WILLIAM FRY

// PRIVACY SOURCE

GDPR and Life Sciences

The EU General Data Protection Regulation (**GDPR**), which took effect on 25 May 2018, is one of the most ground-breaking pieces of EU legislation in the digital era.

It has modernised the legal framework of data protection and privacy in Europe to ensure the consistent protection of personal data by making businesses more accountable for compliance. The implementation of the GDPR has brought about a number of sweeping changes and all types of organisations across the Life Sciences must comply with the biggest change to data protection law in over 20 years.

Some key changes and impacts the GDPR implemented include:

TERRITORIAL SCOPE

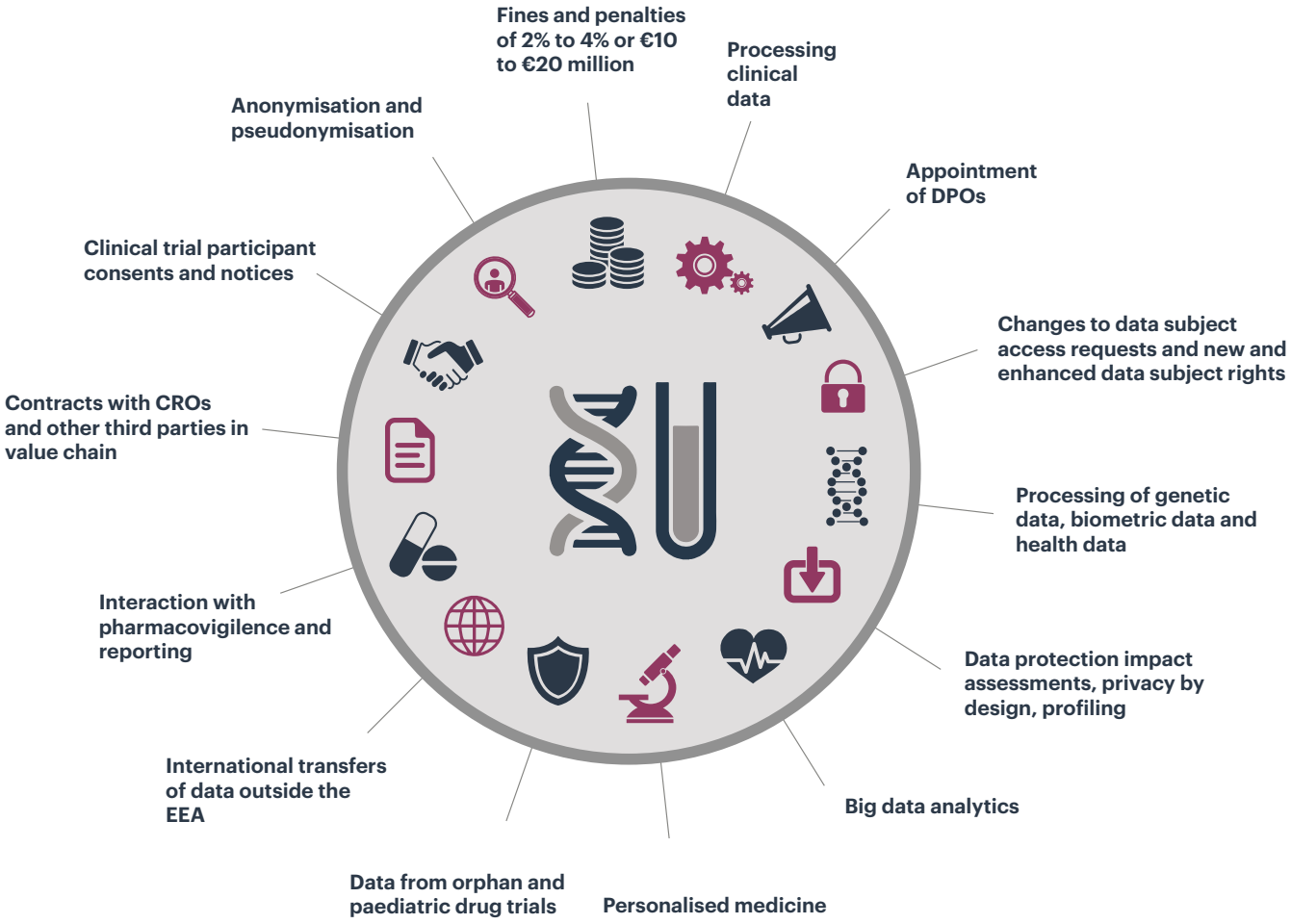
The territorial scope of data protection law includes non-EU businesses (e.g. sponsors and CROs) who monitor the behaviour of or who offer/sell goods to individuals based in the EU (irrespective of whether a payment of the data subject is required).

CONSENT	High threshold for consent which must be specific, freely given, informed and unambiguous. Explicit consent is required for processing special categories of data such as health data, biometric data and genetic data. Pre-GDPR notices and consents in the context of clinical trials should have been or need to be to be revised.
DPIAS (DATA PROTECTION IMPACT ASSESSMENTS)	More detailed data protection notices and updated policies are required. Employers' data protection notices and policies need to be more prescriptive and transparent regarding the processing of personal data. Any notice or policy drafted pre-GDPR will likely need to be replaced or updated.
PENALTIES & CLAIMS	Now as high as €10m or 2% of global annual turnover/€20m or 4% of global annual turnover depending on the nature of the breach. Affected individuals have a right to sue for both material and non-material damage.
DATA PROTECTION BY DESIGN	Requires entities in the Life Sciences sector to incorporate data protection principles into business processes by having measures in place designed to implement data protection principles from the outset.
MANDATORY DPO (DATA PROTECTION OFFICER)	Most likely required by the majority of entities operating in the Life Sciences sector, for example where a business engages in regular and systematic monitoring on a large scale or large-scale processing of special categories of data, such as health data.
SECURITY BREACH REPORTING	Requirement to report to the relevant Data Protection Authority within 72 hours where there is a risk to the rights and freedoms of individuals, e.g. clinical trial participants, employees, etc. Affected individuals must be notified without undue delay where a breach is likely to result in a high risk to their rights and freedoms.

ENHANCED RIGHTS FOR INDIVIDUALS INCLUDING EMPLOYEES

New and enhanced rights include the right to erasure, right to restriction of processing and right to data portability.

GDPR & Life Sciences



Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partners below, our your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 5183
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA