KIENHUIS HOVING

ADVOCATEN EN NOTARISSEN

Aansprakelijkheid en handhaving Nieuwe technologie, nieuwe regels: Nis2, AI en … AVG

Mr. dr. Roeland de Bruin LL.M.
Advocaat KienhuisHoving;
UD Universiteit Utrecht (CAAAi)

Roeland.debruin@kienhuishoving.nl

Previder event 2024

Wat gaan we doen?

Outline

1. NIS2
    1. Enkele regels
    2. Handhaving en aansprakelijkheid
2. AI
    1. Enkele regels: rollen en verantwoordelijkheden
    2. Handhaving en aansprakelijkheid
3. AVG
    1. Enkele regels: rollen en verantwoordelijkheden
    2. Handhaving en aansprakelijkheid

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

1. NIS2

- **Richtlijn inzake netwerk en informatiebeveiliging**
- **Volgt de eerste NIB-richtlijn op (Wet Beveiliging Netwerk- en Informatiesystemen)**
- **Wordt nu geïmplementeerd (omgezet) in Nederlandse regels**
- **Beoogt cyberveiligheid en weerbaarheid van essentiële diensten te vergroten**
- **Strengere beveiligingsnormen, meldingsplichten en meer sectoren in scope**

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

1. NIS2: voor wie?

Sectoren bijlage 1	Sectoren bijlage 2
■ Energie	■ Digitale aanbieders
■ Transport	■ Post- en koeriersdiensten
■ Bankwezen	■ Afvalstoffenbeheer
■ Infrastructuur financiële markt	■ Levensmiddelen
■ Gezondheidszorg	■ Chemische stoffen
■ Drinkwater	■ Onderzoek
■ Digitale infrastructuur	■ Vervaardiging / manufacturing
■ Beheerders van ICT-diensten	
■ Afvalwater	
■ Overheidsdiensten	
■ Ruimtevaart	


Wat betekent de NIS2-richtlijn voor jouw organisatie?
De NIS2-richtlijn richt zich op sectoren die al onder de eerste NIS-richtlijn vallen, en op een aantal nieuwe sectoren. Een belangrijk verschil met de eerste richtlijn is dat de sector Overheid er nu ook binnen valt. De richtlijn bevat een toelichting over welke specifieke overheidsinstanties onder de verplichtingen vallen:
• Onderdelen van de centrale overheid (Rijksoverheid en zelfstandige bestuursorganen) vallen onder de NIS2-richtlijn als essentiële entiteiten.
• Het is aan de lidstaten zelf om lokale overheden (gemeenten, waterschappen en provincies) onder de NIS2-richtlijn te laten vallen. De bedoeling is om medeoverheden onder de richtlijn aan te wijzen. Dit gezien bestaande beleidsvoornemens tot wettelijke verankering van de BIO, en het inregelen van toezicht voor de gehele overheid.
• De NIS2-richtlijn biedt een uitzondering voor overheidsinstanties die vooral activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving (inclusief het voorkomen, onderzoeken en opsporen van strafbare feiten). Dit betekent dat bijvoorbeeld de veiligheidsregio's of de politie van de NIS2-richtlijn zijn uitgesloten. Overheidsinstanties met activiteiten die indirect te maken hebben met bijvoorbeeld nationale veiligheid vallen wel onder toepassing van de richtlijn.

- **Essentiële entiteiten**
  - **Kritieke entiteiten -> CER-richtlijn**
  - **Grote organisaties uit sector 1**
    - **> 250 werknemers, of**
    - **> 50 miljoen euro jaaromzet + > 43 miljoen euro balanstotaal**

- **Belangrijke entiteiten**
  - **Middelgrote organisaties uit sector 1, & grote en middelgrote organisaties uit sector 2:**
    - **> 50 werknemers, of**
    - **> 10 miljoen euro jaaromzet + > 10 miljoen euro balanstotaal**

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

1. NIS2: wat?

- **<u>Zorgplicht</u>: risicobeheer mbt beveiliging van netwerken en informatiesystemen; voorkomen van incidenten; beperken van de gevolgen van incidenten, dmv everedige technische, operationele en organisatorische maatregelen**

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) incidentenbehandeling;
c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

- **<u>Meldplicht</u>: incidenten die de verlening van essentiële diensten ernstig (kunnen) verstoren moeten binnen 24 uur worden gemeld, bij de toezichthouder, én het Computer Security Incident Response Team**

