CONSIDERATI

Privacy & gegevensbescherming kennisdeling

Overzicht van recente ontwikkelingen

April 2020

De Boelelaan 7 • 1083 HJ Amsterdam • 020 737 0069 • info@considerati.com

Beste lezer,

April was in vele opzichten een roerige maand, en niet alleen vanwege het coronavirus. Terwijl de meesten van ons de hele maand vanuit huis hebben gewerkt, waarbij soms ook nog eens gebalanceerd moet worden tussen aandacht voor de kinderen en het werk, waren er ook de nodige ontwikkelingen op het gebied van privacy. Niet in de laatste plaats doordat de Autoriteit Persoonsgegevens zich roerde op verschillende dossiers rondom COVID-19. Aleid Wolfsen, voorzitter van de AP, waarschuwde voor het overboord gooien van privacy in deze coronacrisis.

Ook rondom het ontwikkelen van een app in de strijd tegen corona viel de term privacy veelvuldig. Minister van Volksgezondheid, Welzijn en Sport Hugo de Jonge riep op tot het insturen van voorstellen voor een corona-app, waarin de privacy van Nederlanders gewaarborgd was. Na een mislukt traject bleek geen van de 7 apps aan de vereisten te voldoen. Eén van de apps bleek zelfs een datalek veroorzaakt te hebben. Minister de Jonge begint opnieuw en laat zelf een app ontwikkelen.

Voor veel organisaties blijkt de coronacrisis ook een noodzaak om versneld te digitaliseren, onder andere door videobel-apps uit te rollen in de organisatie. De AP bracht hiervoor een ‘keuzehulp privacy bij videobel-apps’ uit, waarmee organisaties een inschatting kunnen maken van de privacyrisico’s van verschillende beschikbare apps. Dat dit geen overbodige luxe is blijkt wel uit alle commotie die is ontstaan rondom privacy- en securityrisico’s van Zoom; in de VS zelfs aanleiding tot een strafrechtelijk onderzoek. Ook wij hebben bij onze klanten gemerkt dat organisaties behoefte hebben aan ondersteuning, bijvoorbeeld in de vorm van het uitvoeren van DPIA’s op videobel-apps, of meer globaal advies bij de implementatie ervan.

Organisaties zetten niet alleen in op digitalisering, maar denken ook na over mogelijkheden om een veilige werkplek te garanderen voor hun werknemers. Een van de opties is het inzetten van temperatuurmeting, soms zelfs door middel van thermische camera’s. Ook hierover liet de AP van zich horen, door middel van een nieuwsbericht dat temperatuur meten niet zomaar is toegestaan. De mogelijkheden tot het temperaturen van medewerkers lijken echter ruimer dan het nieuwsbericht van de AP doet vermoeden. Het is namelijk maar de vraag of elke temperatuurmeting ook een verwerking van persoonsgegevens inhoudt.

Op de laatste dag van april kwam de AP nog met haar hoogste boete tot nu toe naar buiten, namelijk €725.000 voor het onrechtmatig inzetten van een vingerafdrukscanner.

Al met al een roerige maand, zowel in de maatschappij, als op het gebied van het privacyrecht. In deze editie van onze kennisdeling vindt u dan ook de nodige informatie die gerelateerd is aan COVID-19.

Veel leesplezier!

Bart Schermer (Partner bij Considerati)

Introductie

In dit overzicht nemen we met u de laatste ontwikkelingen in de wereld van privacy en gegevensbescherming door. Deze ontwikkelingen en updates verzamelen we op basis van, onder meer, guidelines van nationale en internationale toezichthouders, Nederlandse en internationale rechtspraak en uitspraken en nieuwsartikelen.

De informatie in dit overzicht is een selectie die op basis van de relevante ontwikkeling deze maand door Considerati is samengesteld en biedt als zodanig geen uitputtend overzicht van alle relevante updates met betrekking tot privacy- en gegevensbescherming, noch geeft dit document (juridisch) advies.

Neem contact op met Considerati als u vragen, opmerkingen of tips heeft over hoe u dit overzicht wilt verbeteren.

Het team van Considerati

INHOUD

1. EUROPEAN DATA PROTECTION BOARD (EDPB)

1.1 21STE PLENAIRE VERGADERING EDPB - BRIEF OMTRENT DE ONTWERPRICHTLIJNEN VAN DE EUROPESE COMMISSIE VOOR APPS TER ONDERSTEUNING VAN DE BESTRIJDING VAN COVID-19[1]

In de 21e Plenaire vergadering heeft de EDPB een brief aangenomen, waarmee de ontwerprichtlijnen omtrent corona-apps van de Europese Commissie ('Commissie') goed worden gekeurd. De brief is door de EDPB geschreven na een verzoek tot raadpleging van de Commissie. De ontwerprichtlijnen vormen een aanvulling op de aanbeveling van de Europese Commissie met betrekking tot corona-apps, die op 8 april is gepubliceerd[2].

Andrea Jelinek, voorzitter van de EDPB: "De EDPB is verheugd over het initiatief van de Commissie om een pan-Europese en gecoördineerde aanpak te ontwikkelen, aangezien dit zal bijdragen tot waarborging van eenzelfde beschermingsniveau ten aanzien van gegevensbescherming voor elke Europese burger, ongeacht waar hij of zij woont".

In deze brief wil de EDPB specifiek aandacht vragen voor het gebruik van apps voor de functionaliteit voor het traceren en waarschuwen van contacten, omdat hierbij – gelet op de gevoeligheid – veel aandacht moet worden besteed aan het zo veel als mogelijk beperken van de inbreuk op de privacy terwijl de verwerking wel mogelijk moet zijn met het oog op de volksgezondheid. De EDPB vindt dat de ontwikkeling van de corona-apps op een verantwoorde manier moet gebeuren, waarbij alle geïmplementeerde mechanismen voor privacy by design en privacy by default moeten worden gedocumenteerd door middel van een Data Protection Impact Assessment. Bovendien moet de broncode openbaar worden gemaakt, zodat de wetenschappelijke gemeenschap daar onderzoek naar kan doen. De EDPB is een groot voorstander van het voorstel van de Commissie dat het gebruik van dergelijke apps plaatsvindt op vrijwillige basis; een keuze die door individuen moet worden gemaakt als blijk van collectieve verantwoordelijkheid.

Ten slotte benadrukt de EDPB dat de raad van bestuur en haar leden, die belast zijn met het geven van advies en het waarborgen van de correcte toepassing van de AVG en de e-Privacy richtlijn, volledig betrokken moeten worden bij proces van uitwerking en uitvoering van deze maatregelen. De EDPB wijst erop dat het voornemen is snel richtlijnen te publiceren over het verwerken van gezondheidsgegevens voor wetenschappelijke onderzoeksdoeleinden en het gebruik van locatiegegevens en technische hulpmiddelen voor het traceren van contacten in het kader van de COVID-19 uitbraak.

1.2 23STE PLENAIRE VERGADERING EDPB – EDPB KEURT COVID-19 RICHTLIJNEN GOED[3]

De EDPB heeft in de 23e plenaire vergadering de aangekondigde richtlijnen over het verwerken van gezondheidsgegevens voor wetenschappelijke onderzoeksdoeleinden en het gebruik van locatiegegevens en technische hulpmiddelen voor het traceren van contacten omtrent de COVID-19 uitbraak gepubliceerd.

1 Klik hier voor de brief

2 Klik hier voor de publicatie

3 Klik hier voor de publicatie

De eerste richtlijn die is vastgesteld omtrent de COVID-19 uitbraak is **de richtlijn voor het verwerken van gezondheidsgegevens voor wetenschappelijke onderzoeksdoeleinden**[4].

Deze richtlijn heeft als doel meer inzicht te geven in de meest urgente juridische kwesties omtrent het gebruik van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van COVID-19, zoals de rechtsgrondslag voor de verwerking, de verdere verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek, de toepassing van adequate waarborgen en de uitoefening van de rechten van de betrokkenen.

