@zwnne

VPR-A SPECIALISATIEOPLEIDING | 12 maart – 21 november 2024

INTRODUCTIE

Prof. mr. G-J. (Gerrit-Jan) ZWENNE

Universiteit Leiden

eLaw Leiden

1

de opleiding

aanvangs- en eindtijden		
9:45-11:00	11:00-11:15	13:30-14:45
11:15-12:30	12:30-13:30	14:45-15:00
		15:00-16:15

12 maart 2024 | DAG I.
- **Achtergrond, context en begrippen** Zwenne
- **Toepassingsbereik** De Vries
- **Wat van de privacyadviseur wordt verwacht** interview interview Simon Hania (DPO Uber)
- *lunch in Sterrenwacht*
- *borrel en diner in Prentenkabinet*

26 maart 2024 | DAG II.
- **Beginselen en grondslagen, en bijzondere gegevens** De Vries
- **Beveiliging en datalekken**
- **bespreking opdracht 1** Dunnik
- *lunch in Prentenkabinet*

23 april 2024 | DAG III.
- **Verwerkings-verantwoordelijke** Kroes
- **Verwerkersovereenkomst** Tholen
- **Inzage en verbetering** Jakimowicz
- **Internationale gegevensdoorgiften** Arnbak
- *Lunch in Sterrewacht*

21 mei 2024| DAG IV.
- **Formaliteiten en accountability** Schermer
- **Rechtsbescherming, handhaving & toezicht** Tjeenk Willink & Drouen
- **bespreking opdracht 2** Dunnik
- *lunch in Prentenkabinet*

18 juni 2023 | DAG V.
SYMPOSIUM
- [….]
- *borrel in KOG*

5 september 2024| DAG VI.
- **Transparantie en overige rechten van betrokkenen** Zwenne
- **Profilering & ePrivacy** Zwenne
- **Cookies & RTB** Wolters Ruckert
- *Lunch in Prentenkabinet*

26 sept 2024 | DAG VII.
- **Collectieve actie en schadevergoeding** Alberdingh Thijm
- **Rechtspraak HvJEU en EHRM** Volgenant
- **PraktijkOefening** Ekker
- **bespreking opdracht 3** Dunnik
- *Lunch in Sterrenwacht*

10 oktober 2024 | DAG VIII.
- **Privacy in het sociale domein: een overzicht** Van Graafeiland & Gillhaus
- **Privacy in de zorg** Van Balen
- **Privacy in arbeidsverhoudingen** Jakimowicz
- *lunch in Sterrenwacht*

31 oktober 2024 | DAG IX.
- **bespreking opdracht 4** Dunnik
- **Verwerkingsgrondslagen** Zwenne
- **Doelbinding en bijzondere gegevens** De Vries
- **Examentraining** Dunnik & De Vries
- *Lunch in Prentenkabinet*

21 november 2024 | DAG X.
- **Examen**
- **Diploma-uitreiking**
- **Borrel**
- **Diner**

2

Te bestuderen

aanbevolen is niet verplicht!

met nu ook een Nederlandse versie!

naslag

vier opdrachten en een mondeling examen

- niet noodzakelijk reeds behandelde stof
- beoordeeld door Dunnik

verplicht voor advocaten

- casus
- gesprek
- cijfer

- vergelijkbaar met casus van opdrachten
- 45 minuten bestuderen

- twee docenten (VPR-A bestuursleden)
- ca. 30 minuten
- open boek, géén communicatie

$$\text{eindcijfer} = \frac{\text{examencijfer} + \text{gemiddelde van 3 opdrachten}}{2}$$

VPR-A SPECIALISATIEOPLEIDING | 12 maart 2024

CONTEXT EN ACHTERGROND
instituties en kernbegrippen

Prof. mr. G-J. (Gerrit-Jan) ZWENNE

Universiteit Leiden

eLaw Leiden

ACHTERGROND
vanwaar privacywetgeving?

7

privacydimensies

1. fysieke privacy
2. territoriale privacy
3. communicatiegeheim
4. informationele privacy

lichamelijke integriteit: visitatie ('cavity search') ademtest, bloed, dna, speeksel, etc.

huisrecht: binnentreden van woning.

briefgeheim, telefoon- en telegraaf-geheim

aanspraken van individu met betrekking tot de informatie die op hem of haar betrekking heeft

Artikel 11 GW

Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.

Artikel 12 GW

1. Het binnentreden in een woning zonder toestemming van de bewoner is alleen geoorloofd in de gevallen bij of krachtens de wet bepaald, door hen die daartoe bij of krachtens de wet zijn aangewezen..

vanaf 22 februari 2023

Artikel 13 Grondwet

Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim.

Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen

Artikel 10 Grondwet

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

8

omnibus-wetgeving met grote reikwijdte, in een nogal dynamische context

het juridisch antwoord daarop: open begrippen en vage normen

want dat is toekomst-bestendig en flexibel

maar (vooralsnog) betrekkelijk weinig rechtspraak

en dus nog veel onopgehelderde begrippen en rechtsonzekerheid

en een (soms wat) grote rol voor (soms wat) activistische toezichthouders

edpb
European Data Protection Board

9

POLITICO

As European governments rushed to embrace technology to fight the coronavirus, a plainspoken Dutchman emerged as a thorn in their side. Aleid Wolfsen's message: Don't pretend your solutions are privacy-friendly.

In a group that normally keeps disagreements quiet, Wolfsen stands out. A former politician and mayor of Utrecht who had no formal training in data protection when he took on his role in 2016, he has repeatedly been at odds with other watchdogs, most of whom do not share his political background.

The official in charge of Europe's grouping of privacy regulators was also keen to play down any disagreements. There is "no difference in the positions" of different privacy regulators and the "Dutch case was a specific case," Andrea Jelinek said, while a spokesperson for the group, the European Data Protection Board, added: "The legal concept of anonymization is not an absolute concept."

!!

Europe's Data Protection Supervisor, who had OK'd the Commission's use of telecoms data to track the coronavirus, said: "There is a difference between the technical impossibility of doing something to the very end, and something which we would call an effective anonymization."

