A quick introduction to data protection law, now and in the near future

Brinkhof

vereniging van compliance officers

prof. mr. Gerrit-Jan Zwenne
29 June 2016

A full program
for this afternoon

A. background
B. key concepts
C. material and territorial scope
D. lawful processing of personal data
E. third country transfers

DP Directive 95/46/EC and, as of 25 May 2018, the General DP Regulation (GDPR)

personal data, data subject, controller, processor, dpo

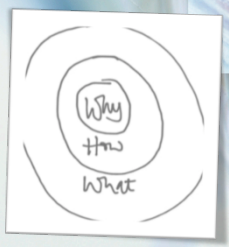
automated processing of personal data, but not: personal or houshold activities, police & justice, intelligence services

processing grounds, purpose specification and purpose limitation, special data, breach notification, access rights, RtbF etc.

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

Brinkhof

A. background
on DPD 95/46/EC and GDPR and the Dutch DP Act



DP Directive 95/46/EC
and the General DP Regulation

legal basis
art 100A (art. 95) TEU

objectives
- *harmonize national DP-law within the EU (or: EC)*
- *high level of data protection*

instruction for member states to implement DP-law in accordance with the Directive

legal basis
art. 16(1) TFEU (art. 8 Charter)

objectives
- *high level of data protection, harmonization, strong and coherent framework, etc.*

EU-law that has binding effect for everyone in the EU (and others)

UK Data Protection Act 1998, Personupgiftslagen, Wet bescherming persoonsgegevens, etc.

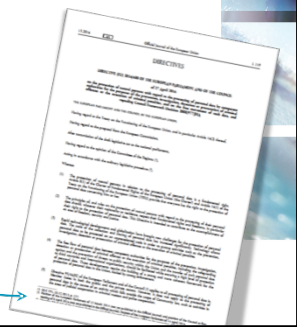
Brinkhof

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

B. key concepts

processing of personal data, data subject, controller and processor, dpo

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 single-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

(23) 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 individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the 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.

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 ay 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

C. 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

CCTV…
compatible with DP-rules?

the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity

data subjects should be informed, have access rights, etc.

not exempted from DP-rules

CJEU 11 December 2014 C-212/13

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 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

D. Lawful processing

processing ground, purpose specification and limitation, special data, data subject rights etc.

lawful processing

- processing grounds
  - *a) unambiguous data subject consent*
  - *b) performance of a contract with data subject*
  - *c) legal obligation*
  - *d) vital interest of datasubject (or other persons)*
  - *e) public task*
  - *f) legitimate interest, unless data subject privacy interests prevail*
- purpose specification and purpose limitation
  - *collected for specified, explicit and legitimate purposes, and*
  - *not further processed in a manner that is incompatible with those purposes*
- security and security breach notification
  - *appropriate technical and organisational measures to ensure a level of security appropriate to the risk*
- transparency obligations and data subject rights etc.
  - *information obligations, access and rectification rights, incl. right to erasure and RtbF, dataportability rights, right not to be subject to automated decisision making, incl. profiling*
- controller and processors
  - *processor contract, sub-processing subject to controller consent, provisions on subject-matter and duration, etc.*

Brinkhof

data protection impact assessment ("dpia")

assessment of the impact of envisaged processing operations on the protection of personal data

accountability

mandatory for

1. systematic and extensive evaluation of personal aspects relating to natural persons
   - based on automated processing, including profiling, and
   - on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
2. processing on a large scale of special categories of data
3. systematic monitoring of a publicly accessible area on a large scale

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 mustl 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

(a) processes only on documented instructions from the controller (incl. with regard to data transfers to third countries)

(b) confidentiality obligations for persons processing the data

(c) security measures

(d) respect for conditions regarding sub-processors

(e) 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

(f) assists the controller in ensuring compliance with security obligations

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services

(h) 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

E. 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 over-riden by datasubject rights (not repetitive, limited number of data subjects etc.)* } *new!*

Brinkhof

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