@zwnne

ELAW BASISCURSUS
Wet bescherming persoonsgegevens
en andere privacywetgeving

inleiding, achtergrond internationale en supranationale regelingen

Gerrit-Jan Zwenne — 19 mei 2016

eLaw Leiden

wat is er mis met richtlijn 95/46/EG?

(7) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity. Differences in the level of protection of the rights and freedoms of individuals, notably to the right to the protection of personal data, with regard to the processing of personal data afforded in the Member States may prevent the free flow of personal data throughout the Union. These differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

fragmentatie en rechtsonzekerheid

public perception of significant risks for protection of individuals'

obstakel voor economische activiteit

verstoring van concurrentie

richtlijn of verordening: wat is het verschil?

verordening
een bindende rechtshandeling die in de hele EU van toepassing is

Europese wet die geldt voor iedereen in de EU

richtlijn
een rechtshandeling die een bepaald doel vastlegt dat alle EU-landen moeten bereiken

maar zij mogen zelf de wetgeving vaststellen om dat doel te bereiken

instructie aan nationale wetgevers

doelstellingen, belangen en rechten

recitals 2, 5

- protection of personal data
- contribution to freedom, security and justice
- economic and social progress
- strengthening and convergence of the economies within the internal market
- the well-being of individuals
- the freedom to conduct a business
- right to respect for private and family life, home and communications
- freedom of expression and information
- freedom of thought, conscience and religion
- right to an effective remedy and to a fair trial
- cultural, religious and linguistic diversity

waarin verschilt *de* verordening van *de* richtlijn?

verordening
- ca. 170 overwegingen (75 bldz.)
- ca. 94 bepalingen (128 bldz.)
- 26 definities (art. 4 GDPR)

richtlijn 95/46/EG:
- *72 overwegingen (7 bldz.)*
- *34 bepalingen (12 bldz.)*
- *8 definities*

- uitgebreidere territoriale werkingssfeer
  - activiteiten van verantwoordelijke én bewerker (art. 3(1) GDPR)
  - aanbieden van diensten aan datasubjects in de EU of monitoren van hun gedragingen (art. 3(2) GDPR)
- gedetailleerdere regels, meer verplichtingen voor verantwoordelijken en bewerkers, meer rechten voor datasubjecten, meer formaliteiten
- meer bevoegdheden voor toezichthouders en hogere boetes

wat regelen lidstaten nog zelf?

- children's consent regarding provision of online services (art. 8(1) GDPR)
- validity of explicit consent for processing special data (art. 9(2) GDPR)
- processing special data in the context of employment or social security, health care and archiving (art. 9(2) GDPR)
- processing criminal data (art. 10 GDPR)
- exemptions to information obligations (art. 14(5)c GDPR)
- restriction to RtbF (art. 17(1)e en (3)b GDPR)
- automated decision making (art. 22(2)b GDPR)
- restrictions to datasubject rights (art. 21 GDPR)
- prior consultation (art. 35(10) GDPR)
- designation of DPO's (art. 37(4) GDPR)
- 3rd country transfer of special data (art. 46(2)d GDPR)
- penalties (art. 84 GDPR)
- freedom of expression and information (art. 85 GDPR)
- employment context (art. 88 GDPR)
- obligations of professional secrecy (art. 90 GDPR)
- churches and religious associations (art. 91 GDPR)

welke lagere EU-regelgeving komt er nog?

The power to adopt delegated acts is conferred on the Commission (art. 92(1) GDPR)

- standardised icons (art. 12(8) GDPR)
- certification mechanisms and DP Seals (art. 42 GDPR)
- exchange of information between DPA's and EDPB (art 67 GDPR)

En verder natuurlijk ook…

- standard contractual clauses (art. 26(2b) GDPR)
- general validity of codes of conduct (art. 40 GDPR)
- adequacy decisions (art. 45 GDPR)

fragmentatie: minder minder..?

- *onverminderd veel vage normen en open begrippen*
- *nationale toezichthouders en nationale rechters blijven bevoegd*
- *veel lagere wetgeving op nationaal niveau*

wat levert het op?

The Regulation will establish a single, pan-European law for data protection meaning that companies can simply deal with one law, not 28.

The new rules will bring benefits of an estimated €2.3 billion per year.