10

Van je schulden hoeft de GGD niet te weten

De AVG dwingt tot nadenken vóór doen

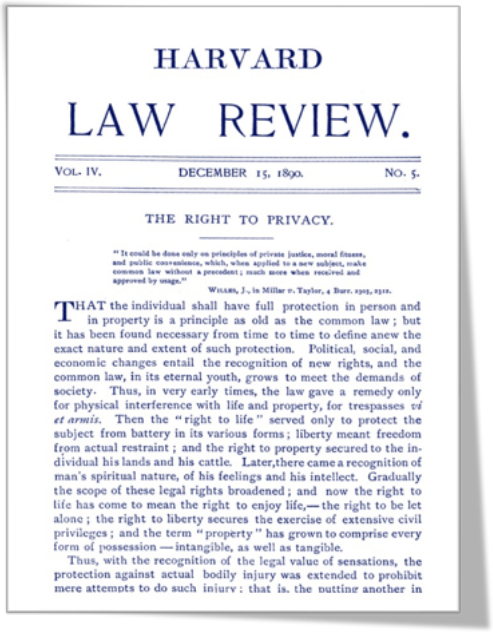
door het RIVM, om zo voorspellingen te doen over de verspreiding van het virus.

Wolfsen eist dat het om maatregelen gaat die de bescherming van persoonsgegevens zo goed mogelijk waarborgen. „Over die spoedwet hebben wij net advies uitgebracht aan het kabinet. Wij sluiten niet uit dat de analyse van die locatiedata op een privacy-vriendelijke manier kan, maar dan moet aan strenge normen worden voldaan. Onze adviezen worden meestal opgevolgd, omdat wij een wet buiten werking kunnen stellen als de AVG wordt geschonden", zegt Wolfsen. ??

leven breder. „Het grootschalig volgen van mensen die daar geen toestemming voor hebben gegeven, is door de AVG echt *not done* geworden. Dat lijkt met die locatiedata nu weer aan de kant te worden geschoven", zegt Be-

11

privacyrecht



HARVARD
LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

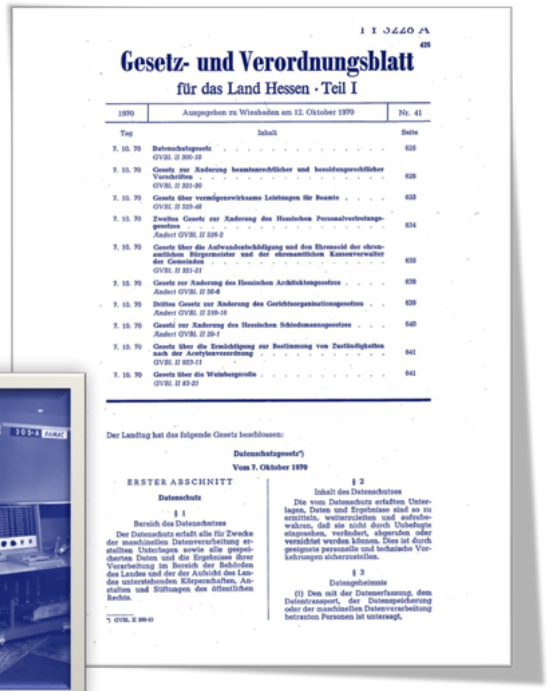
"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."
WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

13

privacywet



Gesetz- und Verordnungsblatt
für das Land Hessen · Teil I

1970 | Ausgegeben zu Wiesbaden am 12. Oktober 1970 | Nr. 41

Tag	Inhalt	Seite
7. 10. 70	Datenschutzgesetz GVBl. II 300-10	625
7. 10. 70	Gesetz zur Änderung beamtenrechtlicher und besoldungsrechtlicher Vorschriften GVBl. II 321-30	628
7. 10. 70	Gesetz über vermögenswirksame Leistungen für Beamte GVBl. II 323-40	633
7. 10. 70	Zweites Gesetz zur Änderung des Hessischen Personalvertretungsgesetzes Ändert GVBl. II 326-2	634
7. 10. 70	Gesetz über die Aufwandsentschädigung und den Ehrensold der ehrenamtlichen Bürgermeister und der ehrenamtlichen Kassenverwalter der Gemeinden GVBl. II 321-21	635
7. 10. 70	Gesetz zur Änderung des Hessischen Architektengesetzes Ändert GVBl. II 50-6	638
7. 10. 70	Drittes Gesetz zur Änderung des Gerichtsorganisationsgesetzes Ändert GVBl. II 310-16	639
7. 10. 70	Gesetz zur Änderung des Hessischen Schiedsmannsgesetzes Ändert GVBl. II 20-1	640
7. 10. 70	Gesetz über die Ermächtigung zur Bestimmung von Zuständigkeiten nach der Acetylenverordnung GVBl. II 823-11	641
7. 10. 70	Gesetz über die Weinbergrolle GVBl. II 83-21	641

Der Landtag hat das folgende Gesetz beschlossen:

Datenschutzgesetz*)
Vom 7. Oktober 1970

ERSTER ABSCHNITT
Datenschutz

§ 1
Bereich des Datenschutzes

Der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.

