CONSIDERATI

PRIVACY & GEGEVENSBESCHERMING KENNISDELING

Overzicht recente privacyontwikkelingen

April 2023

INHOUDSOPGAVE

VOORWOORD

Beste lezer,

In afwachting van de aangekondigde stemming over de AI Act, is er veel gebeurd op het gebied van privacy en gegevensbescherming. De Europese instanties bereiden zich voor op toekomende wetgeving, maar ook oude richtsnoeren worden geüpdatet.

De EDPB heeft een aantal nieuwe richtsnoeren gepubliceerd en aangenomen. Zo wordt het steeds moeilijker om gebruik te maken van het éénloketsysteem, en gaat er minder sprake zijn van een hoofdtoezichthouder. Daarnaast is er vorig jaar een voorstel gedaan voor de nieuwe Wet ter voorkoming van witwassen en financieren van terrorisme, waar de EDPB gevaren ziet. Het advies luidt daarom ook om deze risico's goed in kaart te brengen, en daar op de juiste manier op te reageren. De EDPB brengt ook meer duidelijkheid over rechten van betrokkenen, specifiek het recht op inzage. Naast de EDPB heeft de Europese Commissie ook niet stilgezeten. Deze maand is het Europees Centrum voor Algoritmische Transparantie geopend. Doel van dit centrum is om meer onderzoek te doen naar (black-box) algoritmes, en de mate waarop men transparant kan en wil zijn over deze algoritmes. Een interessante ontwikkeling, zeker met zicht op de Impact Assessment Mensenrechten en Algoritmes (IAMA), die door de toekomende AI Act wellicht verplicht kan worden.

Op eigen bodem heeft de Algemene Rekenkamer een rapport gepubliceerd met een oproep tot betere en duidelijkere implementatie van de AVG door overheidsorganisaties. De huidige implementatie kan namelijk schadelijk zijn voor burgers. De Autoriteit Persoonsgegevens heeft ook niet stilgezeten, en heeft onder andere een boete uitgeschreven aan de Sociale Verzekeringsbank.

Binnen de nationale rechtspraak hebben Londonse taxichauffeurs meer duidelijkheid over hun uit te oefenen rechten. Daarnaast geven we wat meer informatie over het (potentieel) grootste datalek in Nederland tot nu toe en het bijbehorende kort geding.

In Italië is een tijdelijk verbod opgelegd voor ChatGPT, maar waarom eigenlijk? Wellicht dat de vragenlijst van de Britse ICO hier antwoord op heeft. En ook speelde Nederland een grote rol bij het opdoeken van Genesis Market. We gaan daarom ook kijken naar deze cyberoperatie en welke actie de politie heeft ondernomen.

Bovenstaande ontwikkelingen laten zien dat ondanks dat we bijna het vijfjarig jubileum van de inwerkingtreding van de AVG kunnen vieren, men nog niet klaar is met het implementeren en uitvoeren van deze wet.

Veel leesplezier!

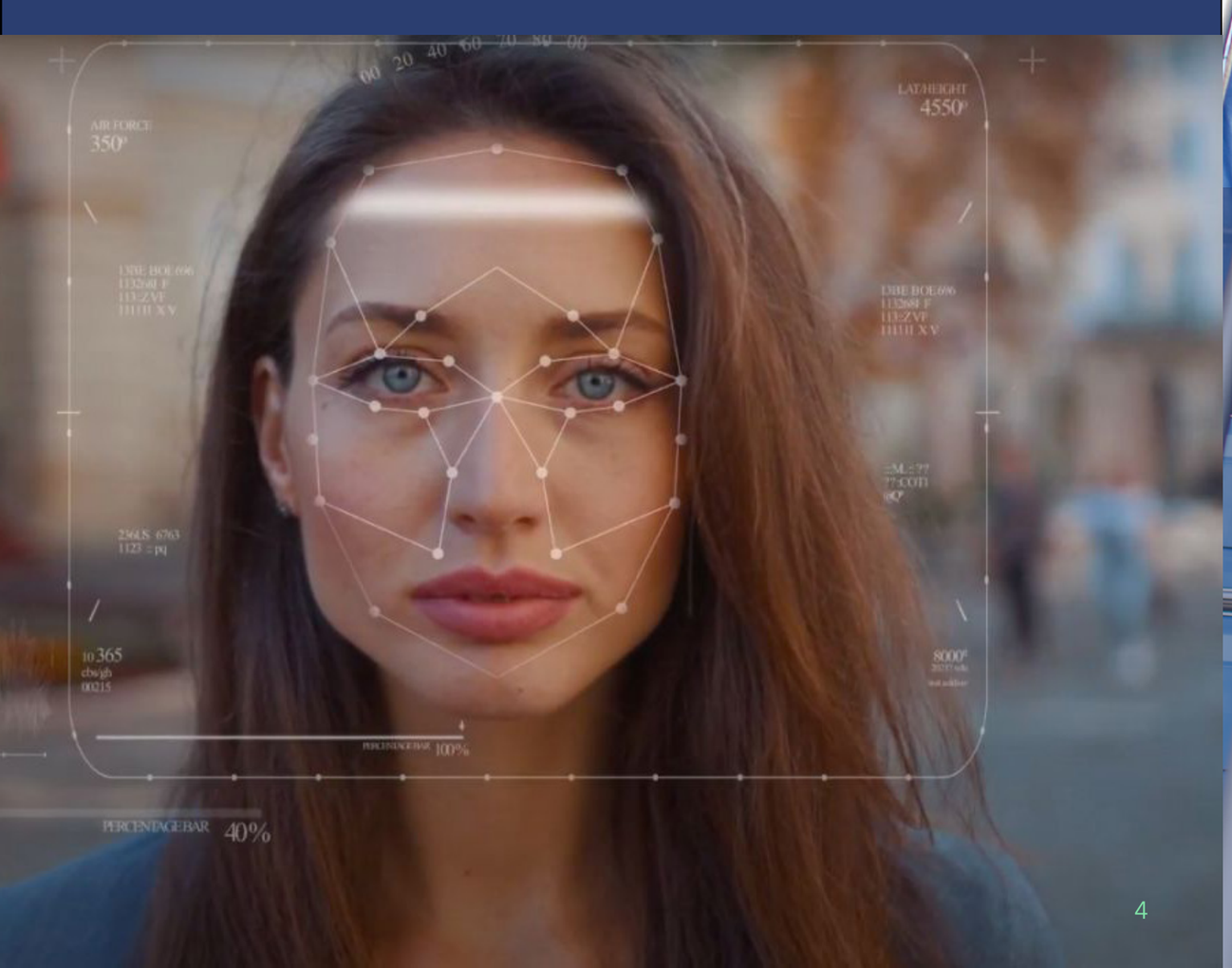
Bart Schermer
Partner Considerati

TOELICHTING

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, richtsnoeren van nationale en internationale toezichthouders en instellingen, Nederlandse en internationale rechtspraak, uitspraken en nieuwsartikelen.

