33 AVG meldt een verwerkingsverantwoordelijke een inbreuk in verband met persoonsgegevens, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Op grond van artikel 34 AVG moet de verwerkingsverantwoordelijke in sommige gevallen de inbreuk meedelen aan de persoon op wie de inbreuk betrekking heeft. De mededelingsplicht geldt niet voor financiële ondernemingen op grond van artikel 42 UAVG.

Hierna worden de statistieken uit jaarverslagen van de AP omtrent de melding van datalekken behandeld. Vooraf dient hierbij de kanttekening te worden gemaakt dat deze cijfers over de jaren heen moeten worden bezien in het licht van ontwikkelingen die impact hebben op het absolute aantal datalekken, zoals voortgaande digitalisering en meer cybercrime. Daarnaast is er ook meer bewustwording van datalekken en de geldende meldplicht, waardoor vermoedelijk relatief gezien ook meer wordt gemeld.

Het aantal datalekken dat werd gemeld nam in de periode tussen 2016 en 2019 toe (zie figuur 5.1). Met name in het tweede kwartaal van 2018 was er een sterke stijging van het aantal gemelde datalekken. De AP geeft hier als mogelijke verklaring voor dat met de invoering van de AVG op 25 mei 2018, de (media)aandacht voor de AVG gestegen is.[183] Een lichte daling van het aantal datalekken deed zich voor in 2020. De AP ontving 23.976 datalekmeldingen. Deze daling had een direct verband met de aanpassing van de werkwijze van incassobureaus, waardoor er veel minder betalingsherinneringen bij verkeerde ontvangers terechtkwamen. In 2021 nam het aantal datalekken met 4% toe ten opzichte van 2020.

[181] Volgens het jaarverslag 2020 van de AP is er in dat jaar 7 keer een bestuurlijke boete opgelegd, 2 keer een last onder dwangsom en 4 keer een berisping. In 2019 ging het om 4 boetes, 2 lasten onder dwangsom en 3 berispingen.
[182] European Commission 2020, p. 15.
[183] Facts & figures meldplicht Datalekken, overzicht feiten en cijfers 2018.

FIGUUR 5.1.: AANTAL GEMELDE DATALEKKEN 2016 – 2021



In 2016 werden 5.693 datalekken gemeld, waarbij de meeste datalekken afkomstig waren uit de sectoren gezondheid en welzijn (28,9%), financiële dienstverlening (17,1%) en openbaar bestuur ((15,1%).[184] In 2017 ontving de AP, zoals het CBP zich vanaf 1 januari 2016 mocht noemen, 10.009 meldingen van datalekken, waarbij de meeste datalekken werden gemeld vanuit de sectoren gezondheid en welzijn (30%), financiële dienstverlening (19%) en openbaar bestuur (19%).[185] De AP ontving in 2018 20.881 datalekken. Hetgeen iets meer dan een verdubbeling was ten opzichte van het voorafgaande jaar. De meeste datalekken werden (wederom) gemeld door organisaties uit de sectoren zorg en welzijn (29%), financiële dienstverlening (26%) en openbaar bestuur (17%).[186]

Het meest voorkomende type datalek in de periode 2016 tot en met 2018 was volgens de jaarverslagen dat persoonsgegevens aan de verkeerde ontvanger waren verstuurd of afgegeven. Daarna werd er het meest gemeld over kwijtgeraakte of gestolen apparaten of papieren met daarop persoonsgegevens, maar ook over hacking, malware en phishing. De meest gelekte gegevens waren NAW-gegevens (naam, adres, postcode en woonplaats), geslacht, geboortedatum en leeftijd en het burgerservicenummer (BSN). Het aantal mensen dat werd geraakt door een datalek varieerde per melding van één enkele persoon tot – in enkele gevallen – honderdduizenden betrokkenen.

De AP nam vanaf 2016 op verschillende manieren actie naar aanleiding van gemelde (en niet-gemelde) datalekken. In veel gevallen gaf de AP uitleg aan organisaties over te nemen beveiligingsmaatregelen, vroeg de AP om aanvullende informatie over het datalek en werden brieven met normuitleg gestuurd en normoverdragende gesprekken met organisaties gevoerd. Daarnaast werd anderszins actie ondernomen richting organisaties die een datalek meldden. Over het algemeen leidden deze acties tot een waarschuwing en beëindiging van de overtreding. Daaronder vielen ook interventies naar aanleiding van mogelijke datalekken bij organisaties die dit niet hebben gemeld bij de AP, aldus de jaarverslagen. Eind 2018 werd de eerste bestuurlijke boete opgelegd aan Uber naar aanleiding van een te laat gemeld datalek (zie paragraaf 5.2.1).

In 2019 ontving de AP 26.956 datalekmeldingen, waarbij meer meldingen (25%) naar aanleiding van hacking, phishing of malware-incidenten ten opzichte van 2018. Vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, lijken hier doelwit van. De meeste

[184] Autoriteit Persoonsgegevens 2017.
[185] Autoriteit Persoonsgegevens 2018.
[186] Autoriteit Persoonsgegevens 2019.

meldingen kwamen uit de sector financiële dienstverlening (30%), gevolgd door de zorgsector (28%) en de sector openbaar bestuur (17%).[69]

Hoewel het totaal aantal meldingen van datalekken in 2020 ten opzichte van 2019 afnam, nam het aantal meldingen naar aanleiding van hacking, malware of phishing-incidenten met 30% toe. De meeste datalekken werden ook in 2020 gemeld vanuit de zorgsector (30%), de financiële sector (22%) en de sector openbaar bestuur (22%). In dat jaar had de AP in het bijzonder aandacht voor te laat gemelde datalekken. De AP heeft verschillende organisaties aangesproken op hun gedrag. Zij hebben vervolgens de AP beloofd concrete maatregelen te nemen om datalekken voortaan wél op tijd te melden.[70] Ook in 2021 nam het aantal datalekken door hacking, malware of phishing opnieuw toe.[187]

De AP deelt in het jaarverslag haar zorg dat er nauwelijks capaciteit is om ernstige datalekken te onderzoeken en dat ook meer in het algemeen veel meldingen van datalekken niet opgepakt kunnen worden.[188]

Hoewel de laatste jaren steeds meer datalekken worden gemeld, betreft dit nog steeds een klein deel van het totaal aantal datalekken. De AP merkt dit zelf als betrokkenen een klacht of tip indienen over een datalek dat niet door de verwerkingsverantwoordelijke is gemeld.[189] Dit kwam onder andere in 2021 naar voren toen het Nationaal Cyber Security Centrum (NCSC) meldde dat er op ten minste 1200 Nederlandse servers waarop Microsoft Exchange stond, was ingebroken. Bij de AP zijn in de weken erna echter slechts 75 meldingen van verwerkingsverantwoordelijken binnengekomen over datalekken met betrekking tot Microsoft Exchange.[190] Dat slechts een deel van de datalekken gemeld wordt, blijkt ook uit de resultaten van de uitgezette vragenlijst onder FG's (zie paragraaf 4.5, tabel 4.17). Van alle datalekken die zich in 2019 hebben voorgedaan bij de 81 organisaties waarvan we cijfers hebben, is 27% gemeld bij de AP. In 2020 lag dit percentage nog iets lager (zie tabel 4.17). In haar reactie geeft de AP aan dat niet alle datalekken gemeld behoeven te worden; dat is uiteraard juist, maar dat laat onverlet dat vastgesteld moet worden dat veel datalekken niet worden gemeld.

Meer dan de helft van de respondenten geeft aan dat het geregeld is voorgekomen dat men geen reactie kreeg van de AP na een melding. Bijna de helft geeft daarnaast aan dat er doorgaans wel een ontvangstbevestiging is verstuurd, maar dat het daar dan bij is gebleven. Slechts een op de drie respondenten verklaart dat er doorgaans een inhoudelijke reactie komt in de vorm van doorvragen, informatieverstrekking, advies op maat of een andere actie. De AP wijst in haar reactie op de tekst op de website waarin is aangegeven dat de AP binnen twee weken contact opneemt met de verantwoordelijke als zij vragen heeft.

Het is denkbaar dat het niet meewegen van het wél en tijdig melden van een datalek bij het bepalen van de boetehoogte geen positieve impuls geeft aan verwerkingsverantwoordelijken om dit te (blijven) doen (zie ook paragraaf 5.1.3, waarin de boete aan PVV Overijssel wordt besproken en het niet melden van het datalek niet leidde tot een verhoging van de boete die de AP oplegde). Een van de geïnterviewde experts geeft aan dat verwerkingsverantwoordelijken soms twijfelen over het wel of niet melden van een datalek bij de AP. Hoewel melden meestal geen consequenties heeft, kán het wel ingrijpende gevolgen hebben om te melden. Dit terwijl de pakkans laag is in geval van niet melden. Tijdig melden leidt bovendien niet altijd

[187] Datalekkenrapportage 2021.
[188] Autoriteit Persoonsgegevens 2021.
[189] Facts & figures meldplicht Datalekken.
[190] Nieuwsbericht Autoriteit Persoonsgegevens 2021.

tot een lagere boete ingeval beveiligingsgebreken worden vastgesteld, waardoor een datalek kon ontstaan. Dit blijkt uit het boetebesluit van de AP aan Transavia.[191] De AP heeft bij de bepaling van de boetehoogte niet als verlagende factor meegewogen dat Transavia het datalek – dat als gevolg van de overtreden beveiligingsnorm kon ontstaan – tijdig heeft gemeld. Volgens de AP heeft Transavia hiermee slechts voldaan aan haar wettelijke meldplicht aan de AP en betrokkenen.

De AP geeft in haar reactie aan dat het toezicht op de meldplicht datalekken (gemelde datalekken en niet gemelde datalekken) risicogestuurd is.[192] Dat betekent dat de AP haar capaciteit zoveel mogelijk inzet op die datalekken die de grootste risico's met zich meebrengen voor de rechten en vrijheden van de betrokkenen. Daarnaast stelt de AP dat gelet op de beperkte capaciteit van de toezichthouder niet alle (serieuze) meldingsplichtige datalekken kunnen worden opgevolgd met een onderzoek en passende handhaving.

Om het melden van datalekken te vereenvoudigen heeft de AP op 1 juni 2021 het meldingsformulier voor datalekken op de website aangepast. Of de aanpassingen aan het formulier het daadwerkelijk makkelijker hebben gemaakt om een melding van een datalek in te dienen is de vraag. Ter verbetering van een aantal elementen hebben de Vereniging Privacyrecht Advocaten (VPR-A) en de Vereniging Privacyrecht (VPR) op 8 november 2021 de AP een brief gestuurd met enkele verbetervoorstellen op basis van hun ervaringen.[193] De reactie van de AP is volgens de AP in maart 2022 aan de afzenders verzonden.[194] Aanpassingen in het formulier zijn nog niet doorgevoerd.

Wanneer naar de rol van de FG bij datalekken wordt gekeken, blijkt uit de resultaten van de vragenlijst dat ongeveer 58% van de FG's denkt te worden betrokken bij alle datalekken in de organisatie. 20% van de FG's denkt bij minimaal driekwart van de datalekken betrokken te zijn. Een op de zes FG's denkt bij minder dan de helft van de datalekken betrokken te worden. In de gevoerde interviews met FG's komt verder naar voren dat zij in de organisatie bewustzijn over datalekken proberen te creëren en eventueel werkwijzen/processen proberen aan te passen, door datalek-boetes die de AP heeft opgelegd onder de aandacht (van het bestuur of management) van de organisatie te brengen.

5.4.2 De boetebevoegdheid en de toepassing van open normen

Op grond van de UAVG[195] is de bevoegdheid om boetes van maximaal twintig miljoen euro of 4% van de wereldwijde jaaromzet op te leggen bij overtreding van de AVG toebedeeld aan de AP. Deze kunnen tevens worden opgelegd aan overheidsinstanties of -organen[196].

Zoals beschreven in paragraaf 2.6.2 wordt het opleggen van een administratieve geldboete gezien als een belangrijk instrument dat in passende omstandigheden gebruikt moet worden. Een weloverwogen en evenwichtige aanpak wordt aanbevolen om een doeltreffende, afschrikkende en evenredige reactie te bewerkstelligen. Het opleggen van een administratieve boete dient op consistente en objectief gerechtvaardigde gronden te gebeuren.[197] In dit kader

[191] Boete Transavia.
[192] Zo blijkt uit de reactie van de AP op de conceptversie van deze rapportage.
[193] Vereniging Privacyrecht 2018.
[194] Zo blijkt uit de reactie van de AP op de conceptversie van deze rapportage.
[195] Artikel 14, derde lid.
[196] Artikel 18.
[197] WP29, WP253, p. 6-8.

bieden nieuwe (op het moment van schrijven van dit rapport in consultatie zijnde) EDPB-Guidelines 'on the calculation of administrative fines under the GDPR'[198] aanknopingspunten.

Uit het vragenlijstonderzoek blijkt dat drie van 125 respondenten te maken hebben gehad met een boete van de AP. Dat is 6% van het totaal aantal interventies dat door de respondenten is gemeld. Adviesgesprekken, waarschuwende brieven en berispingen komen veel vaker voor. Bij een aantal verdiepende interviews met FG's is het instrument van de boete ter sprake gekomen. Een aantal respondenten gaf aan dat het risico op boetes (en de potentiële omvang ervan) helpt bij het onder de aandacht van gegevensbescherming in de organisatie. Een derde suggereerde dat de afschrikwekkende werking vergroot zou worden wanneer er vaker boetes werden opgelegd bij kleinere organisaties.

Om meer te weten te komen over het functioneren van het instrument van de bestuurlijke boete en van de meldplicht datalekken in de praktijk is een aantal casus bestudeerd. In de Uber-datalekcasus was sprake van een datalek, waarop de AP reageerde met een bestuurlijke boete. Bij GGD GHOR was eveneens sprake van een datalek waarop de AP reageerde met een aanzegging tot het treffen van maatregelen. Bij VoetbalTV en BKR ging het in de ogen van de AP om een schending van andere AVG-normen waarop met een bestuurlijke boete werd gereageerd. De vraag bij deze casus is hoe de toezichtstrategie en het handhavingsbeleid van de AP eruit zien en hoe die in de praktijk functioneren en of de boetebevoegdheid een bijdrage levert aan een doelmatige en doeltreffende uitvoering en handhaving van de AVG.

De belangrijkste bevinding is dat in de casus sprake is van een sterk uiteenlopend verloop van het toezicht en de handhaving. Dat verloop laat zich in termen van contact tussen toezichthouder en onder toezicht gestelde typeren als intensief tot en met afwezig. In sommige casus was sprake van uitvoerig contact, variërend van informeel contact in de voorfase tot en met uitgebreide formele correspondentie en uitwisseling van standpunten. In andere casus was sprake van een vrijwel ontbrekend contact, geen informeel contact en nauwelijks formele contacten, afgezien van de genomen formele besluiten. Opvallend is dat in enkele gevallen ook in de formele fase van de relatie tussen toezichthouder en onder toezicht gestelde, ondanks verzoeken daartoe door de onder toezicht gestelde geen reacties werden gegeven door de AP.

In een enkele casus paste de onder toezicht gestelde het gedrag direct aan nadat de toezichthouder de voorbereiding van een boetebesluit was gestart. Opvallend is dat daarmee geen rekening werd gehouden bij het vaststellen van de hoogte van de boete in de gevallen waarin dat speelde, waar dat wel zou kunnen. In de uitspraak van de rechtbank in de zaak van het HagaZiekenhuis oordeelt de rechtbank dat de AP bij het vaststellen van de hoogte van de boete wel degelijk rekening moet houden met de corrigerende werking die de boete heeft gehad.

De AP merkt in haar reactie op dat het vaststellen van de boetehoogte, gelet op de wegingscriteria in artikel 83 AVG en de boetebeleidsregels Autoriteit Persoonsgegevens 2019, is toegespitst op het voorliggende geval. Het betreft volgens de AP geen mathematische exercitie waarmee een vergelijking tussen van elkaar verschillende casusposities casus van weinig betekenis is. De toezichthouder lijkt hiermee te miskennen dat voorspelbaarheid van hoe in verschillende situaties met de wegingscriteria wordt omgegaan, bijdraagt aan rechtszekerheid en dat het partijen beter in de positie brengt om te bepalen en te onderbouwen in hoeverre ze het eens zijn met de boetehoogte.

[198] European Data Protection Board 2022. De consultatie van deze richtsnoeren loopt tot en met 27 juni 2022.

In verschillende casus heeft de toezichthouder de publiciteit gezocht met genomen handhavingsbesluit, tot aan het NOS-journaal en het gebruik van Twitter aan toe. Publiciteit en het openbaar maken van boetebesluiten heeft onmiskenbaar als doel in vergelijkbare gevallen de normnaleving te bevorderen. Daar staat dan weer tegenover dat in andere gevallen het boetebesluit – ook na lange tijd – niet is gepubliceerd, ook daar waar de onder toezicht gestelde daartegen op zichzelf geen bezwaar zou hebben en het uitgangspunt van het beleid wel is handhavingsbesluiten openbaar te maken.[199] De AP heeft geen beleid gepubliceerd waaruit volgt hoe opvolging wordt gegeven aan een boete om zo het effect van de preventieve werking van die boete te maximaliseren.

De wetgever heeft de toezichthouder tot op heden ook niet verplicht boetebesluiten te publiceren.[200] In tegendeel: in de nieuwe Wet open overheid (Woo) is de verplichting opgenomen voor bestuursorganen om een aantal categorieën van documenten actief openbaar te maken, maar daarvan zijn in beginsel uitgezonderd bestuurlijke bestraffende sancties en ook de meeste herstelsancties.[201] Het zou goed zijn als in de Woo een uitzonderingsbepaling wordt opgenomen vergelijkbaar met die in de Bijlage bij artikel 8.8 Woo. Hierin is een uitzondering opgenomen voor openbaarmaking van bestuurlijke sancties en bindende aanwijzingen door toezichthouder Autoriteit Consument & Markt (ACM). De Instellingswet ACM bevat namelijk juist de verplichting voor de ACM om zware boetes te publiceren en biedt voor lichtere boetes een afwegingsmogelijkheid.[202] Deze bepalingen blijven ook onder de Woo gelden. De invoering van dergelijke bepalingen voor de AP in de UAVG zou bijdragen aan het aanhouden van een consistente lijn rondom openbaarmaking van sancties en dienend zijn aan het belang dat met openmaking daarvan gemoeid is. Dit komt immers de rechtszekerheid van onder toezicht gestelden ten goede. Bovendien geven openbaar gemaakte sancties inzicht in hoe bepaalde open normen in de praktijk door de toezichthouder worden toegepast en kan (de dreiging van) openbaarmaking bijdragen aan de beoogde generale preventieve werking van boetes.

Het is goed te volgen dat onder toezicht gestelden niet altijd begrijpen dat een toezichthouder over het vermeende normafwijkende gedrag van de organisatie de publiciteit zoekt, wanneer die ondertussen niet bereid is tot communicatie over de casus. Het lijkt erop dat op deze manier kansen worden gemist op verbetering van de normnaleving. We hebben in de casus ook telkens gezocht naar communicatiebeleid van de AP, maar afgezien van optreden in de algemene media geen aanwijzingen gezien dat communicatie is gericht op normnaleving in de specifieke sector waarin de handhavingsbeslissing was genomen. De vraag is hoe de visie van de toezichthouder eruit ziet, gericht op de versterking van de naleving in een bepaalde sector of van een bepaalde norm uit de AVG, nadat een handhavingsbesluit is genomen.

Bij dit alles is het belangrijkste punt dat in veel van de gesprekken aan de orde is gesteld de onduidelijkheid over de toepassing van de open normen uit de AVG in het voorliggende geval. Er is grote behoefte aan normuitleg en verduidelijking, maar veel gesprekspartners constateren dat de AP niet bereid is met hen daarover het gesprek aan te gaan. Ook niet op een moment dat toezicht en handhavend optreden nog helemaal niet aan de orde zijn. Mogelijk spelen daarbij de telkenmale door de AP genoemde capaciteitsproblemen een belangrijke rol.

[199] *Stcrt*. 2016, 1380.
[200] In tegenstelling tot bijvoorbeeld de Autoriteit Consument en Markt (ACM).
[201] Artikel 3.3, tweede lid, sub k, onder 5 en 6 Woo. Overigens geldt de Woo sinds 1 mei jl. maar is gefaseerde inwerkingtreding van toepassing op artikel 3.3, eerste en tweede lid Woo. De verplichting tot actieve openbaarmaking gaat gelden op een bij koninklijk besluit te bepalen tijdstip
[202] Op basis van artikel 12 u Instellingswet ACM is de ACM verplicht zware boetes te publiceren. Artikel 12 Instellingswet ACM biedt de ACM de mogelijkheid om onder omstandigheden ook minder zware boetes te publiceren.

Hoe dan ook, het is van groot belang dit punt te constateren, want zonder verduidelijking van de open normen uit de AVG lukt het de AP niet in de rol van systeemtoezichthouder terecht te komen. De nog te behandelen casus van de Gedragscode Gezondheidsonderzoek (paragraaf 6.3.1) laat overigens zien hoe lastig het is normuitleg binnen een sector tot ontwikkeling te laten komen.

Tot slot valt in de casus op dat de binnen de organisatie werkzame FG's zich overvallen voelden door het optreden van de AP. De interne toezichthouder is eigenlijk geen speler in een handhavingscasus. De vraag is of dat niet anders zou kunnen en wellicht zou moeten. Wanneer de FG de vooruitgeschoven post zou zijn van de AP past daarbij ook een speciale relatie met de externe toezichthouder. Van die bijzondere verhouding zoals hiervoor bedoeld, is ons in het onderzoek niet gebleken. Dit draagt niet bij aan de totstandkoming van een interne toezichtsprofessie en een gemeenschapsgevoel onder FG's.

6 Het functioneren van de UAVG

6.1 Inleiding

In dit hoofdstuk staat het functioneren van de UAVG centraal. Daarbij maken we gebruik van de informatie uit de gevoerde gesprekken en uit het vragenlijstonderzoek, waarbij we ook de jurisprudentieanalyse betrekken. Daarmee geven we antwoord op de deelvragen 1, 2, 4, 5 en 6 die de duidelijkheid, toegankelijkheid, uitvoerbaarheid en handhaafbaarheid van de normen van de UAVG betreffen. Ook de naleving van de bepalingen van de UAVG en de mate waarin in de UAVG de ruimte is benut die de AVG biedt voor de nationale wetgever komt in dit hoofdstuk aan de orde (vragen 6 en 17).

