

MAYER • BROWN

EUPATI Webinar: The Impact of GDPR on Clinical Trials

Diletta De Cicco

Associate, Brussels

+32 2 551 5974

ddecicco@mayerbrown.com

Charles-Albert Helleputte

Partner, Brussels

+32 2 551 5982

chelleputte@mayerbrown.com

The General Data Protection Regulation

- The General Data Protection Regulation (“**GDPR**”) entered into force on 25 May 2018
- “New” framework for the processing of personal data
- What has GDPR changed for all?
 - › Increased data privacy governance requirements
 - › Strengthening of individuals’ rights to personal data
 - › Obligation to provide specific information to data subjects
 - › Having policies, procedures, contractual framework in place to ensure compliance with the GDPR
 - › Significantly higher fines / reputation risk for non compliance
- Harmonization **but** Member States still have discretion in a number of (important) areas

GDPR is important BUT

- Regulation (EC) No. 45/2001 for processing of personal data carried out by the Commission and the Agency
- NIS Directive and implementing laws (with upcoming November 2018 deadline for MS to identify operators of essential services)
- Upcoming ePrivacy Regulation
- Upcoming EU Cybersecurity Act



How does GDPR Impact Clinical Trials (and the implementation of CTR)?

How does GDPR Impact Clinical Trials

- Focus on 3 GDPR-related topics and their impacts on clinical trials:
 - › Role of the Parties and Responsibilities
 - › New Governance Obligations
 - › Legal basis for processing
- + lessons learned from data breaches management

Controller *versus* processors

GDPR requirements	Controller	Processor
Implement appropriate technical and organizational measures, including security (Art. 24, 28, 32)		
Set of policies and procedures, including a register of processing activities (Art. 30)		
Appoint a DPO / EU representative (Art. 37, 27)		
Cooperate with supervisory authority (Art. 31)		
Identify suitable legal basis for processing, comply with requirements (Art. 6 – 10)		
Inform data subjects, dealing with SARs (Art. 12 – 22)		
DPIA, privacy by design and by default (Art. 35, 25)		
Data breaches (notify DPA, communicate to data subject – Art. 33-34)		
Agreement with processors (Art. 28)		
Assistance to controllers (Art. 28)		

Controller *versus* processors

- GDPR introduces the concept of joint-controllers
 - › As part of their preparation for GDPR, different authorities in different countries have taken ... different approaches (in particular in relation to sites)

Impact on Clinical Trials

HIGH

- Examples:
 - › Documentation (including ICF)
 - › How to reconcile EC template with sites assessment and DPAs' interpretation (cross-border CTs)

New Data Governance Obligations



Impact Assessment

- Organisations are required to map their processing activities and undertake data protection impact assessments for high risk processing



Privacy by Design

- Proactive approach to ensure that an appropriate standard of data protection is the default position taken



Record of Processing

- Organisations have to maintain detailed records of the processing activities they carry out

Impact on Clinical Trials

MODERATE

Legal basis for processing

- Special categories of data have less available legal grounds for processing (and additional safeguards)
- This is an area where Member States may maintain or introduce further conditions, including limitations

Legal basis for processing

- Pre-GDPR, consent was considered as a natural option in relation to clinical trials
- GDPR strengthened consent requirement

Legal basis for processing

- Consent (Art. 9.2.(a) GDPR):
 - › Data subject has given its explicit consent to the processing of personal data for one or more specified purposes
 - › For consent to be valid, it should also be ‘specific’ (clearly distinguishable from any other matters – including CTR opt-in)

Impact on Clinical Trials

MODERATE

Legal basis for processing

- As part of GDPR preparation, attempt to advocate that consent might not be the right legal basis:
 - › Imbalance between the controller and the data subject (see attempt to advocate this might be the case in some clinical trials context – UK HRA on NHS organizations)
 - › Right to be forgotten and withdrawal of consent at any time may put trials at risks (number of subjects, availability and reliability of data, etc.)

Legal basis for processing

- As part of GDPR preparation, attempt to advocate that consent might not be the right legal basis (con't):
 - › New WP29 guidelines on consent acknowledged the issue but made it clear that no exception is available here (unless other legal grounds are available without “swapping”)

Impact on Clinical Trials

MODERATE

Legal basis for processing

- What is / are the alternatives?
 - › Public interest, public interest in the area of public health?
 - › Scientific research?
 - Scientific research (recital 159): broad interpretation and include, for example “technological development”, “fundamental research”, “applied research” and “privately funded research”
 - Available to commercial research?