De informatie in dit overzicht vormt een selectie die op basis van relevante ontwikkelingen van de afgelopen maand, door Considerati is samengesteld. De opgenomen informatie biedt als zodanig geen uitputtend overzicht van alle relevante ontwikkelingen met betrekking tot privacy en gegevensbescherming, noch bevat dit document (juridisch) advies.

Aarzel niet om **contact** op te nemen met Considerati bij vragen en opmerkingen of indien u suggesties heeft over hoe wij onze kennisdeling kunnen verbeteren.



1. EUROPEAN DATA PROTECTION BOARD EN EUROPESE INSTELLINGEN

Hoogtepunten:

- De EDPB schrapt éénloketsysteem
- Advies EDPB over witwaswetgeving
- Nieuwe regels EDPB over rechten van betrokkenen
- Europese Commissie lanceert nieuw Centrum voor Algoritmische Transparantie

1.1 EDPB schrapt het éénloketsysteem voor de melding van datalekken voor verwerkingsverantwoordelijken en verwerkers van buiten de EU

Onlangs publiceerde de European Data Protection Board (EDPB) de definitieve versie van de Richtsnoeren 9/2022 betreffende de melding van datalekken onder de AVG versie 2.0, alsmede de Richtsnoeren 8/2022 betreffende de identificatie van de hoofdtoezichthouder van een verwerkingsverantwoordelijke of verwerker.

De richtsnoeren betreffende datalekken bevatten geen substantiële wijzigingen ten opzichte van de eerder bepaalde richtsnoeren van de Artikel-29 Werkgroep (de voorloper van de EDPB), maar met name één paragraaf werd herzien en bijgewerkt met mogelijk belangrijke gevolgen. De EDPB wilde namelijk de meldingsvoorschriften over datalekken voor niet-EU-instellingen verduidelijken door de mogelijkheid voor verwerkingsverantwoordelijken en verwerkers om een beroep te doen op het éénloketsysteem te schrappen. Artikel 27 van de AVG verplicht voor de verwerkingsverantwoordelijken en verwerkers om een vertegenwoordiger in de EU aan te wijzen wanneer artikel 3, lid 2, AVG van toepassing is, d.w.z. wanneer deze entiteiten niet in de EU zijn gevestigd maar wel aan de AVG zijn gebonden. In de vorige versie van de richtsnoeren heeft de Artikel-29 Werkgroep aanbevolen dat een verwerkingsverantwoordelijke die buiten de EU is gevestigd en een vertegenwoordiger in de EU heeft aangewezen overeenkomstig artikel 27 AVG, een datalek dient te melden aan de toezichthoudende autoriteit in de EU-lidstaat waar de vertegenwoordiger van de verwerkingsverantwoordelijke is gevestigd.

Daarentegen staat in paragraaf 73 van de herziene richtsnoeren dat "de loutere aanwezigheid van een vertegenwoordiger in een lidstaat het éénloketsysteem niet in werking stelt". Daarom zal het datalek moeten worden gemeld aan elke toezichthoudende autoriteit in elke lidstaat waar de door het datalek getroffen betrokkenen verblijven, in plaats van alleen de toezichthoudende autoriteit van de lidstaat waar de hoofdvestiging zich bevindt. Dit valt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke.

De definitieve versie van de paragraaf werd aangenomen na een openbare raadpleging waarbij veel organisaties en personen kritiek hadden op de nieuwe aanpak. Deze kritiek betrof:

- De mogelijkheid dat de verwerkingsverantwoordelijke met grote onnodige kosten wordt opgezadeld;
- De administratieve lasten die voor de toezichthoudende autoriteiten worden gecreëerd;
- Dat niet in de EU gevestigde organisaties in een minder gunstige positie komen te verkeren dan in de EU gevestigde organisaties;
- Dat de procedure ingewikkelder wordt;
- Dat de reeds bestaande moeilijkheid om de termijn van 72 uur voor het melden van inbreuken op gegevens na te leven, nog groter wordt;
- Dat de doelstelling van een geharmoniseerde EU-aanpak van de bescherming van de rechten van de betrokkenen wordt geraakt.

De eerste versie van de herziene paragraaf bevatte de verplichting om de kennisgeving te doen "met inachtneming van het door de verwerkingsverantwoordelijke aan zijn vertegenwoordiger verstrekte mandaat en onder de verantwoordelijkheid van de verwerkingsverantwoordelijke". Dit werd echter, na de raadpleging, gewijzigd in uitsluitend een verantwoordelijkheid van verwerkingsverantwoordelijke. Wat de praktische gevolgen van deze nieuwe aanpak zullen zijn, moet nog blijken.

Wat betreft de bijgewerkte richtsnoeren voor de identificatie van de hoofdtoezichthouder voor een verwerkingsverantwoordelijke of verwerker, heeft de EDPB ook de eerder geldende richtsnoeren van Artikel-29 Werkgroep niet ingrijpend gewijzigd. De uitzondering is het nieuwe regime waar gezamenlijk verantwoordelijken zich aan moeten houden. De richtsnoeren bepalen namelijk dat de toezichthouders niet gebonden zijn aan de contractuele afspraken over welke gezamenlijke verwerkingsverantwoordelijke de hoofdvestiging zal zijn. Dat betekent dat wanneer het gaat om het melden bij de toezichthouder, er niet kan worden gekozen voor één hoofdvestiging die de melding doet. De melding geldt dan niet voor beide partijen.

In praktische zin betekent deze update van het richtsnoer dat wanneer er bijvoorbeeld sprake is van een datalek dat gemeld moet worden aan de toezichthouder, elke partij die gezamenlijke verwerkingsverantwoordelijkheid heeft, dit moet doen bij zijn respectievelijk toezichthouder. Dit is ongeacht of er een overeenkomst is over een hoofdvestiging.

1.2 EDPB dringt erop aan om de bevoegdheid om data te delen voor witwasbestrijding niet op te nemen in de wet

Eerder deze maand publiceerde de European Data Protection Board (EDPB) brieven die zij aan het Europees Parlement, de Raad van de Europese Unie en de Europese Commissie heeft gestuurd over bepalingen rondom het delen van data in het kader van het voorstel voor een nieuwe Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). De brieven werden verstuurd als reactie op het in eind 2022 aangenomen voorstel over de wet. De EDPB heeft met name bezorgdheid geuit over bepalingen inzake het delen van gegevens zoals omschreven in artikel 54 (3a), artikel 55(7) en artikel 55(5) van de Wwft.

