Brinkhof

OUTSOURCING KENNISCONGRES 2016

Outsourcing en dé Privacywet

nieuwe privacyregels uit Brussel, uitgebreide bewerkersverplichtingen, een DPO-plicht en de regels voor internationale doorgifte

Gerrit-Jan Zwenne
Nijkerk 22 september 2016

@zwnne

roadmap

Eg. Art. 23 GDPR, Recital 84 (etc.)

- some general remarks (lost in translation)
- controllers & processors
- material and territorial scope
- processor obligations
- third country transfers

In Dutch: verwerkingsverantwoordelijken' & 'verwerkers'

identification and/or single-out?

context of the activities of an establishment of a controller or a processor

safe harbor and privacy shield, binding corporate rules (BCR), standard contractual clauses (SCCs) or derogations…?

Brinkhof

some general remarks (lost in translation)

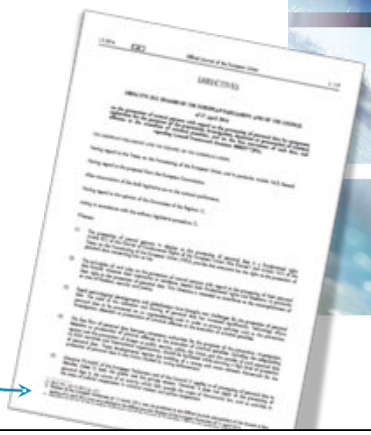
General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 *OJ* 04.05.2016 L.119-188

- same concepts, same principles
- more detailed, more prescriptive, more cost, more rights, more protection (..?)
- much higher fines

entry into force: 25 May 2018..!

law enforcement directive ("LEA")



fragmentation
"minder minder"..?

- *many, many vague norms and open concepts*
- *national authorities and national courts remain competent*
- *many delegated acts*

Brinkhof

lost in translation

Artikel 23

1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn …

lost in translation

Artikel 23

1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die dat artikelen overeenstemtmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, kan worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn …

Article 23

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22…

lost in translation…

Overw. 84

Teneinde de naleving van deze verordening te verbeteren indien de verwerking waarschijnlijk gepaard gaat met hoge risico's in verband met de rechten en vrijheden van natuurlijke personen, dient de verwerkingsverantwoordelijke of de verwerker verantwoordelijk te zijn voor het verrichten van een gegevensbeschermingseffectbeoordeling om met name de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Recital 84

In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk.

lost in translation (..?)

overw. 59, 85, art. 12(3), art. 16, art. 34(1) , art. 61(2), art. 64(4) en (5), art. 65(5) en (6)

'without undue delay'

'without delay'

'onverwijld' of

'onverwijld'

overw. 86, 87, art.17(1), art. 33(1) en (2), art. 70(1)(g)

'zonder onredelijke vertraging'

overw. 127, art. 5(1)(d),12(4), 51(4), 56(3), 60(3), 62(2), 65(5), 66(1), 83(9), 84(2), 85(3), 88(3), 90(2),

controllers & processors
material and territorial scope

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

Idem art. 2(1) Wbp

Brinkhof

processing of personal data by controllers and processors

*any information relating to an identified or identifiable natural person (‘**data subject**’)*

can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Brinkhof

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 …

Brinkhof

(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.

(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 ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.

74. […] Voor de aanbieder van internetdiensten moet het dynamische IP-adres worden gekwalificeerd als een persoonsgegeven, omdat er een derde (de internetprovider) is van wie redelijkerwijs kan worden aangenomen dat de aanbieder van de internetdiensten zich tot hem zal wenden om aanvullende gegevens te verkrijgen die het, in combinatie met het IP-adres, mogelijk maken om een gebruiker te identificeren.

Conclusie AG CAMPOS SÁNCHEZ-BORDONA delivered on 12 May 2016 Case C−582/14 (Breyer)

74. […] A dynamic IP address must be classified, for the provider of Internet services, as personal data in view of the existence of a third party (the Internet service provider) which may reasonably be approached in order to obtain other additional data that, combined with a dynamic IP address, can facilitate the identification of a user.

territorial scope

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

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

new!

irrespective of whether a payment of the data subject is required

Brinkhof

processor obligations

processor obligations

- processor contract (28.3)
- records of processing (art. 30.1)
- cooperation with DPA (art. 31)
- security (art. 32)
- notification of breach to controller (art. 33.2)
- designation of representative (for 3rd country processors) (art 27.1)
- designation of dpo (art. 37.1)
- 3rd country transfer obligations (art. 44)

28.10. … if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing

Brinkhof

processor contract
obligations for controllers

ensure that…

- *processors provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject*
- *processor does not engage a sub processor without prior specific or general written authorisation of the controller*

In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Brinkhof

processor contract requirements

- processes only on documented instructions from the controller (incl. with regard to data transfers to third countries)
- confidentiality obligations for persons processing the data
- security measures
- respect for conditions regarding sub-processors
- assist the controller by appropriate technical and organizational measures, for the fulfillment of the controller's obligation to respond to requests for exercising the data subject's rights
- assists the controller in ensuring compliance with security obligations
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services
- make available to the controller all information necessary to demonstrate compliance with these obligations and allow for and contribute to audits

Brinkhof

special data

new!

