Event Ulys – My Data Trust
28 September 2017

From Data Protection Directive to General Data Protection Regulation (GDPR): Main impacts on the life sciences

Regulation (EU) 2016/679 of 27 April 2016

Dr Thierry Léonard
Member of the Brussels Bar
Professor at the University of Saint-Louis - Brussels
thierry.leonard@ulys.net

Introduction and table of contents

I. Unification of the legal framework

- Legal instrument : from a Directive to a Regulation
  - No need for transposition
  - Directly applicable

BUT offering large flexibility for Members States

I. Unification of the legal framework

BUT offering large flexibility for Members States

⇒ specifically concerning processing of genetic data, biometric or data concerning health (art. 9 §4 GDPR)

⇒ specifically concerning scientific and statistical purposes (art. 89 GDPR)

CSQ for the Life Sciences : specific uncertainty regarding the future legal framework

I. Unification of the legal framework

- **Extended territorial scope** (art. 3 GDPR): GDPR applies to processing:

  (1) in the context of the activities of **an establishment** of a controller/processor in the EU ;

  (2) of personal **data of subjects** who are **in the Union by a controller/processor without establishment** in the Union where the processing activities are related to:

  - the offering of goods/services to data subjects in the EU

  or

  - the monitoring of their behaviours if the behaviour takes place within the EU

I. Unification of the legal framework

- In the case of cross-border processing:
  - A single supervisory authority will be competent to monitor the activities of the controller (the lead supervisory authority) (art. 56)

➡ the supervisory authority of the main establishment or of the single establishment of the controller/processor

II. The definitions and principles

- Some parts of definitions are new and useful (art. 4, GDPR):
  - ‘personal data’: refers to the physical, physiological, genetic and mental identity;
  - ‘profiling’: refers to the analyse and prediction of aspects concerning the health ;
  - ‘pseudonymisation’ replaces the old concept of “données codées”;
  - ‘consent’ becomes more clear but also more restrictive

II. The definitions and principles

- new definition of ‘genetic data’ and ‘biometric data’ and ‘data concerning health’;

But no definition of ‘anonymous data’

II. The definitions and principles

New Basic principle : accountability

(art. 5.2. GDPR)

‘The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)’.

II. The definitions and principles

- No revolution regarding the principles contained in the Directive (art. 6) but article 5 GDPR includes new features:
  - a general principle of transparency (Art. 5, § 1, a));
  - the principle of data minimisation (Art. 5, § 1, c));
  - the obligation of security and confidentiality (Art. 5, § 1, f))

- No revolution regarding the now classic processing legality-related assumptions but the rules regarding consent are reinforced:
  - Given "by a statement or by a clear affirmative action" (art. 4, §1, 11))
  - various consent-related rules: burden of proof, level of accuracy in a written text of a more general coverage, a generalized right of withdrawal, etc. (art. 7 and 8)
  - Becomes the only base for changing purposes of the processing if the new one is not compatible with the old one (art. 6 §4)

II. The principles (chapter II)

- "Consent" becomes the only ground for changing the purpose of the processing if the new one is not compatible with the old one (art. 6 §4)

= Very restrictive solution after a heated debate **BUT** large derogations for scientific or statistical purposes (art. 5 (b) and 89, GDPR)

III. The strengthening of data subjects' rights (chapter III)

- Increased transparency:
  - General principle of transparency (art. 12);
  - Information duty is extended to additional information (art. 13 and 14)
  - Rectification, erasure, restriction of processing are to be in principle communicated to each recipient (art. 19)
- Recognition of new rights with potential exception for scientific and statistical purposes (cfr art. 89 §2 and 17§3):
  - right to erasure ('right to be forgotten') (art. 17)
  - right to restriction of processing (art. 18)
  - right to data portability (art. 20)

IV. Controllers and processors (chapter IV)

- The relationship between Controllers/Processors still be organized by contract with extended obligations for processors :

➡ Specific obligations
- security, confidentiality and accountability

➡ Advising controller
- DPIA, security breaches, security, data destruction, contribution to the audits

➡ Record of processing activities and appointment of DPO

IV. Controllers and processors (chapter IV)

- New duties for controllers :
  - General principle of responsibility (art. 24)
  - Principle of data protection by design (art. 25)
  - Principle of data protection by default (art. 25)
  - Notification of data breaches (art. 33 and 34)
  - Impact assessment (art. 35 and 36)

IV. Controllers and processors (chapter IV)

- Common duties for Controllers/Processors:
  - Appointing a representative (art. 27);
  - Record of processing activities (art. 30);
  - Cooperation with supervisory authorities (art.31);
  - Duty of security (art. 32);
  - Designation of a DPO (art. 37);

V. Data transfers outside the EU

- Prohibition of transfers to countries/organization without adequate level of protection (art. 44) but:
  - The Commission is the only one to decide if there is an adequate level of protection;
  - In absence of a Commission decision, the controllers and the processors have to take adequate safeguards (art. 46):
    - Binding corporate rules
    - Standard contractual clauses
    - Certification mechanism
    - Etc.

VI. Supervisory authorities

- **Strengthening of the powers** of the supervisory authorities (investigative powers, powers to take corrective actions and to advice) (art. 58) ;

- **Increasing of the tasks** of the supervisory authorities (tasks of surveillance, investigation and control, tasks of providing information and advice, management of complaints etc.) (art. 57) ;

- Submitted to specific duties of **cooperation and consistency** (chapter VII)

VI. Supervisory authorities

- Breaking news: the new Belgian DPA is coming!

→ Draft bill (August 23, 2017) - (Doc 54 2648/001)

→ a kind of independant administrative authority (like « Autorité belge de la concurrence », IBPT)

→ end of Sectoral Committees

VII. Remedies, liability and penalties (chapter VIII)

- Administrative sanctions (art. 58 §2):
  - Warning
  - Formal demand
  - Temporary or permanent limitation on processing
  - Suspension of data flows
  - Order to comply with the data subject's requests to exercise his or her rights
  - Order the rectification or erasure of personal data or restriction of processing
  - Withdrawal of certification

VII. Remedies, liability and penalties (chapter VIII)

- Right **to lodge a complaint** (art. 77) and to **a judicial remedy** against Controllers/Processors (art. 79);
- Right to a **judicial remedy** against supervisory authorities (art. 78);
- **Principle of compensation** for the material or immaterial damage suffered by any person as a result of an infringement of this Regulation (art. 82)
- **Administrative fines** (depending on the offence) (art. 83, §3 and §5)
  - 10 or 20 million euros or;
  - 2% up to 4% of the company's annual world-wide turnover (highest amount)

Conclusions

- Uncertainty concerning the legal framework in health sector
- New approach based on the responsibility of the Controllers/Processors who have the burden of proof of compliance
- Increased duties for Controllers and Processors
- Expensive, long, and new processing of implementation BUT with a real added value
- At the source of new jobs at the border of several skills (juridical, technical and operational)

VISIT OUR WEBSITES DEDICATED TO GDPR

https://www.gdpr-expert.eu/

https://www.gdpr-expert.com/

(https://www.droit-technologie.org/)

THANK YOU FOR YOUR ATTENTION