De benoemde artikelen introduceren bepalingen in de Wwft op grond waarvan meldingsplichtige entiteiten, of soms overheidsinstanties, die partij zijn bij het "partnerschap voor informatie-uitwisselingen", onder bepaalde voorwaarden informatie moeten delen over "verdachte transacties" (artikel 54(3a)). Het delen van de informatie gebeurt in de eerste plaats aan een Financial Intelligence Unit (FIU), die in elk Europees land aanwezig is. Naast informatie over de transactie, moeten er persoonsgegevens worden gedeeld die als onderdeel van een onderzoek door de meldingsplichtige entiteit naar voren zijn gekomen (artikel 55(7)). Daarnaast zou de nieuwe Wwft de meldingsplichtige entiteiten toestaan onderling persoonsgegevens uit te wisselen als zij dat in het kader van hun "know-your-customer"-verplichtingen hebben verzameld. Dit mag alleen wanneer deze persoonsgegevens betrekking hebben op "abnormaliteiten of ongebruikelijke omstandigheden die wijzen op witwassen of financiering van terrorisme" (artikel 55(5)).

De EDPB erkent dat de bestrijding van witwassen en financiering van terrorisme een belangrijke taak is met openbaar belang, en de bestrijding een passend beleid en passende maatregelen verdient. Er wordt echter ook benadrukt hoe groot het belang is om een juist evenwicht te vinden tussen dergelijke wetgevingsdoeleinden en de belangen die ten grondslag liggen aan de fundamentele rechten op privacy en bescherming van persoonsgegevens, waarbij wordt verwezen naar het EU-Handvest. Om deze reden wordt in de brieven gewezen op de aanzienlijke risico's die bovengenoemde artikelen inhouden voor onze grondrechten. Ook wordt er bezorgdheid geuit over de rechtmatigheid, de noodzaak en de evenredigheid van de bepalingen inzake gegevensuitwisseling. In de brieven worden de medewetgevers van de EU dan ook dringend verzocht om bovengenoemde bepalingen niet in de definitieve tekst van de voorgestelde verordening op te nemen.

1.3 EDPB stelt nieuwe regels vast over de rechten van betrokkenen

De European Data Protection Board (EDPB) heeft een definitieve versie aangenomen van de Richtsnoeren 01/2022 betreffende de rechten van betrokkenen, specifiek over het recht van toegang, alsmede een handreiking voor de uitoefening van de rechten van betrokkenen in het kader van het Schengeninformatiesysteem (SIS).

In de Richtsnoeren worden de verschillende aspecten van het recht op inzage geanalyseerd en worden gedetailleerde aanwijzingen gegeven over de wijze waarop het recht in verschillende situaties moet worden toegepast. Zo verschaffen de Richtsnoeren duidelijkheid over de reikwijdte van het recht op inzage, de informatie die de verwerkingsverantwoordelijke aan de betrokkene moet verstrekken, het format van het inzageverzoek, de belangrijkste manieren voor het verlenen van inzage en het begrip "kennelijk ongegronde of buitensporige verzoeken".

De Richtsnoeren omschrijven dat het recht op inzage drie elementen omvat, namelijk:

- Bevestiging of persoonsgegevens over een persoon al dan niet worden verwerkt;
- Toegang tot deze data; en
- Informatie over de verwerking zoals omschreven in artikel 15(1) AVG en, waar toepasbaar, artikel 15(2) AVG, zoals het doel, de categorieën persoonsgegevens en ontvangers, de duur van de verwerking, de rechten van betrokkenen en passende waarborgen in geval van doorgifte aan derde landen.

Er zijn geen specifieke vereisten over de vorm waarin een verzoek tot inzage van een betrokkene wordt gedaan. Wat van belang is bij de analyse van het verzoek, is dat de verwerkingsverantwoordelijke moet beoordelen of het verzoek betrekking heeft op de persoonsgegevens van de verzoeker, of het verzoek valt binnen de werkingssfeer van artikel 15 AVG en of andere, sectorspecifieke bepalingen van toepassing zijn die de inzage tot persoonsgegevens regelen.

Een belangrijk element van de Richtsnoeren zijn de manieren voor het verlenen van toegang tot de gegevens, waarbij in de Richtsnoeren staat dat de belangrijkste manier is om de betrokkene een kopie van zijn persoonsgegevens de verstrekken. In sommige omstandigheden kunnen andere methoden geschikt zijn, zoals mondelinge informatie, inzage in bestanden, en toegang ter plaatse of op afstand zonder de mogelijkheid om te downloaden.

Een tweede belangrijk element van de Richtsnoeren is een verduidelijking van wat als een "kennelijk ongegrond of buitensporig verzoek" wordt beschouwd. In de richtsnoeren wordt erop gewezen dat een beroep doen op een "kennelijk ongegronde" uitzondering op artikel 12(5) AVG slechts in zeer beperkte omstandigheden mogelijk is.

Wat betreft “buitensporige” verzoeken, hangt de beoordeling van de “buitensporigheid” af van de door de verwerkingsverantwoordelijke uitgevoerde analyse en de specifieke kenmerken van de sector waarin hij actief is.

Een andere ontwikkeling van de EDPB op het gebied van rechten van betrokkenen is de handleiding voor de uitoefeningen van de rechten van betrokkenen in het kader van SIS. De handleiding beschrijft de voorwaarden voor de uitoefening van het recht op inzage, het recht op rectificatie en aanvulling en het recht op verwijdering van onrechtmatig in het SIS opgeslagen gegevens. De handleiding bevat een beschrijving van het SIS, de rechten die worden toegekend aan personen wier gegevens in het SIS worden verwerkt, en een beschrijving van de procedure voor de uitoefening van de rechten in elk van de bij het SIS betrokken landen. De handleiding bevat ook modelbrieven voor het aanvragen van bovengenoemde rechten.

1.4 Europese Commissie lanceert Europees Centrum voor Algoritmische Transparantie

Het Europees Centrum voor Algoritmische Transparantie heeft officieel zijn deuren geopend in Sevilla, Spanje. Als tak van de interne onderzoeksdienst van de Europese Commissie, het Gemeenschappelijk Centrum voor Onderzoek (GCO), zal het algoritmisch centrum de uitvoerende macht van de EU bijstaan bij de handhaving van de digitale wetgeving door zogenoemd algoritmische black boxes te ontcijferen. Het centrum wordt een internationaal centrum voor onderzoek op dit gebied en levert wetenschappelijke en technologische expertise aan de Commissie voor de handhaving van de Digital Services Act (DSA). De wetgeving voert strenge maatregelen in voor grote online platforms zoals Facebook en Twitter, die onder rechtstreeks toezicht van de Europese Commissie komen te staan. De eerste taak van het Centrum is de Commissie te ondersteunen bij de handhaving van de DSA door methodologie en documentatie te leveren voor de handhaving van nieuwe regels voor algoritmen met betrekking tot kwesties als geestelijke gezondheid, discriminatie, haatzaaiing en desinformatie.