In paragraaf 6.2 gaan we in op de duidelijkheid van de normen uit de UAVG, waarbij in het bijzonder biometrische en strafrechtelijke gegevens aan de orde worden gesteld. Daarna volgt in paragraaf 6.3 een intermezzo: een bespreking van de totstandkoming van de Gedragscode gezondheidszorg. In 6.4 komt de uitvoerbaarheid van de normen van de UAVG aan de orde, waarbij we aandacht besteden aan wetenschappelijk onderzoek en medisch wetenschappelijk onderzoek. Paragrafen 6.5 en 6.6 betreffen belangrijke en specifieke onderwerpen: geautomatiseerde besluitvorming (geregeld in artikel 40 UAVG) en de positie van kinderen in het gegevensbeschermingsrecht (niet geregeld in de UAVG, behalve de grens van 16 jaar in artikel 5 UAVG). Tot slot gaat paragraaf 6.7 kort in op de handhaafbaarheid van de normen van de UAVG.

6.2 Het stelsel van de AVG en UAVG en de duidelijkheid van normen

6.2.1 Algemeen

De AVG is, zoals hiervoor reeds aangehaald, net als de Wbp te kenmerken als omnibuswetgeving. Door de brede toepasselijkheid van deze regelgeving is in de AVG en in de UAVG gebruik gemaakt van open begripsbepalingen en normen, waarbij de invulling van open begripsbepalingen in het concrete geval bepaalt welke verplichtingen gelden. Het gaat hierbij om sleutelbegrippen, zoals persoonsgegevens, verwerking, pseudonimisering, verwerkingsverantwoordelijke, verwerker en hoofdvestiging, maar ook over de invulling van de voorwaarde om bijvoorbeeld biometrische gegevens te mogen verwerken. Tevens dient in veel gevallen de concrete invulling van de beginselen, zoals doelbinding en verenigbaarheid, gegevensminimalisatie, juistheid, opslagbeperking, integriteit en geautomatiseerde besluitvorming door de ver-

werkingsverantwoordelijke zelf te worden gegeven. Het hanteren van open normen maakt het mogelijk om flexibel te kunnen inspelen op de ontwikkelingen die zich voordoen.

Het nadeel van het stelsel van open normen is dat het ingewikkeld is voor verwerkingsverantwoordelijken om aan het gegevensbeschermingsrecht toepassing te geven. Zij worstelen met de vraag of ze verwerkingsverantwoordelijke of verwerker zijn en daarmee of zij doel en middelen van de verwerking bepalen. Andere vragen die spelen zijn of een bepaald gegeven een persoonsgegeven is, de juiste grondslag gebruikt wordt, het verwerkingsverbod om bijzondere persoonsgegevens te verwerken doorbroken mag worden en of de verwerking van persoonsgegevens juist en actueel is en verenigbaar is met het oorspronkelijke doel.

De verwerkingsverantwoordelijke zal zelf in het concrete geval telkens weer invulling moeten geven aan de open normen en een weg moeten vinden in het stelsel van de AVG en UAVG en daar verantwoording over moeten afleggen op grond van artikel 5, tweede lid AVG. Het zal voor de verwerkingsverantwoordelijke vooraf niet altijd duidelijk zijn of de gemaakte keuze en afweging juist is, waardoor het risico bestaat dat niet in overeenstemming met de AVG en/of de UAVG wordt gehandeld. Deze situatie doet zich niet alleen voor bij organisaties die risicovolle en grootschalige verwerkingen van persoonsgegevens verrichten, maar ook organisaties die verwerkingen verrichten met een laag risico hebben hier, zij het in mindere mate, mee te maken.

Ook kan onduidelijkheid bestaan tussen het stelsel van de AVG en de UAVG en sectorale regelgeving. Zo ervaren bijvoorbeeld banken die onduidelijkheid bij de vraag of de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) in voldoende mate een grondslag biedt om bijzondere persoonsgegevens te kunnen verwerken. Een voorbeeld betreft het klantonderzoek dat moet worden gedaan, waarbij banken te kennen geven aan te lopen tegen beperkingen die er zijn op het gebied van de verwerking van bijzondere persoonsgegevens. Sommige gegevens zijn risico-indicatoren, die neigen naar bijzondere persoonsgegevens (bijvoorbeeld als het gaat om het tegengaan van terrorisme financiering). Ook met het oog op het steeds digitaler (moeten) worden van banken, transactiemonitoring en de Wwft zijn banken eigenlijk verplicht om vernieuwde technieken in te zetten. De vraag daarbij is hoe discriminatie kan worden tegengegaan en of wordt voldaan aan artikel 9, tweede lid, onder g AVG. De Wwft blijft een algemene regeling, aldus de banken.

Het zou, zo wordt in de interviews aangegeven, de bankensector helpen als in de Wet op het financieel toezicht (Wft) en de Wwft of de UAVG meer verduidelijkt wordt dat banken bijvoorbeeld bijzondere persoonsgegevens mogen gebruiken ter voorkoming van discriminatie. Hieruit spreekt de wens voor meer eenduidigheid in wat er in de UAVG en wat in sectorale wetgeving aan uitzonderingen wordt opgenomen.

Om tot naleving van deze open normen te kunnen komen, hanteert de AVG net als de Wbp een mix van overheidsregulering en zelfregulering, waarbij zekerheid over de toepassing van het stelsel en de gewisheid van de uitkomst van de toepassing van de begripsbepalingen en normen niet alleen afhankelijk is van de taakuitoefening door de toezichthouder, maar waarbij ook sectoren en organisaties zelf aan zet zijn. De AVG voorziet in het gebruik van gedragscodes, de gegevensbeschermingseffectbeoordeling, de voorafgaande raadpleging, certificering en het intern toezicht door Functionarissen voor Gegevensbescherming. Bovendien kent de AVG een structuur om een gelijk speelveld voor verwerkingsverantwoordelijken te garanderen en een coherentiemechanisme om tot harmonisatie van normuitleg tussen de toezichthouders op de AVG te komen.

Deze mix zou, indien in evenwicht, tot voldoende rechtszekerheid bij verwerkingsverantwoordelijken moeten leiden om ten volle binnen de kaders van de AVG en de UAVG tot het verwerken van persoonsgegevens te kunnen overgaan. Hetgeen de bescherming van de betrokkenen eveneens ten goede komt. Toch blijkt dat evenwicht nog onvoldoende aanwezig.

Een belangrijk instrument om te komen tot zelfregulering is de nationale en Europese gedragscode. De gedragscode geeft een sectorspecifieke invulling van het normenkader van de AVG en, waar nodig, de UAVG. De gedragscode vormt een praktische en zinvolle manier om een grotere mate van consistentie te bereiken in de wijze waarop het gegevensbeschermingsrecht wordt toegepast en zou kunnen fungeren als mechanisme om naleving van de AVG en de UAVG aan te tonen. De Europese gedragscode in het bijzonder kan bijdragen aan het wegnemen van de eventuele verschillen tussen de lidstaten in de manier waarop zij gegevensbeschermingsrecht toepassen. Een gedragscode wordt goedgekeurd door de toezichthouder, zodat verwerkingsverantwoordelijken de zekerheid hebben dat als zij in overeenstemming met de gedragscode handelen ook voldaan wordt aan het geldende normenkader. De goedkeuring van een gedragscode is een besluit in de zin van artikel 1:3, eerste lid Awb, waartegen rechtsmiddelen kunnen worden aangewend.

De AP keurt een gedragscode goed wanneer de in de gedragscode opgenomen regels, gelet op de specifieke kenmerken van de sector(en), waarin deze organisatie werkzaam is, een juiste uitwerking vormen van de (U)AVG en bijdragen aan een juiste toepassing van de (U)AVG. De AP wijst erop dat veel van de aanvragen voor goedkeuring van een gedragsode die bij de AP worden ingediend van onvoldoende kwaliteit zijn. Er zijn volgens de AP drie oorzaken te noemen die problematisch zijn gebleken:[203]

1. Organisaties dienen aanvragen in voor goedkeuring van gedragscodes ten behoeve van verwerkingen die niet rechtmatig zijn. Bijvoorbeeld omdat een gedragscode wordt opgesteld voor een verwerking van bijzondere persoonsgegevens zonder een geldige uitzondering op het verbod daarvan te hebben.
2. Organisaties dienen aanvragen in voor een goedkeuring van een gedragscode, waarbij in onvoldoende mate de (U)AVG verder is uitgewerkt voor de desbetreffende branche. Bijvoorbeeld door alleen letterlijk artikelen uit de AVG over te nemen.
3. Organisaties onderschatten de eisen die gelden voor het toezichthoudende orgaan of ze hebben zich vooraf onvoldoende gerealiseerd wat de kosten zullen zijn voor het oprichten en in stand houden van een toezichthoudend orgaan.

In de procedure rondom een aanvraag om goedkeuring van een gedragscode investeert de AP, zo stelt de toezichthouder, veel tijd in het informeren van de indiener van de aanvraag. Zo kiest ervoor om de aanvrager additionele gesprekken aan te bieden om de door de hem ingediende aanvraag te bespreken. Vervolgens kan de aanvrager de opmerkingen van de AP verwerken. Indien daar meerdere ronden voor nodig zijn, omdat de aanvrager niet in één ronde de aanvraag weet aan te passen tot een voldoende niveau, kan dat geruime tijd in beslag nemen. Het alternatief zou volgens de AP zijn dat de toezichthouder de aanvragen voor goedkeuring van een gedragscode die niet voldoen aanstonds zou afwijzen.

In de praktijk wordt, zo blijkt uit de interviews, het opstellen van een gedragscode en het proces van afstemming met en het verkrijgen van goedkeuring van de toezichthouder door organisaties ervaren als een tijdrovend, langdurig en kostbaar proces met uiteindelijk weinig

[203] Zo blijkt uit de reactie van de AP op de conceptversie van deze rapportage.

concrete voordelen voor sectoren en daarmee de verwerkingsverantwoordelijken. Het animo binnen sectoren om een gedragscode ter goedkeuring aan de AP voor te leggen lijkt laag te zijn. De casestudy over de gedragscode gezondheidsonderzoek, die we hierna in paragraaf 6.3 presenteren, bevestigt dit beeld. De casestudy laat zien dat het komen tot een goedgekeurde gedragscode veel energie kost en dat een gedragscode de eindstreep van de goedkeuring haalt niet een gegeven is. Daarbij speelt een rol dat het voor de betrokken sectoren niet of nauwelijks duidelijk is wat het normenkader is waaraan de toezichthouder de gedragscode toetst als die ter goedkeuring wordt voorgelegd en de reactie van de AP op een concept-gedragscode onvoldoende houvast biedt om tot een aanpassing van het concept te komen. De AP zelf stelt in haar reactie vast dat door de toezichthouder en de EDPB veel tijd is geïnvesteerd in het opstellen en publiceren van guidance ten aanzien van gedragscodes en toezichthoudende organen. Zo zijn begin 2021 de accreditatievereisten die de AP stelt aan toezichthoudende organen gepubliceerd.

Door de kwaliteitseisen die aan de gedragscode worden gesteld, hebben brancheorganisaties zelf richtsnoeren ontwikkeld, soms als eerste stap naar een formele gedragscode. Daarmee worden knelpunten binnen een branche gezamenlijk opgelost en worden praktische handvatten geboden. De AP ziet deze richtsnoeren als een effectieve bijdrage aan de doorwerking van (U)AVG-normen in de sectoren. Dit komt de naleving van de (U)AVG ten goede en zorgt voor duidelijkheid binnen een sector.

Onder de Wbp in de periode tussen 2012 en 2018 ging het om gemiddeld minder dan twee gedragscodes per jaar, waarbij in de jaren 2017 en 2018 geen enkele gedragscode ter goedkeuring aan de toezichthouder is voorgelegd.[204] In 2019 is één ontwerpbesluit tot goedkeuring van een gedragscode gepubliceerd.[205] In 2020 is deze gedragscode met een definitief besluit goedgekeurd.[206] Een en ander duidt erop dat de gedragscode niet (meer) een effectief instrument is om rechtszekerheid voor verwerkingsverantwoordelijken te garanderen en om een juiste balans van overheidsregulering en zelfregulering te bewerkstelligen. Dat klemt te meer nu deze balans niet kan worden bereikt met op brancheniveau ontwikkelde richtsnoeren die formeel geen status hebben. Dit ondanks de bijdrage die deze richtsnoeren bieden om tot de naleving van de (U)AVG te komen.

Om de totstandkoming van het aantal gedragscodes en het vragen van de goedkeuring daarvan te vergroten, kan het behulpzaam zijn om in sectorale wetgeving het hebben van een goedgekeurde gedragscode te verplichten. Op deze wijze worden sectoren gedwongen om tot zelfregulering te komen. Naarmate het aantal gedragscodes dat ter goedkeuring bij de AP moet worden voorgelegd groeit, zullen naar verwachting de ervaren nadelen en complexiteit afnemen vanwege de ervaring die organisaties én de AP opdoen met het toetsen van gedragscodes. Dit zou gepaard kunnen gaan met een op de praktijkgerichte handleiding van de AP, waarin inzicht wordt geboden in het normenkader dat de toezichthouder bij toetsing van gedragscodes hanteert. Op deze manier zou een handreiking kunnen worden geboden aan de sectoren om tot een goedgekeurde gedragscode te komen.

De individuele zelfregulering door een verplichte bredere inzet van de FG lijkt bij te dragen aan het in overeenstemming handelen met de AVG en UAVG door individuele organisaties. In deze organisaties lukt het de functionaris voor de gegevensbescherming steeds beter een

[204] Autoriteit persoonsgegevens, jaarverslagen 2012-2018.
[205] Nieuwsbericht Autoriteit Persoonsgegevens 2019.
[206] Autoriteit persoonsgegeven 2021.

volwaardige positie te verwerven[207], zodat 'maatwerk' bij de uitleg van open normen en sleutelbepalingen beter mogelijk is.

Om als verwerkingsverantwoordelijke zekerheid te krijgen of een nieuwe verwerking van persoonsgegevens rechtmatig is op grond van de AVG kan aan de toezichthouder een voorafgaande raadpleging worden gevraagd. Een dergelijke raadpleging is mogelijk, indien uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zal opleveren en dit risico met maatregelen niet kan worden gemitigeerd[208] dan wel dat de nationale wetgever daartoe verplicht waar het gaat om verwerkingen ter vervulling van een taak in het algemeen belang. Een voorafgaande raadpleging leidt tot een advies van de toezichthouder over de rechtmatigheid van de verwerking. In 2018, 2019 en 2020 zijn er respectievelijk 7, 13 en 8 voorafgaande raadplegingen uitgevoerd.[209] Het advies is geen besluit in de zin van artikel 1:3, eerste lid Awb. Tegen het advies kunnen dan ook geen rechtsmiddelen worden aangewend. De gegeven adviezen dan wel een samenvatting daarvan worden door de AP niet gepubliceerd, waardoor het rechtsvormende karakter daarvan beperkt is tot individuele verwerkingsverantwoordelijken.

Gegevens ontbreken over in hoeverre verwerkingsverantwoordelijken voldoen aan de verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren en of, wanneer deze beoordeling daartoe aanleiding geeft, ook daadwerkelijk aan de toezichthouder om een voorafgaande raadpleging wordt gevraagd. Wel blijkt dat binnen organisaties waar een functionaris voor de gegevensbescherming een volwaardige positie inneemt deze verplichting uit de AVG in processen zijn ingebed.

De AVG voorziet daarnaast in het instellen van een certificeringsmechanisme. De certificering ziet op de verwerking van persoonsgegevens. Het doel daarvan is het versterken van transparantie en naleving van de verordening. Ook bevordert de AVG gegevensbeschermingszegels en -merktekens (zgn. privacy seals), zodat betrokkenen snel het gegevensbeschermingsniveau van producten en diensten ter zake kunnen beoordelen. Deze instrumenten helpen vergaren van inzicht of producten en diensten en de daaruit voortkomende verwerking van persoonsgegevens voldoen aan de AVG en de UAVG. In Nederland ligt het eerstelijnstoezicht bij de certificerende en accrediterende instellingen. De AP fungeert in dit kader als stelseltoezichthouder.

Tot op heden zijn nog geen certificering van verwerkingen en gegevensbeschermingszegels en -merktekens in Nederland uitgegeven. Wel vindt in het private domein certificering plaats op basis van ISO- en NEN-normen[210]. Deze normen zijn een hulpmiddel om tot een goede governancestructuur te komen, waardoor de naleving van de AVG en de UAVG ingebed raakt in de organisatie. Het gaat hierbij echter niet om AVG-certificering.

In haar Evaluatie van de AVG constateert ook de Europese Commissie dat het volledige AVG-instrumentarium, zoals certificeringsmechanismes en gedragscodes, beter benut moet worden om naleving van de AVG beter werkbaar te maken. Zelf stimuleert de Europese Commissie dit onder meer door verlening van financiële steun EU-gedragscodes op het gebied van gezondheid en onderzoek. Daarbij roept zij de EDPB op om verdere ondersteuning te bieden

[207] Autoriteit Persoonsgegevens 2019-2.
[208] Deze beoordeling dient door de verwerkingsverantwoordelijke zelf te worden uitgevoerd.
[209] Feiten en cijfers over de AP.
[210] Zie bijvoorbeeld de NEN-ISO 27001 en de NEN 7510.

bij de volledige inzet van het AVG-instrumentarium. De EDPB heeft op 4 juni 2019 richtsnoeren vastgesteld voor gedragscodes en toezichthoudende organen.[211]

Gezien de beperkte inzet van zelfregulering tot op heden, zal het geven van (rechts)zekerheid over de werking van het stelsel van begripsbepaling en normen en de concrete uitwerking daarvan voor verwerkingsverantwoordelijke in belangrijke mate op de weg liggen van de nationale toezichthouder, de EDPB en uiteindelijk de rechter.

De EDPB geeft net als haar voorganger, WP29, een nadere invulling van de begripsbepalingen en normen door middel van richtsnoeren, aanbevelingen en best practices. Ook de AP verschaft onder meer aan de hand van veel voorkomende vragen uitleg op haar website en door middel van eigen operationele handreikingen.[212] Daarnaast biedt de AP door middel van het Informatie- en Meldpunt Privacy burgers en organisaties de mogelijkheid om, naast het indienen van klachten en het afgeven van signalen, vragen te stellen over de uitleg van de AVG.

Onder de Wbp ging de toezichthouder niet in overleg met individuele verwerkingsverantwoordelijken en gaf ze evenmin individueel advies. Daar is ook onder de AVG geen verandering in opgetreden. De AP spreekt daarentegen wel met organisaties op brancheniveau. Het gaat daarbij volgens de toezichthouder om ruim 350 gesprekken per jaar, waarin aandacht wordt besteed aan normuitleg en guidance. Als voorbeelden worden door de AP genoemd de uitleg over faillissementen en de omgang met transactiedata door banken. Eenzelfde soort gesprekken worden ook gevoerd met wetgevingsjuristen bij ministeries onder meer in de rol van de AP als wetgevingsadviseur.

De AP voorziet in een mogelijkheid om FG's bij de uitoefening van hun taak te ondersteunen door middel van het geven van advies. Echter, niet elke verwerkingsverantwoordelijke is verplicht tot het hebben van een dergelijke functionaris. De reacties van respondenten duiden erop dat functionarissen niet altijd om advies vragen omdat men niet verwacht daadwerkelijk advies te krijgen of omdat men zich zorgen maakt over ongewenste gevolgen van de adviesaanvraag. De AP brengt naar voren dat de toezichthouder in 2021 bij de AP circa honderd vragen per maand binnenkwamen afkomstig van FG's. Deze vragen zijn, zo stelt de AP, direct door de toezichthouder afgehandeld.

Jurisprudentievorming heeft zeker op nationaal niveau onder de Wet persoonsregistraties (Wpr) en Wbp amper plaatsgevonden, waardoor de toetsing van de norminvulling in specifieke casuïstiek nauwelijks heeft plaatsgevonden. Dit kwam door de wijze waarop de toezichthouder destijds haar toezicht had ingericht, maar ook de relatieve onbekendheid met het gegevensbeschermingsrecht. Onder de AVG is het aantal procedures op nationaal en Europees niveau waarin de AVG, en in mindere mate de UAVG, een rol spelen toegenomen.

6.2.2 Biometrische gegevens

Onder de EU-Richtlijn 95/46/EU waren biometrische gegevens nog niet gedefinieerd. Sinds het van toepassing worden van de AVG op 25 mei 2018 geldt een verbod om biometrische gegevens te verwerken. Biometrische gegevens zijn immers ingevolge artikel 9, eerste lid AVG en artikel 22, eerste lid UAVG bijzondere persoonsgegevens.

Op grond van artikel 4, sub 14 AVG worden biometrische gegevens als volgt gedefinieerd:

[211] European Data Protection Board 2019.
[212] *Stcrt.* 2013, 5174; Autoriteit Persoonsgegevens 2017-2.

persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukken.

Volgens de overwegingen bij de AVG[213] mag de verwerking van foto's niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken.[214] In de praktijk gaat het hierbij vooral om biometrische persoonsgegevens die het resultaat zijn van een specifieke technische verwerking, waardoor de gegevens tot een individu herleidbaar zijn.[215,216,217]

Het verwerkingsverbod kan worden doorbroken met een beroep op een van de in artikel 9, tweede lid AVG opgenomen voorwaarden. Het gaat daarbij meer specifiek om de voorwaarden uitdrukkelijke toestemming en het dienen van een zwaarwegend algemeen belang. In het kader van deze subparagraaf wordt nader ingegaan op de voorwaarde van het dienen van een zwaarwegend algemeen belang.

Artikel 9, tweede lid, onder g AVG, laat ruimte voor een uitzondering in nationaal recht op het verbod om biometrische gegevens te verwerken om redenen van zwaarwegend algemeen belang. In artikel 29 UAVG is daar invulling aangegeven. Daarin is bepaald dat het verbod om biometrische gegevens te verwerken met het oog op de unieke identificatie van een persoon niet van toepassing is, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden.