health data, ethnic data, ~~religion~~, political opinions, trade union membership, biometric data, genetic data, criminal records

may not be processed, unless…

- explicit data subject consent
- manifestly made public by data subject
- establishment, exercise or defence of legal claims
- specific obligations and rights in the field of employment and social security and social protection law
- protection of vital interest of data subject or other person
- trade union, not-for-profit bodies with political, philosophical or religious aim
- subtantial public interest and public interets in the area of public health
- preventive of occupational medicine, assessment of woking capacity
- archiving purposes

Brinkhof

specific member state legislation

- freedom of expression and information — *Art.87*
- social security numbers and
- special data in employment context — *Art. 88-89*
- special data
- rights of datasubjects — *Art. 9(4), 10*

Art. 23

Brinkhof

data protection officer ("dpo")
mandatory for controllers or processors

- public authorities
- systematic monitoring on a large scale
- core business processing special data

independent and knowledgeable

- *to inform and advise controller, processor and employees of their DP obligations*
- *to monitor compliance with DP rules, incl. assignment of responsibilities, awareness-raising and training and audits;*
- *to advise on data protection impact assessment*
- *to cooperate with the supervisory authority and to act as the contact point on issues relating to processing, and to consult.*

Brinkhof

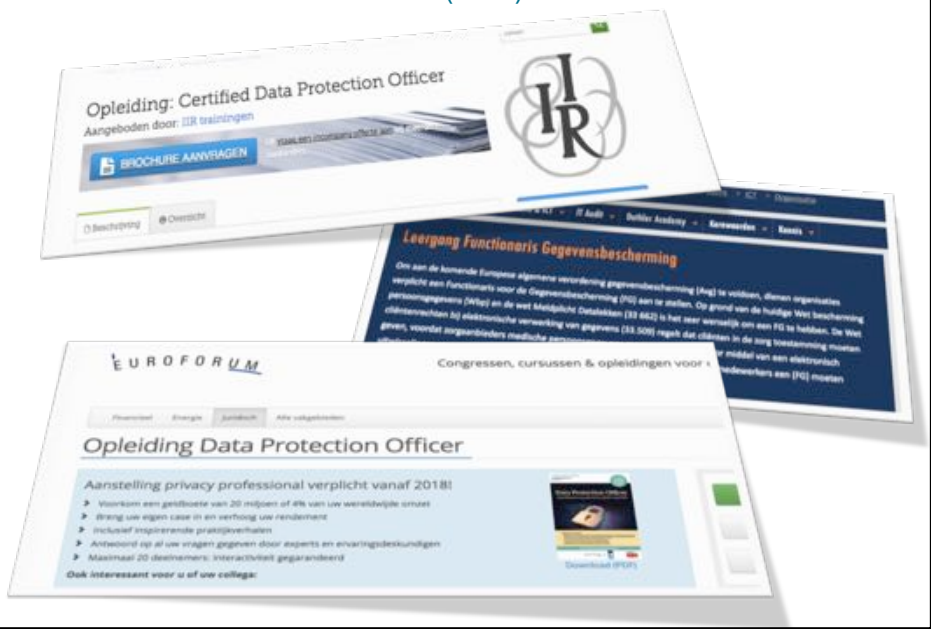
data protection officer (“dpo”) position

- group of companies may appoint a single DPO provided he or she is easily accessible from each establishment
- DPO can also be designated by associations representing controllers or processors

- *data subjects contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights*
- *secrecy or confidentiality obligations concerning the performance of his or her tasks,*
- *may fulfil other tasks and duties*
- *controller or processor to ensure that any DPO tasks and duties do not result in a conflict of interests…*

Brinkhof

‘certified DPO-courses’ (…?)



third country transfers

SCCs, BCR, Safe Harbor, Privacy Shield, derogations

third country transfers

personal data may *not* be transferred to third countries, unless…

Andorra, Switzerland, Israel, Argentina, Uruguay etc. (but not Safe Harbor anymore)

- there is an adequacy decision with respect to that third country, or the
- transfer is subject to appropriate safeguards, or if use can de made of
- derogations

- *binding corporate rules (BCRs)*
- *standard contractual clauses (SCCs)*
- *approved code of conduct*
- *approved certification mechanism*

- *explicit data subject consent*
- *performance of a contract with data subject or in the interest of the data subject*
- *important reasons of public interest*
- *establishment, exercise or defense of legal claims*
- *to protect vital interest of data subject or other persons*
- *public register*
- *compelling legitimate interests, not overriden by datasubject rights (not repetitive, limited number of data subjects etc.)* } *new!*

Brinkhof

PrivacyShield

- *self-certification with monitoring by U.S. Dep. of Commerce*
- *regularly updated list of self-certified companies*
- *an ombudsperson mechanism*
- *no mass and indiscriminate collection of personal data, unless…*

"Adherence to these Principles may be limited: […] to the extent necessary to meet national security, public interest, or law enforcement requirements…"

WP29 would have expected stricter guarantees concerning the independence and the powers of the ombudsperson

WP29 regrets the lack of concrete assurances that such practice does not take place.

gerrit-jan.zwenne@brinkhof.com

Brinkhof N.V.
De Lairessestraat 111-115
1075 HH Amsterdam
T +31 20 305 32 00
F +31 20 305 32 01
E info@brinkhof.com
www.brinkhof.com