- **<u>Toezicht</u>: Er komt een onafhankelijke toezichthouder (welke is nog niet bekend). Die kan inspecteren, audits uitvoeren, beveiligingsscans uitvoeren, inzage verzoeken – en boetes uitdelen!**

4. De lidstaten zorgen ervoor dat essentiële entiteiten die inbreuk maken op artikel 21 of 23 overeenkomstig de leden 2 en 3 van dit artikel onderworpen worden aan administratieve geldboeten met een maximumbedrag van ten minste 10 000 000 EUR of ten minste 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort, afhankelijk van welk bedrag hoger is.

5. De lidstaten zorgen ervoor dat belangrijke entiteiten die inbreuk maken op artikel 21 of 23 overeenkomstig de leden 2 en 3 van dit artikel onderworpen worden aan administratieve geldboeten met een maximumbedrag van ten minste 7 000 000 EUR of ten minste 1,4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort, afhankelijk van welk bedrag hoger is.

1. NIS2: aansprakelijkheid

- **Naast vatbaarheid voor boetes, is een organisatie die regels schendt ook aansprakelijk:**

Artikel 20

Governance

1. De lidstaten zorgen ervoor dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreukendoor de entiteiten op dat artikel.

De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.

2. De lidstaten zorgen ervoor dat de leden van de bestuursorganen van essentiële en belangrijke entiteiten een opleiding moeten volgen, en moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

2. AI?!

https://icthealth.nl/nieuws/negen-op-de-tien-ziekenhuizen-zet-ai-in/

ICT&health
Het officiële kennisplatform voor zorginnovatie

ACTUEEL MAGAZINES EVENEMENTEN INNOVATION PARTNERS REDACTIERAAD VACATURES

NIEUWS

← Bekijk overzicht

30 MEI 2022 AI

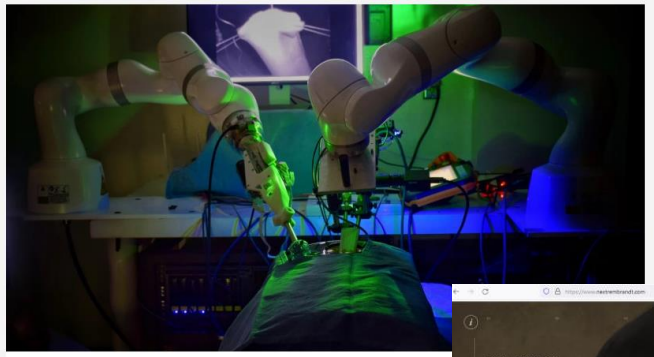
NEGEN OP DE TIEN ZIEKENHUIZEN ZET AI IN

89 procent van de Nederlandse ziekenhuizen zet inmiddels kunstmatig intelligentie (AI) in. Nog altijd worden AI-technologieën zoals machine learning vooral ingezet op gebieden zoals diagnostiek. Dat blijkt uit het jaarlijkse onderzoek van M&I/Partners naar de ontwikkelingen van AI in de zorgsector. Het verbeteren van kwaliteit van de zorg, verlagen zorgkosten en innoveren zijn de belangrijkste drijfveren voor ziekenhuizen om met AI aan de slag te gaan.

https://www.deingenieur.nl/artikel/robot-voert-zelf-kijkoperatie-uit

ROBOT VOERT ZELF KIJKOPERATIE UIT

28 JANUARI 2022



Voor het eerst heeft een robot helemaal autonoom een operatie uitg
machine van Johns Hopkins University naaide twee darmen aan elka
klusje. De operatie gebeurde nu nog bij een varken, maar de onderz

https://www.sciencefocus.com/news/ai-beethovens-symphony/

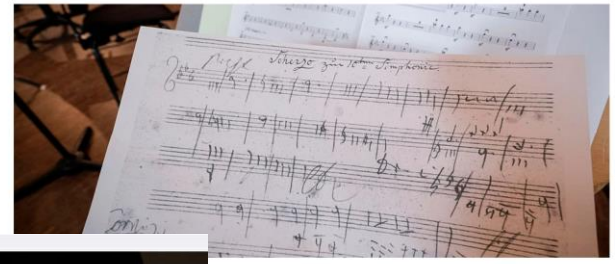
Subscribe to BBC Science Focus Magazine | Previous Issues | Podcast | Q&A