§ 2
Inhalt des Datenschutzes

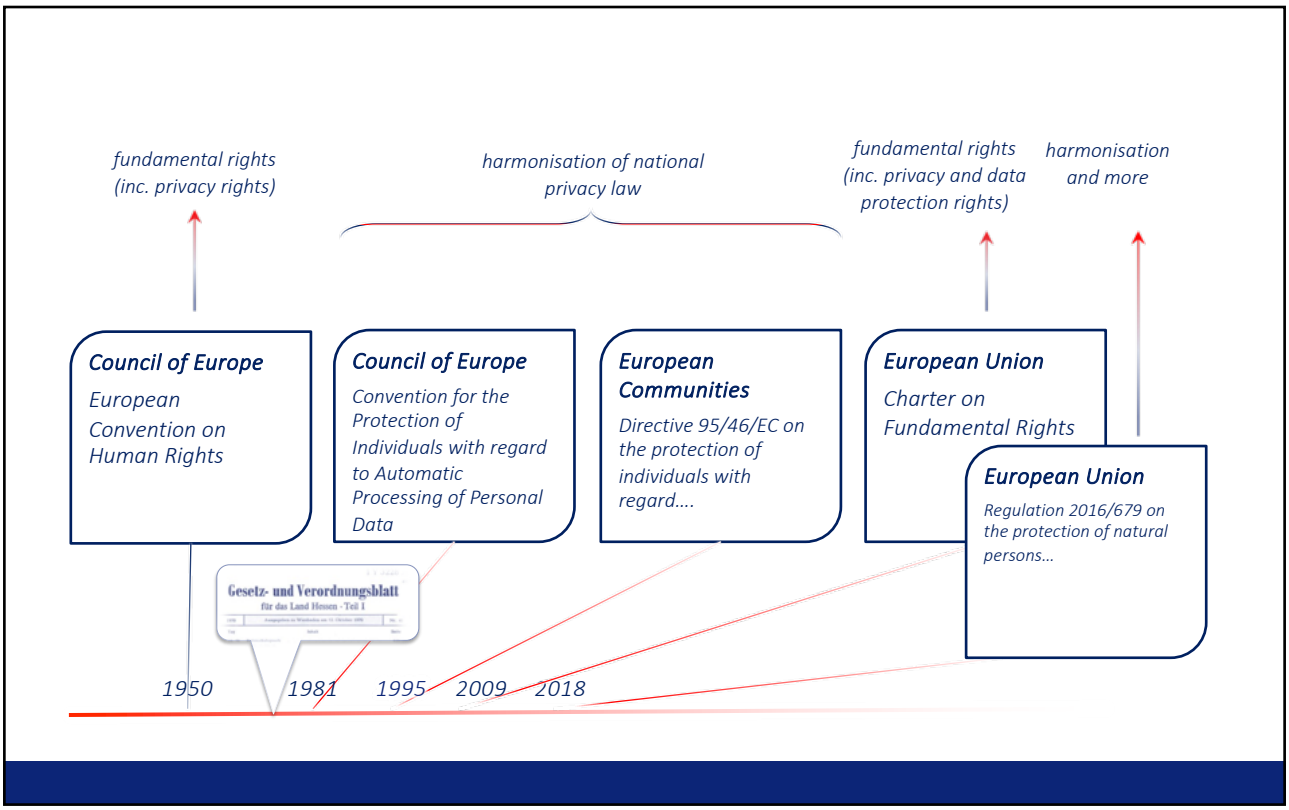
Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte einsehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen.

§ 3
Datengeheimnis

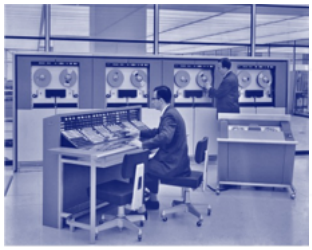
(1) Den mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung betrauten Personen ist untersagt,

*) GVBl. II 300-10

14



16



data processing 1960's

In 1970 verabschiedete Hessen das weltweit erste Datenschutzgesetz

SIEMENS

doorgifteverbod naar landen met lager beschermingsniveau

AVG

Lissabon

Richtlijn 95/46/EG

17

INSTITUTIES
EU EC HJEU RvE EHRM

19

Straatsburg & Luxemburg

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

- Raad van Europa (47 lidstaten)
- EVRM

"concept of 'private life' is a broad term not susceptible to exhaustive definition"

https://hudoc.echr.coe.int

o.a. S. and Marper 30562/04

bijv. Google Spain C131/12

COURT OF JUSTICE OF THE EUROPEAN UNION

- Europese UNIE (27 lidstaten)
- EU Handvest, AVG etc.

"data subject's rights override, as a general rule, interest of internet users"

http://curia.europa.eu/

20

supervisory authorities ("SA's")

AUTORITEIT PERSOONSGEGEVENS

EDPS

Europe Data Protection Board

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

ico. Information Commissioner's Office

An Coimisiún um Chosaint Sonraí Data Protection Commission

aepd agencia española protección datos

Hamburg Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

LDI NRW Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

PRIVACY WAARBORG

GBA Gegevensbeschermingsautoriteit

21

KERNBEGRIPPEN

verwerking persoonsgegevens, identificeren en singling-out, anomimisering en pseudonimisering

«verwerking»

HvJEU 5 oktober 2023, C-659/22, ECLI:EU:C:2023:745 (RK vs. Ministerstvo zdravotnictvi)

Art. 2(1) AVG

1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Art. 4(2) AVG

een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens enz.

«verwerking»

HvJEU 7 maart 2024, C-740/22, ECLI:EU:C:2024:216 (Endemol Shine Finland Oy)

31. Deze opsomming [van art. 4 onderdeel b AVG] heeft onder meer betrekking op het verstrekken door middel van doorzending, verspreiden en „op andere wijze ter beschikking stellen", welke bewerkingen al dan niet geautomatiseerd kunnen zijn. In dit verband stelt artikel 4, punt 2, AVG geen enkele voorwaarde met betrekking tot de vorm van de „niet-geautomatiseerde" verwerking. Het begrip „verwerking" omvat dus ook mondelinge verstrekking.

32. Derhalve omvat het begrip „verwerking" als bedoeld in artikel 4, punt 2, AVG noodzakelijkerwijs de mondelinge verstrekking van persoonsgegevens.

33. De vraag blijft echter of een dergelijke verwerking binnen de materiële werkingssfeer van de AVG valt. Artikel 2 AVG, waarin die werkingssfeer wordt afgebakend, bepaalt in lid 1 dat deze verordening van toepassing is op „de geheel of gedeeltelijk geautomatiseerde" verwerking alsmede op de „[niet-geautomatiseerde] verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen".

maar is het ook verwerking van gegevens opgenomen in een bestand (of daartoe zijn bestemd)…?

?

25

«persoonsgegevens»

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

"de betrokkene"

*kost het al dan niet een **onevenredige inspanning** om de natuurlijke persoon te identificeren?*

wat is identificeren eigenlijk..?

is een uniek nummer (IP-adres, Mac-adres) voldoende om te spreken van identiteit..?

28

«identificeren» wat is dat eigenlijk..?