Wat zegt de Verordening over…

spelers
- betrokkene
- verantwoordelijke
- bewerker

speelveld
- werkingssfeer en reikwijdte
- persoonlijke of huishoudelijke doeleinden
- journalistieke uitzondering

spelregels
- toestemming en andere verwerkingsgrondslagen
- doelbinding en bewaartermijnen
- gegevensminimalisatie
- rechten van betrokkenen, incl. profilering

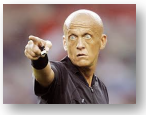
spelers

- betrokkene → *strengthening and detailing the rights of data subjects*
- verantwoordelijke, bewerkers → *more enforceable obligations and responsibilities, for both*
- toezichthouder, functionaris → *mandatory appointment of DPO was deemed acceptable in strictly limited cases*

an essential component of the protection of individuals

functionaris (*'DPO'*)

mandatory
- public authority or body → *except for courts acting in their judicial capacity*
- controller or processor core activities consist of processing operations require regular and systematic monitoring of data subjects on a large scale → *by virtue of their nature, their scope and/or their purposes.*
- controller or processor core activities consist of processing on a large scale of special data



functie-omschrijving functionaris

- inform and advise on DP-obligations
- monitor compliance of obligations
- advise on DPIAS → *Data Protection Impact Assessments*
- co-operate and contact with DPA

identified or singled out…

'data subject' means an identified natural person or a natural 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 or by any other natural or legal person, in particular by reference to a unique identifier …

Cf. Art. 29 WP Opinions 04/2007, 01/2012 and 08/2012

single-out?

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person. To determine whether a 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 any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.

To determine whether a 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 any other person to identify the individual directly or indirectly.

reikwijdte ('material scope')

main rule

- processing of personal data wholly or partly by automated means, and
- processing other than by automated means which form part of a filing system (or are intended to form part of a filing system)

exemptions

- foreign policy and security (Ch. 2 of Title V TEU) and prevention, investigation, detection or prosecution of criminal offences (etc.)
- by a natural person in the course of a purely personal or household activity

Art. 2(1) (2)

Idem art. 2(1) Wbp

'purely personal or household activity'

thus without a connection with a professional or commercial activity, eg.

- *correspondence and the holding of addresses*
- *social networking, and the like*

Idem art. 2(1) Wbp

However, this Regulation does apply to controllers or processors which provide the means for processing personal data for such personal or household activities

Facebook, Twitter, Whatsapp, Instagram etc

territoriale werkingssfeer ('territorial scope')

- processing in the context of the activities of an establishment of a controller or a processor in the Union
- offering of goods or services to such data subjects in the Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the EU

regardless of whether the processing takes place in the Union or not

art. 3

irrespective of whether a payment of the data subject is required

journalistiek, artistiek etc. ('freedom of expression and information')

lidstaten moeten zorgdragen voor uitzonderingen die nodig zijn om gegevensbescherming te verenigen met vrijheid van meningsuiting en informatievrijheid

ID-nrs, employment, archiving, profesional secrecy, churches etc.

art. 80, recital 121

Ch. II principles
Ch. III rights of the data subject
Ch. IV controller and processor
Ch. V 3rd country transfers
Ch. VI supervisory authorities
Ch. VII co-operation and consistency, and
Ch. IX specific data processing situations

spelregels

- toestemming en andere verwerkingsgrondslagen
- doelbinding en bewaartermijnen
- gegevensminimalisatie
- bijzondere gegevens
- rechten van betrokkenen
- internationale doorgifte en toezicht?

verwerkingsgrondslagen ('lawful processing')

a) data subject consent for one or more specific purposes
b) performance of a contract to which the data subject is party
c) compliance with a legal obligation to which the controller is subject
d) to protect the vital interests of the data subject or of another natural person
e) performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
f) legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data

art. 6(1) (a)-(f)

consent

The way in which consent is to be given by data subjects remains "unambiguous" for all processing of personal data, with the clarification that this requires a "clear affirmative action", and that consent has to be "explicit" for sensitive data.

any part of the declaration which constitutes an infringement of this Regulation that the data subject has given consent to shall not be binding…

…It shall be as easy to withdraw consent as to give it

'freely given'

When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract

'childrens consent for online services'

in relation to the offering of information society services directly to a child

- the processing of personal data is only lawful, if and to the extent that such consent is given or authorised by the parent
- controller makes reasonable efforts to verify in such cases that consent is given or authorised by parent, taking into consideration available technology