Het Centrum zal onafhankelijk onderzoek verrichten naar de ethische implicaties van algoritmen, wat van cruciaal belang is, aangezien de interne werking van algoritmen en hun effecten op de samenleving nog steeds een grotendeels onderbelicht onderwerp zijn. Het nieuwe expertisecentrum moet technische maatregelen nemen om te voldoen aan de DSA door trainingsdatasets te analyseren om ervoor te zorgen dat ze niet bevooroordeeld zijn ten gunste van een specifieke demografische groep. Het algoritmecentrum zal niet geïsoleerd werken, maar zal een katalysator zijn voor de onderzoeksgemeenschap en partnerschappen opzetten met overheidsinstanties, onderzoekscentra en deskundigen.

Het eerste partnerschap van het nieuwe centrum is met de Pôle d'expertise de la régulation numérique (PEReN), een Frans orgaan dat beleidsmakers en regelgevers ondersteunt op het gebied van gegevensbescherming, consumentenbescherming en concurrentie. Het Centrum is nog in de opstartfase en zal bestaan uit tien mensen van het GCO plus 20 nieuwe medewerkers, variërend van IT-deskundigen tot sociale wetenschappers. De Commissie heeft meer dan 500 sollicitaties voor deze posities ontvangen. De personeelskosten zullen worden gedekt met de toezichtsvergoeding van de DSA. Het uiteindelijke doel van het Centrum is om bedrijven ter verantwoording te roepen en een echte verandering in het schadelijke gedrag van platforms teweeg te brengen.

2. NATIONAAL NIEUWS

Hoogtepunten:

- Algemene Rekenkamer kritisch over AVG
- Autoriteit Persoonsgegevens gaat gemeentes helpen met inzet schuldhulpverlening
- Boete Sociale Verzekeringsbank na gebrekkige identiteitscontrole

2.1 Algemene Rekenkamer wil eerdere en duidelijkere keuzes AVG

Begin deze maand heeft de Algemene Rekenkamer aan de bel getrokken bij de Tweede Kamer. De Algemene Verordening Gegevensbescherming (AVG) wordt als obstakel ervaren door overheidsorganisaties, wat gevolgen kan hebben voor burgers.

In de afgelopen jaren heeft de Algemene Rekenkamer onderzoek gedaan naar verschillende overheidsorganisaties en de invloed van de AVG op hun werk. Uit angst voor privacyregels stellen overheidsorganisaties zich te terughoudend op als het gaat om het onderling delen van informatie. Ook worden privacyregels mogelijk als gelegenheidsargument gebruikt om informatie niet met andere overheidspartijen te hoeven delen. Daardoor komt de uitvoering van overheidstaken regelmatig in de knel, met mogelijk grote gevolgen voor burgers. De belangrijkste boodschap die de Algemene Rekenkamer naar voren wil brengen is dat de AVG voldoende ruimte biedt om digitalisering van de overheid een kans te bieden. Het probleem ligt daarom ook niet bij de Verordening, maar bij de implementatie van de Verordening. De regering, het parlement en de uitvoeringsorganisaties zelf moeten een afweging maken waar zij de baten van gegevensverwerking afwegen tegen de gevolgen voor de privacy van de burgers.

De Algemene Rekenkamer geeft twee opties om de AVG beter te implementeren binnen de uitvoeringsorganisaties van de Rijksoverheid:

1. In de parlementaire behandeling van wetsvoorstellen moet er structureel aandacht worden gegeven aan de benodigde verwerking van persoonsgegevens;
2. De kennis over de AVG binnen ministeries en uitvoeringsorganisaties moet worden vergroot.

Als de suggesties van de Rekenkamer worden overgenomen, zal privacywetgeving minder vaak als argument worden gebruikt tegen het delen van gegevens, verwacht Barbara Joziasse, collegelid van de Algemene Rekenkamer.

2.2 AP geeft advies over betere hulp aan mensen met ernstige schulden

De Autoriteit Persoonsgegevens (AP) heeft gemeenten en de energiesector geadviseerd over de bescherming van de privacy van mensen met ernstige schulden en hoe zij hen tijdig kunnen helpen. Gemeenten hebben namelijk in sommige gevallen de plicht om hulp te bieden aan mensen met ernstige schulden, maar de nationale wet- en regelgeving is onduidelijk over welke gegevens van mensen zij met elkaar kunnen delen en hoe vaak ze dit kunnen doen. De AP heeft de relevante wet- en regelgeving geanalyseerd en aangegeven welke privacywaarborgen nodig zijn bij het aanbieden van hulp aan mensen met ernstige schulden.

Het initiatief lag bij de Vereniging van Nederlandse Gemeenten (VNG) om de AP te vragen deze kwestie op te helderen. Het doel is om gemeenten en energieleveranciers te helpen bij het bieden van hulp aan mensen met ernstige schulden, vooral nu de energieprijzen stijgen en sommige mensen dreigen afgesloten te worden van gas en elektriciteit. Gemeenten willen graag inwoners met ernstige schulden vaker dan één keer kunnen benaderen met hulp, maar dit zou betekenen dat er ook vaker persoonlijke informatie wordt gebruikt.

De AP steunt een brede interpretatie van de huidige wettelijke mogelijkheden, maar benadrukt dat deze interpretatie ook duidelijker moet worden vastgelegd. Gemeenten en energieleveranciers zijn het hiermee eens en de verantwoordelijke ministeries, Economische Zaken en Klimaat (EZK) en Sociale Zaken en Werkgelegenheid (SZW), zullen het beleid verduidelijken in de wet. De AP heeft aangeboden om hierbij op hoofdlijnen mee te kijken en zal ook een wetgevingsadvies uitbrengen over de wijziging van de Regeling afsluitbeleid voor kleinverbruikers van elektriciteit en gas en de wetswijziging van de Wet gemeentelijke schuldhulpverlening (Wgs).

Katja Mur, AP-bestuurder, benadrukt dat de AP met dit initiatief laat zien dat zij rekening houdt met de vragen waarmee organisaties soms zitten, zonder de rol van de AP als onafhankelijk toezichthouder uit het oog te verliezen. Het doel is om een oplossing te vinden die privacyvriendelijk is en mensen met ernstige schulden tijdig te helpen, zodat zij niet nog verder in de problemen komen.