Over de omstandigheid wanneer de uitzondering kan worden ingeroepen zegt de regering in de memorie van toelichting bij de UAVG dat er een afweging dient te worden gemaakt of identificatie met biometrische gegevens noodzakelijk is voor authenticatie of beveiligingsdoeleinden. De werkgever zal dan moeten afwegen of de gebouwen en informatiesystemen zodanig beveiligd moeten zijn dat dit met biometrie dient plaats te vinden. Dit zal het geval zijn als de toegang beperkt dient te zijn tot bepaalde personen die daartoe geautoriseerd zijn, zoals bij een kerncentrale. Het verwerken van biometrische gegevens dient ook proportioneel te zijn. Als het om de toegang tot een garage van een reparatiebedrijf gaat, zal de noodzaak van de beveiliging niet zodanig zijn dat werknemers alleen met biometrie toegang kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Aan de andere kant kan biometrie soms juist een belangrijke vorm van beveiliging zijn voor bijvoorbeeld informatiesystemen, die zelf veel persoonsgegevens bevatten, waarbij onrechtmatige toegang, ook van werknemers, moet worden voorkomen. Om deze afweging mogelijk te maken in omstandigheden waarin toestemming niet in vrijheid kan worden gegeven, is in de UAVG een bepaling opgenomen die een uitzondering op het verbod voor verwerking van biometrische gegevens mogelijk maakt met het oog op de identificatie van de betrokkene, indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden.[218]

[213] Overweging 51 bij EU-verordening 2016/679. Zie ook de European Data Protection Board 2020, p 19-22.
[214] Zie voor een verdere verdieping over de problematiek rondom gezichtsherkenning het in opdracht van het WODC uitgevoerde onderzoek door dr. B. van der Sloot e.a. zoals neergelegd in het rapport 'Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties' van 12 maart 2020 (Van der Sloot e.a. 2020).
[215] 'Wat verstaat de AVG onder bijzondere persoonsgegevens?'.
[216] Rb. Amsterdam 12 augustus 2019, ECLI:RBAMS:2019:6005.
[217] Boete Vingerafdrukken Personeel.
[218] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 94-95.

De inzet van biometrische gegevens voor authenticatie- of beveiligingsdoeleinden dient noodzakelijk, proportioneel en subsidiair te zijn. Er wordt verwezen naar twee uitersten. Enerzijds de kerncentrale als duidelijk voorbeeld van een situatie dat een beroep kan worden gedaan op de uitzonderingsgrond en anderzijds de garage van een reparatiebedrijf waarbij de uitzonderingsgrond niet opgaat. De uitleg van de regering laat een behoorlijke ruimte voor verwerkingsverantwoordelijke om zelf een afweging te moeten maken of de inzet van biometrische gegevens voor authenticatie en beveiligingsdoeleinden rechtmatig is.

De AP biedt in een besluit, waarbij een boete is opgelegd aan een bedrijf voor het verwerken vingerafdrukken, enige duiding.[219] De toets of voldaan wordt aan artikel 29 UAVG is volgens de AP een strenge toets. In die situatie ging het om een bedrijf waarvan werknemers hun vingerafdrukken hebben moeten laten scannen voor aanwezigheids- en tijdsregistratie. De AP is van oordeel dat het verwerken van biometrische gegevens in het kader van het tegengaan van misbruik bij tijdsregistratie, aanwezigheidscontrole en bevoegd gebruik van apparatuur niet noodzakelijk en proportioneel is. De als eenvoudig aangeduide werkzaamheden benaderen de werkzaamheden binnen een garage van een reparatiebedrijf, waarbij het volgens de memorie van toelichting niet noodzakelijk en proportioneel is om biometrische gegevens te verwerken. Weliswaar heeft het bedrijf een belang om te werken met vingerscanapparatuur voor het tegengaan van misbruik bij tijdsregistratie, maar gelet op dit doel en de bedrijfsactiviteiten rechtvaardigt dat belang geen uitzondering op het verbod van verwerking van biometrische gegevens. Net als bij een garage, is ook bij dit bedrijf de noodzaak van de beveiliging niet zodanig dat werknemers met biometrie toegang moeten kunnen krijgen en daartoe deze gegevens worden vastgelegd om de toegangscontrole uit te oefenen. Daarnaast kunnen andere manieren, die minder inbreuk op de privacy van werknemers maken, dit ook bewerkstelligen, aldus de AP. Deze overtreding leidde eind 2019 tot het opleggen van een bestuurlijke boete van € 725.000,00.

Op 5 juni 2020 plaatste de AP een nieuwsbericht op haar website waarin de AP weergeeft dat zij een brief naar het Centraal Bureau Levensmiddelenhandel heeft gestuurd, waarin supermarkten worden gewaarschuwd voor het gebruik van gezichtsherkenningscamera's. De AP geeft aan dat net als bij een garage, ook bij een supermarkt de noodzaak van de beveiliging niet zodanig is dat van (potentiële) overlastgevers/dieven biometrische gegevens moeten worden vastgelegd om een supermarkt te beveiligen. Andere manieren, zoals een beveiligingscamera zonder gezichtsherkenning, kunnen dit ook bewerkstelligen, aldus de AP.[220] In welke gevallen, los van de kerncentrale, de inzet van biometrische gegevens *wel* mogelijk is, geeft de AP geen inzicht. Wel is duidelijk dat de lat hoog ligt.[221]

Het gebrek aan een nadere verduidelijking van deze norm leidt vooralsnog tot voorzichtigheid bij organisaties bij de inzet van biometrische gegevens. Ook in die gevallen, waarin het niet zonder meer uitgesloten is dat niet voldaan zou kunnen worden aan de strenge toets. Op grond van de Wwft zijn banken verplicht om klanten te identificeren. Dit kan voor kleinere banken ingewikkeld zijn, omdat deze banken veelal geen fysieke kantoren meer hebben. Het is in dat geval lastig om een betrokkene te kunnen identificeren, wanneer er geen gebruik mag worden gemaakt van biometrische gegevens. Daarnaast is het, gelet op maatschappelijke ontwikkelingen en de steeds verdergaande digitalisering, aannemelijk dat in de toekomst steeds meer behoefte zal zijn aan het digitaal communiceren tussen de betrokkene en de bank.

[219] Boete Vingerafdrukken Personeel, p. 17; zie ook Rb. Amsterdam 12 augustus 2019, ECLI:NL:RBAMS:2019:6005.
[220] Brief aan Centraal Bureau Levensmiddelenhandel.
[221] Van der Sloot e.a. 2020-2, p. 11.

Ondanks dat de banken in artikel 29 UAVG wel ruimte zien voor de verwerking van biometrische gegevens, zijn banken voorzichtig nu nadere uitleg ontbreekt.

Het conceptwetsvoorstel 'Verzamelwet gegevensbescherming' beperkt, zoals het zich er nu laat uitzien, het gebruik van biometrische gegevens. In het wetsvoorstel is een wijziging van artikel 29 opgenomen. Artikel 29 zou in dat geval als volgt komen luiden.

Gelet op artikel 9, tweede lid, onderdeel g, van de verordening, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is voor authenticatie of omwille van beveiligingsdoeleinden en slechts voor zover dit noodzakelijk is vanwege een zwaarwegend belang van rechtmatige toegang tot bepaalde plaatsen, gebouwen, diensten, producten, informatiesystemen of werkprocessystemen.

Met deze wijziging wordt een dubbele noodzakelijkheidstoets geïntroduceerd. De verwerking moet dan noodzakelijk zijn voor authenticatie of omwille van beveiligingsdoeleinden én noodzakelijk zijn omwille van een zwaarwegend algemeen belang. In de ontwerp-memorie van toelichting wordt uitgelegd dat het beschermen van de volksgezondheid, het voorkomen van milieuschade of het beveiligen van vitale processen redenen zijn waarmee aan de eis van zwaarwegend algemeen belang wordt voldaan. Er zal in ieder geval een belang gediend moeten worden dat uitstijgt boven louter reguliere bedrijfs- of organisatiebelangen (als efficiëntie of kostenbesparing), wil een verwerkingsverantwoordelijke een beroep op deze uitzondering kunnen doen.[222, 223]

Met deze invulling maakt de regering een slag met het geven van uitleg over de invulling van de norm in artikel 29 UAVG. Deze uitleg laat aan een organisatie ruimte om zelf de afweging te blijven maken of de specifieke verwerking van biometrische gegevens die zij voor ogen heeft noodzakelijk is vanwege een zwaarwegend belang. Wel maakt de regering duidelijk dat het moet gaan om een belang dat uitstijgt boven louter reguliere bedrijfs- of organisatiebelangen. De AP ziet in dat kader ruimte voor verwerkingsverantwoordelijken voor het laten uitvoeren van een voorafgaande raadpleging als mogelijk nuttig instrument om gewenste duidelijkheid van de toezichthouder te verkrijgen. Zij merkt daarbij op dat de toezichthouder nog nauwelijks aanvragen om een voorafgaande raadpleging heeft ontvangen.

Uitgaande van dit conceptwetsvoorstel en de toelichting daarbij lijkt het gebruik van biometrische gegevens om de verdere digitalisering bij banken te faciliteren vanuit een organisatiebelang een onvoldoende belang vertegenwoordigen. Echter, de inzet van biometrische gegevens om te voldoen aan de Wwft en om fraude tegen te gaan, lijken wel onder in de toelichting geschetste kaders te vallen.

Het wetsvoorstel zou aan duidelijkheid op dit punt kunnen winnen door in de memorie van toelichting bij de Verzamelwet gegevensbescherming enkele aansprekende voorbeelden toe te voegen om inzicht te geven in hoe deze dubbele noodzakelijkheidstoets in de praktijk zal uitpakken. Wordt bijvoorbeeld aan de dubbele noodzakelijkheidstoets voldaan, indien biometrie gehanteerd wordt omwille van de beveiliging van grootschalige infrastructurele projecten, zoals bijvoorbeeld destijds de bouw van de Amsterdamse Noord/Zuidlijn, waarbij

[222] Consultatieversie Memorie van Toelichting Verzamelwet gegevensbescherming, p.15.
[223] Zie ook: Van der Sloot e.a. 2020.

hoofdaannemers en vele onderaannemers betrokken zijn en het risico op tekortschietende authenticatie groot kan zijn.

6.2.3 Strafrechtelijke gegevens

Artikel 9, eerste lid AVG bevat een limitatieve opsomming van bijzondere categorieën van persoonsgegevens. Persoonsgegevens van strafrechtelijke aard vallen daar – anders dan onder EU-Richtlijn 95/46 – niet onder. Dergelijke gegevens mogen op grond van artikel 10 AVG uitsluitend worden verwerkt onder toezicht van de overheid dan wel indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen bevatten voor de rechten en vrijheden van betrokkenen. Paragraaf 3.2 van de UAVG ziet op het verwerken van persoonsgegevens van strafrechtelijke aard en geeft algemene en overige uitzonderingsgronden op grond waarvan dergelijke persoonsgegevens mogen worden verwerkt. De bepalingen waarin deze uitzonderingsgronden zijn opgenomen – de artikelen 32 en 33 – komen materieel overeen met de bepalingen over de verwerking van persoonsgegevens van strafrechtelijke aard in de Wbp. Ook wat betreft dit onderwerp heeft de wetgever gekozen voor een beleidsneutrale invulling.

In het kader van de analyse of de normen uit de UAVG duidelijk zijn, wordt stilgestaan bij de vraag wat een persoonsgegeven van strafrechtelijke aard is en bij de systematiek van het sectoraal en cross-sectoraal delen van persoonsgegevens van strafrechtelijke aard door private partijen in verband met fraudebestrijding.

Definitie persoonsgegevens van strafrechtelijke aard
In artikel 1 UAVG wordt onder persoonsgegevens van strafrechtelijke aard verstaan:

> *persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.*

Artikel 1 UAVG herhaalt deels de beschrijving die in artikel 10 AVG gegeven is van een persoonsgegeven van strafrechtelijke aard. De wetgever heeft er echter nog een zinsnede aan toegevoegd: ‘alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag’. In het conceptwetsvoorstel Verzamelwet gegevensbescherming wordt voorgesteld deze herhaling te laten vervallen.[224]

Het Hof van Justitie van de Europese Unie overweegt over het begrip ‘strafbaar feit in strafrechtelijke zin’ dat dit begrip in de gehele Unie autonoom en uniform moet worden uitgelegd, waarbij rekening dient te worden gehouden met het doel van die bepaling en de context ervan, zonder dat de door de betrokken lidstaat aan die strafbare feiten gegeven kwalificatie in dat opzicht beslissend is, aangezien die kwalificatie van land tot land kan verschillen.[225] Het gerechtshof in Den Haag overweegt in dat kader dat het begrip ‘persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten’ in de zin van artikel 10 AVG een Unierechtelijk begrip is dat autonoom moet worden uitgelegd. De AVG geeft de lidstaten niet de mogelijkheid een eigen, ruimere invulling te geven aan dat begrip.[226] Het Hof van Justitie van de Europese Unie overweegt tevens dat de AVG de lidstaten niet de mogelijkheid geeft

[224] Ministerie van Justitie en Veiligheid 2022.
[225] HvJ- EU 22 juni 2021, ECLI:EU:C:2021:504, r.o. 83-85.
[226] Hof Den Haag 24 december 2019; ECLI:NL:GHDHA:2019:3539.

een eigen, ruimere invulling te geven aan dat begrip.[227] De in artikel 1 opgenomen aanvulling is dan ook niet in lijn met deze jurisprudentie.

Wanneer is sprake van een persoonsgegeven van strafrechtelijke aard?
De in artikel 10 AVG bedoelde gegevens gaan over gedragingen die aanleiding geven tot maatschappelijke afkeuring. Toegang tot die gegevens kan voor betrokkene stigmatiserend werken en aldus op ernstige wijze inbreuk maken op diens privé- en/of beroepsleven. Artikel 10 AVG heeft uitsluitend betrekking op strafbare feiten in strafrechtelijke zin. [228]

In artikel 10 AVG gaat het om het verbod op verwerking van persoonsgegevens *betreffende strafrechtelijke veroordelingen* en *strafbare feiten*. Een verwerkingsverantwoordelijke zal moeten vaststellen of hij persoonsgegevens verwerkt die als zodanig kwalificeren. Is dat het geval, dan dient door de verwerkingsverantwoordelijke getoetst te worden of een uitzonderingsgrond geldt op grond waarvan deze gegevens mogen worden verwerkt.

Van een *strafrechtelijke veroordeling* is sprake wanneer het gaat om een gerechtelijk vonnis met een punitief karakter. Daarbij spelen drie criteria een rol:[229]
1. de juridische kwalificatie van de inbreuk naar nationaal recht;
2. de aard zelf van de inbreuk; en
3. de aard en de zwaarte van de sanctie die de betrokkene moet worden opgelegd.

Ten aanzien van de vraag wat onder *strafbare feiten* moet worden verstaan, wordt doorgaans – ook door de AP[230] – aangesloten bij de jurisprudentie van de Hoge Raad, waarin overwogen wordt dat het gaat om zodanige concrete feiten en omstandigheden dat zij als strafbaar feit te kwalificeren bewezenverklaring kunnen dragen en in dit verband als maatstaf genomen of de vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren in die zin dat de te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan.[231]

Zelfs voor strafbare feiten die naar nationaal recht niet als strafbare feiten in strafrechtelijke zin worden gekwalificeerd, kan een dergelijk karakter niettemin voortvloeien uit de aard van het strafbare feit in kwestie en uit de zwaarte van de sancties die daarvoor kunnen worden opgelegd. Minder ernstige overtredingen vallen buiten de werkingssfeer van artikel 10 AVG.[232]

Berkvens[233] wijst op de betekenis van de term *betreffende (*in de zinsnede *'*persoonsgegevens *betreffende* strafrechtelijke veroordelingen en strafbare feiten'), nu deze term een relatie legt tussen strafbare feiten en strafrechtelijke veroordelingen enerzijds en persoonsgegevens anderzijds en daarmee een belangrijke rol inneemt bij het bepalen of sprake is van een persoonsgegeven van strafrechtelijke aard. De vraag die in dat kader dient te worden beantwoord is wanneer persoonsgegevens betrekking hebben op een strafrechtelijke veroordeling of een strafbaar feit. Als handvat om deze vraag te kunnen beantwoorden sluit Berkvens aan bij de criteria 'inhoud', 'doel' en 'resultaat'.[234] De drie criteria moeten in samenhang worden toegepast en kunnen leiden tot de conclusie dat de context waarin de gegevens worden verwerkt

[227] HvJ-EU 17 december 2020, ECLI:EU:C:2020:1054 en HvJ-EU 22 juni 2021, ELCI:EU:C:2021:504.
[228] HvJ-EU 22 juni 2021, ECLI:EU:C:2021:504, r.o. 75-77.
[229] HvJ-EU 22 juni 2021, ECLI:EU:C:2021:504, r.o. 87.
[230] Besluit Autoriteit Persoonsgegevens 19 juni 2019 en Besluit Autoriteit Persoonsgegevens 8 oktober 2021.
[231] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, zie ook in gelijke strekking het arrest van het Gerechtshof Arnhem-Leeuwarden 9 november 2017, ECLI:NL:GHARL:2017:10752.
[232] HvJ-EU 22 juni 2021, ECLI:EU:C:2021:504, r.o. 88 en HvJ-EU 20 maart 2018, ECLI: EU:C:2018:193, punten 28 en 32.
[233] Berkvens 2021.
[234] Gelijk aan het advies van WP29 inzake het begrip persoonsgegevens (WP 136).

het wel of niet waarschijnlijk maakt dat deze onder de reikwijdte vallen van artikel 10 AVG en artikel 1 UAVG en of getoetst moet worden aan de artikelen 32 en 33 UAVG om persoonsgegevens van strafrechtelijke aard te mogen verwerken.

Met name het bepalen of sprake is van de verwerking van persoonsgegevens betreffende een strafbaar feit kan in de praktijk leiden tot onduidelijkheid. De AP leek voor de inwerkingtreding van de AVG/UAVG de strafrechtelijke aard van een persoonsgegeven snel aan te nemen.[235] In recente besluiten inzake de weigering van een vergunning op grond van artikel 33, vierde lid, aanhef en onder c AVG lijkt de AP echter met name belang te hechten aan het doel waarvoor deze persoonsgegevens worden verwerkt.

Sectoraal en cross-sectoraal delen van persoonsgegevens tussen private partijen als bedoeld in artikel 33, vierde lid UAVG

In deze paragraaf wordt ingegaan op het in de UAVG opgenomen vergunningenstelsel ten behoeve van het delen van persoonsgegevens van strafrechtelijke aard tussen private partijen en de vraag of een nadere normering door de wetgever aangewezen is.

Artikel 33 UAVG biedt private partijen verschillende mogelijkheden om persoonsgegevens van strafrechtelijke aard te verwerken ten behoeve van fraudebestrijding.

Op grond van artikel 33, tweede lid, aanhef en onder b UAVG mag een verwerkingsverantwoordelijke persoonsgegevens van strafrechtelijke aard ten eigen behoeve verwerken ter bescherming van zijn eigen belangen, voor zover het gaat om strafbare feiten die zijn of – naar redelijkerwijs te verwachten is – zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn. Deze bepaling biedt een grondslag voor een zwarte lijst die uitsluitend wordt gebruikt *binnen één bepaald bedrijf*. Gedacht kan worden aan een supermarkt die een zwarte lijst opstelt van personen die zich in die winkel schuldig hebben gemaakt aan winkeldiefstal.

Op grond van artikel 33, vierde lid, aanhef en onder b UAVG mogen persoonsgegevens van strafrechtelijke aard ten behoeve van derden worden verwerkt, indien deze derde deel uitmaakt van *hetzelfde concern* als de verwerkingsverantwoordelijke. Deze bepaling maakt het mogelijk om zwarte lijsten te delen tussen ondernemingen die deel uitmaken van hetzelfde concern.

Verder is het mogelijk om persoonsgegevens van strafrechtelijke aard *ten behoeve van derden* te verwerken indien de AP hiervoor een vergunning heeft verleend als bedoeld in artikel 33, vierde lid, aanhef en onder c. De AP kan ingevolge artikel 33, vijfde lid UAVG een dergelijke vergunning verlenen, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Een zwaarwegend belang alleen is echter niet voldoende. De verwerking dient noodzakelijk te zijn met het oog op dit zwaarwegend belang. Het is volgens de wetgever aan de AP om vooraf, dat wil zeggen via de vergunningsaanvraag, noodzaak en evenredigheid te toetsen. [236]

Om tot vergunningverlening te komen hanteert de AP thans de werkwijze dat door de verwerkingsverantwoordelijke eerst om een voorafgaande raadpleging dient te worden verzocht, indien uit de uitgevoerde gegevensbeschermingseffectbeoordeling volgt dat sprake is van hoge restrisico's en dat na afronding van de voorafgaande raadpleging een vergunning bedoeld in

[235] Zie bijvoorbeeld College bescherming persoonsgegevens 2015-2.
[236] *Kamerstukken II* 2017/18, 34851, nr. 7, p.55

artikel 33, vierde lid, aanhef en onder c, kan worden aangevraagd. De vraag is wel of én een voorafgaande raadpleging én een vergunningaanvraag niet dubbelop is. Mogelijk dat kan worden overwogen om in de UAVG het uitvoeren van een gegevensbeschermingseffectbeoordeling randvoorwaardelijk te laten zijn bij het aanvragen van een dergelijke vergunning.

De noodzakelijkheid van een verwerking wordt onder andere getoetst aan de proportionaliteit en de subsidiariteit. Met andere woorden: een verwerking dient noodzakelijk te zijn om het vastgestelde doel van de verantwoordelijke te bereiken, waarbij dient te worden nagegaan of het middel opweegt tegen de inbreuk op de persoonlijke levenssfeer en of er geen minder verstrekkend middel is waarmee het doel ook wordt bereikt. Volgens de wetgever kunnen onder andere de volgende omstandigheden een rol spelen bij de proportionaliteitstoets.[237]

1. de mate waarin opname van een individu in het systeem waarop de gegevensuitwisseling betrekking heeft, kan betekenen dat betrokkene wordt uitgesloten van bijvoorbeeld eerste levensbehoeften of van goederen of diensten die betrekking hebben op een (klassiek of sociaal) grondrecht;
2. de kwetsbaarheid van bepaalde groepen betrokkenen, zoals minderjarige klanten en werknemers, oudere werknemers en werknemers die geen mogelijkheid hebben om een eventueel ontslag aan te vechten;
3. de reikwijdte van het systeem, in termen van zowel degenen die het systeem kunnen vullen, degenen die gegevens in het systeem kunnen raadplegen en degenen van wie persoonsgegevens in het systeem worden verwerkt. Hoe groter de reikwijdte, hoe ingrijpender de gevolgen voor opname van de betrokkene in het systeem kunnen zijn. Naarmate de reikwijdte van een systeem groter is, zullen derhalve de waarborgen voor betrokkenen zwaarder moeten zijn of zal het systeem in het geheel niet door de toetsing komen.

Ter illustratie volgen hierna enkele voorbeelden van aanvragen voor een vergunning op grond van artikel 33, vierde lid, aanhef en onder c, UAVG.

