AUTORITEIT
PERSOONSGEGEVENS

GDPR, the health care sector and the Data Protection Authority

Mrs. Loes Markenstein, LL.M,
Amsterdam, June 13, 2016

Disclaimer

'now that the dust has settled, it is time to start the assessment of the potential impact'

- Publication finalized text GDPR May 2016
- GDPR compliance deadline in May 2018

- Increased harmonisation across the EU, adressing new technological developments; directly applicable across the EU, without the need for national implementation; fewer national variations in data protection compliance obligations

- Changes in role DPA's (+++)
- Changes in requirements controllers/processors (+++)
- Changes in rights data subjects (++)
- Changes in principles and substantive requirements (+)

Main principles and concepts

- Personal data
  - General processing conditions (performance of contract, compliance with legal obligation, vital interest data subject or another individual, task in the public interest of offical authority, legitimate interests of data controller or third party, consent)
  - Anonymisation not defined; pseudonymisation is defined (= processing of personal data)

- Data concerning health: special category personal data
  - Processing prohibited without explicit consent; processing without consent for purposes mentioned in article 9

Health care sector

- article 9(2)h 'for the purpose of …the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragrap 3 (processed under the responsiblity of a professional subject to the obligation of professional secrecy under Union or Member State law or rules ….or by another person also subject to an obligation of secrecy under Union or Member State law or rules …)
- Article 9(2)j: processing is necessary for archiving purposes in the public interest, scientific or historical purposes or statistical purposes in accordance with article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Health care industry: Consent

- Consent must relate to the processing of personal data for a specific purpose
- Consent must be distinghuishable from other matters in contract
- Invalid where the performance of a contract is made conditional upon giving consent to the processing of personal data which are not necessary for the performance of the contract
- Data controller must demonstrate that consent was given
- Data concerning health: explicit consent, article 9(2)a
- Consent and minors

Health care sector/industry: Additional Member state law?

Article 9(4): Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Additional rights data subjects

- Right to be forgotten
- Dataportability
- Prevention of automated decision-making and profiling
- Prevention of direct marketing

Changes in requirements controllers/processors

- Demonstrate accountability (be able to ensure and demonstrate, including through the adoption and implementation of appropriate data protection policies, that the processing activities comply with the requirements of the Regulation)
- DPIAs: perform a DPIA in the event that the relevant processing operations present high risks to the rights and freedoms of the data subjects (eg. processing special categories of data on a large scale)
- Privacy by design, privacy by default
- Written agreements in case of multiple controllers
- Data processing agreements (articles 28-30)
- Appointment of a DPO

Changes in role DPA's

- Cooperation among DPA's (mutual assistance and joint operations)
- EDPB (new EU body with legal personality and power to make binding decisions on enforcement, but also an advisory role)
- One Stop Shop
- Consistency Mechanism

Autoriteit Persoonsgegevens

UK Information Commissioner's Office Twelve steps to take now (1)

- Awareness: make sure you understand GDPR
- Information gathering: assess and verify what personal data you hold
- Transparancy: ensure that you have in plain language and transparant statements as to how you process personal data
- Individual rights: understand the new rights and anticipate how you will need to amend your business practices to respect those rights
- Subject access requests: update you policies and procedures
- Legitimate processing: understand how you can lawfully process personal data and identify the legal basis for the use of personal data that you hold

Autoriteit Persoonsgegevens

UK Information Commissioner's Office Twelve steps to take now (2)

- Consent: consider what plain language 'permissioning' statements you will need to have in place
- Children: start thinking about putting systems in place to verify individuals' ages and to gather parental or guardian consent
- Data breaches: have the right procedures to detect, report and investigate a personal data breach
- Data protection by design and DPIA's: work out how and when to implement them
- Data protection officers: designate a DPO
- International: if your organisation operates internationally, determine which DPA you come under

Autoriteit Persoonsgegevens