In de richtlijn staat dat de AVG verschillende bepalingen bevat met betrekking tot de verwerking van gezondheidsgegevens ten behoeve van wetenschappelijk onderzoek. Deze bepalingen zijn ook van toepassing in het kader van de COVID-19 pandemie. De AVG voorziet in de mogelijkheid om bepaalde bijzondere categorieën van persoonsgegevens, zoals gezondheidsgegevens, te verwerken wanneer dit noodzakelijk is voor wetenschappelijk onderzoek. Daarnaast wordt ingegaan op vraagstukken die zien op de doorgifte van de gezondheidsgegevens buiten de EU, met name wanneer er geen adequaatheidsbesluit of andere passende waarborgen zijn.

Andrea Jelinek, voorzitter van de EDPB: "Op dit moment worden er grote onderzoeks-inspanningen gedaan in de strijd tegen COVID-19. Onderzoekers hopen zo snel mogelijk resultaten te boeken. De AVG staat wetenschappelijk onderzoek niet in de weg, maar maakt de rechtmatige verwerking van gezondheidsgegevens mogelijk om het doel van het vinden van een vaccin of behandeling voor COVID-19 te ondersteunen".

De tweede richtlijn die is vastgesteld omtrent de COVID-19 uitbraak is **de richtlijn omtrent het gebruik van locatiegegevens en technische hulpmiddelen voor het traceren van contacten**[5]. Deze richtlijn heeft tot doel om de voorwaarden en beginselen voor het gebruik van locatiegegevens en technische hulpmiddelen voor het traceren van contacten voor twee specifieke doelen te verduidelijken:

- het gebruik van locatiegegevens om de verspreiding van het virus te modelleren en de algemene doeltreffendheid van de 'lock down' maatregelen te beoordelen;
- het traceren van contacten met als doel personen die mogelijk in de nabijheid zijn geweest van iemand die drager van het virus blijkt te zijn, te informeren zodat de besmettingsketens zo vroeg mogelijk doorbroken kunnen worden.

In de richtlijn wordt benadrukt dat de AVG en de e-Privacy richtlijn specifieke bepalingen bevatten die het gebruik van anonieme of persoonlijke gegevens mogelijk maken om overheidsinstanties en andere actoren op zowel nationaal als EU-niveau te ondersteunen bij hun inspanningen om de verspreiding van COVID-19 te monitoren en in te dammen. De algemene beginselen van doeltreffendheid, noodzakelijkheid en evenredigheid moeten als leidraad dienen voor alle maatregelen die door de lidstaten of de EU-instellingen worden genomen die betrekking hebben op de verwerking van persoonsgegevens om de COVID-19 pandemie te bestrijden. De EDPB onderstreept daarbij het standpunt dat zij in haar brief aan de Commissie heeft ingenomen, namelijk dat het gebruik van toepassingen voor het traceren van contacten

4 Klik hier voor de richtlijn

5 Klik hier voor de richtlijn

vrijwillig moet zijn en niet moet berusten op het traceren van individuele bewegingen, maar op informatie in de nabijheid van de gebruikers (deze brief is behandeld onder 1.1).

Voorzitter Jelinek voegde hieraan toe: "Apps kunnen nooit de plaats innemen van verpleegkundigen en artsen. Ondanks dat data en technologie belangrijke hulpmiddelen kunnen zijn, moeten we er rekening mee houden dat ze intrinsieke beperkingen hebben. Apps kunnen alleen een aanvulling zijn op de effectiviteit van volksgezondheidsmaatregelen en de toewijding van gezondheidswerkers die nodig is om COVID-19 te bestrijden. De mensen zouden in ieder geval niet moeten kiezen tussen een efficiënt antwoord op de crisis en de bescherming van de grondrechten".

Daarnaast heeft de EDPB als bijlage bij de richtlijn een handleiding voor contact traceer-apps aangenomen. Het doel van deze handleiding is algemene richtlijnen te verstrekken aan ontwerpers en uitvoerders van technische hulpmiddelen voor het traceren van contacten De handleiding is niet uitputtend.

1.3 24E PLENAIRE VERGADERING EDPB – EDPB BENADRUKT DE RICHTLIJNEN OMTRENT COVID-19 IN NIEUW AANGENOMEN BRIEVEN[6]

In de 24e plenaire vergadering heeft de EDPB drie brieven aangenomen, waarin verschillende elementen uit de onder 1.2 beschreven richtlijnen worden benadrukt en aangescherpt.

De eerste brief betreft een antwoord op een **brief van de Verenigde Staten**[7]. De EDPB onderzoekt de doorgifte van gezondheidsgegevens buiten de EU waardoor internationale samenwerking voor de ontwikkeling van een vaccin mogelijk wordt. In de brief van de VS wordt vervolgens nader onderzocht of het mogelijk is een beroep te doen op een van de gronden in artikel 49 AVG voor doorgifte van de persoonsgegevens.

De EDPB heeft dit onderwerp uitvoerig behandeld in de onder 1.2 besproken richtlijn omtrent wetenschappelijk onderzoek. De EDPB herhaalt in de brief dat de AVG samenwerkingen mogelijk maakt tussen wetenschappers binnen de EU en buiten de EU, bij het zoeken naar vaccins en behandelingen tegen COVID-19, terwijl tegelijkertijd de fundamentele rechten op het gebied van gegevensbescherming binnen de EU worden beschermd.

Wanneer gegevens worden verstrekt buiten de EU, moet volgens de EDPB de voorkeur worden gegeven aan oplossingen die de bescherming van de grondrechten van de betrokkenen blijvend garanderen, zoals adequaatheidsbesluiten of andere passende waarborgen (opgenomen in art. 46 AVG). De EDPB is van mening dat de strijd tegen COVID-19 door de EU en de lidstaten is erkend als een belangrijk openbaar belang, nu deze strijd heeft geleid tot een uitzonderlijke sanitaire crisis van ongekende aard en omvang. Dit kan vereisen dat het nodig is op het gebied van wetenschappelijk onderzoek urgent actie te ondernemen, waardoor de overdracht van persoonsgegevens aan derde landen of internationale organisaties noodzakelijk wordt. Bij gebrek aan een adequaatheidsbesluit of passende waarborgen, kunnen overheidsinstanties en

6 Klik hier voor de publicatie

7 Klik hier voor de brief

particuliere entiteiten ook een beroep doen op de in artikel 49 AVG opgenomen afwijkingen.

Andrea Jelinek, voorzitter van de EDPB: "De wereldwijde wetenschappelijke gemeenschap racet tegen de klok om een COVID-19 vaccin of behandeling te ontwikkelen. De AVG biedt voldoende instrumenten voor de internationale overdracht van gezondheidsgegevens. Deze instrumenten zijn flexibel genoeg om snelle tijdelijke oplossingen te bieden in deze dringende medische situatie."

De tweede brief die is aangenomen door de EDPB betreft een **antwoord op de brief van de leden Lucia Ďuriš Nicholsonová en Eugen Jurzyca van het Europees Parlement**. In deze brief wezen de leden van het Parlement de EDPB op de noodzaak om gemeenschappelijke richtsnoeren te ontwikkelen met betrekking tot de toepassing van de wetgeving op het gebied van privacy en gegevensbescherming in de strijd tegen de COVID-19 pandemie.[8]

De EDPB geeft in haar antwoord aan dat in de wetgeving op het gebied van gegevens-bescherming al rekening wordt gehouden met de gegevensverwerking die nodig is om een pandemie te helpen bestrijden, zodat er - volgens de EDPB - geen reden is om AVG-bepalingen op te heffen, maar om ze in acht te nemen. De EDPB verwijst naar de in 1.2 beschreven richtlijnen.

Andrea Jelinek, voorzitter van de EDPB, voegde daaraan toe: "De AVG is ontworpen om flexibel te zijn. Daardoor is het mogelijk om met de AVG de bestrijding van de pandemie te ondersteunen en tegelijkertijd de fundamentele mensenrechten en vrijheden te beschermen. In sommige gevallen is het noodzakelijk om persoonsgegevens, die verband houden met het COVID-19 virus, te verwerken. Wanneer er sprake is van een dergelijk geval dan is het van essentieel belang om de persoonsgegevens goed te beschermen. De gegevensbescherming is van essentieel belang om vertrouwen op te bouwen. Daarnaast is het beschermen van gegevens ook een voorwaarde voor maatschappelijke aanvaardbaarheid van elke mogelijke oplossing en is het nodig de doeltreffendheid van de genomen maatregelen te garanderen."