VODIOM
Op 5 juli 2021 heeft de vereniging VODIOM een aanvraag voor een vergunning op grond van artikel 33, vierde lid, aanhef en onder c UAVG ingediend bij de AP. Het betrof een vergunningaanvraag over *cross*-sectorale gegevensdeling t.b.v. fraudebestrijding (Frauderegistratiesysteem); VODIOM wil persoonsgegevens van vermoedelijke daders van fraude gaan uitwisselen tussen bedrijven in verschillende sectoren: de betaalindustrie, online retail en telecommunicatie. Ten behoeve van de aanvraag is door VODIOM een protocol, een data protection impact assessment (gegevensbeschermingseffectbeoordeling, DPIA) en een deelnemersreglement opgesteld. In het Frauderegistratiesysteem wil men relevante gegevens betreffende fraudegevallen tussen verschillende sectoren delen. In het bijzonder gaat het om (identificerende) gegevens van de vermoedelijke fraudeplegers zoals naam, adres en woonplaats.[238] De gevraagde vergunning wordt door de AP op 8 oktober 2021 *afgewezen*. De AP concludeert weliswaar dat het doel van vereniging VODIOM om fraude tegen te gaan waar zowel bedrijven als burgers het slachtoffer van kunnen worden kwalificeert als een zwaarwegend belang van derden in de zin van artikel 33, vijfde lid UAVG, maar is van oordeel dat de vereniging VODIOM de proportionaliteit, subsidiariteit van de verwerking van strafrechtelijke persoonsgegevens onvoldoende toereikend heeft gemotiveerd. Het cross-sectoraal delen van de strafrechtelijke gegevens is daarmee niet toegestaan. Daarnaast is de AP van oordeel dat de vereniging VODIOM niet aannemelijk heeft gemaakt dat de invoerende en

[237] *Kamerstukken II* 2017/18, 34 851, nr. 7, p. 55
[238] Besluit Autoriteit Persoonsgegevens 8 oktober 2021, onder 19.

raadplegende deelnemers gezamenlijk verwerkingsverantwoordelijkheid dragen voor de beoogde gegevensverwerking in het Frauderegistratiesysteem. Vereniging VODIOM lijkt eerder (primair) verwerkingsverantwoordelijke voor de gegevensverwerking in het Frauderegistratiesysteem. Tenslotte is de AP van oordeel dat door het gebruik van de aparte beveiligde database bij verwerker CIFAS, die deze laat hosten in de Microsoft Azure Cloud, er waarschijnlijk sprake is van doorgifte naar derde landen (VS). In het protocol zijn verder geen aanwijzingen gevonden dat er een studie is gemaakt van het beschermingsniveau van de VS, noch is er sprake van 'standard contractual clauses' met aanvullende maatregelen voor de doorgifte van persoonsgegevens naar de VS. Het protocol voldoet daarmee – gelet op de vereisten in AVG en Recommendations –niet aan de AVG.[239] In het persbericht over dit besluit neemt de AP de meer politieke stellingname in dat het aanpakken en opsporen van fraude een overheidstaak is, belegd bij politie en justitie. Zij mogen strafrechtelijke gegevens, zoals namen, telefoonnummers en e-mailadressen van vermoedelijke daders, verzamelen en beheren. 'Bij politie en justitie zijn er allerlei waarborgen ingebouwd, die ervoor zorgen dat gegevens veilig zijn en dat je jezelf kunt verweren tegen beschuldigingen. (…) Opsporing en het voorkomen van fraude is een belangrijke taak. In Nederland ligt die taak primair bij de overheid. Bedrijven die te maken hebben met fraude kunnen bijvoorbeeld aangifte doen bij de politie of advies krijgen van een organisatie als de Fraudehelpdesk. Het bijhouden van een fraudeursdatabase is daarom dus echt een taak van de politie en niet voor een vereniging. Bij VODIOM werken geen politieagenten, laat staan rechters. Dat de politie nu geen tijd heeft voor fraudezaken, is een serieus probleem. Maar de oplossing voor dat probleem zou niet moeten zijn dat we dan politietaken overhevelen naar een vereniging of andere private organisaties, aldus de AP'[240]

Safecin
Op 19 juni 2019 heeft de AP een gelijksoortige aanvraag van de Stichting aanpak financieel-economische criminaliteit in Nederland (Safecin) afgewezen. Safecin heeft naar aanleiding van de wens om informatie over fraude uit te wisselen de Fraudehelpdesk in het leven geroepen. Hiermee beoogt zij de Nederlandse samenleving te behoeden en weerbaarder te maken voor financieel-economische criminaliteit en om daarmee (verdere) schade onder burgers en het bedrijfsleven te voorkomen. De aangedragen grondslag voor de voorgenomen verwerking van persoonsgegevens van strafrechtelijke aard is gelegen in het zwaarwegende belang van derden, zijnde burgers en bedrijfsleven, om fraude tegen te gaan. De AP is van oordeel dat Safecin de noodzaak en proportionaliteit van de voorgenomen verwerking onvoldoende heeft aangetoond. Daarnaast heeft Safecin niet voldaan aan de verantwoordingsplichten in de AVG.[241] Ook in dit besluit wordt expliciet verwezen naar de wettelijke waarborgen van het strafrecht, dat primair het domein van de overheid is. 'Dit is een van de grondbeginselen van de Nederlandse rechtsorde hetgeen bijvoorbeeld blijkt uit de onschuldpresumptie en het ne bis in idem-beginsel, respectievelijk uit het exclusieve vervolgingsrecht van het Openbaar Ministerie en de politietaak zoals neergelegd in de Politiewet.'[242]

PIFI
Op 1 april 2020 heeft de AP een vergunning ex artikel 33 UAVG verleend op basis van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI 2021). Dit protocol regelt de uitwisseling van gegevens over incidenten, zoals fraude en misleiding, tussen

[239] Besluit Autoriteit Persoonsgegevens 8 oktober 2021, onder 102-105.
[240] Nieuwsbericht Autoriteit Persoonsgegevens 2021-3.
[241] Besluit Autoriteit Persoonsgegevens 19 juni 2019, onder 57.
[242] Besluit Autoriteit Persoonsgegevens 19 juni 2019, onder 38.

financiële instellingen. De instellingen kunnen bij de AP een individuele vergunning aanvragen om deel te mogen nemen aan het systeem. Het betreft sectorale, dus geen cross-sectorale, informatiedeling van gegevens van strafrechtelijke aard. De grondslag voor de verwerking betreft een zwaarwegend belang voor financiële instellingen om schade aan de eigen bedrijfsvoering te voorkomen en te bestrijden en dient een maatschappelijk belang om de integriteit van het financiële stelsel te borgen. Het PIFI 2021 geeft voldoende blijk van een zorgvuldige belangenafweging tussen het gerechtvaardigde belang van de financiële instellingen en de belangen van betrokkenen op bescherming van hun rechten en vrijheden, in het bijzonder de bescherming van de persoonlijke levenssfeer die leiden tot de conclusie dat de belangen van financiële instellingen daarbij prevaleren. Het PIFI 2021 geeft een adequate uitwerking van de inhoudelijke waarborgen die een behoorlijke en zorgvuldige gegevensverwerkingen aannemelijk maken. Daarnaast voorziet het PIFI 2021 in organisatorische waarborgen die een juiste en zorgvuldige gegevensverwerking aannemelijk maken en waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Het protocol kent verder een uitwerking van de rechten van betrokkenen die voor de noodzakelijke balans- en correctiemogelijkheden zorgen. Op grond van het voorgaande concludeert de AP dat de voorgenomen verwerking onder het PIFI voldoende waarborgen bevat, zodat de AP besluit de aangevraagde vergunning te verlenen.[243] Ook in dit besluit wordt expliciet verwezen naar de wettelijke waarborgen van het strafrecht, dat primair het domein van de overheid is maar in deze beoordeling komt de AP tot de conclusie dat er een zwaarwegend belang is aangetoond en in voldoende waarborgen is voorzien.

Overige
De overige sinds de inwerkingtreding van de UAVG indiende aanvragen voor gegevensdeling zien op een collectief winkelverbod (gebaseerd op een modelprotocol voor de branche).[244]

Het voorgaande laat zien dat indien aantoonbaar voldaan kan worden aan de voorwaarden uit de UAVG – noodzakelijke verwerking, zwaarwegend belang van derden en voldoende waarborgen – de AP een vergunning kan verlenen voor sectorale gegevensdeling.

Tot vergunningverlening ten aanzien van het cross-sectoraal delen van gegevens is de AP vooralsnog niet overgegaan. In de begeleidende persberichten kiest de AP een meer politieke insteek en wordt benadrukt dat de oplossing voor het gebrek aan tijd bij de politie voor de aanpak van fraude niet zou moeten zijn dat de politietaken de facto worden overgeheveld naar een vereniging of andere private organisatie. Daarnaast wordt gewezen op het bijzondere karakter en de waarborgen in het Nederlandse strafrechtdomein. Ook in de Handreiking cross-sectorale gegevensdeling tussen private partijen van de AP wordt cross-sectorale gegevensdeling in AVG-termen uiterst problematisch genoemd en wordt het uitgangspunt uitgedragen dat cross-sectorale gegevensdeling tussen private partijen van gegevens op een zwarte lijst niet is toegestaan. De (U)AVG biedt binnen het Nederlandse rechtsbestel weinig tot geen juridische mogelijkheden voor cross-sectorale gegevensdeling tussen partijen. Hierbij verwijst de AP naar de wetsgeschiedenis waaruit volgens de toezichthouder volgt dat het vergunningstelsel gegevensuitwisseling binnen een bepaalde branche of in een afgebakend geografisch gebied voor ogen heeft.[245]

[243] Besluit Autoriteit Persoonsgegevens 1 april 2020, onder 45-47.
[244] Zie bijvoorbeeld Besluit Autoriteit Persoonsgegevens 5 augustus 2021.
[245] Kamerstukken II, 2017/18, 34851, nr. 7 (Nota naar aanleiding van het verslag, vraag 63).

Op 19 september 2018 hebben VNO-NCW en MKB Nederland in een brief gevraagd de UAVG te wijzigen in die zin dat de UAVG een expliciet wettelijke grondslag zal bevatten voor het cross-sectoraal uitwisselen van gegevens over fraudeurs. In zijn kamerbrief van 11 juni 2019[246] geeft de Minister voor Rechtsbescherming aan dat er eerst ervaringen moeten zijn opgedaan met de huidige wijze waarop gegevensdeling in de UAVG is geregeld voordat er aanleiding kan zijn om wijziging van de UAVG te overwegen. Met VNO-NCW en MKB Nederland en de AP heeft de Minister gesproken over de mogelijkheden rondom een vergunning op grond van de UAVG. Het gesprek heeft volgens de Minister over en weer verhelderd waartoe een vergunningaanvraag zou kunnen dienen en aan welke eisen deze dient te voldoen. De Minister geeft aan de ervaringen die door private organisaties worden opgedaan met hun voornemen tot cross-sectorale gegevensdeling ten behoeve van fraudebestrijding en eventuele daarbij spelende knelpunten binnen het huidige wettelijke gegevensbeschermingskader af te wachten. Afhankelijk van die ervaringen zal zo nodig nieuwe wetgeving kunnen worden overwogen.

Gezien de grote impact op betrokkenen en de waarborgen die vereist zijn om cross-sectorale gegevensdeling door private partijen mogelijk te maken is het, mede gelet op de bedoeling van de vergunning als bedoeld in artikel 33, vierde lid, aanhef en onder c UAVG, maar de vraag of cross-sectorale gegevensdeling door private partijen door middel van vergunningverlening door de toezichthouder geregeld kan worden. In het geval er een politieke wens ligt om cross-sectorale gegevensdeling tussen private partijen mogelijk te maken, dan zou het meer voor de hand liggen om dit in afzonderlijke wetgeving met de nodige waarborgen omkleed te regelen waar democratische controle van het parlement op mogelijk is. Het gaat daarbij volgens de AP om waarborgen die een verdachte heeft in de strafrechtketen. Ook kan daarbij worden gekeken naar de waarborgen die gelden voor particuliere recherchebureaus, aldus de AP. Indien het op deze wijze cross-sectoraal delen van gegevens niet wenselijk wordt geacht, dan zou de UAVG op dit punt aan duidelijkheid kunnen winnen door deze wijze van delen van persoonsgegevens expliciet in artikel 33 van vergunningverlening uit te sluiten.

6.3 De Gedragscode gezondheidsonderzoek

6.3.1 Schets van de situatie

De Gedragscode Gezondheidsonderzoek is voorbereid met het oog op het spanningsveld tussen de belangen van privacy en gegevensbescherming enerzijds, en wetenschappelijk onderzoek anderzijds. De AVG bestaat uit open normen, die in concrete situaties moeten worden ingevuld. Hoe die invulling gestalte moet krijgen is niet altijd op voorhand duidelijk. Een gedragscode voorziet in die duidelijkheid. Een gedragscode heeft bovendien als voordeel dat sectorgewijs dezelfde regels worden gehanteerd, waardoor ook op het gebied van gegevensbescherming een level playing field ontstaat.

De AVG regelt de bevoegdheid van de toezichthouder om gedragscodes goed te keuren in artikel 40, vijfde lid. Volgens artikel 14, tweede lid UAVG is op de voorbereiding van een besluit over de goedkeuring van een gedragscode, dan wel de wijziging of uitbreiding daarvan, als bedoeld in artikel 40, vijfde lid AVG en afdeling 3.4 van de Awb (de uniforme openbare voorbereidingsprocedure) van toepassing. Aan goedgekeurde gedragscodes kunnen organisaties

[246] *Kamerstukken II* 2018/19, 32761, nr. 135. Dit als beleidsreactie op het rapport van Considerati (2019), Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding. In dit onderzoek concentreren de onderzoekers zich op aanvulling van artikel 33, vierde lid, aanhef onder c en het vijfde lid UAVG met een specifiek kader voor (cross-sectorale) gegevensdeling ten behoeve van fraudebestrijding dan wel een uitzonderingsgrond voor organisaties en een eventueel beherende partij om persoonsgegevens van strafrechtelijke aard te verwerken om fraude te bestrijden zonder dat daarvoor een vergunning wordt aangevraagd.

die met die gedragscode werken bepaalde waarborgen ontlenen. Doel van het opstellen van gedragscodes is het bevorderen van de juiste toepassing van de regels over gegevensbescherming zoals neergelegd in de AVG (zie ook artikel 40, eerste lid AVG).

Volgens artikel 40, tweede lid AVG kunnen Gedragscodes voorzien in de regeling van onderwerpen zoals behoorlijke en transparante verwerking, de gerechtvaardigde belangen die door verwerkingsverantwoordelijken in een specifieke context worden behartigd, de verzameling van gegevens, de pseudonimisering van persoonsgegevens, de aan het publiek en betrokkenen verstrekte informatie of de uitoefening van de rechten van betrokkenen.

Volgens artikel 40, eerste lid AVG bevorderen de lidstaten, de toezichthouders, het EDPB en de commissie de totstandkoming van Gedragscodes.

Gedragscodes kunnen worden gezien als een belangrijk mechanisme van zelfregulering dat de adequate werking van het stelsel, dat bestaat uit algemene, open normen en het toezicht op de werking van die normen, in een specifieke sector kan bevorderen. Om die reden is gekozen voor het bestuderen van de totstandkoming van de Gedragscode Gezondheidsonderzoek.

Gedragscodes kunnen een nuttige functie vervullen bij het ondersteunen van organisaties binnen sectoren die zoeken naar de goede uitleg van de gegevensbeschermingsnormen. En daarmee kunnen gedragscodes de druk wegnemen bij toezichthouders die met behulp van het horizontale instrument van gedragscodes de positie van systeemtoezichthouder kunnen vervullen. Daarvoor is het nodig dat vanuit sectoren initiatieven tot stand komen die het opstellen van gedragscodes bevorderen, ondersteund door de toezichthouder die na een voorbereidingsproces de code kan goedkeuren.

6.3.2 Totstandkoming

Er was ook onder de Wet persoonsregistraties (Wpr) al een door de Registratiekamer goedgekeurde Gedragscode Gezondheidsonderzoek, opgesteld door COREON.[247] In 2004 werd een aan de Wbp aangepaste en geactualiseerde Gedragscode Gezondheidsonderzoek goedgekeurd door het College Bescherming Persoonsgegevens.[248]. Het CBP maakte kritische kanttekeningen bij een aangepaste conceptcode in 2013. Deze is daarop niet ter beoordeling voorgelegd. In 2019 bleek na een inventariserend onderzoek door NIVEL en MedLaw Consult Foundation dat de ‘code Goed Gedrag’ aan een snelle actualisatie toe was. De inmiddels van toepassing zijnde AVG, de gegevensverwerking bij Wmo-onderzoek en het bij onderzoek gebruik maken van app’s en sociale media maakten actualisering noodzakelijk.

Het totstandkomingsproces bleek heel wat voeten in de aarde te hebben. Na een lang voorbereidingstraject dat eind 2019 van start ging, is de herziene Gedragscode Gezondheidsonderzoek op 24 januari 2022 door COREON gepubliceerd.[249]

Over de doelstelling van de gedragscode is in de toelichting bij de code te lezen: ‘De wet- en regelgeving voor gegevensbescherming bij gezondheidsonderzoek is complex en gaat deels uit van algemene, open normen die verder moeten worden ingevuld voor toepassing in de praktijk. De voorliggende Gedragscode werkt deze uit tot een set concrete, voor onderzoekers toegankelijke normen voor het Nederlandse gezondheidsonderzoek. (…) Bij de uitwerking is ernaar gestreefd dat deze normen:

[247] *Stcrt*. 1995, 140, p. 1.
[248] *Stcrt.* 2004, 82, p. 22.
[249] Coreon 2022.

— volgens het Europees en Nederlands recht juridisch sluitend zijn;
— ethisch gerechtvaardigd zijn;
— zo werkbaar mogelijk zijn voor onderzoekers en onderzoeksinstellingen.

De Gedragscode beoogt op deze manier duidelijk te maken aan welke regels het Nederlandse gezondheidsonderzoek behoort te voldoen. Een set duidelijke spelregels voorkomt bovendien dat onderzoekers verschillende normen hanteren, en dat instellingen gezondheidsonderzoek aan verschillende normen toetsen. Die verschillen staan een goede samenwerking binnen het Nederlandse gezondheidsonderzoek in de weg. Daarnaast beoogt de Gedragscode bij te dragen aan het vertrouwen dat burgers en patiënten mogen hebben in het gezondheidsonderzoek.'

De Gedragscode Gezondheidsonderzoek heeft een bredere strekking dan de AVG. De code sluit bijvoorbeeld ook aan bij het Wetsvoorstel zeggenschap lichaamsmateriaal en de Wet op de geneeskundige behandelovereenkomst (WGBO). Daarnaast betreft de AVG alleen de bescherming van persoonsgegevens van levende personen. De code sluit ook aan bij de bescherming die in o.a. de WGBO wordt geboden aan eerder verzamelde gegevens en lichaamsmateriaal van overleden patiënten. De code betreft daarmee ook het verantwoord omgaan met lichaamsmateriaal omdat dit ook drager is van persoonsgegevens.

Opmerkelijk is dat de Gedragscode Gezondheidsonderzoek niet voor goedkeuring aan de AP is voorgelegd. In het document wordt de AP op enkele plaatsen genoemd, zoals in de inleiding waar de AP wordt genoemd als een van de doelgroepen van de code, die deze zou kunnen gebruiken in haar toezichtspraktijk. Toch is er tijdens het proces van totstandkoming wel overleg gevoerd met de AP, dat door de AP als 'informeel overleg' werd getypeerd. Maar een formeel standpunt van de AP is dus niet verkregen, noch gevraagd.

6.3.3 Inhoud

De opstellers van de gedragscode geven aan dat er op meerdere punten een relatie met de UAVG is. Het verwerkingsverbod van artikel 9, eerste lid AVG en artikel 22, eerste lid UAVG regelt dat het verwerken van bijzondere persoonsgegevens, waarover het bij gezondheidsonderzoek bij uitstek gaat, is verboden. De artikelen 24, 28, 29 en 30 UAVG geven daarop uitzonderingen voor wetenschappelijk onderzoek, genetische en biometrische gegevens en gegevens over de gezondheid. Onder meer is de regeling in artikel 24 UAVG van belang die gaat over de uitzondering om bijzondere persoonsgegevens te gebruiken voor onder meer wetenschappelijk onderzoek, uiteraard een belangrijk onderdeel van de Gedragscode Gezondheidsonderzoek. De Gedragscode zoekt op dit punt een middenweg. Sommige partijen die waren betrokken bij het opstellen van de code pleiten ervoor dat in veel gevallen geen toestemming behoeft te worden gevraagd (overeenkomstig artikel 24, sub c, het vragen van uitdrukkelijke toestemming is onmogelijk of vraagt een onevenredige inspanning), terwijl andere partijen daaraan vaak wel hechten. De code laat onder voorwaarden ook ruimte voor het vragen van toestemming 'aan de poort', die fungeert als een inspanningsplicht voor toestemming voor nader gebruik. Komt daarop geen reactie, dan kan de onderzoeker onder voorwaarden terugvallen op de uitzondering op toestemming, mits de betrokkene geen bezwaar tegen verwerking voor onderzoek heeft gemaakt.

De Gedragscode is in de eerste plaats bedoeld voor onderzoekers die een onderzoeksopzet vormgeven en die zich daarbij afvragen hoe ze met persoonsgegevens moeten omgaan. Daarnaast is de code een hulpmiddel voor het beoordelen van gezondheidsonderzoek, als het gaat om opdrachtverstrekking en subsidiering. Dat alles heeft vervolgens effect op de wijze waarop

onderzoek wordt gedaan. Na afronding van het onderzoek kunnen de normen van de Gedragscode behulpzaam zijn bij de verantwoording van het uitgevoerde onderzoek en bij de beoordeling van publicaties. Verder is de code nuttig voor de toetsing van onderzoek door juristen en toetsings- en beoordelingscommissies, zoals de METC's. Tot slot is er de rol van de FG waar elke onderzoeksinstelling over dient te beschikken en die ook terug kan vallen op de code. Een toezichthoudend orgaan, dat toezicht houdt op de Gedragscode Gezondheidsonderzoek, zoals bedoeld in artikel 41 AVG, is (vooralsnog) niet tot stand gekomen. De stap naar goedkeuring van de Gedragscode door de AP is nog niet gezet.