~ **vaststellen wie iemand is**: *ze hebben de dode geïdentificeerd*

~ **aantonen wie je bent:** *kunt u zich identificeren?*

zich ~ *voorstellen dat hij een ander is: hij identificeert zich met het slachtoffer*

Art. 27a WvSv

De verdachte wordt ten behoeve van het vaststellen van zijn identiteit gevraagd naar zijn naam, voornamen, geboorteplaats en geboortedatum, het adres waarop hij in de basisregistratie personen is ingeschreven en het adres van zijn feitelijke verblijfplaats. Het vaststellen van zijn identiteit omvat tevens een onderzoek van een identiteitsbewijs

NN.PL133C.V.071030.100

HR 4 september 2012
ECLI:NL:HR:2012:BX4153

casus

verdachte weigert bekend te maken wie zij is en daarom wordt zij in de stukken aangeduid met een nummer

zo een verdachte wordt aangemerkt als een anonieme, d.w.z. niet geïdentificeerde verdachte

deugdelijke vaststelling van identiteit

Artikel 12.6 AVG
[...] [D]e verwerkingsverantwoordelijke [kan], wanneer hij redenen heeft om te twijfelen aan de identiteit van de natuurlijke persoon die het verzoek indient als bedoeld in de artikelen 15 tot en met 21, om aanvullende informatie vragen die nodig is ter bevestiging van de identiteit van de betrokkene.

Alle antwoorden op mijn vragen

AUTORITEIT PERSOONSGEGEVENS

Vragen over het recht op inzage

Hoe weet een organisatie of ik het ben als ik een inzageverzoek doe?

Voordat de organisatie uw inzageverzoek in behandeling neemt, zal de organisatie meestal controleren wie u bent. Zij kan dat op verschillende manieren doen.

Minst privacygevoelig
Wil een organisatie uw identiteit controleren? Dan moet zij daarvoor die manier kiezen die het minst privacygevoelig is.

Het is bijvoorbeeld lang niet altijd noodzakelijk om een kopie van uw identiteitsbewijs te vragen. Vraagt u bijvoorbeeld om inzage bij een webshop? Dan is uw klantnummer in combinatie met uw naam en adres meestal genoeg om uw identiteit te controleren.

«identificeerbaar»

Art. 4(1) AVG

als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator

IP-adres, MAC-adres

bijvoorbeeld een naam, identificatienummer, locatiegegevens, online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

«identificeerbaar»

(26) […] Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

(26) […] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

«redelijkerwijs valt te verwachten»

(26) Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.
Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen

Kamerstukken II
1997/98, 25 892, nr. 3,
p. 47-48

In concrete gevallen moet [..] rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke. Het gaat dus enerzijds om objectivering naar een redelijk toegeruste verantwoordelijke en anderzijds om subjectivering naar bijzondere expertise.
[…]
Niet elk technisch of toevallig verband tussen een gegeven en een persoon is dus voldoende om dat gegeven een persoonsgegeven te doen zijn. [Er is niet] vereist dat iedere mogelijkheid de gegevens met betrekking tot personen te gebruiken, is uitgesloten. Is deze mogelijkheid weliswaar theoretisch aanwezig maar is ondenkbaar dat dit ook daadwerkelijk gebeurt, dan kan ervan worden uitgegaan dat de gegevens niet als persoonsgegevens worden aangemerkt.

«identificeerbaar»

(30) Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ont-vangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.

Lindqvist Breyer
Mircom, Scania

36

«single-out»

A very common family name will not be sufficient to identify someone - i.e. to single someone out - from the whole of a country's population, while it is likely to achieve identification of a pupil in a classroom. Even ancillary information, such as 'the man wearing a black suit' may identify some one out of the passers-by standing at a traffic light.

WP29 Opinion 4/2007

[data subject is] a natural person person who can be identified or singled out, directly or indirectly, alone or in combination with associated data, by means reasonably likely to be used by the controller ...

Draft LIBE-report of Albrecht January 2013

Art. 4(1) AVG

[data subject is] an identifiable natural person is one who can be identified, ~~or singled out~~, directly or indirectly, in particular by reference to an identifier ...

37

kamerbrief

Wat artikel 4 (begripsbepalingen) betreft, is er geen enkele steun voor het verder verfijnen van het begrip «persoonsgegevens» met categorieën als «singling out». De voorgestelde definitie lijkt Nederland en veel lidstaten al gecompliceerd genoeg.

Kamerstukken II 2012/13, 32761, nr. 51

Tweede Kamer der Staten-Generaal **2**

Vergaderjaar 2012–2013

32 761 **Verwerking en bescherming persoonsgegevens**

Nr. 51 **BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 2 september 2013

In het algemeen overleg van 7 maart 2012 (Kamerstuk 32 761, nr. 27) heb ik toegezegd u periodiek op de hoogte te houden van de stand van zaken over de onderhandelingen in Brussel over de Algemene verordening gegevensbescherming en de richtlijn gegevensbescherming opsporing en vervolging.

In deze brief doe ik verslag van de onderhandelingsronden die in april, mei en juni 2013 hebben plaatsgevonden. Het betreft de tweede helft van de periode waarin Ierland het voorzitterschap van de Raad bekleedt. Ook deze periode heeft zich gekenmerkt door een hoge frequentie, lange duur en grote intensiteit van de onderhandelingen. In deze periode is de artikelsgewijze behandeling van verordening en richtlijn voortgezet. Ditmaal zijn de behandelingen echter gericht op het bereiken van een vorm van een akkoord in de JBZ Raad van 6 en 7 juni 2013. Het steeds verder verhogen van de druk op de delegaties om dat doel te bereiken, vooral in de allerlaatste periode van het Ierse voorzitterschap, is niet productief gebleken. Met name de grote lidstaten hebben uiting gegeven aan hun irritatie daarover. In deze verslagperiode is één vergadering aan de richtlijn gewijd. Alle overige vergaderingen betreffen de verordening.

Raadswerkgroep 9, 10 en 11 april 2013

In deze raadswerkgroep is een begin gemaakt met de tweede behandeling van de tekst van de hoofdstukken I tot en met IV van de verordening op basis van een door het voorzitterschap opgestelde nieuwe tekst. Nederland blijft vragen houden bij artikel 1, derde lid. Het betreft een gebod om geen beperkingen of verboden op het vrij verkeer van persoonsgegevens binnen de Unie vast te stellen om redenen die verband houden met het beschermen ervan. Het is Nederland op zichzelf genomen duidelijk dat het beginsel van vrij verkeer van persoonsgegevens aan geen andere beperkingen mag worden onderworpen dan de beperkingen die de verordening zelf vaststelt. Maar onduidelijk blijft of deze norm

Tweede Kamer, vergaderjaar 2012–2013, 32 761, nr. 51 1

wifi-tracking…

…organisaties maken gebruik van wifi-tracking. Zo gebruiken winkels deze techniek om bedrijfseconomische informatie te genereren: hoeveel mensen passeren de winkel, hoeveel bezoekers gaan de winkel in en hoelang blijven zij op een bepaalde plaats in de winkel.