De derde brief van de EDPB betreft een **reactie op twee brieven van Sophie In 't Veld, lid van het Europees Parlement**[9], waarin een reeks vragen werden gesteld over de nieuwste technologieën die worden ontwikkeld om de verspreiding van COVID-19 tegen te gaan.

In de brief verwijst de EDPB naar de in 1.2 beschreven richtlijn omtrent het gebruik van locatiegegevens en technische hulpmiddelen voor het traceren van contacten, waarin onder meer wordt benadrukt dat dergelijke hulpmiddelen een vrijwillig karakter moeten hebben, er zo weinig mogelijk gegevens moeten worden verwerkt en er geen individuele bewegingen moeten worden getraceerd, maar dat gebruik moet worden gemaakt van informatie in de nabijheid van de gebruikers.

8 Klik hier voor de brief

9 Klik hier voor de brief

2. NATIONAAL NIEUWS

2.1 AP: BOETE VOOR BEDRIJF VOOR VERWERKEN VINGERAFDRUKKEN WERKNEMERS[1]

Aanleiding

Op 5 juli 2018 heeft de Autoriteit Persoonsgegevens ('AP') een melding ontvangen dat bij het betreffende bedrijf[2] werknemers verplicht zijn om hun vingerafdruk te laten scannen. Uit de melding heeft de AP opgemaakt dat werknemers met behulp van een vingerafdruk in- en uitklokken ten behoeve van tijdsregistratie. Naar aanleiding van dit signaal is de AP een onderzoek[3] gestart naar de naleving van artikel 9 van de Algemene Verordening Gegevensbescherming (AVG), dat onder meer ziet op het gebruik van de verwerking van biometrische gegevens, zoals een vingerafdruk.

Eind oktober 2018 is het onderzoek gestart. De AP heeft onder meer onderzoek ter plaatse verricht.

Beweegredenen van het bedrijf

Het betreffende bedrijf heeft aangegeven gebruik te maken van de vingerscanapparatuur om misbruik bij het in- en uitklokken tegen te gaan.

Ook het praktische deel heeft meegewogen in de keuze voor deze apparatuur. Door gebruik van de vingerscanapparatuur waren er ook geen kosten meer voor de aanschaf, verlies of beschadiging van druppels waarmee kon worden in- en uitgeklokt.

Andere redenen voor gebruik van de vingerscanapparatuur waren, volgens medewerkers van het bedrijf, gelegen in het feit dat het systeem een sluitende aanwezigheidsregistratie biedt, dat de vingerscanapparatuur het verouderde systeem met druppelscanners moet vervangen en dat het in de toekomst onderdeel kan zijn van de veiligheid van het computernetwerk (hackpogingen, bedrijfsspionage).

Beoordeling

Vingerafdrukken, oftewel biometrische gegevens, zijn bijzondere persoonsgegevens.

De vingerscanapparatuur was sinds begin 2017 in gebruik binnen het betreffende bedrijf. De AP heeft vastgesteld dat het betreffende bedrijf de vingerafdrukken van 337 huidig en voormalige werknemers heeft opgeslagen. De vingerafdrukken werd opgeslagen als templates en bleven ook opgeslagen, ook als werknemers uit dienst waren. Zodra een werknemer uit dienst trad, werd de vingerafdruktemplate wel op niet actief gezet. Daardoor kon geen koppeling meer worden gemaakt tussen de vingerafdruktemplate en de softwareapparatuur. Van werknemers die nog wel in dienst zijn, zijn de vingerafdruktemplates gekoppeld aan een softwareprogramma zodat zij kunnen in- en uitklokken met hun vingerafdruk. In de arbeidsovereenkomst is geen informatie opgenomen over het gebruik van vingerafdrukken.

De AP heeft in haar onderzoek beoordeeld of het betreffende bedrijf een geslaagd beroep

1 Klik hier voor het boetebesluit van de AP

2 De rechter heeft bepaald dat de naam niet openbaar mag worden

3 Klik hier voor het onderzoek van de AP

kan doen op één van de voor de betreffende verwerking relevante uitzonderingsgronden in artikel 9 lid 2 AVG, meer specifiek artikel 9 lid 2 sub a en artikel 9 lid 2 sub g AVG jo. artikel 29 UAVG en de biometrische gegevens dan ook gerechtvaardigd worden verwerkt. Dit betreft de uitzonderingsgrond "uitdrukkelijke toestemming van de betrokkene" en "noodzakelijk voor authenticatie of beveiligingsdoeleinden".

De AP heeft gedurende het onderzoek geen bewijs aangetroffen dat medewerkers voor het afnemen of gebruik van de vingerafdrukken hun uitdrukkelijke toestemming hebben gegeven, dan wel deze hadden geweigerd. Ten tijde van het onderzoek is door verscheidene medewerkers aangegeven dat het inscannen van de vingerafdruk verplicht was en er geen toestemming is gevraagd voor het gebruik van de vingerafdruk. Daarbij werd door medewerkers ook aangegeven dat als het inscannen van de vingerafdruk werd geweigerd, er een gesprek met de directeur of het bestuur volgde, waardoor in de praktijk iedereen zijn of haar vingerafdruk liet inscannen. Daardoor hadden medewerkers geen vrije keuze, aldus de AP. De uitzonderingsgrond "uitdrukkelijke toestemming" van de betrokkene kan in dit geval dan ook geen basis bieden voor de verwerking van de vingerafdrukken.

De verwerking van biometrische gegevens zou verder toegestaan kunnen zijn indien dit noodzakelijk is voor authenticatie of beveiligingsdoeleinden. Daarvoor moet er een afweging worden gemaakt of identificatie door middel van biometrie noodzakelijk en proportioneel is voor authenticatie of beveiligingsdoeleinden. 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 bij het bedrijf niet noodzakelijk en proportioneel is. Voor de werkzaamheden bij het bedrijf, is de noodzaak van de beveiliging niet zodanig hoog dat hiertoe een biometrisch identificatiemiddel dient te worden gebruikt teneinde de toegangscontrole uit te oefenen. Daarnaast kunnen andere minder ingrijpende middelen dit ook bewerkstelligen. Het betreffende bedrijf kan zich wat betreft de verwerking van vingerafdrukken daarom tevens niet beroepen op de uitzonderingsgrond in artikel 9, lid 2, onder g, AVG jo. artikel 29 UAVG.

Gelet op het voorgaande kan geconcludeerd worden dat het betreffende bedrijf in strijd handelt met het verbod uit artikel 9 lid 1 AVG.

Boete

De AP maakt voor de vastgestelde overtreding gebruik van haar bevoegdheid om aan het bedrijf een bestuurlijke boete op te leggen op grond van artikel 58 lid 2, aanhef en sub i en artikel 83 lid 5 AVG jo. artikel 14 lid 3 UAVG. De AP hanteert hiervoor de Boetebeleidsregels 2019.44. Aan het betreffende bedrijf is een boete opgelegd van €725.000,-

Gelet op het feit dat de overtreding ruim tien maanden heeft geduurd waarbij 337 betrokkenen zijn getroffen, is er sprake geweest van een ernstige situatie. Het betreffende bedrijf heeft daarbij niet alleen de biometrische gegevens van huidige werknemers maar ook van voormalig werknemers zonder noodzaak langere tijd bewaard. Bovendien waren de werknemers onvoldoende geïnformeerd over de verwerking en staat niet vast staat dat zij (in vrijheid) toestemming hebben gegeven, waardoor naar het oordeel van de AP sprake is van een ernstige overtreding waarin de bijzondere persoonsgegevens van betrokkenen onder onjuiste

voorwaarden zijn verwerkt.

Het betreffende bedrijf heeft bezwaar gemaakt tegen de boete van de AP.

Wat valt op?