6.3.4 Analyse

Gedragscodes die adequaat functioneren kunnen de toezichtslast van de AP sterk terugdringen. Zelfregulering kan bijdragen aan het internaliseren van de gegevensbeschermingsnormen in een bepaald domein, waardoor de tweedelijns toezichthouder (AP) een stap terug kan zetten. Toch zijn er nog maar weinig gedragscodes tot stand gekomen. Dat heeft onder andere te maken met de administratieve last die de totstandkoming van een gedragscode met zich meebrengt. De Gedragscode Gezondheidsonderzoek is daarvan een goed voorbeeld: het heeft meerdere jaren geduurd en de inspanning van velen gevergd. Daarbij zijn de eisen die de AVG stelt ook stevig. Voordat sprake kan zijn van goedkeuring door een toezichthouder moet een sector of branche zelf voorzien in een toezichtsmechanisme, dat geaccrediteerd is. De toezichthouder kan een code ook goedkeuren – en dat gebeurt ook – onder de opschortende voorwaarden dat een toezichtsmechanisme wordt ingericht. Dat vraagt erg veel van de organisatiegraad van een sector en ook van de aard van de Gedragscode zelf. Die moet gestandaardiseerde normen bevatten, keuzeopties bieden of op een geabstraheerd niveau afhankelijk van de omstandigheden aanreiken welke afwegingen gemaakt kunnen worden.

Bezien we het totstandkomingsproces van de Gedragscode Gezondheidsonderzoek, dan moet de conclusie zijn dat de code een goede poging is tot operationalisering van de normen uit de AVG op een wat abstracter niveau. Tegelijkertijd is het veld van het gezondheidsonderzoek zo groot en divers, dat het niet gelukt is tot eenduidige en gestandaardiseerde normen te komen. De Gedragscode is eerder een handleiding die keuzeopties voorlegt, dan een gebruiksaanwijzing en een samenstel van Standard Operating Procedures.

In augustus 2020 werd de door NLDigital tot stand gebrachte Data Pro Code door de AP goedgekeurd. In mei 2022 keurde de AP de door Netbeheer Nederland tot stand gebrachte gedragscode Slim Netbeheer goed onder een opschortende voorwaarde, omdat het vereiste toezichthoudende orgaan er nog niet is. Dit zijn tot dusver de enige codes die (bijna) de eindstreep hebben gehaald. Het is goed te wijzen op artikel 40, eerste lid AVG, dat zowel bij de toezichthouder als de lidstaat en de commissie en de EDPB de verantwoordelijkheid legt de totstandkoming van gedragscodes te stimuleren. In de AVG-evaluatie door de Europese Commissie wordt hiervoor dan ook aandacht gevraagd.

Om de totstandkoming van het aantal gedragscodes en het vragen van de goedkeuring daarvan te vergroten, zou overwogen kunnen worden, zoals in paragraaf 6.2.1 naar voren werd gebracht, om in sectorale wetgeving het hebben van een goedgekeurde gedragscode te verplichten en te komen tot een op de praktijkgerichte handleiding, waarin het door de AP gehanteerde normenkader voor sectoren inzichtelijk wordt gemaakt. Daar staat tegenover dat een verplichting vooral goed gaat werken wanneer de organisatiegraad in een sector groot is en de toepasselijke wetgeving overzichtelijk van aard is.

6.4 Uitvoerbaarheid van de normen in de UAVG

6.4.1 Algemeen

Een van de onderzoeksvragen betreft de vraag hoe juristen en verwerkers van persoonsgegevens de uitvoerbaarheid van de UAVG beoordelen. Om deze vraag te beantwoorden hebben we veel interviews gehouden. Zoals blijkt uit de inleiding hebben we de kring van geïnterviewden uitgebreid zodat we niet alleen met mensen hebben gesproken die uit hoofde van hun professie dagelijks de AVG en UAVG ter hand nemen. Opvallend terugkerend element in deze gesprekken is de onbekendheid met de UAVG. Daar waar de AVG een grote bekendheid geniet onder juristen, al dan niet gecombineerd met een juist begrip daarvan, is de UAVG nauwelijks bekend. Respondenten geven aan dat zij bij juridische vragen eerder teruggrijpen op artikel 8 EVRM, het verbod op discriminatie (als het gaat om bijzondere categorieën van persoonsgegevens) en de AVG. Dit blijkt ook uit uitspraken van rechters die materieel over vraagstukken gaan die de UAVG probeert te reguleren. Voor dit onderzoek voert het te ver dit uit te werken, verwezen wordt naar de uitspraken waarin de bestuursrechter oordeelde over een besluit dat is genomen naar aanleiding van een controle die werd verricht op basis van een risicoprofiel.[250]

Systematische aandacht voor de uitvoerbaarheid van de UAVG per sector dan wel in brede zin, is er niet. Het enige dat is aangetroffen, is een rapportage van een uitvraag 'gegevensverwerking zieke werknemer'.[251] Dit maakt het lastig om verantwoorde conclusies te trekken. Ook is hierbij belangrijk welk perspectief dan centraal staat; de uitvoerbaarheid voor de betrokkenen of voor de verwerkingsverantwoordelijken? Dit is niet noodzakelijkerwijs hetzelfde. Zie het voorbeeld waarbij een minister aan de landsadvocaat heeft gevraagd of er nadere mogelijkheden zijn om regelgeving op grond van de UAVG te maken om inzageverzoeken categorisch te weigeren op grond van toezichts- en opsporingsbelangen.[252] Voor het overige verwijzen we naar de onderstaande bespreking.

Wetenschappelijk onderzoek

In artikel 89, eerste lid AVG is bepaald dat verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden onderworpen is aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene. Op zichzelf is deze bepaling al ingewikkeld zoals Ducato laat zien.[253]

Artikel 89, tweede lid AVG biedt lidstaten de mogelijkheid te voorzien in afwijkingen van de in de artikelen 15, 16, 18 en 21 genoemde rechten, behoudens de in het eerste lid van dit artikel bedoelde voorwaarden en waarborgen, voor zover die rechten de verwezenlijking van de specifieke doeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De regels voor het verwerken van persoonsgegevens voor wetenschappelijk onderzoek zijn in de UAVG op verschillende plekken neergelegd. Voor de vraag of bijzondere categorieën gegevens mogen worden gebruikt zoals gezondheidsgegevens, dan zijn de regels hiervoor op verschillende plekken neergelegd. In artikel 24 UAVG is geregeld dat het verbod om bijzondere

[250] CRvB, 8 december 2020, ECLI:NL:CRVB:2020:3294 en overwegingen van de Hoge Raad over de gevolgen van een plaats op de FSV fraudelijst, HR, 10 december 2021, ECLI:NL:HR:2021:1748
[251] *Kamerstukken II* 2020/21, 34851, nr. 24.
[252] Ministerie van Financiën 2021.
[253] Ducato 2020.

categorieën van persoonsgegevens te verwerken kan worden doorbroken. Voor onderzoek met genetische gegevens geldt artikel 28 UAVG en voor onderzoek met strafrechtelijke gegevens geldt 32, onder f UAVG. Vervolgens zijn er uitzonderingen mogelijk voor academische uitdrukkingsvormen. In artikel 43, derde lid UAVG is bepaald dat het verbod om bijzondere categorieën van persoonsgegevens te verwerken of strafrechtelijke gegevens, niet van toepassing zijn voor zover de verwerking van de in die artikelen bedoelde gegevens noodzakelijk is voor de academische uitdrukkingsvorm. Vervolgens biedt artikel 44 UAVG een uitzondering voor instellingen of diensten voor wetenschappelijk onderzoek of statistiek om artikelen 15, 16 en 18 van de verordening buiten toepassing te laten.

6.4.2 Medisch wetenschappelijk onderzoek

Gedurende de coronacrisis werd veelvuldig de vraag gesteld op welke wijze wetenschappelijk onderzoek kon worden uitgevoerd in overeenstemming met de bescherming van persoonsgegevens.[254] In het medisch-wetenschappelijke onderzoek gelden daarnaast meer wettelijke regels dan de AVG en UAVG. Ook de WGBO is van toepassing. Uit onderzoek van NIVEL blijkt dat binnen de EU een grote variatie is aan regels over medisch wetenschappelijk onderzoek maar ook dat Nederland minimaal gebruik maakt van de mogelijkheden die de AVG biedt.[255]

Volgens Van den Boom is artikel 24 UAVG ronduit ‘problematisch’ voor onderzoekers in het medisch wetenschappelijke onderzoeksveld.[256] Hij doelt daarmee op de eis om vooral in te zetten op het verkrijgen van toestemming van betrokkenen. Hooghiemstra & Lokin waarschuwden voor misinterpretatie van regels die de uitvoering hinderen maar geen juridische grond hebben, maar pleiten daarnaast ook voor een verruiming van de mogelijkheden om persoonsgegevens te verwerken voor medisch-wetenschappelijk onderzoek alsmede voor secundair, historisch en kwaliteitsonderzoek.[257]

Een blik in het beslisplan en stroomschema dat ontwikkeld is voor onderzoekers van Universiteit Twente laat zien dat het voor de uitvoering op z’n zachts gezegd niet heel overzichtelijk is.[258] Dit wordt bevestigd door de rapporteur AVG die in de beschrijving van de casus Kankeronderzoek observeert dat het beter was geweest als de AVG in relatie tot medisch-wetenschappelijk onderzoek helder en haalbaar zou zijn geregeld, zowel via de AVG alsmede de UAVG. [259]

Naast artikel 24 UAVG biedt artikel 7:458 Burgerlijk Wetboek (BW) – de WGBO zijnde een lex specialis ten opzichte van de UAVG – een mogelijke juridische grondslag om patiëntgegevens te verwerken voor medisch-wetenschappelijk onderzoek en statistiek in het belang van de volksgezondheid, zoals onderzoek in verband met de coronacrisis. Naast dezelfde hoofdregel als in artikel 24 UAVG dat als dat redelijkerwijs mogelijk is toestemming dient te worden gevraagd bij de patiënt, biedt artikel 7:458 BW een geen-bezwaar-systeem indien toestemming toch niet redelijkerwijs mogelijk blijkt te zijn. Het delen van gegevens dient dan te gebeuren op basis van coderen/pseudonimiseren). Daarnaast is een voorwaarde van artikel 7:458 BW dat mensen goed geïnformeerd worden, zodat zij in staat zijn om bezwaar te maken. Goede informatieverstrekking ligt ten grondslag aan het verkrijgen van zowel het verkrijgen van toestemming, als aan de bezwaarregeling in de WGBO.

[254] Ministerie van Volksgezondheid, Welzijn en Sport 2021.
[255] European Commission DG Health and Food Safety 2021.
[256] Van den Boom 2020.
[257] Hooghiemstra & Lokin 2021.
[258] Universiteit Twente 2021.
[259] Rapporteur 2021, p. 10.

De AVG biedt de wetgever de mogelijkheid om medisch wetenschappelijk onderzoek en statistiek en ook ander onderzoek en statistiek bij wet te regelen.

Het wetsvoorstel kwaliteitsregistraties zorg regelt het secundair gebruik van medische gegevens in de zorg, niet ten behoeve van wetenschappelijk onderzoek, maar ten behoeve van 'leren en verbeteren en samen beslissen'.[260] Hiermee wordt door de wetgever dus ook voor aankomende wetgeving, naast de al lang bestaande WGBO (uit 1995) nadrukkelijk voor een sectorale oplossing gekozen en wordt de algemene route van de UAVG verlaten. Hoe voorstelbaar ook, voor de overzichtelijkheid en uitvoerbaarheid op het terrein van onderzoek in de zorg is dit niet bevorderlijk.

Een van de respondenten wees op het probleem dat artikel 24 UAVG spreekt van onderzoek dat een algemeen belang moet dienen. Dit leidt tot de vraag of belangrijk toegepast onderzoek, zoals onderzoek naar het verbeteren van een MRI-apparaat, wel of niet onder algemeen belang valt. Bij de WGBO, artikel 7:458 BW wordt het belang van de volksgezondheid centraal gesteld. Daarbij is discussie mogelijk over de vraag wat nog wel en niet meer daaronder valt. Denk aan: verkeersveiligheid, is dat volksgezondheid?

Bovenstaande doet niet af aan soortgelijke problemen voor andere wetenschappelijke, historische onderzoeken of het verwerken van statistische doeleinden. Er zijn diverse oplossingsrichtingen mogelijk waarbij een uitstapje naar andere EU-lidstaten al veel verheldering en inspiratie kan bieden. In onze ogen blinkt de Luxemburgse oplossing uit in eenvoud en betere uitvoerbaarheid. In artikel 65 van de Uitvoeringswet in Luxemburg zijn aanvullende eisen neergelegd voor wetenschappelijk, historisch of statistisch onderzoek waarbij van de verwerkingsverantwoordelijke wordt verwacht de daarin genoemde maatregelen te implementeren.[261]

6.5 Geautomatiseerde besluitvorming

Uit de memorie van toelichting bij de UAVG blijkt dat de wetgever artikel 22 AVG ziet als een verbod op profilering en geautomatiseerde besluitvorming. Weliswaar geen algemeen of absoluut verbod, maar wel een verbod.[262] De letterlijke tekst van artikel 22 AVG spreekt echter niet over een verbod. In artikel 22 AVG, dat bovendien is geplaatst in hoofdstuk III Rechten van betrokkene, staat dat de betrokkene het recht heeft om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Ook in de internationale literatuur wordt deze discussie benoemd: behelst artikel 22 AVG een recht voor betrokkene of een voorwaardelijk verbod ('qualified prohibition')?

Tosoni presenteert volgens Bygrave de meest uitgebreide analyse tot nu in dit 'right-vs-prohibition' debat.[263] Hij laat zien dat de opvatting van de wetgever mogelijk niet strookt met de tekst, de plaats en de toelichting van de Europese wet.[264]

[260] *Kamerstukken II* 2021/22, 29477, nr. 743, p.3.
[261] Artikel 65 van 'The Act of 1 August 2018 on the organisation of the National Data Protection Commission, implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), amending the Labour Code and the amended Act of 25 March 2015 stipulating the rules of remuneration and the terms and conditions for the promotion of State civil servants.'
[262] *Kamerstukken II* 2017/18, 34851, nr. 3, p. 46.
[263] Bygrave 2021.
[264] Tosoni 2021.

Over de opinie van WP29 (dat artikel 22 AVG een verbod is), stelt hij vast dat deze geen ander licht werpt op zijn analyse en dat niet valt uit te sluiten dat de opvolger van WP29, de EDPB van gedachten verandert. Uiteindelijk ligt het definitieve antwoord bij het Europees Hof van Justitie en gaat dit onderzoek niet verder in op deze vraag. Belangrijke constatering is echter wel dat een recht van de een niet gelijk is aan een verbod voor de ander.

Voor Nederland geldt daar bovenop dat de eerdergenoemde wens van de wetgever om te komen tot een beleidsneutrale uitvoeringswet zich slecht verhoudt met de interpretatie van een verbod. Artikel 15 van de Richtlijn 95/46/EG en artikel 42 Wbp kenden namelijk het recht om niet te worden onderworpen aan een geautomatiseerd besluit.

Als het wordt gezien als een recht, dan zou het gezien kunnen worden op eenzelfde wijze als het recht van inzage en het recht op verzet. De uitvoering mag voortgezet worden, maar komt er iemand langs die gebruik maakt van zijn recht, dan moet er een alternatieve route bewandeld worden: iemand heeft recht op een handmatig besluit.

Het lijkt er echter op dat, juist omdat artikel 22 AVG in Nederland wordt gezien als een verbod, de wetgever zich direct voor een groot probleem gesteld zag. Want in de samenleving bestond al op grote schaal een praktijk van geautomatiseerde besluitvorming die volgens de opvatting van de wetgever dus met ingang van 25 mei 2018 verboden zou zijn.

Vervolgens heeft de wetgever besloten ruime uitzonderingen te creëren met een beroep op de mogelijkheden uit artikel 22, tweede lid AVG. Deze zijn vastgelegd in artikel 40 UAVG. Hierin werd bepaald dat artikel 22, eerste lid AVG niet geldt als geautomatiseerde individuele besluitvorming (niet zijnde profilering) noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang. In het tweede lid is bepaald dat de verwerkingsverantwoordelijke passende maatregelen treft ter bescherming van rechten en vrijheden en gerechtvaardigde belangen van de betrokkene.

De wetgever kiest voor twee mogelijkheden, of de verwerkingsverantwoordelijke is een bestuursorgaan, of het is het niet. Daarbij hoort ook nog de onderverdeling of er sprake is van profilering of geautomatiseerde individuele besluitvorming en -als het om bestuursorganen gaat over de vraag of er sprake is van een besluit in de zin van artikel 1:3 Awb of een beslissing die iemand anderszins in aanmerkelijke mate raakt (feitelijk handelen dus).

In de memorie van toelichting is de volgende tekst opgenomen: ‘Niet in alle gevallen van geautomatiseerde besluitvorming is er sprake van het tegenwerpen van generieke kenmerken aan een persoon, of van verwerkingen van persoonsgegevens die risicovol zijn in het licht van potentiële discriminatie. Er kan ook sprake zijn van geautomatiseerde individuele besluitvorming op basis van strikt individuele kenmerken bijvoorbeeld bij gebonden besluitvorming in het kader van het toekennen van bepaalde toeslagen. Er is geen reden om bij dergelijke besluitvorming menselijke tussenkomst te vergen, omdat dit geen toegevoegde waarde heeft. Daarenboven geldt voor alle overheidsbesluiten, ook voor overheidsbesluiten op basis van geautomatiseerde besluitvorming, dat de gebruikelijke bestuursrechtelijke rechtsbescherming openstaat.’[265]

[265] *Kamerstukken II* 2017/18, 34851, nr.3, p. 120.

De uitzonderingen voor geautomatiseerde besluiten zijn dus erg ruim geformuleerd. Dit doet de vraag rijzen of de wetgever hiermee de aard en omvang van artikel 22 AVG recht heeft gedaan. De hoofdregel dat iemand het recht heeft om er niet aan te worden onderworpen, is nu geworden: het is toegestaan als het noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vulling van een taak van algemeen belang. Vervolgens zijn aan de individuele verwerkingsverantwoordelijken taken opgedragen: zij moeten maatregelen treffen die strekken tot bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. Omwille van de duidelijkheid bespreken we hierna alleen de uitwerking van artikel 40 UAVG voor bestuursorganen.

Artikel 40 UAVG voor bestuursorganen

De door de wetgever gekozen benadering betekent voor bestuursorganen een tweedeling:

1. worden er geautomatiseerde besluiten genomen waarbij in een individueel geval een wet wordt toegepast dan geldt het recht om niet daaraan te worden onderworpen, niet. Wel is het dan nodig dat de verwerkingsverantwoordelijke passende maatregelen treft ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van betrokkenen. Hierbij wordt aangenomen dat altijd bezwaar en beroep openstaat. Dat is niet per definitie het geval, denk aan het gesloten stelsel van rechtsmiddelen in het belastingrecht.[266] Ook wordt aangenomen dat het openstellen van bezwaar en beroep passen maatregelen zijn.
2. worden er geautomatiseerde besluiten genomen op basis van profielen, dan geldt het recht om daaraan niet te worden onderworpen.

De veronderstelling dat bij het nemen van geautomatiseerde besluiten door bestuursorganen voldaan is aan artikel 22 AVG omdat betrokkenen als belanghebbenden in bezwaar kunnen, werd door de Afdeling advisering van de Raad van State ter discussie gesteld. De afdeling wees erop dat in een geautomatiseerd besluitvormingsproces bepaalde persoonlijke omstandigheden niet meegewogen worden. De aan die besluitvorming inherente automatismen kunnen onder omstandigheden leiden tot disproportionele gevolgen. De Afdeling wees op de automatische boetes voor onverzekerde voertuigen en de onmogelijkheid die in dergelijke gevallen vaak bestaat om fouten met terugwerkende kracht terug te draaien. In die gevallen kunnen geautomatiseerde besluiten, anders dan de regering lijkt te veronderstellen, onbillijk uitvallen voor betrokkenen. Deze gevolgen kunnen niet worden gerechtvaardigd met het argument dat bestuursrechtelijke rechtsbescherming openstaat. Naar het oordeel van de Afdeling kan ‘een redelijke en zorgvuldige besluitvorming niet afhankelijk gemaakt worden van het al dan niet instellen van bezwaar of beroep.’[267]

Ook uit empirisch onderzoek blijkt dat de rechtsbescherming bij geautomatiseerde ketenbesluiten van bestuursorganen is afgenomen ondanks bezwaar-en beroepsmogelijkheden.[268]

Widlak stelt expliciet dat juist die gebruikelijke waarborgen, ‘en dat is alles wat we in Nederland hebben’ onvoldoende zijn.[269] De algemene uitzondering die werd gecreëerd, vindt Widlak dan ook niet in de geest van de AVG. Hij wijst erop dat het maken van bezwaar geen opschortende werking heeft, dat er beperkte bezwaartermijnen zijn en dat er niet kan worden gegarandeerd dat fouten met terugwerkende kracht worden hersteld.

[266] Soms vult de belastingrechter de leemte in, Hoge Raad 5 februari 2021, ECLI:NL:HR:2021:179.
[267] *Kamerstukken II* 2017/18, 34851, nr. 4, p. 48.
[268] Van Eck 2018.
[269] Widlak, 2021, p. 267.

De uitvoerbaarheid van artikel 40 UAVG voor bestuursorganen lijkt samen te hangen met de keuze van de wetgever om de uitwerking van de nationale bevoegdheden in een generieke wet neer te leggen. In andere landen zoals Noorwegen of Frankrijk heeft de wetgever ervoor gekozen om voor de overheid invullingen te maken in materiewetten (Noorwegen)[270] of in een samenstel van wetten, zoals door het combineren van de uitvoeringswet van de AVG met de algemene bestuursrechtwetgeving (Frankrijk)[271].[272]

Hier komt bij dat er meer belangen betrokken zijn bij het nemen van geautomatiseerde besluiten door de overheid dan het belang van bescherming van persoonsgegevens. Vanuit rechtsstatelijk perspectief kan het belangrijk zijn om naar veranderingen in macht voor de uitvoering te kijken, vanuit de beginselen van behoorlijk bestuur lijkt het logisch te kijken naar de transparantie van de beslisregels. Vanuit het beginsel van wapengelijkheid kunnen de gevolgen voor de bewijsrechtelijke verdeling beschouwd worden als een geschil over een geautomatiseerd besluit door de bestuursrechter beslecht moet worden.[273]

Uit de gesprekken die zijn gevoerd over geautomatiseerde besluiten bij de overheid, blijkt dat artikel 40 UAVG nauwelijks bekendheid geniet of wordt toegepast. En hoewel er in het bestuursrecht veel geprocedeerd wordt bij geschillen over primaire geautomatiseerde besluiten, is zelden waar te nemen dat artikel 40 UAVG (en 22 AVG) als rechtsbron wordt gebruikt. De onderzoekers vermoeden dat dit is veroorzaakt doordat er geen expliciete relatie is gelegd met sectorale wetgeving of de Algemene wet bestuursrecht. Als algemeen punt geldt dit breder voor het bestuursrecht. De geschiedenis laat zien dat het gegevensbeschermingsrecht en het bestuursrecht twee gescheiden werelden bleven.[274] Dit is dan ook geen verrassende conclusie maar wel een die met ongewijzigde keuzen niet als vanzelf tot veranderingen leidt. Berkvens' waarschuwing dat omnibuswetgeving die niet wordt ingevuld door bijzondere wetten van het begin af aan achterhaald zal zijn en lastig toe te passen, geldt dan ook nog steeds.[275] Voor geautomatiseerde besluiten en feitelijke handelingen die daaraan voorafgaan, is dit een reëel probleem.