Sign in | Register

Science Focus

News Future tech Nature Space Human body Everyday science Planet Earth Newsletters

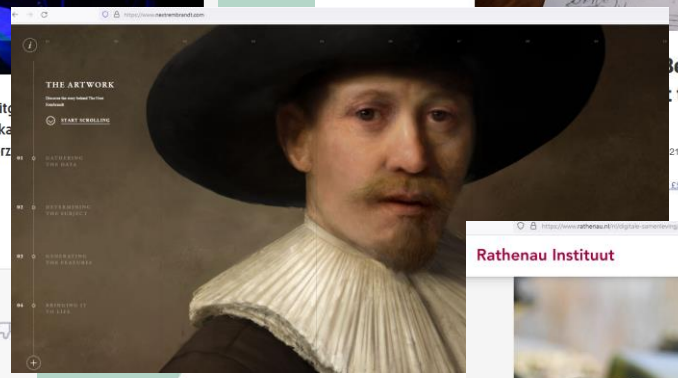
Home › Science news › How an AI finished Beethoven's last symphony and what that means for the future of music



eethoven's last
that means for the

21 at 04:00

Ad served by Google
Ad options
Send feedback
Why this ad?



EL write a moderate view on climate change with an arrogant joke at the end

Climate change is a complex issue that requires a thoughtful and nuanced approach. While some may argue that it is a purely man-made problem, the reality is that it is a combination of natural and human factors. However, it is clear that human activities, such as burning fossil fuels and deforestation, are contributing to the problem.

It is important that we take action to address climate change and reduce our carbon footprint. This can include implementing renewable energy sources, investing in green technology, and making changes to our daily habits.

But let's be real, if the polar bears can adapt to the melting ice caps, I'm sure we can handle a little warmer weather. *sips latte*

Rathenau Instituut

Thema's Dossiers Wetenschap in cijfers Over ons Contact NL | EN

NIEUWS DIGITALE SAMENLEVING 17 JANUARI 2019

Uitdagingen voor regulering van drones en killer robots

TWEEDE KAMER RONDETAFEL

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

AI-verordening: typen AI

- Onacceptabele risico's (verboden)
- Hoog-risico AI (streng gereguleerd)
- Foundation Models (Gen AI; minder streng?!)
- Laag-risico AI (minst gereguleerd)

EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

Verboden AI

Article 5

1. The following artificial intelligence practices shall be prohibited:

   (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

   (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

   (c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

      (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

      (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

   (d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

      (i) the targeted search for specific potential victims of crime, including missing children;

      (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

      (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[62] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements:

   (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

   (b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

   In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.

   The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

Hoog-risico AI

Article 6
Classification rules for high-risk AI systems

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

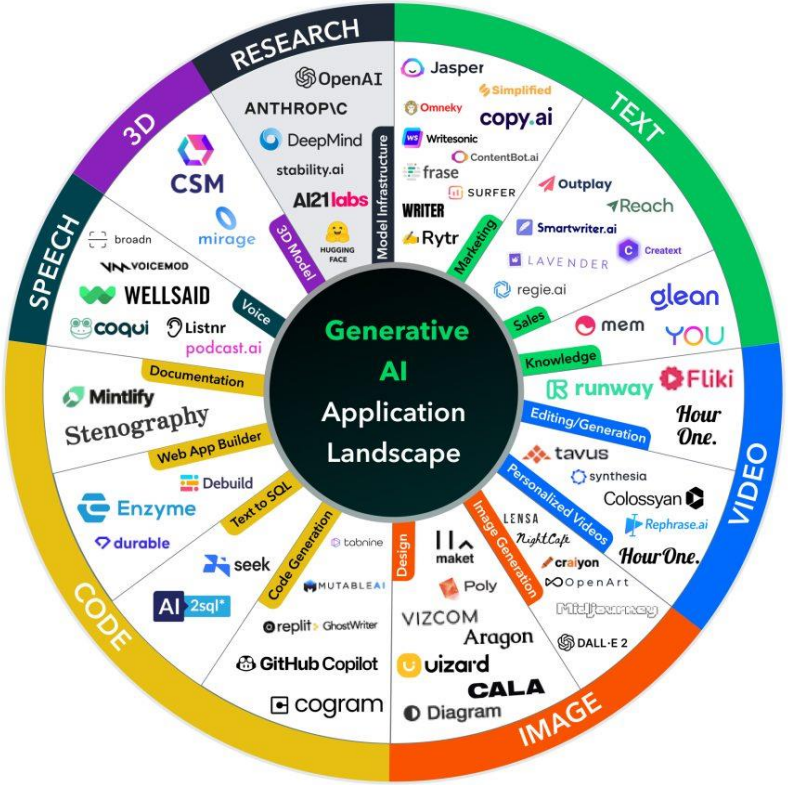
   (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