Voordat u als organisatie besluit gebruik te gaan maken van biometrische gegevens van uw medewerkers voor authenticatie en beveiligingsdoeleinden, dient goed te worden beoordeeld of het vanuit beveiligingsoogpunt daadwerkelijk nodig is de identificatie op deze wijze in te richten. Het boetebesluit van de AP maakt duidelijk dat een strenge toets geldt bij de afweging of gebouwen en informatiesystemen beveiligd moeten worden door middel van het gebruik van biometrische gegevens. Daarbij wordt meegegeven dat de beveiliging van een kerncentrale het bijvoorbeeld noodzaakt dat voor de toegangscontrole gebruik wordt gemaakt van biometrie. Bij een dergelijk gevoelige locatie, is het belang van een goede beveiliging aanzienlijk en mogen uitsluitend enkele personen toegang verkrijgen. Het is van belang dat voorafgaand goed bekeken wordt of het gebruik van biometrie proportioneel is en of er geen andere middelen bestaan die minder ingrijpend zijn, zoals volgens de AP mogelijk was bij het bedrijf aan wie de boete is opgelegd.

De AP rekent het de organisatie zwaar aan dat onrechtmatig gebruik wordt gemaakt van biometrische gegevens en handhaaft streng. Het waarborgen van de privacy van een individu is van groot belang bij de inzet van biometrie. Biometrische gegevens, zoals een vingerafdruk, zijn namelijk bijzondere persoonsgegevens in de zin van artikel 9 AVG. Dit zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn omdat de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden van mensen. Het verwerken van biometrische persoonsgegevens verdient specifieke bescherming. Het is dus van belang een goede afweging te maken voordat gebruik gaat worden gemaakt van biometrische gegevens.

Graag wordt nog opgemerkt dat het betreffende bedrijf met succes de publicatie van de naam van de organisatie heeft weten te voorkomen; belangrijk punt ter voorkoming van reputatieschade. Het betreffende bedrijf voerde daarbij aan dat zolang de rechtmatigheid van het boetebesluit nog niet is bekrachtigd door een rechter, de organisatie beschermd moet worden tegen het publiekelijk maken van de naam.

2.2 AP: INZAGE MEDISCH DOSSIER MAG ALLEEN MET TOESTEMMING PATIËNT[4]

De Minister van het Ministerie van Volksgezondheid, Welzijn en Sport ('VWS') heeft de AP door middel van een brief geïnformeerd over het voorstel om het toestemmingsvereiste uit artikel 15a lid 1 Wet algemene bepalingen verwerking van persoonsgegevens in de zorg ('Wabvpz') tijdelijk buiten toepassing te laten. Op grond van artikel 15a lid 1 Wabvpz mag een zorgaanbieder gegevens van een patiënt pas beschikbaar stellen via een elektronisch uitwisselingssysteem, denk hierbij aan het Elektronisch patiëntendossier, nadat toestemming van de patiënt is verkregen. De Minister wil een technische mogelijkheid creëren die het mogelijk maakt voor

4 Klik hier voor de brief

zorgverleners op huisartsenposten ('HAP') en op de spoedeisende eerstehulpafdelingen ('SEH') om huisartsinformatie te raadplegen zonder toestemming van de patiënt.

De AP acht een dergelijke ingreep om de raadpleging van noodzakelijke patiëntgegevens op de HAP of SEH technisch mogelijk te maken, onder de gegeven omstandigheden niet bezwaarlijk. De AP acht het daarbij wel van belang dat ook in de gecreëerde constructie de naleving van het toestemmingsvereiste leidend blijft, tenzij de patiënt niet meer in staat is zijn/haar wil te uiten. Ook acht de AP het van belang dat geen afbreuk wordt gedaan aan de andere belangrijke beginselen die in acht moeten worden genomen ten aanzien van het medisch beroepsgeheim van artsen en de vertrouwelijke gegevensuitwisseling tussen hulpverleners. Dat maakt dat die technische mogelijkheid zodanig moet worden vormgegeven dat handhaving – ook strafrechtelijk – van overtreding van een schending van het beroepsgeheim en van het zonder toestemming raadplegen van patiëntgegevens mogelijk blijft.

Door het plan van VWS verandert niets voor betrokkenen die al toestemming hebben gegeven, dan wel toestemming hebben geweigerd. In beide gevallen blijft die keuze gerespecteerd. Daarnaast is er een grote groep mensen die nog geen keuze heeft doorgegeven. Het voorstel van VWS is bedoeld voor betrokkenen die nog geen toestemming hebben gegeven ten aanzien van de uitwisseling van hun persoonsgegevens. Het voorstel van VWS ziet niet op het gehele dossier van de betrokkene, maar betreft uitsluitend een samenvatting.

De AP acht het voorstel van VWS acceptabel, maar geeft daarbij wel aan dat de AP die patiënten ter plekke, op de HAP of SEH, toestemming moeten kunnen geven voor raadpleging van hun medische gegevens, dit kan ook mondeling. Is een patiënt niet in staat om ter plekke toestemming te geven, bijvoorbeeld omdat de gezondheidstoestand van een patiënt dat niet toelaat, dan mag de arts zonder toestemming van deze patiënt de samenvatting raadplegen. De AP geeft tot slot nog aan betrokkenen mee dat zij nu, voordat zij mogelijk ziek worden, goed na te denken over hun keuze en deze door te voeren.

2.3 AP: KEUZEHULP PRIVACY BIJ VIDEOBEL-APPS[5]

De AP heeft een keuzehulp voor videobel-apps gelanceerd, waarbij naar de belangrijkste privacyaspecten van dertien verschillende apps wordt gekeken. De AP heeft geen uitgebreid, technisch onderzoek naar de apps uitgevoerd, maar is afgegaan op de informatie die opgenomen is in documentatie met betrekking tot de apps, bijvoorbeeld in de privacyverklaring.

Van de 13 beoordeelde apps zijn Jitsi, Signal en Nextcloud de enige app die geen gegevens van gebruikers verzamelen. De overig beoordeelde apps verwerken wel gegevens van gebruikers, zoals het adresboek van de gebruiker, locatiegegevens, gespreksgegevens en metadata. Jitsi, Signal en Nextcloud Talk zijn ook de enige drie apps waarvan de broncode open source is. Tevens bieden de apps end-to-end encryptie. Dit geldt ook voor Facetime. In het geval van Skype is end-to-end encryptie alleen mogelijk bij privégesprekken[6].

5 Klik hier voor de publicatie

6 De 13 beoordeelde apps: Discord, FaceTime, Google Hangouts, Google Hangouts Meets, Houseparty, Jitsi, Facebook Messenger, Signal, Skype, Nextcloud Talk, Microsoft Teams, Whatsapp en Zoom

De AP heeft aan de hand van een aantal criteria vragen opgesteld aan de hand waarvan de videobel-apps beoordeeld zijn:

- Wat heeft de videobel-app te bieden;
- Welke gegevens verzamelt de betreffende app en voor welk doeleinde;
- Hoe zit het met de gegevensstromen bij de betreffende videobel-app; waar worden de gegevens opgeslagen en worden gegevens doorgegeven buiten de EU;
- Wordt de communicatie, die via de videobel-app verloopt, beveiligd. Een belangrijke beveiligingsmaatregel is daarbij end-to-end versleuteling. De AP heeft de 13 videobel-apps ook gescreend op end-to-end versleuteling. De apps: Whatsapp, Signal, Jitsi, Talk, Facetime en Skype (alleen in privégesprekken) hebben end-to-end versleuteling.

Wanneer videogesprekken gevoerd moeten worden voor werk, dan is de werkgever verantwoordelijk om de juiste videobel-app te kiezen die aansluit bij uw werkzaamheden en de gesprekken die u voert met bijvoorbeeld uw cliënten. De videobel-app dient dan ook uw privacy en die van bijvoorbeeld uw cliënten te beschermen.

2.4 AP: PRIVACY CORONA-APPS NIET AANGETOOND[7]

"Corona-apps alleen als privacy gewaarborgd is"[8]

Tijdens de persconferentie op 7 april 2020 maakte minister Hugo de Jonge bekend dat de regering apps wil inzetten in de strijd tegen het coronavirus.