2.3 Boete Sociale Verzekeringsbank na gebrekkige identiteitscontrole

De Autoriteit Persoonsgegevens (AP) heeft de Sociale Verzekeringsbank (SVB) een boete opgelegd van 150.000 euro.

De SVB is verantwoordelijk voor het uitvoeren van verschillende wetten die verband houden met sociale zekerheid, waaronder de AOW en de kinderbijslag. De SVB zorgt ervoor dat klanten weten waarop zij recht hebben, en dat zij eventuele vergoedingen ook ontvangen. Om deze taak te vervullen, verwerkt de SVB persoonsgegevens van onder andere verzekerden, pensioengerechtigden, nabestaanden en andere uitkeringsgerechtigden. Cliënten kunnen onder andere telefonisch contact opnemen met de SVB. Dit doen gemiddeld zo'n 20.000 mensen per week.

In 2019 is er een melding gedaan bij de AP door een SVB-cliënt, van wie de persoonsgegevens in handen zijn gekomen van iemand anders. De klaagster ontdekte namelijk dat een familielid persoonlijke informatie over haar zou hebben ontvangen van een medewerker van de SVB, terwijl zij de SVB geen toestemming had gegeven voor het delen van deze informatie. Op dezelfde dag van de melding, heeft de SVB ook een melding gedaan bij de AP van een datalek. In deze melding gaf de SVB onder andere aan dat er onbevoegd mondeling persoonsgegevens zijn gedeeld met een onbevoegde ontvanger. Omdat de AP in de eerste instantie geen reden zag tot onderzoek, heeft de klaagster bezwaar gemaakt. Naar aanleiding van dit bezwaar is de AP alsnog gestart met het onderzoek. Het onderzoek richt zich op naleving van artikel 5(1) en artikel 32 AVG.

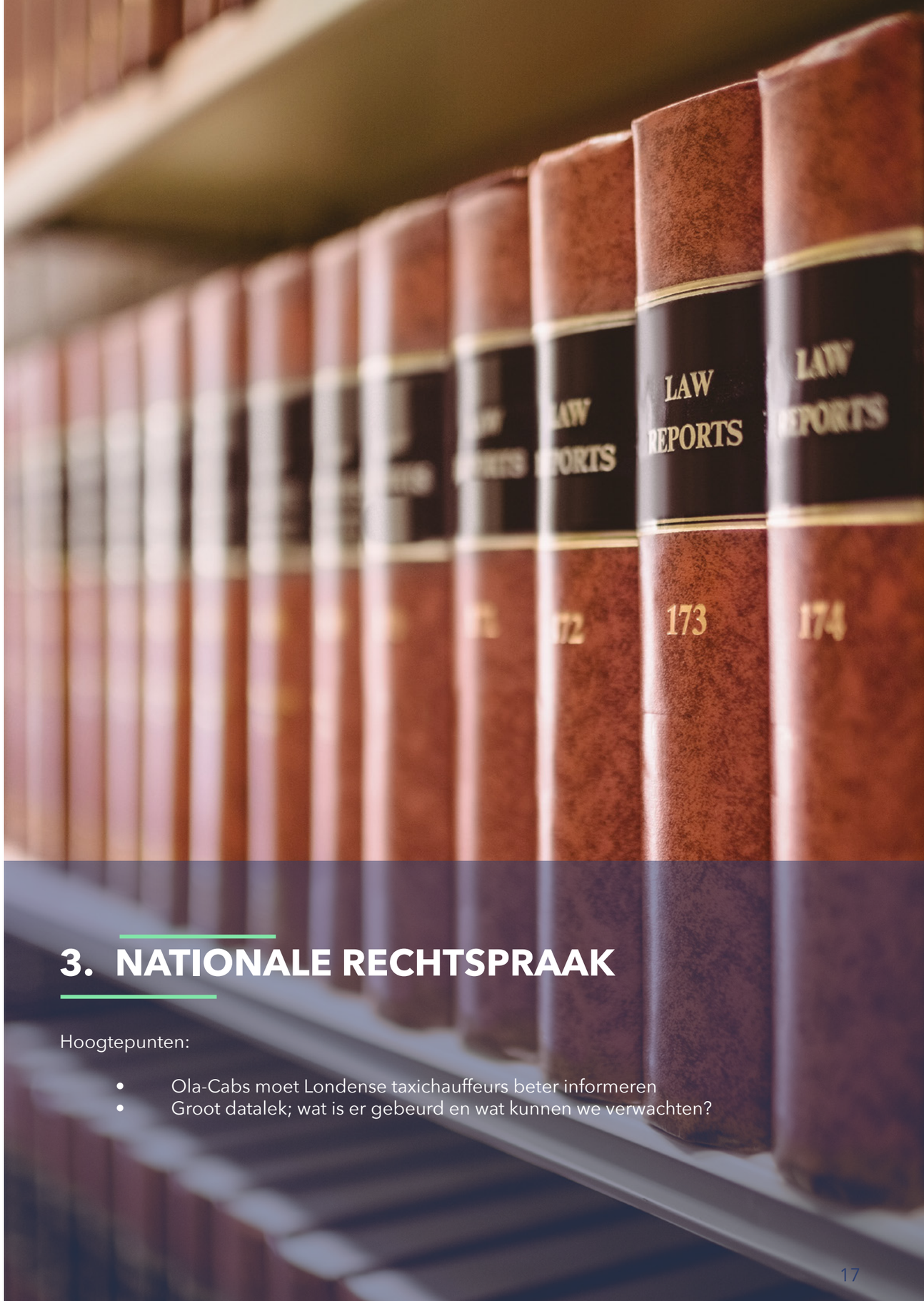
Uit het onderzoek kwam naar voren dat de SVB te weinig deed om privacy risico's van de telefonische dienstverlening in kaart te brengen. In het systeem van SVB staan onduidelijke werkinstructies over het authentiseren van de identiteit van de persoon die belt. Zo zijn de controlevragen vaak makkelijk te beantwoorden voor buitenstaanders. De uitvoering van het beleid werd ook niet goed genoeg gecontroleerd door de SVB, wat ertoe leidde dat het beleid niet goed werd nageleefd.

Naast authenticatie is bewustwording een beveiligingsmaatregel die door de SVB is ingezet om persoonsgegevens te beschermen tijdens het telefonisch klantcontact. Dit gebeurde onvoldoende. Bovenstaande overtredingen duurden van mei 2018 tot mei 2022.

In reactie op het onderzoek heeft de SVB een risico-inventarisatie voorgelegd aan de AP. Volgens de AP worden in deze inventarisatie risico's voldoende geïdentificeerd en beoordeeld. Daarnaast is er een plan van aanpak vastgesteld door de SVB, waarin een pakket verbetermaatregelen is opgenomen om de risico's te beperken. In juni 2022 zijn deze maatregelen ook geïmplementeerd. De AP ziet deze maatregelen als toereikend.