Gemeenten en evenementenorganisatoren zetten de techniek bijvoorbeeld in om loopstromen in kaart te brengen en bij te houden hoe lang bezoekers op een bepaalde plaats verblijven.

Grondslag

Via wifi-tracking worden locatiegegevens samen met het unieke nummer van een mobiel apparaat opgeslagen en verwerkt. Organisaties mogen deze persoonsgegevens volgens de Wet bescherming persoonsgegevens (Wbp) alleen verwerken als zij daar een zogenoemde wettelijke grondslag voor hebben.

AUTORITEIT PERSOONSGEGEVENS

Home Actueel Over privacy Onderwerpen Zelf doen

AP wijst winkels en gemeenten op voorwaarden wifi-tracking

Nieuwsbericht / 16 juni 2016 Categorie: Internet en telecom

De Autoriteit Persoonsgegevens (AP) heeft winkels en gemeenten gewezen op de wettelijke eisen die gelden wanneer zij gebruik maken van wifi-tracking. Het volgen van mensen via het wifisignaal van hun mobiele apparaat maakt een grote inbreuk op hun persoonlijke levenssfeer. "Mensen komen in bestanden waaruit bijvoorbeeld valt af te leiden waar zij wanneer waren en wat hun winkelgedrag is", zegt Wilbert Tomesen, vicevoorzitter van de AP. "Zij moeten hier op zijn minst over worden geïnformeerd".

Verschillende organisaties maken gebruik van wifi-tracking. Zo gebruiken winkels deze techniek om bedrijfseconomische informatie te genereren: hoeveel mensen passeren de winkel, hoeveel bezoekers gaan de winkel in en hoelang blijven zij op een bepaalde plaats in de winkel.

Gemeenten en evenementenorganisatoren zetten de techniek bijvoorbeeld in om loopstromen in kaart te brengen en bij te houden hoe lang bezoekers op een bepaalde plaats verblijven.

De Autoriteit Persoonsgegevens ontvangt regelmatig signalen van mensen die zorgen hebben over de impact van wifi-tracking op hun privacy.

Bodil Lindqvist

EHJ 6 november 2003, C-101/01, ECLI:EU:C:2003:596

artikel 2, sub a, daarvan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hieronder valt vanzelfsprekend iemands naam tezamen met zijn telefoonnummer of gegevens over zijn werksituatie en zijn liefhebberijen.
[..]
27. Derhalve moet op de eerste vraag worden geantwoord, dat het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens [..] is aan te merken.

Scarlet SABAM

51 Het staat namelijk vast dat het rechterlijk bevel tot invoering van het litigieuze filtersysteem een systematische analyse van alle inhoud veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen. Aangezien *die IP-adressen* de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens..

HvJEU 24 november 2011, C-70/10, ECLI:EU:C:2011:771

Breyer

HJEU 19 oktober 2016 C-582/14 ECLI:EU:C:2016:779

48. De aanbieder van onlinemediadiensten lijkt dan ook te beschikken over middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om de betrokken persoon met behulp van derden, te weten de bevoegde autoriteit en de internetprovider, te identificeren aan de hand van de bewaarde IP-adressen.

*redelijkerwijs **'kunnen'** worden ingezet om iemand te identificeren?*

48. [It] appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.

*redelijkerwijs **'zullen'** worden ingezet om iemand te identificeren!*

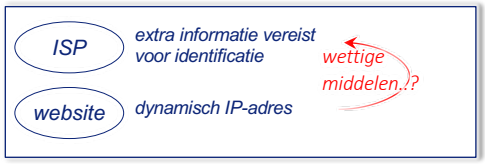
Breyer

Zie ook:
- HvJEU 17 juni 2021, C-597/19, ECLI:EU:C:2021:492 (*Mircom*)
- HvJEU 9 November 2023, C-319/22, ECLI:EU:C:2023:837 (*Gesamtverband*)

HJEU 19 oktober 2016 C-582/14 ECLI:EU:C:2016:779

48. De aanbieder van onlinemediadiensten lijkt dan ook te beschikken over middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om de betrokken persoon met behulp van derden, te weten de bevoegde autoriteit en de internetprovider, te identificeren aan de hand van de bewaarde IP-adressen.

49. [E]en dynamisch IP-adres dat door een aanbieder van onlinemediadiensten wordt geregistreerd telkens als een persoon een website bezoekt die door deze aanbieder toegankelijk wordt gemaakt voor het publiek, ten aanzien van die aanbieder [vormt] een persoonsgegeven [..], wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.



verondersteld wordt dat er géén sprake is van een onevenredige inspanning d.w.z. dat identificatie redelijkerwijs valt te verwachten)

GAR/EDPS

HJEU 26 april 2023C-T-557/20
ECLI:EU:C:2023:219

SRB/EDPS

105. Aangezien de EDPS niet heeft onderzocht of Deloitte over wettelijke en in de praktijk uitvoerbare middelen beschikte om toegang te krijgen tot de aanvullende gegevens die nodig waren voor de heridentificatie van de auteurs van de opmerkingen, kon de EDPS dus niet tot de slotsom komen dat de informatie die aan Deloitte was doorgezonden, informatie vormde die betrekking had op een „identificeerbare natuurlijke persoon" in de zin van artikel 3, punt 1, van verordening 2018/1725.

de 'Avg' voor EU-instellingen

GAR	extra informatie vereist voor identificatie	wettelijk en praktische middelen..?
Deloitte	dynamisch IP-adres	

*een persoonsgegeven voor degene die beschikt over de **wettige en in de praktijk uitvoerbare middelen** om de voor identificate benodigde aanvullende gegevens te verkrijgen*

*en dat kan niet worden verondersteld maar moet door de toezichthouder worden **aangetoond**…*

IAB Europe

HJEU 7 maart 2024 C604/22
ECLI:EU:C:2024:214

44 [Vast staat] dat de koppeling van de in een TC-string vervatte informatie aan een identificator zoals met name het IP-adres van het toestel van de betrokken gebruiker het mogelijk kan maken om een profiel van deze gebruiker op te stellen en om de persoon waar die informatie specifiek betrekking op heeft, daadwerkelijk te identificeren.