Aleid Wolfsen, voorzitter bestuur van de AP: "Zulke apps kunnen alleen als de privacy volledig geborgd is. De AP zal daar heel scherp op letten, want mensen moeten erop kunnen vertrouwen dat de overheid zorgvuldig met deze gevoelige, medische informatie omgaat. We willen namelijk niet over een paar maanden wakker worden in een samenleving met een soort Chinese toestanden, waar de overheid voortdurend meekijkt, je de hele dag kan volgen, zorggegevens kan inzien en er allerlei consequenties aan kan verbinden."

"Corona-apps worden getoetst"[9]

Het kabinet heeft 750 reacties gekregen op de inschrijving voor de ontwikkeling van een corona-app. Uit deze 750 reacties zijn zeven apps gekozen. Het gaat om de volgende apps: Covid19, DDT Consortium, Accenture, Capgemini Nederland, ITO, DEUS en Sia Partners. Deze zeven apps hebben deelgenomen aan de door VWS op 18 en 19 april jl. georganiseerde Appathon. De AP heeft daarnaast onderzocht of deze zeven apps voldoen aan de vereisten uit de AVG. Op maandag 20 april heeft de AP haar bevindingen gepubliceerd.

De AP heeft onder meer gekeken of de apps niet meer data verzamelden dan nodig en of de gegevens goed beveiligd waren. Daarnaast heeft de AP gekeken naar de risico's die apps

7 Klik hier voor het onderzoek

8 Klik hier voor de publicatie

9 Klik hier voor de publicatie

met zich mee zouden brengen, bijvoorbeeld het risico dat de gegevens voor een ander doel gebruikt worden dan waarvoor deze in beginsel worden verwerkt en het risico dat de persoonsgegevens in handen van kwaadwillenden zouden vallen.

Wilt u meer lezen over de Appathon? Lees dan onze blog: "Haastige spoed is zelden goed: terugblik op de Appathon?"[10].

Conclusie van de beoordeling

In haar beoordeling heeft de AP aangegeven dat het op basis van de beschikbare en aangeleverde informatie niet mogelijk is de voorgestelde app te kunnen beoordelen. VWS heeft de kaders voor de apps niet duidelijk genoeg gesteld, waardoor de AP geen toetsing kan uitvoeren of de voorgestelde apps voldoen aan deze kaders.

Uit de beoordeling van de AP is gebleken dat met name bezwaren bestaan tegen het feit dat de noodzakelijkheid van de apps niet is aangetoond, de kaders van de apps onduidelijk zijn, de doelen onscherp zijn geformuleerd, de juridische grondslagen onvoldoende zijn onderbouwd, het onduidelijk is welke gegevens minimaal benodigd zijn, het is onduidelijk omschreven wie verantwoordelijk is voor de verwerking van de gegevens en zijn de rechten van betrokkenen onvoldoende gewaarborgd. De AP heeft daarnaast ook nog vragen met betrekking tot de effectieve inzet van bluetooth-technologie en verschillende andere technische aspecten van de apps.

Daarnaast is onduidelijk of alternatieven voor een app minder effectief zijn om verspreiding van het virus tegen te gaan. De AP heeft daardoor niet goed kunnen beoordelen of de inzet van corona-apps proportioneel is. "Informatie over hoe de app 'aan de achterkant' werkt is niet aangeleverd. Daardoor is onvoldoende aangetoond dat de privacy technisch maar ook organisatorisch gezien gewaarborgd is", zo stelt de AP. De ontwikkelaars hebben ook niet onderbouwd waarom gebruik wordt gemaakt van een bepaalde techniek en wat de beperkingen van die techniek zijn. "Het is nog maar de vraag of die app er wel kan komen", zegt Aleid Wolfsen, voorzitter van de AP. Maar alleen als de effectiviteit, de kaders, de plannen en de apps beter uitgewerkt zijn."

Wat valt op?

Ondanks dat de bevindingen van de AP terechte kritiekpunten bevatten, valt het ook op dat geen handvatten of oplossingsrichtingen worden aangereikt door de AP. Juist in deze uitzonderlijke tijden is het wenselijk dat de toezichthouder niet alleen examineert, maar ook adviseert. Het enige aanknopingspunt dat op dit moment wordt geboden aan VWS en de appontwikkelaars is dat apps, die gebruik maken van een decentrale oplossing zonder het gebruik van (aanvullende) persoonsgegevens, de grootste potentie hebben. De AP heeft aangegeven eventuele voorstellen voor apps opnieuw te beoordelen, mocht de overheid dat vragen. Maar alleen als de effectiviteit, de kaders, de plannen en de apps beter uitgewerkt zijn."

10 Klik hier voor de blog

2.5 AP: ZORGEN OM DATAVERZAMELING BIJ THUISONDERWIJS[11]

Naar aanleiding van zorgen die geuit zijn door ouders, docenten, leerlingen en studenten, is de AP een onderzoek gestart naar het gebruik van videobellen door onderwijsinstellingen en het toepassen van digitale surveillance bij online tentamens.

"Er is veel informatie te halen uit de beelden die bij videobellen en proctoring (digitaal surveilleren) worden verzonden naar onderwijsinstellingen of medestudenten", zo laat de AP weten. Het gaat dan over de prestaties van de leerlingen of studenten, hoe goed ze zich concentreren, maar ook religieuze uitingen of wat gezinsleden op de achtergrond doen, kan zichtbaar zijn. "In tegenstelling tot de normale lespraktijk, kunnen deze observaties nu makkelijk worden opgeslagen en verspreid", waarschuwt de AP.

De AP heeft een aantal punten meegegeven aan onderwijsinstellingen waarop gelet dient te worden wanneer gebruik gemaakt gaat worden van beeldbellen:

- Maak gebruik van de Keuzehulp videobel-apps van de AP en de website lesopafstand.nl, samengesteld door onder meer het ministerie van OCW en brancheverenigingen.
- Wanneer wordt gekozen voor een softwareleverancier, dan moet deze voldoen aan de privacywetgeving. Er moeten eisen gesteld worden aan het gebruik van data van leerlingen, studenten en personeel, waaronder (kwetsbare) kinderen. De nadruk dient gelegd te worden op het direct wissen van gegevens die niet noodzakelijk zijn.
- Leerlingen, studenten en ouders dienen geïnformeerd te worden over wat er met hun gegevens gebeurt, in voor hen begrijpelijke taal.
- Er dient een oplossing gekozen te worden in samenwerking met de medezeggenschapsraad. Belangrijk is dat docenten, leerlingen en ook ouders betrokken zijn bij deze keuzes.
- Er dient samengewerkt te worden met andere schoolbesturen. Het wordt aanbevolen kennis en ervaringen uit te wisselen en samen op te trekken richting grote spelers op de markt.
- Als onderwijsinstelling bent u verantwoordelijk voor de manier waarop het beeldbellen plaatsvindt. Daarbij kunnen bijvoorbeeld leerlingen geïnstrueerd worden om persoonlijke zaken buiten beeld te laten.
- Wanneer er te veel gevoelige, persoonlijke informatie in beeld komt, wordt het aanbevolen de leerling te vragen om de camera uit te zetten of ervoor te zorgen dat de camera kan worden uitgezet om de leerling te beschermen.
- Een datalek of ander incident kan nooit helemaal worden uitgesloten, hoe goed alles ook is ingericht. Als organisatie dient u daarop voorbereid te zijn en met leerlingen en docenten te bespreken wat zoal mis kan gaan en wat te doen in deze situaties.