Desalniettemin heeft de SVB artikel 32(1)(2) AVG overtreden. In de periode van mei 2018 tot juni 2022 heeft de SVB volgens de AP nagelaten passende technische en organisatorische maatregelen te treffen met betrekking tot het verwerken van persoonsgegevens in het kader van telefonisch klantcontact met AOW-klanten.

Omdat de SVB inmiddels voldoet aan bovenstaande, vindt de AP het gepast om de boete aanzienlijk te verlagen ten opzichte van de basisboetes.



3. NATIONALE RECHTSPRAAK

Hoogtepunten:

- Ola-Cabs moet Londense taxichauffeurs beter informeren
- Groot datalek; wat is er gebeurd en wat kunnen we verwachten?

3.1 Ola-Cabs moet Londense taxichauffeurs beter informeren

Het Gerechtshof Amsterdam heeft begin april 2023 uitspraak gedaan ten aanzien van een aantal zaken die door Londense taxichauffeurs, gesteund door hun vakbond (de App Drivers & Couriers Union), bij de Nederlandse rechter waren aangespannen tegen de digitale platforms Uber en Ola-Cabs.

De zaak tegen Ola-Cabs kwam tot stand nadat de taxichauffeurs Ola-Cabs onder meer verzochten om inzage in de persoonsgegevens op grond van artikel 15 AVG, uitvoering van hun recht op dataportabiliteit zoals beschreven in artikel 20 AVG en verstrekking van informatie over geautomatiseerde besluitvorming in lijn met artikel 22 AVG. In reactie hierop heeft Ola-Cabs een aantal digitale bestanden en kopieën van documenten aan de taxichauffeurs verstrekt.

Bij gebrek aan toereikende informatie, hebben de taxichauffeurs Ola-Cabs in eerste aanleg bevolen de opgevraagde informatie te verschaffen. Naar aanleiding hiervan heeft de rechtbank Ola-Cabs bevolen inzage te verschaffen ten aanzien van bepaalde persoonsgegevens, waaronder de persoonsgegevens die zijn gebruikt voor het opstellen van het risicoprofiel, het 'earning profile', de 'rating history' en ook heeft de rechtbank Ola-Cabs bevolen om, in het kader van het geautomatiseerde besluitvormingsproces, de taxichauffeurs te informeren over de belangrijkste beoordelingscriteria en de rol hiervan op het geautomatiseerde besluit, zodat zij kunnen begrijpen op grond van welke criteria de besluiten zijn genomen en zij in staat zijn de juistheid en rechtmatigheid van de gegevensverwerking te controleren.

Volgens de uitspraak was de wens van de chauffeurs te algemeen, waardoor niet alle gewenste gegevens werden gevorderd. In reactie hierop gingen de taxichauffeurs in hoger beroep. Naar aanleiding waarvan het Hof de taxichauffeurs voor een deel in het gelijk heeft gesteld. Het Hof komt namelijk tot het oordeel dat er sprake is van besluiten die volledig geautomatiseerd zijn en zonder menselijke tussenkomst worden genomen. Deze geautomatiseerde besluiten raken de taxichauffeurs ernstig omdat zij bepalend zijn voor hun inkomsten. Daarnaast kunnen geautomatiseerde besluiten rondom fraude-vermoedens ook andere gevolgen voor de taxichauffeurs met zich meebrengen, bijvoorbeeld implicaties rondom het behoud van de Londense taxilicentie.

Om deze reden is Ola-Cabs verplicht om de taxichauffeurs te informeren op basis waarvan Ola-Cabs tot voornoemde besluiten komt en moet zij de taxichauffeurs voorzien van andere informatie die nodig wordt geacht om de redenen van een besluit te kunnen begrijpen. Dit alles maakt het voor de taxichauffeurs mogelijk om hun rechten op grond van de AVG uit te kunnen oefenen. Tot slot, bepaalde het Hof in deze zaak dat in deze zaak door Ola-Cabs geen beroep kon worden gedaan op het recht op bescherming van hun bedrijfsgeheimen aangezien het voor de bescherming van dat recht niet noodzakelijk was voor Ola-Cabs om de door de chauffeurs opgevraagde informatie te weigeren.

3.2 Blauw wint kort geding tegen Nebu

Onlangs is er een groot datalek aan het licht gekomen. Dat datalek is het resultaat van een cyberaanval op softwareleverancier Nebu. Als gevolg daarvan is mogelijk de persoonlijke informatie van miljoenen personen in handen van cybercriminelen gekomen.

Blauw is een marketingonderzoeksbureau dat namens verschillende organisaties, waaronder NS en VodafoneZiggo, klanttevredenheidsonderzoeken verricht. Blauw gebruikt software van Nebu voor het uitvoeren van deze onderzoeken. Op 10 en 11 maart is Nebu het slachtoffer geworden van een cyberaanval. Hierbij hebben de aanvallers gegevens buitgemaakt. Welke gegevens dit precies zijn, is momenteel nog niet bekend. Blauw meent "in principe" de naam, het e-mailadres, klantsoort en enquêteresultaten van de betrokkenen te bewaren. Of deze gegevens ook daadwerkelijk gelekt zijn, moet nog blijken uit het onderzoek dat momenteel wordt gedaan naar het datalek. De NS benadrukt dat het in ieder geval niet gaat om financiële gegevens of wachtwoorden.

Nadat Nebu Blauw informeerde over het datalek, vroeg Blauw Nebu om meer informatie te verstrekken over de precieze feiten van het lek, hoe het datalek is ontstaan en of het datalek redelijkerwijs voorkomen had kunnen worden. Toen Nebu deze informatie niet verstrekte, spande Blauw bij de rechtbank Rotterdam een kort geding aan tegen Nebu. Blauw vorderde, samengevat, informatie over het datalek en een extern forensisch onderzoek naar de oorzaak van het lek.

In zijn beslissing kijkt de rechtbank onder andere naar de uitleg van de verwerkersovereenkomst die tussen Blauw en Nebu geldt. Hierin is, onder meer, opgenomen dat Blauw onmiddellijk (of in ieder geval binnen 24 uur na het optreden van het incident) in kennis wordt gebracht van elk incident in verband met de verwerking van persoonsgegevens, Nebu volledige medewerking verleent aan Blauw en instructies van Blauw in dit kader opvolgt. Dit zodat Blauw in staat wordt gesteld het incident naar behoren te onderzoeken, een reactie naar de buitenwereld kan formuleren en passende vervolgstappen kan nemen. De opgenomen clausule is gebaseerd op de in artikel 28(3) AVG geformuleerde informatie en bijstand-verplichting van de verwerker.