Transparency and Consent String ("TC-string")

- *een gecodeerde letter- en tekenreeks waarmee voorkeuren van internetgebruikers worden geregistreerd*
- *gedeeld met 'makelaars in persoonsgegevens en advertentieplatsforms'*
- *gecombineerd met cookie ('euconsent-v2') en gekoppeld aan IP-adres*

45. Aangezien een gebruiker kan worden geïdentificeerd door een letter- en tekenreeks als de TC-string te koppelen aan aanvullende gegevens, zoals met name het IP-adres van het toestel van deze gebruiker of andere identificatoren, dient te worden geoordeeld dat de TC-string informatie over een identificeerbare gebruiker bevat en dus een persoonsgegeven in de zin van artikel 4, punt 1, AVG is, hetgeen wordt bevestigd door overweging 30 van de AVG, waarin uitdrukkelijk wordt verwezen naar een dergelijke situatie.

TC-string in combinatie met andere identificatoren maakt identificatie mogelijk

Nota bene. IAB-leden moeten aan IAB alle gegevens verstrekken waarmee de brancheorganisatie de identiteit van gebruikers kan achterhalen

fietsendepot

Rechtbank Den Haag 20 oktober 2020, ECLI:NL:RBDHA:2020:9590

7. [V]erweerder [heeft] aannemelijk gemaakt dat binnen de gemeente Den Haag géén IP-adressen worden vastgelegd, opgeslagen en gekoppeld aan personen. Er is dan ook geen sprake van directe of indirecte herleidbaarheid naar personen. Daartoe is van belang dat verweerder heeft toegelicht dat IP adressen indirect herleidbaar kunnen zijn tot een persoon, maar dat daarvoor middelen moeten worden ingezet om dit te kunnen vaststellen. Verweerder heeft daarbij aangegeven dat het ondoenlijk qua tijd en mankracht is om van alle burgers met wie gecommuniceerd wordt, de identificatie via een IP-adres te achterhalen. Daarbij is van belang dat de gemeente niet zelf over de gegevens om een koppeling te kunnen maken tussen een IP-adres en een burger beschikt, maar zijn er gegevens nodig van een Internet Service Provider. Nu de verwerking een excessieve inspanning van verweerder vergt, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegeven.

48

fietsendepot

ABRvS 13 juli 2022 ECLI:NL:RVS:2022:1993

5.3 [...] [D]e Afdeling [is] met de rechtbank van oordeel dat het college aannemelijk heeft gemaakt dat binnen de gemeente die IP-adressen niet worden opgeslagen, vastgelegd en gekoppeld aan personen en dat de gemeente zelf niet beschikt over de benodigde gegevens om een koppeling te kunnen maken tussen die IP-adressen en een burger. Een daadwerkelijk gevaar voor identificatie is onbeduidend.

49

Brein/Ziggo

Rechtbank Midden NLD 2 februari 2022 ECLI:NL:RBMNE:2022:297

Een IP-adres is dus een persoonsgeven voor degene die wettelijke mogelijkheden heeft om dat IP-adres met behulp van informatie van een isp aan een persoon te koppelen. Uit het [Breyer-]arrest lijkt te volgen dat het begrip "wettelijke mogelijkheden" door het Europese Hof ruim wordt opgevat. In het Breyer-arrest is immers overwogen dat van die wettelijke mogelijheden geen sprake is indien de identificatie van de betrokkene bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, zodat het gevaar voor identificatie in werkelijkheid onbetekenend lijkt. De voorzieningenrechter concludeert daarom dat de mogelijkheid om (al dan niet via de rechter) NAW-gegevens van de gebruiker van een IP-adres bij de isp op te vragen, wel onder de in het Breyer-arrest bedoelde wettelijke middelen valt.

AUTORITEIT PERSOONSGEGEVENS

Boete gemeente Enschede om wifitracking

Persbericht / 29 april 2021 Categorie:

De Autoriteit Persoonsgegevens (AP) geeft de gemeente Enschede een boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de binnenstad op een manier die niet mag. Daardoor was het mogelijk winkelend publiek en mensen die in de binnenstad wonen of werken te volgen.

Wifitracking in Enschede

De gemeente Enschede besloot in 2017 om via sensoren de drukte in de binnenstad te gaan meten. De gemeente huurde daarvoor een bedrijf in dat is gespecialiseerd in het tellen van passanten.

Meetkastjes in de winkelstraten vingen de wifisignalen op van de mobiele telefoons van passerende mensen. Ieders telefoon werd apart geregistreerd, met een unieke code.

Door te tellen hoeveel telefoons er op een bepaald moment rond een meetkastje zijn, weet je hoe druk het is. Houd je over een langere periode bij welke telefoon langs welk meetkastje komt, dan verandert dit 'tellen' in het volgen van mensen.

Uit onderzoek van de AP bij de gemeente Enschede blijkt dat dit aan de hand was. De privacy van burgers was dus niet goed gewaarborgd, omdat zij konden worden gevolgd zonder dat dit noodzakelijk was.

Het was niet de intentie van de gemeente om individuen te volgen. En de AP heeft ook geen aanwijzingen gevonden dat dit is gebeurd. Maar het inzetten van wifitracking die dit mogelijk maakt, is op zichzelf al een ernstige overtreding van privacywet AVG.

Enschede: geen onevenredige inspanning – volgens AP

Bij [LEVERANCIER] is [..] de exacte locatie van de sensoren bekend en heeft men toegang tot het werkgeheugen en de software die draait op elke sensor. Tegelijk met een nieuwe detectie van een mobiel apparaat door een sensor is het bijvoorbeeld voor iemand van [LEVERANCIER] mogelijk om ter plaatse of via een camera waar te nemen welke persoon binnen het bereik van de sensor komt lopen. Vooral op stille momenten in de binnenstad leidt dit direct tot identificatie van de natuurlijke persoon. Ter controle kan de persoon worden gevraagd naar zijn/haar MAC-adres. Dezelfde manier van identificeren is mogelijk in geval van gepseudonimiseerde MAC-adressen en de bijbehorende locatiegegevens, omdat ook dan op het moment van detectie ter plaatse of via een camera de persoon in kwestie waargenomen kan worden

alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt…?