Rechtsbescherming bij (semi) geautomatiseerde besluitvorming door bestuursorganen
Dat een belanghebbende in bezwaar kan gaan tegen een besluit wil nog niet zeggen dat deze in dezelfde procedure bescherming krijgt van de bestuursrechter tegen het schenden van belangen die door de AVG worden geborgd. We doelen hiermee op de voorbereidingsfase en de feitelijke handelingen die vooraf zijn gegaan aan het besluit.

Illustratie
Een bestuursorgaan voert een wet geautomatiseerd uit en hanteert een risicoprofiel gebaseerd op data analyses om te bepalen welke aanvragen direct geautomatiseerd worden toe- of afgewezen, en welke aanvragen eerst door een ambtenaar worden gecontroleerd. In de woorden van Binns en Veale valt de eerste routine onder 'single-step automated decision making' en de tweede onder 'multi stage profiling systems', in het bijzonder 'triaging'.[276]

[270] Zie voor een voorbeeld van de standaardbepalingen hiervoor, § 4 a, tweede zin van de Lov om arbeids- og velferdsforvaltningen (arbeids- og velferdsforvaltningsloven) [NAV-loven], https://lovdata.no/lov/2006-06-16-20/§4a.
[271] Zie artikel L 311-3-1 Code des relations entre le public et l'administration, toegevoegd door artikel 4 van de Loi pour une Republique numerique, Loi n° 2016-1321. En artikel R 311-3-1-2, Code des relations entre le public et d'administration, bij Décret van de minister-president, Décret n° 2017-330 en artikel 47 van de Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertes. https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624/#LEGIARTI000006528059.
[272] Zie Malgieri 2019 voor meer informatie.
[273] Albers 2021, p. 11-35.
[274] Zie het werk van Overkleeft-Verburg en Groothuis.
[275] Zwenne e.a. 2007, p. 66.
[276] Bins & Veale 2021.

Bezien vanuit de UAVG valt de eerste routine onder artikel 40 UAVG. De bestuursrechtelijke weg staat open voor de belanghebbende. De tweede routine is lastiger te duiden. Vaak wordt gesuggereerd dat dergelijke controles zijn toegestaan omdat er sprake is van menselijke tussenkomst.[277] Maar wat betekent dit voor de rechtsbescherming? De bestuursrechter krijgt het gevolg, het besluit ter beoordeling voorgelegd. Daaraan voorafgaand heeft de belanghebbende misschien een lijst met vragen moeten beantwoorden of is bij hem een 'huisbezoek' verricht op basis van een controlehandeling die weliswaar door een mens wordt verricht maar gestart is op basis van een profiel.

De Raad van State observeert dat deze problematiek in het verlengde ligt van de principiële discussie over het besluit begrip en de bestuursrechtelijke rechtsbetrekking. Zij stelt zelfs onomwonden dat de bestuursrechter bij algoritmische besluitvorming niet in alle gevallen rechtsbescherming kan verlenen.[278] Als een discriminerende behandeling volgend uit de profilering zich vertaalt in een juridisch juist besluit, zal de bestuursrechter er dan consequenties aan kunnen verbinden? Anders dan de burgerlijke rechter, kan de bestuursrechter het gebruik en de inzet van het algoritme in ieder geval niet onrechtmatig verklaren.[279]

In het belastingrecht ligt dit mogelijk nog beperkter zoals blijkt uit jurisprudentie van de Hoge Raad over selectieregels. Door de belastingdienst wordt op basis van selectieregels bepaald welke aangifte IB geautomatiseerd conform de aangifte resulteert in een besluit (de aanslag) en welke aangiften eerst door een ambtenaar wordt gecontroleerd. Door het nieuws over de zwarte lijst (Fraude Signalerings Voorziening) bij de belastingdienst werd bekend dat de selectieregels mede door deze informatie werden gevoed.

Los van de vraag of dit profilering is geweest in de zin van de AVG, suggereerde de advocaat-generaal (A-G) dat beroep in cassatie gegrond moet worden verklaard omdat niet kon worden vastgesteld of aangifte op rechtmatige grond was geselecteerd. Door de kwestie terug te verwijzen zou onderzoek gedaan kunnen worden naar de vraag of de selectie en dus de (voor belanghebbende negatief uitgepakte) handmatige beoordeling het gevolg was van de vermelding op de zwarte lijst. Voor belanghebbenden van wie het besluit al formele rechtskracht had, adviseerde de A-G het mogelijk te maken dat alsnog bezwaar en beroep kon worden ingesteld.[280]

De Hoge Raad volgde hem niet: in de rechtsoverwegingen ten overvloede oordeelt de cassatierechter dat schending van de AVG niet tot vernietiging van een op zich juist berekende belastingaanslag kan leiden. En de belastingrechter kan dan ook geen schadevergoeding toekennen. Dat kan namelijk alleen als de aanslag onrechtmatig is.[281]

Er zijn daarmee dus serieuze vraagtekens te stellen bij zowel het uitgangspunt van de UAVG dat de praktijk van geautomatiseerde besluiten bij de overheid voldoet aan artikel 22 AVG omdat bezwaar en beroep mogelijk is, als het uitgangspunt dat er rechtsbescherming wordt geboden bij een uitvoering die *deels* geautomatiseerd is.

Het idee dat er veel is toegestaan als de risicoprofilering leidt tot controle door een mens noemt Meuwese zelfs de 'schijnveiligheid van de voorbereidingsfase'. Zij constateert dat in

[277] Zoals in het wetsvoorstel wijziging BRP Landelijke aanpak adreskwaliteit, *Kamerstukken II* 2020/21, 35772, nr. 3, p. 34.
[278] Raad van State 2021, p. 56.
[279] Raad van State 2021, p. 58.
[280] Parket HR 17 juni 2021, ECLI: NL:PHR:2021:618.
[281] HR 10 december 2021, ECLI:NL:HR:2021:1748.

het bestuursrecht een datagedreven voorbereiding het effect kan hebben dat de voorfase en de besluitvorming in elkaar over gaan lopen.[282]

Het meest pregnant komt dit naar voren in het wetsvoorstel Landelijke aanpak adreskwaliteit waarbij de toepassing van risicoprofielen moet leiden tot een onderzoek door een ambtenaar maar dit 'vooronderzoek' tegelijk leidt tot een aantekening bij de gegevens van de betrokkene.[283] Een aantekening die gevolgen heeft omdat burgers zo van 'een onbekende hoeveelheid dienstverlening' worden afgesloten.[284]

De onderzoekers zijn van mening dat deze prangende actuele kwesties de wetgever aangaan en een mooie kans bieden om het bestuurs(proces)recht en de invulling van de AVG met elkaar te verenigen. We verwijzen daarbij ook naar hetgeen op dit punt in hoofdstuk 3 over de aansluiting (U)AVG en Awb is gesteld.

6.6 Kinderen

Artikel 8 AVG bepaalt dat als er sprake is van een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind en de verwerking van persoonsgegevens gebaseerd wordt op artikel 6, eerste lid, onder a AVG, de verwerking van persoonsgegevens van het kind alleen rechtmatig is wanneer het kind tenminste zestien jaar is en toestemming heeft gegeven. Voor jongere kinderen is de toestemming nodig van de persoon die de ouderlijke verantwoordelijkheid draagt. Lidstaten mogen jongere kinderen hierover zelf laten beslissen maar de minimumleeftijd hiervoor is dertien jaar.

Nederland heeft in de UAVG geen gebruik gemaakt van de mogelijkheid om kinderen tussen de dertien en zestien jaar zelf te laten beslissen. In de memorie van toelichting is hierover opgemerkt dat een dergelijke beleidswijziging niet paste vanwege het beleidsneutrale karakter van het wetsvoorstel.[285]

Wel is in artikel 5 UAVG geregeld dat de leeftijdsgrens van zestien jaar ook geldt als artikel 8 AVG niet van toepassing is, dus bij een andere dienstverlening dan diensten van de informatiemaatschappij. In het conceptwetsvoorstel Verzamelwet gegevensbescherming blijft dit in stand maar wordt voor sommige toestemmingen de leeftijdgrens verlaagd naar twaalf jaar. Ook het intrekken van toestemming wordt dan mogelijk vanaf twaalf jaar. Dit laat zich lastig rijmen met voornoemde mogelijkheid tot het verlagen van de leeftijd naar dertien jaar in de AVG.

De regeling wijkt af van die in andere landen die de leeftijdgrens bij een rechtstreeks aanbod van diensten van de informatiemaatschappij hebben verlaagd.[286] Landen die dit hebben gedaan lijken dan ook veel werk te maken van de weerbaarheid van kinderen zodat zij beseffen waar ze eigenlijk toestemming voor geven.[287]

Voor wat betreft de uitvoering van artikel 5 UAVG (maar dus ook artikel 8 AVG) geldt dat het voor verwerkingsverantwoordelijken niet eenvoudig is om uitvoering te geven aan deze

[282] Meuwese 2022.
[283] *Handelingen II* 2021/22, 35772, nr. 11.
[284] Widlak 2022.
[285] *Kamerstukken II* 2017/18, 34851, nr.3, p. 93.
[286] Milkaite & Lievens 2019.
[287] Zie bijvoorbeeld https://www.dubestemmer.no/.

bepaling. Dit komt omdat het noodzakelijk is te weten dat degene die de vervangende toestemming geeft, daadwerkelijk bevoegd is omdat deze het ouderlijk gezag heeft of vertegenwoordigingsbevoegd is. Dit vergt op zichzelf al het verwerken van persoonsgegevens en enige mate van controle op de gegeven informatie. Van der Hof houdt zich in Europees verband bezig met een onderzoek naar 'online age verification and parental consent'. Het doel is om te komen tot een kindgerichte oplossing.[288] Vanuit het kind bezien, is het vragen van toestemming van de ouder op een zekere leeftijd, ook een inbreuk op de persoonlijke levenssfeer.

In het Verenigd Koninkrijk heeft de Information commissioner een gedragscode opgesteld ter bescherming van de persoonsgegevens van kinderen 'Age appropriate design: a code of practice for online services.' In Frankrijk is regelgeving in de maak om de fabrikanten van producten te dwingen opties te installeren die ouderlijk toezicht mogelijk maken.[289] In Nederland is in opdracht van het ministerie van BZK de Code voor Kinderrechten ontwikkeld, bestaande uit tien beginselen met praktische voorbeelden waarmee ontwerpers en ontwikkelaars de fundamentele rechten van kinderen kunnen waarborgen in digitale diensten.

Dit neemt niet weg dat de positie van kinderen in een steeds meer digitale wereld zwak kan worden genoemd. Dit komt omdat kinderen zich enerzijds in een kwetsbare positie bevinden en anderzijds juist tot de generatie behoren waarvan het leven zich voor een groot deel online afspeelt.[290] Ouders zijn zich daarbij soms niet altijd bewust van de rol die zij spelen, denk aan de opkomst van 'mom influencers' of aan kleuters van vier die 'influencer' zijn. [291]

Tot slot is belangrijk dat in overweging 38 van de AVG wordt vermeld dat kinderen met betrekking tot hun persoonsgegevens recht hebben op specifieke bescherming, vooral voor het gebruik van persoonsgegevens van kinderen voor marketingdoeleinden of voor het opstellen van persoonlijkheids- of gebruikersprofielen en het verzamelen van persoonsgegevens over kinderen bij het gebruik van rechtstreeks aan kinderen verstrekte diensten. Al met al komt dit in de UAVG niet uit de verf.

6.7 Handhaafbaarheid van de normen in de UAVG

Handhaafbare normen zijn duidelijke normen. Een belangrijk kenmerk van de normen uit de UAVG is dat ze open zijn geformuleerd. Daarmee behoeven de normen uitleg in een concreet geval, voordat ze handhaafbaar zijn. In de UAVG is de wetgever doorgegaan op de generiek voet van de AVG. Daardoor is de mogelijkheid van een meer specifieke invulling en concretisering per domein, niet benut. Het lijkt erop dat er nu onvoldoende houvast is en veel wordt verwacht van de toezichthouder en de ontwikkeling van normen, bijvoorbeeld door gedragscodes. De evaluatie laat zien dat zo'n uitvoerings- en handhavingspraktijk maar beperkt tot stand is gekomen. De toezichthouder zet in op toezicht en handhaving aan de achterkant en niet op normuitleg, advisering en het beantwoorden van individuele vragen of standpuntbepalingen aan de voorkant.

Vanuit sectoren zijn ook slechts beperkte inspanningen geleverd om bij te dragen aan normontwikkeling. Tot nu toe is slechts een gedragscode goedgekeurd door de AP, de Data Pro gedragscode van brancheverenigingen NLDigital, waarbij bedrijven uit de ICT-sector zich kunnen

[288] News - EuConsent.
[289] Politico 2021.
[290] https://www.mediawijsheid.nl/ en voor kinderen: https://www.hoezomediawijs.nl/
[291] 'Enorme stijging minderjarige influencers in Nederland: 'Gevaar voor ontwikkeling kind', RTLnieuws.nl.

aansluiten. De AP keurde deze code goed op 27 augustus 2020. Recent, op 3 mei 2022, publiceerde de AP het goedkeuringsbesluit van de gedragscode Slim Netbeheer. Bij deze code kunnen netbeheerders zich aansluiten. Dit besluit is overigens genomen onder een opschortende voorwaarde, de gedragscode voorziet namelijk nog niet in de oprichting van een toezichthoudend orgaan, geaccrediteerd door de AP of een buitenlandse toezichthouder. Overigens is ook in andere lidstaten nog geen uitgebreide praktijk van gedragscodes tot ontwikkeling gekomen. De website van de EDPB laat zien dat enkel in Spanje, België, Duitsland en Oostenrijk, telkens één gedragscode tot stand is gekomen.[292] [293]

[292] European Data Protection Board 2019/2020. Op 20 mei keurde de Belgische toezichthouder GBA, haar eerste gedragscode goed: https://www.gegevensbeschermingsautoriteit.be/burger/de-gegevensbeschermingsautoriteit-keurt-zijn-eerste-europese-gedragscode-goed

[293]https://www.gegevensbeschermingsautoriteit.be/burger/de-gegevensbeschermingsautoriteit-keurt-zijn-eerste-europese-gedragscode-goed

7 Conclusies en aanbevelingen

7.1 Inleiding

In dit hoofdstuk ronden we het onderzoek af. Dat betekent dat we hier de centrale onderzoeksvraag beantwoorden:

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?

We presenteren in paragraaf 7.2 eerst een aantal conclusies. Vervolgens recapituleren we in paragraaf 7.3 de antwoorden op de deelvragen die in de voorgaande hoofdstukken centraal stonden. Daarbij komt ook deelvraag 15 vraag aan de orde of er aanleiding is de bevoegdheden van de AP te wijzigen, een vraag die hiervoor nog niet van een antwoord is voorzien. We sluiten af met een slotbeschouwing in paragraaf 7.4. Door het hele hoofdstuk heen formuleren we op onderdelen aanbevelingen gericht tot de wetgever en de toezichthouder.

7.2 Conclusies en aanbevelingen

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. En dat kan worden betreurd nu de in de AVG neergelegde normen voor velen lastig te hanteren zijn.

In de systematiek van het gegevensbeschermingsrecht werd in het samenstel AVG, UAVG en sectorale gedragscodes 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.

Bestuurlijke boete
Dit onderzoek ging behalve over de UAVG ook over de bestuurlijke boete en de meldplicht datalekken. Door het uitvoeren van een aantal casestudy's is getracht zicht te krijgen op de toepassing van de bestuurlijke boete en het toezicht op de naleving van de meldplicht datalekken door de toezichthouder. We zijn daarbij aanzienlijk beperkt door de aanvankelijke weigering van de AP om aan het onderzoek mee te werken. Gelukkig was de toezichthouder in een later stadium wel bereid op een geclausuleerde wijze vragen van de onderzoekers te beantwoorden, maar helaas kon daarmee het perspectief van de toezichthouder slechts op een beperkte manier in het onderzoek worden meegenomen.

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 escalatie, maar werden toezichtsinstrumenten, waaronder de bestuurlijke boete, ingezet. 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.

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.

Uitzonderingsgrond verwerking biometrische gegevens
De onderzoeksbevindingen wijzen erop dat de uitzonderingsgrond voor de verwerking van biometrische gegevens onvoldoende duidelijk is. Het conceptwetsvoorstel Verzamelwet gegevensbescherming voorziet in een nadere aanscherping en duiding wanneer de uitzonderingsgrond van toepassing is en is in dat opzicht een verbetering.

Uitzonderingsgrond verwerking strafrechtelijke gegevens
Wat betreft de persoonsgegevens van strafrechtelijke aard verhoudt de definitie in artikel 1 UAVG zich niet tot de jurisprudentie van het HvJ-EU inzake de autonome uitleg van het begrip strafbaar feit in strafrechtelijke zin. In het conceptwetsvoorstel Verzamelwet wordt voorgesteld deze definitie in de UAVG te laten vervallen. Wanneer sprake is van een persoonsgegeven van strafrechtelijke aard laat behoorlijk wat interpretatieruimte voor verwerkingsverantwoordelijken. Normuitleg door bijvoorbeeld de toezichthouder ontbreekt. De wetgever zal een nadrukkelijke rol moeten pakken waar het gaat om beantwoording van de vraag of het

wenselijk is om cross-sectorale gegevensdeling door private partijen toe te staan. Dit vergroot de duidelijkheid en de reikwijdte van de norm uit artikel 33, vijfde lid UAVG (over de voorwaarden waaronder een vergunning voor de verwerking van strafrechtelijke gegevens kan worden verleend) en helpt de werking van artikel 33, vierde lid AVG (over de verwerking ten behoeve van derden) op een heldere wijze af te bakenen.

Rechtsbescherming
In het jurisprudentieonderzoek zijn vooral uitspraken gevonden waarbij partijen zelf expliciet een op de UAVG gebaseerde stelling hebben betrokken en uitspraken waarbij een besluit van de AP voorligt waarin de UAVG aan bod komt. In andere zaken komen we de (U)AVG niet veel tegen. Rechters en partijen baseren zich dan veeleer op bepalingen uit het EVRM; de beschermende werking van de (U)AVG blijkt geen gemeengoed te zijn. Wel speelt de UAVG expliciet een rol ten aanzien van de artikelen 34 en 35 UAVG (bestuursrechtelijke en civielrechtelijke rechtsbescherming) en wanneer zich een toetsing op een uitzondering op de rechten van betrokkenen voordoet.

In een aantal uitspraken van 1 april 2020 en de uitspraak van 2 februari 2022 heeft de Afdeling bestuursrechtspraak in de UAVG door het hanteren van een ruime connexiteitseis (beperkte) ruimte gevonden om te oordelen over een onrechtmatige gegevensverwerking. Hierdoor kan de burger ook toegang tot bestuursrechtelijke rechtsbescherming krijgen wanneer een onrechtmatige gegevensverwerking bij een bestuursorgaan heeft plaatsgevonden. Dit leidt tot de volgende aanbeveling.

Het zou de rechtsbescherming van betrokkenen tegen feitelijke bestuurshandelingen op grond van de (U)AVG ten goede komen, indien de wetgever een brug weet te slaan indachtig de aangehaalde uitspraak van de Afdeling bestuursrechtspraak van de Raad van State tussen deze bestuurshandelingen en de rechtsbescherming op grond van de Awb. Daartoe zou een eerste stap kunnen worden gezet door in het verlengde van de eerder aangehaalde uitspraken van de Afdeling bestuursrechtspraak van de Raad van State artikel 8:88, eerste lid, aanhef en onder b Awb aan te passen in die zin dat de connexiteit tussen de onrechtmatige handeling van een bestuursorgaan en het daaropvolgende onrechtmatige besluit wordt losgelaten.

Een andere mogelijkheid zou kunnen zijn om in de UAVG een bepaling op te nemen die in afwijking van artikel 8:88, eerste lid, aanhef en onder b Awb beroep bij de bestuursrechter openstelt voor degene die op grond van artikel 82 AVG aanspraak stelt te maken op vergoeding van schade die het gevolg is van het onrechtmatig verwerken van persoonsgegevens en daarmee het onrechtmatig bestuurlijke handelen door een bestuursorgaan zonder dat reeds een (onrechtmatig) besluit doordat bestuursorgaan is genomen.

De verzoekschriftprocedure beperkt zich tot het bevel om een verzoek als bedoeld in de artikelen 15 tot en met 22 UAVG (rechten van betrokkene) af of toe te wijzen. Indien om aanvullende acties wordt verzocht om de onrechtmatige handeling ongedaan te maken, gaat dit de in artikel 35 UAVG weergegeven reikwijdte van de verzoekschriftprocedure te buiten en zal een dagvaardingsprocedure dienen te worden geïnitieerd. Waar voor de uitoefening van de rechten van betrokkene een laagdrempelige toegang tot de rechter geregeld is, dient voor het wegnemen van de (andere) gevolgen van de onrechtmatige verwerking een dagvaardingsprocedure te worden gestart. Een verbreding van de reikwijdte van artikel 35 UAVG in lijn met het vorenstaande draagt niet alleen bij aan een vereenvoudiging voor de betrokkene om zijn

recht te halen, maar draagt ook bij tot een effectievere bescherming van de betrokkene in verband met de verwerking van persoonsgegevens.

Aanbevolen wordt de reikwijdte van artikel 35 UAVG te verbreden, waardoor een laagdrempelige toegang van de rechtsbescherming voor betrokkenen in een verzoekschriftprocedure in een ruimere categorie van gevallen mogelijk wordt.

Op basis van de jurisprudentie heeft de betrokkene alleen recht op informatie over geautomatiseerde besluitvorming (al dan niet in het kader van een inzageverzoek), indien aan alle drie voormelde cumulatieve voorwaarden is voldaan. Dit bewijs zal hij doorgaans niet gemakkelijk kunnen leveren, juist dóór het gebrek aan informatie over de geautomatiseerde besluitvorming en de onderliggende logica, het belang ervan en de te verwachten gevolgen voor betrokkene kan de betrokkene. Uiteindelijk is het voor de betrokkene dan ook moeilijk om een beroep te doen op zijn recht om niet aan geautomatiseerde besluitvorming te worden onderworpen. De UAVG kent geen bepaling, waarin in afwijking van de hoofdregel een andere verdeling van de bewijslast is neergelegd. Een omkering van de bewijslast ligt, gezien de eisen van redelijkheid en billijkheid daarmee meer voor de hand. Dit mede gezien de structurele onevenwichtigheid die anders de rechtsbescherming voor betrokkene frustreert. Het toevoegen van een bepaling aan de UAVG, waarin in afwijking van de hoofdregel de bewijslast anders wordt verdeeld, is op dit moment prematuur, nu de jurisprudentie zich op dit punt nog nader moet uitkristalliseren.