Volgens de kortgedingrechter moet Nebu op "loyale en royale wijze" aan deze verplichtingen voldoen. De rechter wijst de vorderingen van Blauw in de procedure dan ook grotendeels toe. Nebu moet, onder meer, informatie verstrekken over de details van de cyberaanval, hoe het herstel van de systemen is verlopen, van welke klanten persoonsgegevens zijn gelekt, wie de daders van de cyberaanval zijn en de maatregelen die zijn genomen. Ook de eis om een extern forensisch onderzoek naar de oorzaak van het lek te doen, wordt door de rechter toegewezen: binnen vijf werkdagen na de uitspraak moet Nebu een externe partij aan boord brengen om dit onderzoek uit te voeren. Binnen vier weken moet het rapport worden opgeleverd.

4. WERELDWIJDE ONTWIKKELINGEN

Hoogtepunten:

- Italiaanse toezichthouder verbiedt tijdelijk ChatGPT
- Arrestaties na uit de lucht halen Genesis Market
- Advies ICO over Generatieve Kunstmatige Intelligentie

4.1 Italiaanse toezichthouder beperkt tijdelijk de verwerking van persoonsgegevens van Italiaanse gebruikers door OpenAI via ChatGPT

Het besluit van de Italiaanse toezichthouter (Garante) om ChatGPT te verbieden werd genomen kort na het datalek bij OpenAI op 20 maart, waarbij de betalingsgegevens en de conversatiegeschiedenis van ChatGPT-gebruikers waren uitgelekt. Het besluit belicht enkele van de potentiële gegevensbeschermingsproblemen die ChatGPT, een generatieve AI-tool, veroorzaakt bij de verwerking van persoonsgegevens om de onderliggende machine learning-algoritmen te "trainen".

Garante merkte vooral op dat OpenAI's ChatGPT de AVG op de volgende punten schond:

1. OpenAI verzuimde de gebruikers van ChatGPT transparante informatie te verstrekken over de wijze waarop zij hun persoonsgegevens verwerkte, en over de wijze waarop de persoonsgegevens van andere personen werden verzameld;
2. OpenAI ontbeerde een rechtsgrondslag om persoonsgegevens te verwerken voor het trainen van het algoritme dat het platform van ChatGPT aandrijft;
3. OpenAI stond ChatGPT toe persoonsgegevens onnauwkeurig te verwerken, aangezien de antwoorden van ChatGPT niet altijd actueel waren;
4. OpenAI heeft nagelaten de leeftijd van gebruikers te verifiëren, waardoor minderjarige gebruikers onder de 13 jaar werden blootgesteld aan antwoorden die ongeschikt waren voor hun niveau van bewustzijn en ontwikkeling.

Garante bepaalde echter op 11 april dat als OpenAI voor 30 april bepaalde "concrete maatregelen" neemt, de tijdelijke beperking van de gegevensverwerking door ChatGPT wordt opgeheven. Garante eist dat OpenAI:

1. Een transparante en toegankelijke kennisgeving verstrekt over bijvoorbeeld de methoden en logica van de werking van ChatGPT en de rechten van gebruikers en niet-gebruikers voorafgaand aan elke gegevensverwerking, met inbegrip van registratie. De informatie moet ook worden verstrekt zodra ChatGPT opnieuw wordt geactiveerd, aan geregistreerde gebruikers;
2. Ten minste Italiaanse gebruikers een instrument ter beschikking stellen waarmee zij bezwaar kunnen maken tegen gegevensverwerking ten behoeve van de training van de algoritmen van ChatGPT, om rectificatie van door ChatGPT gegenereerde onjuiste inhoud kunnen verzoeken en persoonsgegevens kunnen wissen;
3. De rechtsgrondslag van ChatGPT voor verwerking wijzigen van contractuele verplichting in toestemming of legitieme belangen;
4. Een leeftijdsgrens invoeren voor Italiaanse gebruikers, ongeacht of zij geregistreerd zijn of niet, om minderjarige gebruikers uit te sluiten.

Bovendien moet OpenAI uiterlijk op 31 mei een plan indienen voor het inzetten van instrumenten voor leeftijdscontrole en uiterlijk op 15 mei via alle Italiaanse massamedia een informatiecampagne opzetten over de manier waarop ChatGPT gegevens verwerkt en over de rechten die gebruikers en niet-gebruikers hebben.

In het besluit van Garante wordt echter niet (i) verwezen naar het recht op gegevensportabiliteit van gebruikers, (ii) duidelijkheid verschaft over hoe organisaties zoals OpenAI zich precies kunnen beroepen op legitieme belangen bij het verwerken van gegevens voor het trainen van een algoritme en wat de afwegingstoets moet zijn, (iii) een onderscheid gemaakt tussen OpenAI dat persoonsgegevens gebruikt en gebruikers die zelf persoonsgegevens invoeren in een reeds getraind algoritmisch model. Het is ook uiterst verrassend dat Garante OpenAI niet onmiddellijk heeft beboet voor privacyschendingen, maar hen in plaats daarvan de tijd heeft gegeven om deze recht te zetten. Interessant genoeg paste Garante onlangs dezelfde aanpak toe bij het verbieden van Replika, een AI-gestuurde chatbot, wegens schendingen van de AVG.

Nu de Spaanse, Franse en Duitse gegevensbeschermingsautoriteiten soortgelijke acties tegen ChatGPT overwegen en het Europees Comité voor gegevensbescherming onlangs een taskforce heeft opgericht om de samenwerking tussen de gegevensbeschermingsautoriteiten te versterken en handhavingsacties te coördineren, zullen generatieve AI-instrumenten die persoonsgegevens verwerken binnenkort zwaar onder de loep worden genomen door regelgevers in de EU.

4.2 Nederlandse politie arresteert cybercriminelen na internationale operatie die wereldwijde hackersmarkt neerhaalt

De Nederlandse politie heeft zeventien Nederlanders gearresteerd in een internationale operatie tegen een grootschalige online marktplaats voor online identiteitsfraude. Het gaat om verdachten die gebruik maakten van de zogenaamde Genesis Market. Hierop werden onder meer persoonsgegevens zoals bankrekeningnummers van miljoenen mensen verhandeld, maar ook bots die op basis van die gegevens hacks konden uitvoeren. Daarmee was Genesis Market een van de grootste en belangrijkste online platforms voor cybercriminelen. De site was alleen toegankelijk via een uitnodiging van andere gebruikers en werd over de hele wereld gebruikt.