52

rechtbank Overijssel

rb Overijssel 2 feb. 2024, ECLI:NL:RBOVE:2024:594

10. De rechtbank merkt op dat de AP bij de weerlegging van de bezwaren van eiser bij herhaling uitgaat van de onaannemelijkheid van omstandigheden en gelijkwaardige bewoordingen in plaats van zich te baseren op onderzoek naar feiten. […]

13. De rechtbank is van oordeel dat de AP onvoldoende heeft onderzocht of de door haar genoemde manieren het inderdaad, in de gegeven situatie, mogelijk maken om de identiteit van een gebruiker van een mobiel apparaat met het blote oog te achterhalen.

De enkele stelling van de AP dat bedoelde medewerkers dit redelijkerwijs zouden kunnen doen overtuigt de rechtbank niet. De AP had, gelet op overweging 26 van de AVG moeten onderzoeken of het redelijkerwijs te verwachten is dat de genoemde middelen worden gebruikt om de natuurlijke persoon direct of indirect te identificeren, waarbij de kosten en de benodigde tijd voor identificatie met in achtneming van de beschikbare technologie op het tijdstip van verwerken en de technologische ontwikkelingen betrokken hadden moeten worden.

niet voldaan aan (verzwaarde) bewijslast…!

want punitieve sanctie

53

rechtbank Overijssel

rb Overijssel 2 feb. 2024, ECLI:NL:RBOVE:2024:594

10. De rechtbank merkt op dat de AP bij de weerlegging van de bezwaren van eiser bij herhaling uitgaat van de onaannemelijkheid van omstandigheden en gelijkwaardige bewoordingen in plaats van zich te baseren op onderzoek naar feiten. […]

13. De rechtbank is van oordeel dat de AP onvoldoende heeft onderzocht of de door haar genoemde manieren het inderdaad, in de gegeven situatie, mogelijk maken om de identiteit van een gebruiker van een mobiel apparaat met het blote oog te achterhalen.

De enkele stelling van de AP dat bedoelde medewerkers dit redelijkerwijs zouden kunnen doen overtuigt de rechtbank niet. De AP had, gelet op overweging 26 van de AVG moeten onderzoeken of het redelijkerwijs te verwachten is dat de genoemde middelen worden gebruikt om de natuurlijke persoon direct of indirect te identificeren, waarbij de kosten en de benodigde tijd voor identificatie met in achtneming van de beschikbare technologie op het tijdstip van verwerken en de technologische ontwikkelingen betrokken hadden moeten worden.

verkeerde maatstaf..!
*het gaat niet om wat eventueel zou **kunnen***
*maar om wat redelijkerwijs is te **verwachten***

!

Kst II 2020/21, 35479, nr. 3, p. 6-7

Wetsvoorstel Tijdelijke wet informatieverstrekking RIVM in verband met COVID-19

De informatie […] is wegens het hoge aggregatieniveau en het minimale getal van 15 per groep per gemeente per uur, naar het oordeel van de regering niet herleidbaar tot identificeerbare natuurlijke personen.

Hoewel er studies zijn die de – theoretische – mogelijkheid aantonen om in bepaalde gevallen ook geaggregeerde locatiedata te herleiden tot identificeerbare natuurlijke personen, valt niet redelijkerwijs te verwachten dat de verwerkingsverantwoordelijke of een andere persoon deze middelen gebruikt.

De kosten van en de tijd benodigd voor identificatie zonder daarbij gebruik te kunnen maken van de brongegevens (de locatie- en verkeersgegevens die de aanbieders beheren) maken een dergelijke identificatie onwaarschijnlijk. Belangrijk hierbij is dat het de aanbieders op grond van de Telecommunicatiewet verboden is om de brongegevens aan derden ter beschikking te stellen.

Er is misschien een theoretische mogelijkheid om te identificeren.

Maar daarmee zijn het nog geen persoons-gegevens…!

«persoonsgegeven» kenteken

Hof A'dam 7 januari 2016 ECLI:NL:GHAMS:2016:146
Uitgaande van de definitie van artikel 1, onderdeel a, Wbp vormt een kentekengegeven voor de heffingsambtenaar in beginsel wel een persoonsgegeven, omdat hij via Cition de beschikking krijgt over onversleutelde kentekengegevens van voertuigen die binnen de Gemeente Amsterdam geparkeerd zijn en die door hem, na gegevensverstrekking door de RDW, aan een natuurlijk persoon kunnen worden gerelateerd.

Zie ook:
HvJEU 9 November 2023, C-319/22, ECLI:EU:C:2023:837 (Gesamtverband)

«geautomatiseerde verwerking»

art. 2

1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het onderscheid tussen handmatig en geautomatiseerde verwerkte of te verwerken gegevens is niet altijd in alle scherpte te maken.
Kamerstukken II 97/98, 25892, nr. 3, p. 69

«gedeeltelijk geautomatiseerd»

bundeling van verwerkingshandelingen die in het maatschappelijk verkeer als een eenheid wordt beschouwd

Kamerstukken II 97/98, 25892, nr. 3, p. 51

geautomatiseerd gevoerde gegevens en een handmatige gegevensverzameling [zijn] zodanig [...] verweven dat zij als één bestand moeten worden aangemerkt

Kamerstukken II 97/98, 25892, nr. 3, p. 69

- *verkeersopvattingen*
- *verwevenheid*
- *gemeenschappelijke bestemming*

voorschriften die van toepassing zijn op de niet-geautomatiseerde verwerking van persoonsgegevens.

Kamerstukken II 97/98, 25892, nr. 3, p. 60

papieren back-up van digitale bestanden (prints van e-mails)

dossierkast met verwijsindex

Voorbeelden:

- [e]en handmatig bijgehouden hulpbestand van bron-documenten dat met betrekking tot de geautomatiseerd gevoerde gegevens een bewijsfunctie toekomt
- als met behulp van de geautomatiseerd gevoerde gegevens toegang kan worden verkregen tot het handmatige bestand

Kamerstukken II 97/98, 25892, nr. 3, p. 69

«bestand» d.w.z. niet geautomatiseerde verwerking

Art. 4(6) AVG

elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid

(15) [...] De bescherming van natuurlijke personen dient te gelden bij zowel geautomatiseerde verwerking van persoonsgegevens als handmatige verwerking daarvan indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand.