   (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

Generative AI/foundation models



Source: https://www.rapidops.com/blog/generative-ai-tools/

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

Rollen, verantwoordelijkheden en eisen

- Prominente rollen:
  - Aanbieders (ontwikkelaars/producenten)
  - Gebruikers (toepassers)

- Hoog-risico AI = strikt gereguleerd (Hoofdstuk 2)
  - Systeem voor risicobeheer (pdca) + register (documentatieplicht) + systeem voor kwaliteitsbeheer
  - Datakwaliteit en databeheer
  - Bijhouden technische documentatie
  - Loggingplicht (!) om traceerbaarheid te borgen
  - Transparatie en informatieverstrekking aan gebruikers (“explainable AI”)
  - Menselijk toezicht (“human oversight”)
  - Nauwkeurigheid, robuustheid en cyberbeveiliging

- Laag-risico AI = veel minder strikt gereguleerd
  - Transparantie en informatieverstrekking
  - Monitoring

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

Handhaving: publieke en civiele mechanismen

- Publiekrechtelijke handhavingsinstrumenten
  - Passende maatregelen […], ultimo:
  - Boetes in 3 categorieën (€ 35, 15 & 7,5 mln, of 7, 3, 1% wereldwijde jaaromzet)

- Civielrechtelijke aansprakelijkheid
  - Geen “82 AVG”-mechanisme, maar wel:
  - Voorgestelde (gewijzigde) Richtlijn Productaansprakelijkheid (VRPA)
  - Voorgestelde Richtlijn AI-aansprakelijkheid (RAIA, *geen materieel aansprakelijkheidsrecht!*)

Civiele aansprakelijkheid - VRPA

- Software en algoritmes => product idz VRPA
- Gebrekscriteria uitgebreid: zelflerend vermogen en beheers-/controlemogelijkheiden producent na marktintroductie toegevoegd
- Non-compliance met veiligheids- en cybersecurityverplichtingen eveneens

- Procedurele hulpmiddelen voor slachtoffers: log en leg uit, of aansprakelijkheid wordt verondersteld
- Maar, de bewijslast (gebrek, schade, causaliteit) blijft bij slachtoffers
- Verweren teruggeschroefd: ontwikkelingsrisicoverweer en het verweer aangaande na marktintroductie ontstane gebreken kunnen niet worden ingeroepen als een producent niet aan zijn after-marketverplichtingen heeft voldaan (tot updaten/veilighouden/herroepen)

- = leidt tot strengere regels voor producenten, maar ook tot betere bescherming van consumenten/slachtoffers

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

Civiele aansprakelijkheid: RAIA

- Geen enkele materiële harmonisering, wel
- Procedurele regels/hulpmiddelen voor slachtoffers, aangaande
  - Bewaren (loggen) en ontsluiten (aan potentiële eisers) van bewijsmateriaal
- Worden die verplichtingen geschonden, leidt dat tot een weerlegbaar vermoeden van normschending door de aangesproken partij
  - Normen zoals onder meer voorgesteld in de AI-verordening, en aanzien van bijv. loggen, uitlegbaarheid, datakwaliteit, cyberveiligheid, monitoring, etc
- Geen hulpmiddelen ten aanzien van causaliteit (ondanks de suggestieve formulering)
- Wél een extra criterium voor het vestigen van aansprakelijkheid, ten aanzien van de relatie tussen een normschending en de output (of gebrek daaraan) van een AI-systeem
- Ook geen regeling inzake de verwerking van persoonsgegevens, ondanks de logging- en bewijsoverleggingsregels

- Dus: meer compliancedruk voor innovatoren, maar wat schieten de slachtoffers ermee op?