Wetenschappelijk onderzoek

Het verwerken van persoonsgegevens voor wetenschappelijk onderzoek en de verschillende bepalingen in de UAVG voor het verwerken van bijzondere categorieën persoonsgegevens zijn op verschillende plaatsen in de wet neergelegd. De regels rond het verwerken van persoonsgegevens voor medisch wetenschappelijk onderzoek zijn bovendien niet alleen in de (U)AVG neergelegd. Er is ook sectorale wetgeving. Soms is dit historisch verklaarbaar, soms kiest de wetgever recent ook nog voor sectorale wetgeving. Dit zal de uitvoerbaarheid niet bevorderen.

De wetgever wordt aanbevolen de bepalingen over het verwerken van persoonsgegevens voor wetenschappelijk onderzoek geclusterd in de UAVG op te nemen.

Geautomatiseerde besluiten

Vanwege de reikwijdte van artikel 22 AVG is bij deze evaluatie het onderzoek beperkt naar de uitvoerbaarheid van artikel 40 UAVG voor besluiten die worden genomen door bestuursorganen. Er zijn hierbij meerdere problemen voor de uitvoerbaarheid gesignaleerd: de wetgever is ervanuit gegaan dat het kunnen instellen van bezwaar voldoende is om aan artikel 22 AVG te voldoen bij (deels) geautomatiseerde besluiten. Bovendien is, mede door het besluitbegrip in het algemeen bestuursrecht, de beslissing om (deels) geautomatiseerd de uitvoering vorm te geven niet gereguleerd terwijl dit gevolgen heeft die bovenindividueel zijn. Het feitelijk handelen blijft daarom grotendeels buiten beeld. Dat leidt tot de volgende aanbeveling.

Aanbevolen wordt het hiaat tussen de AVG en de Awb te dichten door te kiezen voor een andere invulling van artikel 22 AVG in de UAVG.

Kinderen
De UAVG kent geen nadere normstelling voor de bescherming van de positie van kinderen bij het verwerken van hun persoonsgegevens, gebaseerd op artikel 6, eerste lid, onder a AVG. Volgens artikel 8 AVG is de verwerking van persoonsgegevens als er sprake is van een rechtstreeks aanbod van diensten van de informatiemaatschappij aan een kind alleen rechtmatig wanneer het kind tenminste zestien jaar is en toestemming heeft gegeven. Voor jongere kinderen is de toestemming nodig van de persoon die de ouderlijke verantwoordelijkheid draagt. Lidstaten mogen jongere kinderen hierover zelf laten beslissen maar de minimumleeftijd hiervoor is dertien jaar. In het conceptwetsvoorstel Verzamelwet gegevensbescherming wordt voor sommige toestemmingen de leeftijdgrens verlaagd naar twaalf jaar. Ook het intrekken van toestemming wordt dan mogelijk vanaf twaalf jaar. Dit laat zich lastig rijmen met de mogelijkheid tot het verlagen van de leeftijd naar dertien jaar, zoals bepaald in de AVG. Gezien overweging 38 van de AVG lijkt de bescherming van de persoonsgegevens van kinderen niet uit de verf te komen in de UAVG.

Aanbevolen wordt de voorgenomen wijziging in het wetsvoorstel Verzamelwet gegevensbescherming op het punt van de verlaging van de leeftijdsgrens voor sommige toestemmingen naar twaalf jaar te heroverwegen.

Handhaafbaarheid
De normen uit de UAVG zijn open geformuleerd en behoeven dus uitleg in een concreet geval, voordat ze handhaafbaar zijn. In de UAVG is de wetgever doorgegaan op de generiek voet van de AVG. Daardoor is de mogelijkheid van een meer specifieke invulling en concretisering per domein, niet benut. Daarmee verschuift de nadruk naar de toezichthouder en naar het sectoraal ontwikkelen van gedragscodes. De evaluatie laat zien dat de toezichthouder inzet op toezicht en handhaving aan de achterkant en niet op normuitleg, advisering en het beantwoorden van individuele vragen of standpuntbepalingen aan de voorkant. Gedragscodes zijn slechts zeer beperkt tot ontwikkeling gekomen, waardoor anders dan gehoopt, de handhaafbaarheid niet is verbeterd. AP en EDPB publiceren richtlijnen voor gedragscodes. Een hierop gericht aanbeveling luidt als volgt.

Aanbevolen wordt in de UAVG voor te schrijven dat de toezichthouder een normenkader publiceert dat houvast geeft voor het opstellen van sectorale gedragscodes.

7.3 Beantwoording onderzoeksvragen

In hoofdstuk 1 is een zestiental deelvragen geformuleerd. Bij de inleiding bij de hoofdstukken 2 tot en met 6 is telkens aangegeven welke deelvragen in dat specifieke hoofdstuk aan de orde komen en van een antwoord worden voorzien. We geven een samenvattend antwoord op de vragen zonder ze telkens afzonderlijk te behandelen.

Het onderzoek laat zien dat de duidelijkheid en toegankelijkheid van de UAVG kritisch wordt beoordeeld. Al eerder is daarover opgemerkt dat mede de ‘beleidsneutrale’ invulling van de wet en de korte tijd waarin deze tot stand moest komen daartoe hebben 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 deze rapportage 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.

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, zijn daarover opmerkingen gemaakt, bijvoorbeeld over de bepalingen over geautomatiseerde besluiten en over wetenschappelijk onderzoek (zie ook hiervoor 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.

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. FG's worden kennelijk gehinderd door de vrees dat contact met de AP kan leiden tot interventies of versterkte controle.

Het is niet gelukt de toezichtstrategie en het handhavingsbeleid van de AP in het onderzoek te achterhalen. De toezichthouder zelf spreekt over risicogericht toezicht, maar de onderzoekers hebben niet kunnen vaststellen hoe dat toezicht er in de praktijk uit ziet. Er is geen gepubliceerd toezichts- en handhavingsbeleid, anders dan bij veel andere toezichthouders het geval is. In het onderzoek is een aantal gevallen bestudeerd waarin sprake was van de oplegging en een bestuurlijke boete. De vergelijking van die gevallen heeft niet goed duidelijk kunnen maken hoe de AP de hoogte van de boetes vaststelt. Er zijn boetebeleidsregels vastgesteld

waarin AP factoren opsomt die bij de berekening van de boete kunnen worden betrokken. Maar daarover stelt de AP: 'Het vaststellen van een boete is, gelet op voornoemde factoren en de weging daarvan die is toegespitst op de voorliggende zaak, geen mathematische exercitie.' Het boete-instrument is zonder twijfel een belangrijk instrument waarvan op de onder toezicht gestelden een generaal-preventieve werking uitgaat. De boetebedragen zijn stevig en maken indruk. Er is geen reden om wijziging te brengen in bevoegdheden van de AP, zoals een van de deelvragen luidt. Wel is een advies aan de AP meer duidelijkheid te verschaffen over de wijze waarop zij van haar bestaande bevoegdheden gebruik maakt.

De AP wordt aanbevolen toezichts- en handhavingsbeleid te ontwikkelen zodat kenbaar wordt op welke wijze de toezichthouder van haar bevoegdheden gebruik maakt.

7.4 Slotbeschouwing

Het is niet eenvoudig een eenduidige en algemene beschouwing op het functioneren van de UAVG te geven. Dat wordt in sterke mate veroorzaakt door het karakter van de wet. Die is aanvullend op de AVG en voor een belangrijk deel een voortzetting van regelgeving die er voor de AVG ook al was. Er is niet of nauwelijks sprake van een samenhangende regeling. Eerder is sprake van een catalogus aan normen, die onderling geen eenheid vormen.

Een tweede reden waarom een sluitende slotbeschouwing op de UAVG, de toepassing van de wet en de handhaafbaarheid daarvan lastig is, heeft te maken met een beperkte medewerking van de toezichthouder aan het onderzoek. Daardoor moest om de AP heen worden gewerkt bij het doen van casestudy's en het benaderen van FG's. Maar vooral ook de invalshoek van de AP zelf kon daardoor slechts in beperkte mate in de bevindingen doorklinken.

Dat neemt niet weg dat wel een beeld te geven is van de werking van de UAVG. Dat beeld is dat sprake is van een regeling die bestaat uit open normen die zich in de praktijk niet altijd eenvoudig laten toepassen. Dat neemt niet weg dat in de loop van de jaren wel meer helderheid in de toepassing van een aantal van de bepalingen is gekomen, onder meer door jurisprudentie, maar ook door de toezichthouder, al dan niet op Europees niveau. Van de Verzamelwet Gegevensbescherming wordt een volgende slag in de verduidelijking en aanscherping van de normen verwacht.

Het samenstel van AVG, UAVG, bijzondere wetgeving en sectorale gedragscodes zou voldoende handvatten moeten opleveren voor de praktijk van het gegevensbeschermingsrecht. Tegen die achtergrond is het te betreuren dat gedragscodes niet of nauwelijks van de grond zijn gekomen. Behalve in dat samenstel van regelingen, is het ook van belang vast te stellen dat ook in sectorale wetgeving uitzonderingen op verwerkingsverboden zijn opgenomen. Dat leidt tot de volgende aanbeveling.

Het is wenselijk dat de wetgever beziet hoe meer eenduidigheid kan komen in wat er in de UAVG en wat in sectorale wetgeving aan uitzonderingen opgenomen wordt. Denkbaar is een kader van algemene uitzonderingen in de UAVG en (sector)specifieke uitzonderingen op het verwerkingsverbod in sectorale wetgeving.

Dit laatste punt hangt ook samen met een ander punt van wetgevingssystematiek. In afwijking van het 'overschrijfverbod' zijn (mede omdat overweging 8 van de AVG dat mogelijk maakte) bepaalde elementen van de AVG overgenomen in de UAVG. De onderzoekers constateren dat deze wetgevingsarchitectuurkeuze niet heeft geleid tot meer duidelijkheid over de normstelling en kunnen zich een heroverweging op dit punt goed voorstellen.

Aanbevolen wordt het overnemen van elementen van de AVG in de UAVG te heroverwegen nu dat niet tot meer duidelijkheid voor de uitvoeringspraktijk heeft geleid.

Een specifiek punt is dat de onderzoekers zich afvragen of artikel 41, tweede lid UAVG recht doet aan artikel 23, tweede lid AVG. Artikel 41, tweede lid UAVG laat aan de verwerkingsverantwoordelijke om rekening te houden met de in artikel 23 genoemde aspecten bij de afweging om te komen tot het buiten toepassing laten van de rechten en verplichtingen van artikel 12 tot en met 21 AVG. Dit leidt tot de volgende aanbeveling.

De onderzoekers adviseren om te bezien of meer recht gedaan kan worden aan artikel 23 AVG door bij of krachtens sectorale wetgeving de rechten van betrokkenen op maat te beperken in plaats van in algemene zin en door deze verantwoordelijkheid te leggen bij de verwerkingsverantwoordelijke zelf ten aanzien van de eigen verwerking. [294]

Dit onderzoek betrof naast de UAVG ook de boetebevoegdheid en de meldplicht datalekken. De onderzoeksbevindingen wijzen erop dat beide instrumenten nuttige instrumenten 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. Hiervoor is reeds gewezen op de wenselijkheid om toezichts- en handhavingsbeleid vast te stellen waarin de bestuurlijke boete een plaats krijgt in het escalatiemodel van de AP, hetgeen veel duidelijkheid kan 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. Voor wat betreft de meldplicht valt op dat de inzet van de toezichthouder zich in sterke mate concentreert op het toezicht op meldingen en veel minder op niet-melden. Risicogericht toezicht, dat de AP stelt na te streven, zou juist een focus op grote risico's met zich meebrengen en die schuilen vermoedelijk juist in de categorie niet-melders.

[294] Zie op dit punt ook Autoriteit Persoonsgegevens 2020-2.

Bijlage 1: Geraadpleegde bronnen

Literatuur

Albers 2021
C.L.G.F.H. Albers, 'Digitaal bewijs in het bestuursrecht…. Over geautomatiseerde besluitvorming, efficiency en een rechtsbeschermingsvacuüm', in: P.T.J. Wolters, R.M. Hermans, A.U. Janssen & P. Ortolani, *Digitalisering en conflictoplossing (O&R nr. 130)*, Deventer: Wolters Kluwer 2021.

Autoriteit Persoonsgegevens 2016
Autoriteit Persoonsgegevens, *Jaarverslag 2015,* Den Haag: april 2016.

Autoriteit Persoonsgegevens 2017
Autoriteit Persoonsgegevens, *Jaarverslag 2016,* Den Haag: mei 2017.

Autoriteit Persoonsgegevens 2017-2
Autoriteit Persoonsgegevens, *Praktijkgids Patiëntgegevens in de cloud*, Den Haag: juli 2017.

Autoriteit Persoonsgegevens 2018
Autoriteit Persoonsgegevens, *Jaarverslag 2017,* Den Haag: april 2018.

Autoriteit Persoonsgegevens 2019
Autoriteit Persoonsgegevens, *Grip op persoonsgegevens. Jaarverslag 2018,* Den Haag: 2019.

Autoriteit Persoonsgegevens 2019-2
Autoriteit Persoonsgegevens, *Hoe opereert de FG in het ziekenhuis? Onderzoek naar de positie en taakuitoefening van functionarissen voor de gegevensbescherming in elf ziekenhuizen*, Den Haag: juni 2019.

Autoriteit Persoonsgegevens 2020
Autoriteit Persoonsgegevens, *Normuitleg grondslag 'gerechtvaardigd belang'*, Den Haag: januari 2020, te raadplegen via : https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf (voor het laatste geraadpleegd op 16 februari 2022).

Autoriteit Persoonsgegevens 2020-2
Autoriteit Persoonsgegevens, *Advies over het concept voor een wetsvoorstel Verzamelwet gegevensbescherming (Inventarisatie eerste ervaringen UAVG)*, november 2020.

Autoriteit Persoonsgegevens 2021
Autoriteit Persoonsgegevens, *Jaarverslag 2020,* Den Haag: april 2021.

Bins & Veale 2021
R. Bins & M. Veale, 'Is that your final decision? Multi-Stage Profiling, Selective Effects, and article 22 of the GDPR', *International Data Privacy Law* Volume 11 issue 4 2021, p. 319-332.

Bos, van den & Van der Velden 2013
K. van den Bos & L. van der Velden, 'Legitimiteit van de overheid, aanvaarding van overheidsbesluiten en ervaren procedurele rechtvaardigheid.' *Prettig Contact met de Overheid 4*. Den Haag: 2013

Bygrave 2021
L. Bygrave, 'Article 22 Automated individual decision making, including profiling' in: C. Kuner, L. Bygrave & C. Docksey, *The EU General Data Protection Regulation: A commentary. Update of Selected Articles*, Oxford: Oxford University Press, May 2021, p. 96-101.

Berkvens 2021
J.M.A. Berkvens, 'Wat is (g)een strafrechtelijk gegeven?', *P&I* 2021/4.

Van den Boom 2020
R. Van den Boom, 'Herziening van de UAVG', *OpenRecht* 12 augustus 2020.

College Bescherming Persoonsgegevens 2010
College Bescherming Persoonsgegevens, *Het CBP in 2009,* Den Haag: april 2010.

College Bescherming Persoonsgegevens 2013
College Bescherming Persoonsgegevens, *Jaarverslag 2012,* Den Haag: april 2013

College Bescherming Persoonsgegevens 2014
College Bescherming Persoonsgegevens, *Het CBP in 2013,* Den Haag: maart 2014

College Bescherming Persoonsgegevens 2015
College Bescherming Persoonsgegevens, *Het CBP in 2014,* Den Haag: april 2015

College Bescherming Persoonsgegevens 2015-2
College bescherming persoonsgegevens, *Onderzoek naar het gebruik van identiteitsdocument-scanners in de horeca - Rapport definitieve bevindingen*, Den Haag: augustus 2015

Comité van de Regio's 2012
Comité van de Regio's, *Advies van het Comité van de Regio's — Het pakket gegevensbescherming* (2012/C 391/13).

Data Protection Working Party 2018
Data Protection Working, *Party Guidelines on Personal data breach notification under Regulation 2016/679, WP 250*, 6 februari 2018.

Ducato 2020
R. Ducato, 'Data protection, scientific research, and the role of information', *Computer Law & Security Review*, Volume 37, 2020, 105412, ISSN 0267-3649.

Van Eck 2018
B.M.A. Van Eck, *Geautomatiseerde ketenbesluiten & rechtsbescherming. Een onderzoek naar de praktijk van geautomatiseerde ketenbesluiten over een financieel belang in relatie tot rechtsbescherming*. (Diss. Tilburg University), Tilburg: Tilburg University 2018.

Groep Gegevensbescherming Artikel 29 2014
Groep Gegevensbescherming artikel 29, *Advies 06/2014 over het begrip 'gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke' in artikel 7 van Richtlijn 95/46/EG' (WP217)* 9 april 2014.

Groothuis 2014
M. Groothuis, *Beschikken en digitaliseren: over normering van de elektronische overheid* (Diss. Universiteit Leiden), Leiden: Universiteit Leiden 2014.

Europese Commissie 2010
Europese Commissie, *Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's. "Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie"* (COM (2010) 609 definitief).

European Commission 2012
European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM (2012) 11 final).

European Commission 2020
European Commission, *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation* (COM(2020) 264 final).

European Commission DG Health and Food Safety 2021.
European Commission DG Health and Food Safety, *Assessment of the EU Member States' rules on health data in the light of GDPR,* 2021.

European Data Protection Board 2019
European Data Protection Board, *Richtsnoeren 1/2019 voor gedragscodes en toezichthoudende organen in de zin van Verordening 2016/679*, 4 juni 2019.

European Data Protection Board 2020
European Data Protection Board, *Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur*, 29 januari 2020.

European Data Protection Board 2019/2020
European Data Protection Board, *Register for Codes of Conduct, amendments and extensions*.

European Data Protection Board 2021

European Data Protection Board, *Guidelines 01/2021 on Examples regarding Data Breach Notification*, 14 december 2021.

European Data Protection Board 2022
European Data Protection Board, *Guidelines 04/2022 on the calculation of administrative fines under the GDPR*, 12 mei 2022.
Groenhart 2021
N.W. Groenhart, 'De Uber/Ola- uitspraken', *Tijdschrift voor Internetrecht*, 2021/5.

Hoboken e.a. 2020
Hoboken e.a., *Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content*, Amsterdam: Universiteit van Amsterdam 1 september 2020.

Malgieri 2019
G. Malgieri, 'Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations.', *Computer Law & Security Review* 2019/35, issue 5.

Meuwese 2022
A. Meuwese, 'Artificiële Intelligentie en bestuursrecht: menselijk en digitaal', *NTB* 2022/37.

Overkleeft-Verburg 1995
G. Overkleeft-Verburg, *De Wet persoonsregistraties: norm, toepassing en evaluatie*, Tilburg: Tilburg Univeristy 1995.

Overkleeft-Verburg 2009
G. Overkleeft-Verburg, 'Basisregistraties en rechtsbescherming. Over de dualisering van de bestuursrechtelijke rechtsbetrekking', *NTB* 2009/4.

Raad van State 2021
Raad van State, *Digitalisering. Wetgeving en bestuursrechtspraak*, Den Haag: mei 2021.

Raad van State 2020
Raad van State, *Advies over de Verzamelwet gegevensbescherming*, Den Haag: mei 2022.

Rapporteur 2021
Rapporteur Twee jaar toepassing van de AVG, *Verslag Rapporteur Twee jaar toepassing van de AVG*, 15 januari 2021, 2021D02008, aangeboden aan Tweede Kamer.

Tosoni 2021
L. Tosoni, 'The right to object to automated individual decisions: resolving the ambiguity of article 22 (1) of the General Data Protection Regulation', *International Data Privacy Law* 2021/11, issue 2, p. 145–162.

Universiteit Twente 2021
Universiteit Twente, *Beslishulp en Stroomschema Universiteit Twente, 'Zorgvuldig gebruik van persoonsgegevens in onderzoek volgens de AVG,* 19-11-2021.

Van der Sloot e.a. 2020
B. Van der Sloot e.a., *Op het eerste gezicht: Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*, Den Haag: WODC maart 2020.

Van der Sloot e.a. 2020-2
B. Van der Sloot e.a., 'Gezichtsherkenning in Nederland: een toekomstperspectief', *Tijdschrift voor Internetrecht*, 2020/6.

Wárlám 2015
I.M. Wárlám, 'De Belastingdienst met het BSN niet omdopen tot BTW-nummer', *Privacy & Informatie*, 2015/5, p. 172-178.

Widlak 2021
A.C. Widlak, *Volwassen Digitale Overheid*, Den Haag: Boom Bestuurskunde 2021.

Widlak 2022
A.C., 'Tucht bij voorschot', *AG Connect* 9 februari 2022.

WP29-opinie WP 253
WP29, WP253, *Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten in de zin van Verordening (EU) 2016/679*", 3 oktober 2017.

Zwenne e.a. 2007
G.J. Zwenne ea, '*Eerste fase evaluatie Wet bescherming persoonsgegevens*.' Den Haag: WODC 2007.

Besluiten en brieven Autoriteit Persoonsgegevens

Besluit Autoriteit Persoonsgegevens 19 juni 2019
Besluit z2018-12010, Autoriteit Persoonsgegevens 19 juni 2019 (Besluit inzake de vergunningaanvraag voor de verwerking van gegevens van strafrechtelijke aard ten behoeve van derden van de verwerking 'Fraudehelpdesk' van Safecin).

Besluit Autoriteit Persoonsgegevens 1 april 2020
Besluit z2021-03355, Autoriteit Persoonsgegevens 1 april 2020.

Besluit Autoriteit Persoonsgegevens 5 augustus 2021
Besluit z2021-12229, Autoriteit Persoonsgegevens 5 augustus 2021 (Bulkbesluit inzake de vergunningaanvragen voor de verwerking van gegevens van strafrechtelijke aard ten behoeve van derden van de verwerking 'Collectief Winkelverbod' door de in de bijlage genoemde winkeliers van het winkelgebied Amsterdam The Style Outlets).