Impact on Clinical Trials

VALUABLE

Legal basis for processing

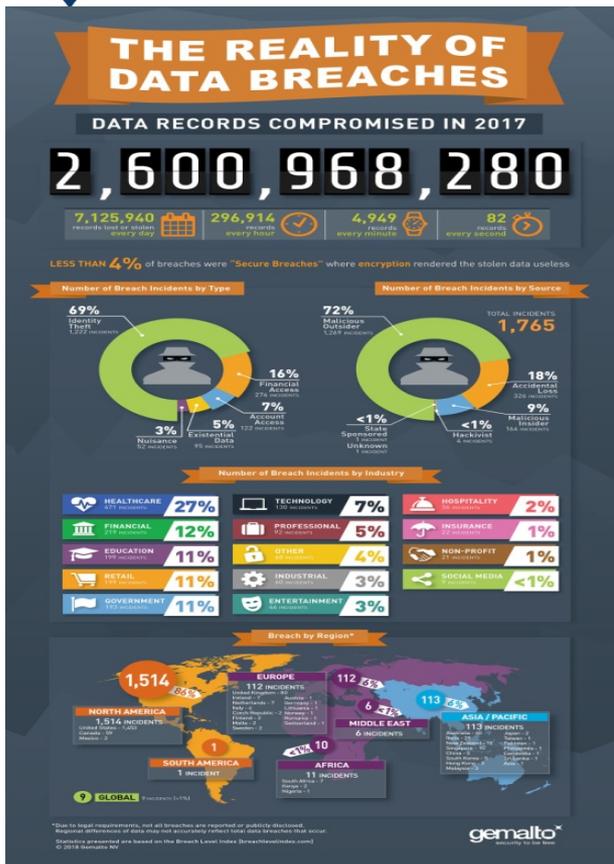
- Some of the benefits ... and boundaries
 - › Option to restrict by Union or Member State law some of the rights (right to access, right to rectify, to restrict processing, right to object) of data subjects
 - › Further processing not be considered to be incompatible with the initial purpose
 - › Subject to safeguards such as technical and organization measures and fulfill the principle of data minimization. E.g., pseudonymization



Data Breaches management:
5 lessons learned

Data Breaches: 5 lessons learned

- Breaches happened, were notified to DPAs and communicated to data subjects since GDPR Day:



Getting struck by a lightning

1 in 960.000

Dating a millionaire

1 in 220

Experiencing a data breach

1 in 4

Sources: 2017 breachlevelindex.com & Ponemon Institute's 2017 Cost of Data Breach Study

Data Breaches: 5 lessons learned

What have we learned from assisting our clients in this area?

1. GDPR is important but ... there is more than GDPR
2. Interaction with DPAs requires caution
3. Data breach notification is a test for your LSA's election
4. Notifying DPAs might be (un)easy
5. The When, How and Why of communication to data subjects



Charles-Albert Helleputte

Partner (Brussels)

T: + 32 (0) 2 551 59 82

E: Chelleputte@mayerbrown.com



Diletta De Cicco

Associate (Brussels)

T: +32 (0) 2 551 59 74

E: Ddecicco@mayerbrown.com

Disclaimer

The material in this presentation is provided for informational purposes only and does not constitute legal or other professional advice. You should not and may not rely upon any information in this presentation without seeking the advice of a suitably qualified attorney who is familiar with your particular circumstances. Mayer Brown Practices assumes no responsibility for information provided in this presentation or its accuracy or completeness and disclaims all liability in respect of such information.

Mayer Brown Practices is, unless otherwise stated, the owner of copyright of this presentation and its contents. No part of this presentation may be published, distributed, extracted, reutilized or reproduced in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) except if previously authorized in writing.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the “Mayer Brown Practices”) and non-legal service providers, which provide consultancy services (the “Mayer Brown Consultancies”). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website.

MAYER • BROWN

Mayer Brown is a global legal services provider comprising legal practices that are separate entities (the "Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP and Mayer Brown Europe-Brussels LLP, both limited liability partnerships established in Illinois USA; Mayer Brown International LLP, a limited liability partnership incorporated in England and Wales (authorized and regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown, a SELAS established in France; Mayer Brown Mexico, S.C., a sociedad civil formed under the laws of the State of Durango, Mexico; Mayer Brown JSM, a Hong Kong partnership and its associated legal practices in Asia; and Tauli & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. Mayer Brown Consulting (Singapore) Pte. Ltd and its subsidiary, which are affiliated with Mayer Brown, provide customs and trade advisory and consultancy services, not legal services. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.