Dossiers of een verzameling dossiers en de omslagen ervan, die niet volgens specifieke criteria zijn gestructureerd, mogen niet onder het toepassingsgebied van deze verordening vallen.

«bestand» systematische toegankelijkheid

Het kan hierbij gaan om een systematische opbouw van de dossiers volgens een vaste structuur die de toegang tot de inhoud van de dossiers gemakkelijk maakt of om het gebruik van een geautomatiseerde index ter ontsluiting van die dossiers. [..] Dossiers waarbij dergelijke maatregelen niet zijn genomen, vallen [..] niet onder de WBP.

Hieraan doet geen afbreuk dat de dossiers volgens een enkel criterium, bijvoorbeeld alfabetisch of op datum van binnenkomst worden opgeborgen

Kamerstukken II 1998/99, 25892, nr. 9, p. 2

62

«verwerking»

HvJEU 7 maart 2024, C-740/22, ECLI:EU:C:2024:216 (Endemol Shine Finland Oy)

33. [..] Artikel 2 AVG [..] bepaalt in lid 1 dat deze verordening van toepassing is op „de geheel of gedeeltelijk geautomatiseerde" verwerking alsmede op de „[niet-geautomatiseerde] verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen".

maar is het ook verwerking van gegevens opgenomen in een bestand (of daartoe zijn bestemd)…?

34. [Art. 4(6) AVG geeft] een ruime omschrijving [..] van het begrip „bestand" in de zin van „elk" gestructureerd geheel van persoonsgegevens. Bovendien beoogt het vereiste dat het geheel van persoonsgegevens moet zijn „gestructureerd volgens specifieke criteria", uitsluitend ervoor te zorgen dat de persoonsgegevens gemakkelijk kunnen worden teruggevonden. […]

een structuur die maakt dat de gegevens gemakkelijk kunnen worden teruggevonden

38. In casu blijkt […] dat de [..] gegevens zijn opgenomen in „een bestand met persoonsgegevens dat door een rechterlijke instantie wordt bijgehouden". Deze gegevens lijken dus te zijn opgenomen in een bestand in de zin van art. 4(6) AVG, hetgeen de verwijzende rechter evenwel dient na te gaan, zonder dat het van belang is of die gegevens zijn opgenomen in elektronische databanken dan wel in fysieke dossiers of registers.

63

«bestand» zwartboek

HR 3 juni 2005 ECLI:NL:HR:2005:AT1093

[er wordt terecht onderscheid gemaakt tussen] enerzijds de verzameling dossiers van alle in het ziekenhuis van de Stichting werkzame medisch specialisten [...] die alle bij elkaar in een dossierkast worden bewaard en welke tezamen een bestand vormen als bedoeld in art. 1, onder c, Wbp en anderzijds het dossier "[verzoeker]", dat noch feitelijk noch naar de aard van de inhoud deel uitmaakt van dat bestand noch is bestemd om in dat bestand te worden opgenomen; niet alleen wordt het dossier "[verzoeker]" afzonderlijk bewaard en is het alleen voor [betrokkene 2], de directeur van de Stichting, toegankelijk, ook bevat dit dossier geheel andere gegevens (over het functioneren van [verzoeker]) dan het bestand van de dossiers van de medisch specialisten.

«bestand» Dexia

HR 29 juni 2007 NL:HR:2007:AZ4663

Dexia [bewaart] de opnamen met het oog op haar procespositie en de banden waarop de telefoongesprekken met [verweerder] voorkomen, [zijn] reeds ontsloten door Dexia, aangezien Dexia op het overzicht van 11 mei 2005 de data en exacte tijdstippen heeft vermeld van de telefoongesprekken die zij met [verweerder] heeft gevoerd.

Voorts geldt [..] dat een financiële instelling als Dexia, [...] verplicht is technische en organisatorische voorzieningen te treffen om opgenomen telefoongesprekken en andere persoonsgegevens betreffende de opgenomen telefoongesprekken zonodig te kunnen traceren en reconstrueren

Bouwvakkers bezorgen dossiers bij De Telegraaf

Geheime rechtbankdossiers bij oud vuil

10 FEB 2017

AMSTERDAM - UPDATE 11.00 uur - "Dit had nooit mogen gebeuren", stelt de Raad voor de Rechtspraak, in reactie op het enorme datalek bij de rechtbank Amsterdam, waarover De Telegraaf vanmorgen bericht. Duizenden pagina's uit geheime en privacygevoelige rechtbankstukken zijn bij de verbouwing van de rechtbank Amsterdam op straat komen te liggen. Bouwvakkers hebben delen van lopende strafzaken, inclusief namen en adressen van verdachten en getuigen, en rapportages van de Raad voor de Kinderbescherming gevonden, die als oud vuil in verlaten kamers lagen.

Interne memo's over de beveiliging van de rechtbank, protocollen over transport en begeleiding van verdachten en gedragsrichtlijnen voor het personeel zijn tevens uitgelekt. Daaruit blijkt onder meer dat er jarenlang is geruzied over de veiligheid op de rechtbank. Ook wordt melding gemaakt van een 'angstcultuur' onder het veiligheidspersoneel, dat klaagt over onderbezetting en slechte uitrusting. De stukken zijn woensdag aan het einde van de middag bezorgd bij de redactie van De Telegraaf. Gisteren heeft de hoofdredactie van de krant de stukken teruggegeven aan een medewerker van de rechtbank.

De rechtbank reageert bijna laconiek. Woordvoerder Ton van den Brandt: „Het gaat om oud papier. Het lijkt erop dat iemand de inhoud heeft meegenomen uit een van onze papiercontainers."

De Amsterdamse advocaat Van Oppen maakt korte metten met die versie. „Als de driehoek advocatuur, OM of rechtbank iets weggooit, hoort dat de versnipperaar in te gaan."

De Leidse hoogleraar privacyrecht Gerrit-Jan Zwenne spreekt van „een datalek van ongekende proporties".

vragen?
g.j.zwenne@law.leidenuniv.nl