De operatie tegen Genesis Market was een gezamenlijke actie van opsporingsdiensten uit verschillende landen, waaronder de Verenigde Staten, Australië, het Verenigd Koninkrijk, Duitsland en Nederland. Bij de operatie werden wereldwijd meer dan 200 mensen gearresteerd. De FBI, die ook de website van Genesis offline haalde, doopte de actie om tot 'Operation Cookie Monster'. Het Nederlandse deel van het onderzoek geldt als het meest omvangrijke cybercrime-onderzoek tot nu toe op nationaal niveau.

De Nederlandse verdachten werden gearresteerd na invallen op verschillende locaties in het land. Onder meer computers, telefoons en geld werden in beslag genomen. De verdachten worden beschuldigd van betrokkenheid bij de handel in illegale goederen en diensten via Genesis Market. De operatie tegen Genesis Market is een belangrijke slag tegen de wereldwijde cybercriminaliteit. Het toont aan dat internationale samenwerking tussen opsporingsdiensten essentieel is om deze vorm van criminaliteit aan te pakken.

Vermoed wordt dat de persoonsgegevens, die van 1,5 miljoen computers zouden zijn gestolen, betrekking hebben op meer dan twee miljoen potentiële slachtoffers. De Nederlandse politie heeft een website opgezet waar iedereen kan controleren of zijn e-mailadres voorkomt in pakketten met gehackte gegevens. De website is te vinden op: https://www.politie.nl/en/information/checkyourhack.html

4.3 ICO publiceert vragenlijst voor verantwoorde omgang met persoonsgegevens bij de ontwikkeling en gebruik van Generatieve Kunstmatige Intelligentie

Met de razendsnelle ontwikkelingen in de wereld van zogeheten 'generatieve kunstmatige intelligentie' (GKI), zijn steeds meer academici, technici en andere partijen van mening dat het belangrijk is om een stap terug te doen en na te denken over de manier waarop persoonsgegevens binnen de populaire toepassingen van deze technologie – waaronder ChatGPT – worden gebruikt.

GKI heeft, net als iedere andere technologie die de afgelopen jaren de revue heeft gepasseerd, bij onverantwoord gebruik het potentieel om inbreuk te maken op de privacy van gegevens. Hoewel de technologie nieuw is, blijven de beginselen van de gegevensbeschermingswetgeving echter dezelfde en zijn deze ook van toepassing op GKI.

Organisaties die GKI ontwikkelen of hiervan gebruikmaken, dienen al vanaf het begin af aan na te denken over de wijze waarop zij aan hun verplichtingen op het gebied van gegevensbescherming zullen voldoen. Dit geldt ook wanneer zij persoonsgegevens verwerken die afkomstig zijn uit openbaar toegankelijke bronnen.

Ter ondersteuning bij de invulling van hun verplichtingen, heeft de Britse ICO een lijst met vragen opgesteld die organisaties die GKI ontwikkelen of hiervan gebruikmaken zichzelf kunnen stellen, namelijk:

1. **Wat is uw rechtsgrondslag voor de verwerking van persoonsgegevens?** Waar persoonsgegevens worden verwerkt, dient deze verwerking plaats te vinden op basis van een passende rechtsgrondslag zoals neergelegd in artikel 6 AVG.
2. **Bent u verwerkingsverantwoordelijke, gezamenlijk verwerkingsverantwoordelijke of verwerker?** Afhankelijk van de rol die een organisatie bekleedt, gelden onder de AVG specifieke verplichtingen ten opzichte van betrokkenen.
3. **Heeft u een DPIA uitgevoerd?** Eventuele risico's voor gegevensbescherming moeten voordat persoonsgegevens verwerkt worden, beoordeeld en beperkt worden middels het uitvoeren van een DPIA. Naarmate de verwerkingsactiviteiten en de gevolgen daarvan zich ontwikkelen, dient de reeds opgestelde DPIA te worden bijgewerkt.
4. **Hoe garandeert u transparantie?** Informatie over de verwerking dient openbaar toegankelijk gemaakt te worden, tenzij een vrijstelling van toepassing is. Indien dit geen onevenredige inspanning vergt, dient deze informatie rechtstreeks bekend gemaakt te worden aan de personen op wie de gegevens betrekking hebben.
5. **Hoe bent u voornemens de beveiligingsrisico's te beperken?** Naast de risico's van het lekken van persoonsgegevens dienen de risico's van zogeheten model inversion en membership inference, data poisoning en andere vormen van vijandige aanvallen zo veel mogelijk overwogen en beperkt te worden.
6. **Hoe bent u voornemens onnodige verwerking te beperken?** Organisaties mogen alleen die gegevens verwerken die toereikend zijn om de voorgenomen doelen te bereiken. Hierbij geldt dat de gegevens relevant moeten zijn en beperkt moeten blijven tot het noodzakelijke.
7. **Hoe bent u voornemens te voldoen aan verzoeken van betrokkenen tot het uitoefenen van hun rechten?** Waar betrokkenen een beroep doen op hun rechten onder de AVG, waaronder verzoeken om toegang, rectificatie, uitwissing of andere rechten op informatie, dient hieraan in beginsel gehoor te worden gegeven.
8. **Gaat u GKI gebruiken om uitsluitend geautomatiseerde beslissingen te nemen?** Zo ja - en deze hebben wettelijke of vergelijkbaar significante gevolgen (bijv. belangrijke diagnoses in de gezondheidszorg) - dan hebben individuen verdere rechten op grond van artikel 22 van de AVG.

De ICO heeft aangegeven deze vragenlijst voor te zullen leggen aan organisaties die GKI ontwikkelen of hiervan gebruikmaken om hen op die wijze te ondersteunen en aan te moedigen zich aan de wetgeving rondom privacy en gegevensbescherming te houden. Waar organisaties zich niet aan deze wetgeving houden, stelt de ICO hiertegen op te zullen treden.

Onlangs heeft de ICO een bijgewerkte versie van haar leidraad over AI en gegevensbescherming beschikbaar gesteld. Hierin biedt zij een stappenplan voor gegevensbescherming voor ontwikkelaars en gebruikers van GKI. Daarnaast biedt zij ook een bijbehorende risicotoolkit aan de hand waarvan organisaties risico's rondom gegevensbescherming kunnen identificeren en beperken.

Tot slot is het voor organisaties die innoveren middels data en GKI mogelijk om eventuele vragen over de toepassing van wetgeving rondom gegevensbescherming voor te leggen aan de ICO middels haar Regulatory Sandbox en nieuwe dienst Innovation Advice. In aanvulling hierop is de ICO verder bezig met een proefproject voor een zogeheten Mullti-Agency Advice Service voor digitale innovators die behoefte hebben aan gezamenlijk advies van meerdere regelgevende instanties, samen met de ICO-partners in het Digital Regulation Cooperation Forum.