Wanneer gebruik gemaakt wordt van online proctoring (digitaal surveilleren), dient gelet te worden op de volgende punten:

11 Klik hier voor de publicatie

- Beoordeeld dient te worden of het noodzakelijk is om online proctoring in te zetten, waarbij goed bekeken moet worden of het niet mogelijk is gebruik te maken van een minder ingrijpende methode (bijvoorbeeld door leerlingen of studenten een werkstuk of essay te laten inleveren).
- Wanneer beoordeeld wordt dat het noodzakelijk is gebruik te maken van online proctoring, dient ervoor gezorgd te worden dat de inbreuk op de privacy zo klein mogelijk is. In veel gevallen is bijvoorbeeld eyetracking een te zwaar middel.
- Er dient een leverancier te worden gekozen die voldoet aan de privacywetgeving.
- De voorgestelde oplossingen voor het afleggen van examens dienen te worden besproken met de studentenraad.
- De gegevens mogen niet gebruikt worden voor andere doeleinden dan het bestrijden van examenfraude.
- De leerlingen of studenten dienen geïnformeerd te worden in begrijpelijke taal over wat er met hun gegevens gebeurt.
- Leerlingen of studenten dienen geïnstrueerd te worden over online proctoring. Leerlingen en studenten moeten weten hoe zij op een zo privacyvriendelijk mogelijke manier hun toets of tentamen kunnen afleggen.
- Een datalek of ander incident kan nooit helemaal worden uitgesloten, hoe goed alles ook is ingericht. Als organisatie dient u daarop voorbereid te zijn en met leerlingen en docenten te bespreken wat zoal mis kan gaan en wat te doen in deze situaties.

Katja Mur, bestuurslid van de AP: 'Alle leerlingen moeten zonder stempel kunnen opgroeien. Hun privacy is van groot belang en wordt extra beschermd in de privacywetgeving. Onveilige oplossingen kunnen risico's opleveren voor de toekomst van leerlingen. Deze dataverwerking mag geen ondergeschoven kind van de coronacrisis worden. Wij wijzen onderwijsinstellingen er daarom op zorgvuldige keuzes te maken en ondersteunen hen hierin met een aantal tips.'

Wilt u meer lezen over proctoring en privacy? Lees dan onze blog: "Hoe kan online proctoring op een verantwoorde manier worden ingezet?"[12].

2.6 AP: TEMPERATUUR METEN MAG NIET ZOMAAR[13]

De AP heeft signalen ontvangen dat allerlei organisaties middelen inzetten om medewerkers op koorts te controleren. Het gaat dan zowel om thermometers als thermische camera's. De AP wijst erop dat dit niet mag en dat dit vanuit de AVG als een ernstige overtreding wordt gezien. De AP geeft daarbij aan dat zij handhavend zullen optreden wanneer dit gebeurt.

Uitsluitend wanneer werkgevers aan een groot aantal voorwaarden voldoen mogen ze de temperatuur van werknemers meten. Bedrijven en organisaties proberen dit op te lossen door

12 Klik hier voor de blog

13 Klik hier voor de publicatie

hun personeel om toestemming te vragen, maar de AP geeft aan dat dit in een arbeidsrelatie niet kan, omdat daar geen sprake is van gelijkwaardigheid. Een werknemer kan zich dan onder druk gezet voelen om toestemming te geven.

De AP adviseert werknemers waarvan hun temperatuur wordt gemeten om naar de ondernemingsraad te stappen en dit te rapporteren bij de functionaris gegevensbescherming (FG). Wanneer bedrijven niet per direct stoppen kan de AP handhavend optreden en het meten van de temperatuur laten stilleggen.

2.7 MINISTER J&V INFORMEERT TWEEDE KAMER: AUDIT WET POLITIEGEGEVENS[14]

De Minister van Justitie en Veiligheid ('JenV') heeft op 21 april jl. de Tweede Kamer geïnformeerd over de uitkomsten van de privacy onderzoeken die de Auditdient Rijk (ADR) en de afdeling Concernaudit van de politie hebben verricht naar de naleving van de Wet politiegegevens door de politie. De korpschef moet op grond van artikel 33 van de Wpg ten minste elke vier jaar een externe privacy audit laten verrichten. In december 2015 is het vorige auditrapport aangeboden aan de Kamer.

De politie heeft destijds, op verzoek van de ambtsvoorganger van de huidige Minister van JenV, een verbeterplan opgesteld met daarin maatregelen die genomen moeten worden voor een betere naleving van de Wpg. Daarbij kregen het autorisatieproces, rechten van betrokkenen en informatiebeveiliging voorrang, omdat daar het te beschermen belang het grootst was. Daarnaast zijn er gedurende de looptijd van het verbeterplan nieuwe regels bijgekomen als gevolg van de Europese Richtlijn gegevensbescherming opsporing en vervolging (hierna: de dataprotectie richtlijn).

Net zoals in de rest van de samenleving is het van groot belang dat de politie de privacyregels, in casu de Wpg, naleeft. Veiligheid en het respecteren van privacy zodat wij in vrijheid kunnen leven, zijn in de maatschappij onlosmakelijk met elkaar verbonden.

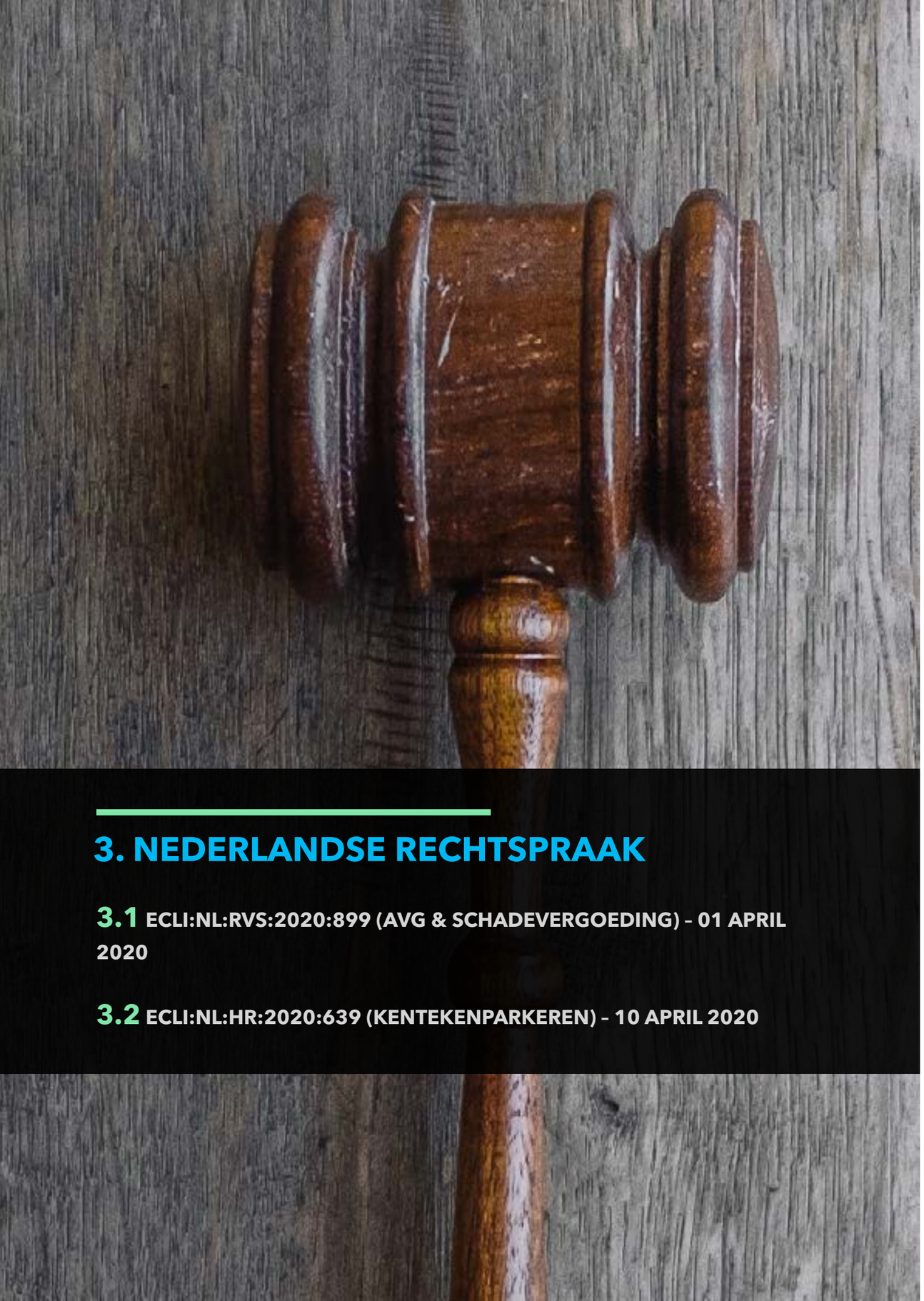
De voorliggende audits leiden tot de conclusie dat ten opzichte van de vorige keer vooruitgang is geboekt. De onderwerpen 'rechten van betrokkenen' en 'autoriseren' scoren voornamelijk groen. Dat geldt ook voor de twee onderwerpen 'privacy by design' en 'functionaris gegevensbescherming' die op grond van de dataprotectie richtlijn aan de Wpg zijn toegevoegd.