3. AVG rollen en verantwoordelijkheden

- **Algemene Verordening Gegevensbescherming**
  - Verwerkersverantwoordelijke: bepaalt doel en middelen van de gegevensverwerking
  - Verantwoordelijkheden (een kleine selectie)
    - Rechtmatigheid, behoorlijkheid en transparantie van de gegevensverwerking
    - Minimale gegevensverwerking en opslagbeperking, juistheidsbeginsel, doelbinding,
    - Veiligheid en integriteit
      - **TOMs**
      - **Melden datalekken**
  - Verwerker: verwerkt ten behoeve en onder verantwoordelijkheid van de vw.verantwoordelijke
    - Moet instructies (op basis verwerkersovereenkomst) naleven
    - Moet verantwoordelijke assisteren, o.a. bij TOMs, datalekken en naleving rechten betrokkenen

3. AVG rollen en verantwoordelijkheden

- **Algemene Verordening Gegevensbescherming**
  - Verwerkersverantwoordelijke: bepaalt doel en middelen van de gegevensverwerking
  - Verantwoordelijkheden (een kleine selectie)
    - Rechtmatigheid, behoorlijkheid en transparantie van de gegevensverwerking
    - Minimale gegevensverwerking en opslagbeperking, juistheidsbeginsel, doelbinding,
    - Veiligheid en integriteit
      - **TOMs**
      - **Melden datalekken**
  - Verwerker: verwerkt ten behoeve en onder verantwoordelijkheid van de vw.verantwoordelijke
    - Moet instructies (op basis verwerkersovereenkomst) naleven
    - Moet verantwoordelijke assisteren, o.a. bij TOMs, datalekken en naleving rechten betrokkenen

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

3. Een datalek: wat te doen?

- **Inbreuk in verband met persoonsgegevens**

12) „inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

- Verwerkersverantwoordelijke: meldplicht
  - Autoriteit Persoonsgegevens, binnen 72 uur na ontdekken o.a.:
    - Aard van de inbreuk; categorieën en aantal betrokkenen + registers
    - Waarschijnlijke gevolgen van de inbreuk; vermelding FG/contactpersoon
    - Mitigerende maatregelen
    - Verwerking in register
  - Betrokkenen, indien waarschijnlijkheid "hoog risico voor de rechten en vrijheden natuurlijke personen", zo snel mogelijk en in klare taal
- Verwerker: verwerkt ten behoeve en onder verantwoordelijkheid van de vw.verantwoordelijke
  - *"informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens"*

KIENHUIS HOVING
ADVOCATEN EN NOTARISSEN

3. Wie is aansprakelijk?

- **Boetes/bestuurdlijke handhaving**
  - Verwerkersverantwoordelijke én verwerker:
    - Boete voor schending meldplicht datalek max. € 10.000.000 of 2% jaaromzet wereldwijd
    - Boete voor bepaalde andere schendingen AVG verantwoordelijkheden (o.a. basisbeginselen): € 20.000.000 of 4% wereldwijde jaaromzet

- **Civiele aansprakelijkheid**
  - Verwerkingsverantwoordelijke is aansprakelijk voor de schade die is veroorzaakt door verwerkingen in strijd met de AVG
  - Verwerkers ook, maar alleen "*voor de schade die door verwerking is veroorzaakt wanneer bij de verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van deze verordening of buiten dan wel in strijd met de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld*".

  - DUS: "ketenverantwoordelijkheid" van de verwerkingsverantwoordelijke

4. Enkele tips en adviezen

- **Nieuwe technologie vraagt om nieuwe regels – en die zijn er gekomen….**
- **De AI-act en NIS-2 regels zijn weliswaar nog niet “af”, maar**
- **Voorbereiding is geboden!**

- **Non-compliance met AI- NIS- en AVG-regels kan leiden tot**
- **Boetes én**
- **Civiele aansprakelijkheid**

- **Begin alvast …. Wij weten hoe!**

Contact

Roeland de Bruin
Advocaat Intellectueel eigendom, ICT-recht en Privacyrecht
Universitair Docent Universiteit Utrecht,
Center for Access to and Acceptance of Autonomous Intelligence (CAAAi)
Centrum voor Intellectueel Eigendomsrecht (CIER)
T 053 - 480 47 22
E roeland.debruin@kienhuishoving.nl

www.kienhuishoving.nl

Pantheon 25 Postbus 109 7500 AC Enschede T +31(0)53 480 42 00 F +31(0)53 480 42 99

KIENHUIS HOVING

ADVOCATEN EN NOTARISSEN