Besluit Autoriteit Persoonsgegevens 8 oktober 2021
Besluit z2021-12791, Autoriteit Persoonsgegevens 8 oktober 2021 (besluit inzake de vergunningaanvraag voor de verwerking van persoonsgegevens van strafrechtelijke aard ten behoeven van derden van de verwerking 'Frauderegistratiesysteem' van de Vereniging Veilig Ondernemen Door Informatie Op Maat (VODIOM)).

Boete Booking.com
Boetebesluit Booking.com, Autoriteit Persoonsgegevens december 2020, te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf.

Boete BKR

Boetebesluit BKR, Autoriteit Persoonsgegevens juli 2019, te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf.

Boete PVV Overijssel
Boetebesluit PVV Overijssel, Autoriteit Persoonsgegevens juni 2020, te raadplegen via: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_pvv_overijssel.pdf.

Boete Transavia
Boetebesluit Transavia, Autoriteit Persoonsgegevens september 2021, te raadplegen via: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_transavia.pdf.

Boete vingerafdrukken personeel
Boetebesluit vingerafdrukken personeel, Autoriteit Persoonsgegevens december 2019, te raadplegen via: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf.

Brief aan Centraal Bureau Levensmiddelenhandel
Brief aan Centraal Bureau Levensmiddelenhandel, Autoriteit Persoonsgegevens mei 2020, te raadplegen via:
https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_regels_voor_gezichtsherkenning_in_supermarkten.pdf.

Eindbrief GGD GHOR en GGD'en
Eindbrief onderzoek beveiliging persoonsgegevens GGD GHOR en GGD'en, Autoriteit Persoonsgegevens november 2021, te raadplegen via:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_beveiliging_ggd_corona.pdf.

Online bronnen en nieuwsberichten

Coreon 2022
'Gedragscode Gezondheidsonderzoek gereed', Coreon.nl 24 januari 2022.

Cijfers datalekken 2018
'Cijfers datalekken 2018', Autoriteitpersoonsgegevens.nl.

Cijfers datalekken 2020
'Cijfers datalekken 2020', Autoriteitpersoonsgegevens.nl.

Cijfers datalekken 2021
'Cijfers datalekken 2021', Autoriteitpersoonsgegevens.nl

Feiten en cijfers over de AP
'Feiten en cijfers over de AP', Autoriteitpersoonsgegevens.nl.

European Data Protection Board 2019-2020
'Register for Codes of Conduct, amendments and extensions', Edpb.europa.eu.

Enorme stijging minderjarige influencers in Nederland: 'Gevaar voor ontwikkeling kind',

‘Enorme stijging minderjarige influencers in Nederland: ‘Gevaar voor ontwikkeling kind’, RTLnieuws.nl.

Facts & Figures Meldplicht Datalekken
‘Facts & Figures Meldplicht Datalekken’, QSN.nl 4 maart 2021.

Financieel Dagblad 2022
‘Zorgen over ontwrichting economie en samenleving door privacywet’, *Financieel Dagblad* 8 februari 2022.

Hooghiemstra & Lokin 2021
Hooghiemstra & Lokin, ‘Bestrijd de hardnekkige mythe rond privacy en medisch-wetenschappelijk onderzoek, NRC, 11 mei 2021.

Informatie Functionaris Gegevensbescherming
‘Functionaris Gegevensbescherming’, Autoriteitpersoonsgegevens.nl

Ministerie van Financiën 2021
Ministerie van Financiën*, Openbaar gemaakte documenten WOB verzoeken, Rechtsvragen landsadvocaat en toelichting- Inzagerecht en FSV* -, Den Haag: 27 januari 2021, te raadplegen via: https://www.rijksoverheid.nl/documenten/wob-verzoeken/2021/01/27/besluit-op-uw-wob-verzoek-fsv-zwarte-lijsten-financien.

Ministerie van Justitie en Veiligheid 2020
‘Consultatieversie Memorie van Toelichting Verzamelwet gegevensbescherming’, Internetconsultatie.nl mei 2020.

Ministerie van Justitie en Veiligheid 2020
‘*Tekst en toelichting - Verzamenwet gegevensbescherming*’, Ministerie van Justitie en Veiligheid, mei 2022.

Ministerie van Volksgezondheid, Welzijn en Sport 2021
Ministerie van Volksgezondheid, Welzijn en Sport*, Interne beleidslijn inzake het verzamelen van onderzoeksdata en doorgifte buiten EU vanwege COVID-19*, Den Haag: 14 april 2020.

Milkaite & Lievens 2019
I. Milkaite and E. Lievens, ‘Better Internet for Kids - The GDPR child’s age of consent for data processing across the EU – one year later’ Betterintetnetforkids.eu.

Nieuwsbericht Autoriteit Persoonsgegevens 2019
‘Ontwerpbesluit AP gedragscode Nederland ICT’, Autoriteitpersoonsgegevens.nl 13 augustus 2019.

Nieuwsbericht Autoriteit Persoonsgegevens 2021
‘AP ontvangt 75 datalekmeldingen na lekken in Microsoft Exchangeservers’, Autoriteitpersoonsgegevens.nl 19 maart 2021.

Nieuwsbericht Autoriteit Persoonsgegevens 2021-2
‘AP verzwaart toezicht op gemeente’, Autoriteitpersoonsgegevens.nl 6 mei 2021.

Nieuwsbericht Autoriteit Persoonsgegevens 2021-3
'AP wijst aanvraag vergunning zwarte lijst VODIOM af', Autoriteitpersoonsgegevens.nl 21 oktober 2021.

Nieuwsbericht Autoriteit Persoonsgegevens 2021-4
'GGD moet persoonsgegevens beter beschermen', Autoriteitpersoonsgegevens.nl 9 november 2021.

Olsthoorn 2022.
P. Olsthoorn, 'Hoe VoetbalTV botste met de AP', Netwerkkwesties.nl 13 maart 2022.

Prins 2022
C. Prins, 'Rutte IV: toezichtsreflex en Autoriteit Persoonsgegevens', NJB.nl 25 januari 2022.

Politico 2021
'Macron pushes parental control for internet access', Politico.eu 18 november 2021.

Vereniging Privacyrecht 2018
'Meldingen datalekken via het meldloket - aanbevelingen voor verbetering', Verenigingprivacyrecht.nl 8 november 2021.

'Wat verstaat de AVG onder bijzondere persoonsgegevens?'
'Wat verstaat de AVG onder bijzondere persoonsgegevens?' Autoriteitpersoonsgegevens.nl (https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wat-verstaat-de-avg-onder-bijzondere-persoonsgegevens-6339).

Kamerstukken

Kamerstukken II 2005/06, 26671, nr. 20.
Kamerstukken II 2010/11, Aanhangsel 2648 (Antwoord van de staatssecretaris van Financiën op vragen van Omtzigt).
Kamerstukken II 2011/12, 32761, nr. 40.
Kamerstukken II 2011/12, Aanhangsel 1219.
Kamerstukken II 2012/13, 33662, nr. 3.
Kamerstukken II 2012/13, 33662, nr. 4.
Kamerstukken II 2013/14, 31066 nr. 210.
Kamerstukken II 2014/15, 33662, nr. 9.
Kamerstukken II 2014/15, 33662, nr. 16.
Kamerstukken II 2014/15, 33662, nr. 19.
Kamerstukken II 2014/15, 33662, nr. 20.
Kamerstukken II 2015/16, 33662, nr. 20.
Kamerstukken II 2015/16, Aanhangsel 3113 (Antwoord van de staatssecretaris van Financiën).
Kamerstukken II 2017/18, 34851, nr. 3.
Kamerstukken II 2017/18, 34851-2, nr. 3.
Kamerstukken II 2017/18, 34851, nr. 4.
Kamerstukken II 2017/18, 34851, nr. 7.
Kamerstukken II 2017/18, 34851, nr. 19.
Kamerstukken II 2018/19, 32761, nr. 132.

Kamerstukken II 2018/19, 32761, nr. 135
Kamerstukken II 2018/19, 32761, nr. 576 (Brief van de minister voor Rechtsbescherming van 11 juni 2019 inzake beleidsreactie onderzoek 'Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding).
Kamerstukken II 2020/21, 34851, nr. 24 (Brief van de Minister van Sociale Zaken en Werkgelegenheid van 3 maart 2021).
Kamerstukken II 2020/21, 35772, nr. 3, p. 34
Kamerstukken II 2021/22, 29477, nr. 743.

Handelingen II 2017/18, nr. 59, item 4.
Handelingen II 2017/18, aanhangsel 1841.
Handelingen II 2021/22, 35772, nr. 11

Wet- en regelgeving

Consultatieversie Memorie van Toelichting Verzamelwet gegevensbescherming, te raadplegen via: https://www.internetconsultatie.nl/verzamelwetgegevensbescherming.

Stb. 2015, 281.

Stcrt. 1995, 140 (Gedragscode Gezondheidsonderzoek. Verklaring van overeenstemming inzake de gedragscode).
Stcrt. 2004, 82.
Stcrt. 2013, 5174 (CBP Richtsnoeren: Beveiliging van persoonsgegevens).
Strct. 2014, 34523 (Advies Raad van State nota van wijziging inzake wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken)).
Stcrt. 2015, 46128.
Stcrt. 2016, 2043 (Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015)
Stcrt. 2016, 34960 (Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015 met betrekking tot het opleggen van bestuurlijke boetes).
Stcrt. 2016, 1380 (Beleidsregels van de Autoriteit Persoonsgegevens van 12 januari 2016 met betrekking tot openbaarmaking)
Stcrt. 2019, 14586 (Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes).

NEN-ISO 27001
NEN 7510

Jurisprudentie

Rb. Amsterdam 13 november 2013 ECLI:NL:RBAMS:2013:7840.
Rb. Amsterdam 20 juni 2019, ECLI:NL:RBAMS:2019:4418.
Rb. Amsterdam 12 augustus 2019, ECLI:RBAMS:2019:6005.
Rb. Amsterdam 17 september 2019, ECLI:NL:RBAMS:2019:6817
Rb. Amsterdam 25 september 2019, ECLI:NL:RBAMS:2019:8329, *JBP* 2020/24 m.nt. K. Konings.
Rb. Amsterdam 3 december 2020, ECLI:NL:RBAMS:2020:7536.
Rb. Amsterdam 21 januari 2021, ECLI:NL:RBAMS:2021:174
Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1018.

Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1019.
Rb. Amsterdam 11 maart 2021, ECLI:NL:RBAMS:2021:1020.

Rb. Den Haag 10 oktober 2019, ECLI:NL:RBDHA:2019:13029.
Rb. Den Haag (vzr.) 13 november 2019, ECLI:NL:RBDHA:2019:12031.
Rb. Den Haag 15 mei 2020, ECLI:NL:RBDHA:2020:4789.
Rb. Den Haag 31 maart 2021, ECLI:NL:RBDHA:2021:3090.

Rb. Midden-Nederland 29 mei 2019, ECLI:NL:RBMNE:2019:2434.
Rb. Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111.

Rb. Noord-Nederland 1 maart 2021 ECLI:NL:RBNNE:2021:738

Rb. Oost-Brabant 2 maart 2022, ECLI:NL:RBOBR:2022:787

Rb. Rotterdam 14 januari 2020, ECLI:NL:RBROT:2020:293

Rb. Zeeland-West-Brabant 13 augustus 2020, ECLI:NL:RBZWB:2020:3789.

Vzr. Rb. Gelderland 29 juni 2020, ECLI:NL:RBGEL:2020:3159.

Hof Amsterdam 5 november 2019, ECLI:NL:GHAMS:2019:3966.
Hof Amsterdam 2 februari 2021, ECLI:NL:GHAMS:2021:312.

Hof Arnhem-Leeuwarden 9 november 2017, ECLI:NL:GHARL:2017:10752
Hof Arnhem-Leeuwarden 7 januari 2020, ECLI:NL:GHARL:2020:126.
Hof Arnhem-Leeuwarden 22 februari 2022, ECLI:NL:GHARL:2022:1322.

Hof Den Haag 24 december 2019, ECLI:NL:GHDHA:2019:3539.
Hof Den Haag 5 oktober 2021 ECLI:NL:GHDHA:2021:1924

HR 29 mei 2009, ECLI:NL:HR:2009:BH4720.
HR 12 juli 2011, ECLI:NL:HR:2011:BP6878, *NJ* 2012/78,
HR 3 december 2021, ECLI:NL:HR:2021:1814.
HR 10 december 2021, ECLI:NL:HR:2021:1748

Parket HR 17 juni 2021, ECLI: NL:PHR:2021:618.

ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, *JBP* 2020/56, m.nt. J.A.N. Baas.
ABRvS 1 april 2020, ECLI:NL:RVS:2020:898, *JB* 2020/104, m.nt. R.J.N. Schlössels.
ABRvS 1 april 2020, ECLI:NL:RVS:2020:899
ABRvS 1 april 2020, ECLI:NL:RVS:2020:900
ABRvS 1 april 2020, ECLI:NL:RVS:2020:901
ABRvS 1 april 2020, ECLI:NL:RVS:2020:957
ABRvS 2 februari 2022, ECLI:NL:RVS:2022:319

Gerecht van eerste aanleg van de EG 12 september 2007, T-25/04, (*González y Díez SA, SA*).

EHRM 11 november 1996, ECLI:CE:ECHR:1996:1115JUD001786291.
EHRM 17 september 2009, ECLI:CE:ECHR:2009:0917JUD001024903 (*Scoppola*)

HvJ-EU 24 november 2011, nrs. C-468/10 en C-469/10, ECLI:EU:C:2011:777 (*ASNEF*)
HvJ-EU 29 maart 2011, C-352/09 P, (*Thyssen Krupp)*
HvJ-EU 20 maart 2018, ECLI: EU:C:2018:193
HvJ-EU 22 juni 2021, ECLI:EU:C:2021:504
HvJ-EU 17 december 2020, ECLI:EU:C:2020:1054

A-G HvJ,-EU 27 januari 2017, nr. C-13/16, ECLI:EU:C:2017:43.
A-G HvJ-EU 19 december 2018, nr.C-40/17, ECLI:EU:C:2018:1039

Bijlage 2: Gesprekspartners

- Bart Jan van Ettekoven, voorzitter Afdeling bestuursrechtspraak Raad van State
- Jenneke Evers, Afdeling advisering Raad van State
- Luc Verheij, Staatsraad, Afdeling advisering Raad van State
- Eric Daalder, Staatsraad, Afdeling bestuursrechtspraak Raad van State
- Michiel Tjepkema, unithoofd kennisunit Directie bestuursrechtspraak Raad van State
- Anton Ekker, advocaat privacyrecht
- Lokke Moerel, advocaat privacyrecht
- Jan de Zeeuw, voorzitter NGFG
- Barend Bon, FG Vrije Universiteit Amsterdam
- Simon Hania, FG Uber
- Fatma Çapkurt, promovendus, Universiteit Leiden
- Bart van der Sloot, senior onderzoeker aan het Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University
- Simone van der Hof, hoogleraar aan Centrum voor recht en Digitale Technologie (eLaw), Universiteit Leiden
- Mariette Lokin, ministerie van Financiën, casestudy BTW-nummer
- Jaap Uijlenbroek, voormalig DG Belastingdienst, casestudy BTW-nummer
- Hielke Hijmans, toezichthouder België
- Joris Groen, voormalig projectleider implementatie AVG, ministerie JenV
- Just Stam, voormalig raadsadviseur in algemene dienst, ministerie JenV
- Edwin Brijder, coördinerend raadsadviseur, ministerie van JenV
- Sanne Van der velde, voormalig raadsadviseur privacy en gegevensbescherming, ministerie JenV
- Jeroen Terstegge, voorzitter commissie privacy, VNO-NCW en MKB Nederland
- Floor Terra, privacy adviseur bij Privacy Company
- Leonie van der Spek, Ilse Meyer en Marta Borrat i Frigola van de Nederlandse Vereniging van Banken
- Nadia Benaissa, juridisch beleidsadviseur bij Bits of Freedom
- Joëlle Staps, adjunct-directeur GGD GHOR NL, casestudy GGD GHOR
- Quinten Kroes, advocaat privacyrecht, casestudy VoetbalTV
- Mark Boetekees, casestudy VoetbalTV
- Maarten Hoffer, casestudy VoetbalTV
- Evert-Ben van Veen, directeur MLC Foundation, Gedragscode gezondheidsonderzoek

- Martin Boeckhout, senior consultant MLC Foundation, Gedragscode gezondheidsonderzoek
- Hester de Vries, advocaat privacyrecht, casestudy BKR
- Isabelle Wárlám, advocaat, casestudy BTW-nummer
- Drie FG's bij een bestuursorgaan en een provinciesecretaris, twee FG's bij een maatschappelijke instelling, drie FG's bij een commercieel bedrijf en één manager. Zes FG's zijn werkzaam op basis van een dienstverband en twee FG's worden ingehuurd.

Bijlage 3: Voorstel aanpassingen Verzamelwet

In het wetsvoorstel voor de Verzamelwet dat in consultatie is gebracht, zijn de onderstaande overgenomen wijzigingen voorgesteld:

- Een jongere tussen 12 en 16 jaar, een onder curatele gestelde of een betrokkene ten behoeve van wie bewind of mentorschap is ingesteld, die van mening is dat er geen verwerking van persoonsgegevens meer zou moeten plaatsvinden, kan voortaan onafhankelijk van zijn vertegenwoordiger besluiten om de toestemming in te trekken voor de verwerking van hem betreffende persoonsgegevens. Tenzij de Wet op de geneeskundige behandelingsovereenkomst zich hiertegen verzet, kunnen de rechten uit Hoofdstuk III van de AVG van jongeren tot 12 jaar door zijn wettelijk vertegenwoordiger worden uitgeoefend en vanaf 12 jaar daarnaast ook door de jongere zelf (artikel I, onderdeel C, onder 3 en 4).
- In de regeling van de benoeming van leden van de Autoriteit persoonsgegevens (AP) zijn grondslagen opgenomen om nadere regels te stellen over onder meer de noodzakelijke kwalificaties waarover een lid dient te beschikken, en de benoemingsprocedure (artikel I, onderdeel).
- Inbreuken op de artikelen in de AVG en UAVG die zien op de verwerking van persoonsgegevens van strafrechtelijke aard, kunnen voortaan eveneens worden beboet indien zij worden begaan door overheidsinstanties of overheidsorganen (artikel I, onderdeel G).
- Het verbod om bijzondere categorieën van persoonsgegevens te verwerken is niet langer van toepassing indien de verwerking noodzakelijk is voor een door een accountant te verrichten bij wettelijk voorschrift voorgeschreven controle. Voor zover het om gegevens gaat die onder het medisch beroepsgeheim vallen, dienen die eerst te worden gepseudonimiseerd. In het verlengde hiervan wordt geregeld dat onder meer ook toezichthouders van de AFM en de Nederlandse Beroepsorganisatie van Accountants bijzondere categorieën van persoonsgegevens mogen verwerken, voor zover dat noodzakelijk is voor de uitvoering van hun taken (artikelen I, onderdeel J, VIII en IX).
- In de regeling van de uitzondering op het verbod om biometrische gegevens te verwerken met het oog op de unieke identificatie van een persoon, indien de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden, is onder meer de doelbeperking expliciet gemaakt, namelijk de rechtmatige toegang tot bepaalde plaatsen, gebouwen, diensten, producten, informatiesystemen of werkprocessystemen (artikel I, onderdeel L).
- Verenigingen voor cliëntenbelangen in zorg en welzijn, zoals patiëntenverenigingen maar ook verenigingen van gehandicaptensport mogen voortaan voor intern gebruik, ook buiten het geval dat daarvoor uitdrukkelijk toestemming is

gegeven, gegevens over de gezondheid van hun leden verwerken. Voorts wordt voor het bewaren en beheren van medische dossiers ingeval van bijzondere omstandigheden bij bijvoorbeeld het faillissement van de hulpverlener een wettelijke voorziening getroffen die een grondslag geeft om deze taken aan een andere hulpverlener over te dragen (artikel I, onderdeel M).

- Aan inroeping van de in artikel 41 UAVG geboden generieke mogelijkheid voor een verwerkingsverantwoordelijke om bepaalde rechten van betrokkenen in te perken, wordt de voorwaarde verbonden dat de verwerkingsverantwoordelijke zijn afweging en de onderbouwing van meet af aan transparant maakt en de AP een afschrift krijgt van zijn besluit en de bijbehorende motivering (artikel I, onderdeel P).
- De in artikel 45 UAVG geregelde uitzondering voor archiefbewaarplaatsen om rechten van betrokkenen te moeten honoreren als het recht op correctie of het recht op vernietiging gaat ook gelden voor andere voor het publiek toegankelijke instellingen die archieven van blijvende waarde voor het algemeen en historisch belang beheren en die geen winstoogmerk hebben (artikel I, onderdeel S)
- Voor het geval dat een tijdelijke onafhankelijke onderzoekscommissie of een eenmalig adviescollege wordt ingesteld, met als opdracht om voortvarend onderzoek te doen naar een specifiek en afgebakend onderwerp van aanmerkelijk maatschappelijk belang waarbij persoonsgegevens moeten worden verwerkt, wordt in de UAVG bepaald dat in de ministeriële regeling ter instelling van deze commissie of dit adviescollege tevens een aantal onderwerpen met betrekking tot de verwerking van persoonsgegevens regelt (artikel I, onderdeel V).
- In de Wet Huis voor klokkenluiders wordt een grondslag opgenomen om bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard te mogen verwerken (artikel II).
- In de Wet op de rechtsbijstand (Wrb) wordt voorzien in de noodzakelijke grondslag om de relevante ketenpartners van het bestuur van de raad voor rechtsbijstand in staat te stellen het burgerservicenummer te gebruiken om te waarborgen dat de gegevens die zij ter uitvoering van de Wrb met het bestuur uitwisselen, ook daadwerkelijk betrekking hebben op de juiste personen (artikel VI).
- In de Wet op het financieel toezicht (Wft) wordt verduidelijkt dat financiële ondernemingen in het kader van het uitvoeren van transactiemonitoring zo nodig ook geautomatiseerd transacties kunnen blokkeren of opschorten als hiervoor aanleiding is, en wordt ook de verplichting tot het uitvoeren van transactiemonitoring zelf in de Wft opgenomen (artikel VII).
- In de Wegenverkeerswet 1994 wordt een duidelijke grondslag opgenomen voor de verwerking van de persoonsgegevens door de eigenaar of kentekenhouder, of voor de (door)verstrekking van die gegevens aan de daadwerkelijke bestuurder dan wel de houder van het motorrijtuig met het oog op het achterhalen van de bestuurder, of voor het verhaal van het reeds door de eigenaar of kentekenhouder betaalde boetebedrag (artikel XII).


pro facto