Ondanks deze positieve ontwikkeling kan nog niet geoordeeld worden dat de politie volledig conform de Wpg werkt. Reeds uit de audit van 2015, maar ook uit de evaluatie van de Wpg is gebleken dat de wet op bepaalde onderdelen te complex is en onvoldoende aansluit op de uitvoeringspraktijk. De beleidsvoorbereiding voor de herziening van de Wpg is mede daarom inmiddels in gang gezet. Deze herziening heeft onder anderen tot doel de complexiteit voor de uitvoeringspraktijk terug te dringen.

Het verbeterprogramma dat in 2016 is opgestart naar aanleiding van het verbeterplan wordt binnenkort opgeleverd. Het programma heeft beleidsmatige maatregelen genomen die in de 'opzet' voorzien. De eenheden moeten deze implementeren. Daarbij is het een lijnverantwoordelijkheid binnen de politie om zorg te dragen voor de uitvoering. De volgende vierjaarlijkse audit kan het bestaan en de werking van deze maatregelen toetsen.

Naar aanleiding van de audits door de ADR en de politie, wordt een verbeterrapport opgesteld waarin de maatregelen worden beschreven die getroffen worden ter verbetering van de geconstateerde tekortkomingen. De Kamer wordt daar door de Minister van Jen nader over geïnformeerd.

14 Klik hier voor de brief



3. NEDERLANDSE RECHTSPRAAK

ECLI:NL:RVS:2020:899 (AVG & SCHADEVERGOEDING) – 01 APRIL 2020[1]

Korte samenvatting

In deze zaak beslist de Raad van State dat om voor schadevergoeding, wegens een overtreding van de AVG, in aanmerking te komen, voldaan moet zijn aan de eisen die artikel 6:106 Burgerlijk Wetboek stelt. Dat betekent voor deze gevallen dat sprake moet zijn van aantasting van de eer of goede naam van betrokkene dan wel van aantasting van de persoon op andere wijze. De Raad van State sluit daarbij aan bij de rechtspraak van de Hoge Raad. Anders dan de rechtbank deed, wordt besloten dat appellant geen aanspraak kan maken op een schadevergoeding. Verlies van controle over je persoonsgegevens door overtreding van de AVG betekent niet automatisch dat er schade is ontstaan waarvoor de wederpartij dient op te draaien.

Achtergrondinformatie

De oorspronkelijke zaak was aangespannen door een bekende van de gemeente Deventer, meer specifiek iemand die veelvuldig Wob-verzoeken indient. Deze raakte met de gemeente Deventer in de clinch na een inzageverzoek en een daaropvolgende bezwaarprocedure. De gemeente bleek de naam en de woonplaats van de man te hebben gedeeld met andere gemeenten die met soortgelijke Wob-verzoeken te maken hadden. De rechtbank oordeelde dat het handelen van de gemeente jegens de man tot ‘verlies van de controle over zijn persoonsgegevens’ leidde. De rechtbank vond dat ter compensatie een schadevergoeding van 500 euro billijk was op grond van artikel 82 van de AVG, in samenhang met artikel 6:106 van het Burgerlijk Wetboek.

De Raad van State oordeelde echter dat het algemene uitgangspunt dat schade moet worden onderbouwd ook geldt ingeval schadevergoeding wordt geëist op grond van de AVG. Er is geen grond voor het oordeel dat een inbreuk op de AVG zonder meer aantasting van de integriteit van een persoon impliceert en daarmee tot vergoedbare schade leidt. Anders dan de klager betoogt, kan dit niet worden afgeleid uit overwegingen 85 en 146 van de AVG. Dat een inbreuk op persoonsgegevens kan resulteren in (im)materiële schade en dat een betrokkene volledige en daadwerkelijke vergoeding van de door hem geleden schade moet ontvangen, betekent niet dat een normschending per definitie tot schade leidt en dat schade niet reëel en zeker moet zijn geleden. (Ro 33.)

Het uitgangspunt is dus dat de schade aannemelijk gemaakt dient te worden en met concrete gegevens moet worden onderbouwd. Het CBb heeft, aldus de Raad van State, terecht betoogd dat klager geen concrete gegevens ter onderbouwing van de door hem gestelde schade heeft overlegd. Onvoldoende aannemelijk is gemaakt dat de inbreuk heeft geleid tot de aantasting van de integriteit van de persoon van klager en dat de gevolgen van de inbreuk hem rechtstreeks hebben getroffen. Daarnaast is niet inzichtelijk gemaakt waarom het noemen van de naam en woonplaats in de mededeling, dat de klager twee, niet-gespecificeerde, Wob-verzoeken heeft ingediend als reactie op een verzoek van een andere gemeente, als aantasting van de persoon kan worden gekwalificeerd. Ook is niet aannemelijk gemaakt welke nadelige gevolgen voor hem zijn voortgevloeid uit het noemen van zijn naam en woonplaats. Er zijn geen aanwijzingen

1 Klik hier voor de gehele uitspraak

dat de gegevens zijn misbruikt. (Ro 37.)

3.2 ECLI:NL:HR:2020:639 (KENTEKENPARKEREN) – 10 APRIL 2020[2]

Korte samenvatting

De gemeente Amsterdam heeft een systeem van kentekenparkeren waarbij een parkeerder via de parkeerautomaat of mobiele telefoon het kenteken van zijn auto moet opgeven om parkeerbelasting te voldoen. Controle vindt plaats met gebruik van scanauto's. De daarmee verkregen gegevens worden in versleutelde vorm bewaard. Indien de parkeerbelasting niet is voldaan, wordt de versleuteling ongedaan gemaakt en vraagt de heffingsambtenaar bij de Rijksdienst voor het Wegverkeer (RDW) de persoonsgegevens van de kentekenhouder op, waarna een naheffingsaanslag parkeerbelasting kan worden opgelegd. In deze zaak stelde de belanghebbende dat het kentekenparkeersysteem onder meer in strijd is met artikel 8 EVRM. Deze bepaling beschermt het recht op respect voor het privéleven van eenieder. De Hoge Raad is gelet op rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) van oordeel dat bij het kentekenparkeersysteem in Amsterdam sprake is van een inmenging door de gemeente in het recht van belanghebbende op respect voor zijn privéleven als bedoeld in artikel 8 EVRM. Bij dit systeem van kentekenparkeren (het invoeren van het kenteken en controle door scanauto's in de openbare ruimte) gaat het namelijk om het systematisch verzamelen, vastleggen, bewerken, gedurende enige tijd bewaren en gebruiken van gegevens. De Hoge Raad acht deze inmenging echter gerechtvaardigd omdat de eis van het opgeven van het kenteken is te lezen in de Parkeerverordening 2013 van de gemeente Amsterdam in combinatie met de Gemeentewet.

"Per 1 juli 2013 is in de Parkeerverordening 2013 van de gemeente Amsterdam de volgende omschrijving van het begrip 'parkeerrecht' opgenomen: "kentekenregistratie in het digitale parkeerbelastingbestand waarbij is voldaan aan parkeerbelastingplicht voor het gebruik van parkeerapparatuurplaatsen op basis van of krachtens deze verordening door middel van parkeervergunningen, bijzondere vergunningen, tijdgebonden parkeerrechten en/of door middel van het in werking stellen van de parkeerapparatuur." (Ro 2.5.8.)