- *below the age of 16 years, or*
- *if provided for by Member State law a lower age (but not be below 13 years)*

verzamel en verwerkingsdoelen ('purpose specification and limitation')

- collection for specified, explicit and legitimate purposes, and
- not further processed in a way incompatible with those purposes

Art. 5(1) (b)

niet-onverenigbaar ('compatability')

inter alia:

a) any link between the purposes for which the data have been collected and the purposes of the intended further processing
b) context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller
c) nature of the personal data (eg. special data)
d) possible consequences of the intended further processing
e) appropriate safeguards (incl. encryption or pseudonymisation)

Art. 6(3a)

Vgl. art. 9(2) Wbp

The controller shall be responsible for and be able to demonstrate compliance ("accountability")

bewaartermijnen ('storage limitation')

- personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

Art. 5(1) (e)

Art. 89(1)

subject to implementation of the appropriate technical and organisational measures [..] in order to safeguard the rights and freedoms of the data subject

bijzondere gegevens ('special categories of data')

Art. 9

Art. 16-23 Wbp

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs, trade-union membership
- genetic data
- biometric data in order to uniquely identify a person
- data concerning health
- sex life and sexual orientation

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.

verwwerkingsverbod voor bijzondere gegevens, tenzij…

- explicit consent
- obligations or specific rights in the field of employment, social security and social protection law
- vital interests of tdata subject or of another person (where the data subject is incapable of giving consent)
- non-profit-seeking political, philosophical, religious or trade-union body
- manifestly made public by data subject
- establishment, exercise or defence of legal claims
- reasons of substantial public interest, on the basis of Union or Member State law
- preventive or occupational medicine or public interest in the area of public health
- archiving purposes in the public interest, or scientific and historical research purposes.

further conditions in national law with regard to the processing of genetic data, biometric data or health data

geen meldplicht maar accountability en documentatieplichten (etc.)

controller is responsible for and be able to demonstrate compliance with data protection principles

DP Impact Assessment

- *systematic description of processing operations and the purposes of the processing*
- *assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- *an assessment of the risks to the rights and freedoms of data*
- *measures to address the risks, including safeguards, security measures*
- *and mechanisms to ensure the protection of personal data and to demonstrate compliance*

data protection by design & by default

Art. 25(1) - (2)

appropriate technical and organisational measures

- designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing
- for ensuring that, by default, only personal data which are necessary for each specific purpose are processed

informatieplichten en inzagerechten ('transparancy, data subject access rights')

Art. 14-15

- controller's identity and contact details
- DPO contact details (if any)
- purposes of processing and legal basis
- legitimate interests of the controller or 3rd party (art. 6(1)f)
- categories of recepients
- third country transfers
- retention periods
- data subject rights
- withdrawal of consent
- automated decision making and profiling
- statutory or contractual obligation
- how to lodge complaints at the DPA…

Art. 33-34 Wbp

- *identiteit van verantwoordelijke*
- *verwerkingsdoeleinden*
- *nadere informatie voor zover dat […] nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen*

'right to be forgotten' ('recht op vergetelheid')

Art. 17

(1) gegevens moeten worden verwijderd
- als deze niet meer nodig zijn
- als toestemming wordt ingetrokken en er is geen andere verwerkingsgrondslag (etc.)

(2) én andere verantwoordelijken moeten worden geïnformeerd over het verwijderverzoek
- althans 'redelijke stappen, incl. technische maatregelen' moeten worden genomen
- als gegevens openbaar zijn gemaakt door de verantwoordelijke

(3) tenzij
- vrijheid van meningsuiting, archivering, wettelijke plichten…

"dataportability"

Art. 20 → *in a structured and commonly used and machinereadable format*

recht om eigen persoonsgegevens overgedragen te krijgen (c.q. over te laten dragen naar een andere verantwoordelijke) } *by automated means*

- als de verwerking is gebaseerd op toestemming (resp. art. 6(1)(a) en 9(2)a), of
- als de verwerking nodig is ter uitvoering van een contract met betrokkene (art. 6(1)b)

...?

opt-out recht voor profiling

right

- not to be subject to a decision based solely on automated processing, including profiling
- which produces legal effects concerning him or her or similarly significantly affects him or her

exemptions

- necessary for entering into (or performance of), a contract with data subject
- authorized by EU or Member State law
- data subject's explicit consent.

vragen?

zwenneblog • g.j.zwenne@law.leidenuniv.nl