"Gelet op de in 2.5.8 weergeven tekst van de Parkeerverordening 2013, die ook gold ten tijde van het belastbare feit, in combinatie met het bepaalde in de artikelen 225 en 234 van de Gemeentewet is ten tijde van het opleggen van de naheffingsaanslag ten aanzien van de eis van opgave van het kenteken van het te parkeren voertuig voldaan aan de eis "bij wet voorzien" als bedoeld in artikel 8, lid 2, EVRM." (Ro 2.5.9.)

Achtergrondinformatie

Belanghebbende had een parkeerboete gekregen en ging hiertegen in beroep. Belanghebbende wilde naar eigen zeggen wel voor het parkeren betalen, maar stelde dat dit niet mogelijk was zonder zijn privacy te schenden. Er kon namelijk niet met cash worden betaald. Eind 2017 stelde de rechter dat er in deze zaak geen inbreuk is op de privacy en werd de belanghebbende in het ongelijk gesteld, waarop door belanghebbende hoger beroep is ingesteld bij het gerechtshof Amsterdam.

2 Klik hier voor de gehele uitspraak

Het gerechtshof Amsterdam oordeelde dat geen sprake is van een inbreuk op het privéleven. Als dit al wel het geval zou zijn, dan was sprake van een gerechtvaardigde inmenging als bedoeld in artikel 8, lid 2, EVRM, omdat de verplichting tot het opgeven van het kenteken bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van het economisch welzijn van het land. Er was volgens het gerechtshof dan ook geen strijd met artikel 8 EVRM. Tegen deze beslissing stelde belanghebbende beroep in cassatie in bij de Hoge Raad. De Hoge Raad heeft nu geoordeeld dat kentekenparkeren in de gemeente Amsterdam een gerechtvaardigde inmenging is op het recht op privacy. Er is wel sprake van een inmenging, maar deze inmenging is bij wet voorzien en daardoor gerechtvaardigd, aldus de Hoge Raad. Nu in de uitspraak niet beoordeeld is of de inmenging proportioneel is, heeft belanghebbende aangegeven de zaak aan te gaan brengen bij het Europese Hof voor de Rechten van de Mens.

4. WERELDWIJDE ONTWIKKELINGEN

4.1 RECENTE COVID-19 ONTWIKKELINGEN

Overzicht ontwikkeling COVID-19 contact-tracing apps in Europa

De punten hieronder beschrijven kort verschillende artikelen die de afgelopen maand zijn gepubliceerd naar aanleiding van contact-tracing apps ter bestrijding van COVID-19. Wat is de stand van zaken?

06-04-2020 EU privacy watchdog calls for pan-European mobile app for virus tracking – "The European Data Protection Supervisor (EDPS) called on Monday for a pan-European mobile app to track the spread of the new coronavirus instead of the current hodge-podge of apps used in various EU countries which could breach people's privacy rights."[1]

21-04-2020 Frankrijk vraagt Apple om de werking van bluetooth op iOS aan te passen voor de corona-app - "Leden van de Franse overheid hebben Apple gevraagd om de werking van bluetooth op iOS aan te passen voor de eigen contactonderzoek-app Stop COVID. Apple lijkt dat niet van plan te zijn en brengt in mei de eigen api uit."[2]

23-04-2020 De Jonge houdt mogelijkheid open dat corona-app er niet komt - "Minister De Jonge van Volksgezondheid houdt de mogelijkheid open dat de veelbesproken corona-app er niet komt. Dat liet hij gisteren weten tijdens een debat in de Tweede Kamer over de ontwikkelingen rondom het coronavirus."[3]

24-04-2020 Britse overheid lanceert komende weken eigen bluetooth corona-app - "De Britse overheid zal in de komende weken een eigen bluetooth corona-app voor contact onderzoek lanceren. Dat heeft de National Health Service (NHS) vandaag bekendgemaakt. De technologie waar de app gebruik van maakt is gebaseerd op onderzoek van epidemiologen, wiskundigen en ethici van de Universiteit van Oxford."[4]

24-04-2020 Bluetooth-uitvinder vindt bluetooth niet nauwkeurig genoeg voor contactonderzoek - "Bluetooth is niet nauwkeurig genoeg om te worden ingezet voor contactonderzoek naar corona, zo laat bluetooth-uitvinder Jaap Haartsen weten. De Nederlandse elektrotechnicus vond in 1994 de Bluetooth-technologie uit. Hoewel de technologie allerlei toepassingen heeft is die volgens Haartsen nog niet voor contactonderzoek geschikt."[5]

28-04-2020 Duitse overheid kiest toch niet voor corona-app die data centraal opslaat – "De Duitse overheid kiest toch niet voor een corona-app die data centraal opslaat, zo hebben kabinetschef Helge Braun en minister van Volksgezondheid Jens Spahn in een verklaring laten weten. Vorige week maakte de Duitse overheid nog bekend dat het een corona-app wilde gaan inzetten gebaseerd op de PEPP-PT-technologie, waarbij gepseudonimiseerde gegevens van burgers centraal worden opgeslagen."[6]

1 Klik hier voor de publicatie (en klik hier voor de originele publicatie van de EDPS)
2 Klik hier voor de publicatie
3 Klik hier voor de publicatie
4 Klik hier voor de publicatie
5 Klik hier voor de publicatie
6 Klik hier voor de publicatie

01-05-2020 Belgische privacytoezichthouder: noodzaak corona-app niet aangetoond – "De Belgische regering wil mogelijk ook een corona-app uitbrengen, maar de vereiste noodzaak en proportionaliteit hiervoor zijn nog niet aangetoond, zo laat de Belgische Gegevensbeschermingsautoriteit (GBA) weten. De privacytoezichthouder boog zich over twee voorstellen voor het gebruik van corona-apps en het oprichten van een database om de verspreiding van het coronavirus te voorkomen."[7]

4.2 NIEUWS VAN TOEZICHTHOUDENDE AUTORITEITEN IN EUROPA

Privacytoezichthouders in de EU zijn niet uitgerust om de AVG te handhaven[8]

De browserontwikkelaar Brave heeft een klacht ingediend tegen alle 27 lidstaten bij de Europese Commissie voor het niet juist implementeren van de AVG.

Brave heeft dit gebaseerd op eigen onderzoek waaruit blijkt dat EU-privacytoezichthouders over onvoldoende technisch personeel en budget beschikken. Zelfs wanneer privacy overtredingen van grote techbedrijven duidelijk blijken, zullen toezichthouders niet ingrijpen omdat ze de kosten van een juridisch proces tegen "big tech" niet kunnen veroorloven, stelt de browserontwikkelaar verder. De problemen worden veroorzaakt omdat overheden hun toezichthouders niet voldoende hebben uitgerust om hun taken uit te voeren, ook al zou dit volgens de AVG wel moeten.

Uit het onderzoek van de browserontwikkelaar blijkt dat van de 28 EU-privacytoezichthouders, 23 het met tien of minder technisch specialisten moeten doen om techbedrijven te onderzoeken. Zeven toezichthouders hebben zelfs twee of minder technisch specialisten in dienst. Bij elkaar genomen werken er voor de Europese toezichthouders 305 technisch specialisten of zijn er nog openstaande vacatures. Daarvan zijn er 101 in Duitsland actief. Volgens Brave zijn er bij de AP vier technisch specialisten in dienst.

De toezichthouders hebben niet alleen een gebrek aan voldoende technische expertise, ook als het om geld gaat trekken ze aan het kortste einde. 14 van de 28 EU-privacytoezichthouders moeten het doen met een jaarlijks budget van 5 miljoen euro of minder.

Artikel 52 van de AVG stelt dat elke lidstaat ervoor moet zorgen dat de nationale toezichthouder over voldoende personele, technische en financiële middelen beschikt voor het effectief uitvoeren van taken en uitoefenen van bevoegdheden. Brave is van mening dat de lidstaten dit niet hebben gedaan en heeft daarom een klacht bij de Europese Commissie ingediend. De browserontwikkelaar vindt dat overheden meer in technisch onderzoekers moeten investeren voor het doen van onderzoek. Daarnaast moeten toezichthouders voldoende budget krijgen om kostbare juridische processen tegen grote techbedrijven te voeren.

7 Klik hier voor de publicatie

8 Klik hier voor de publicatie