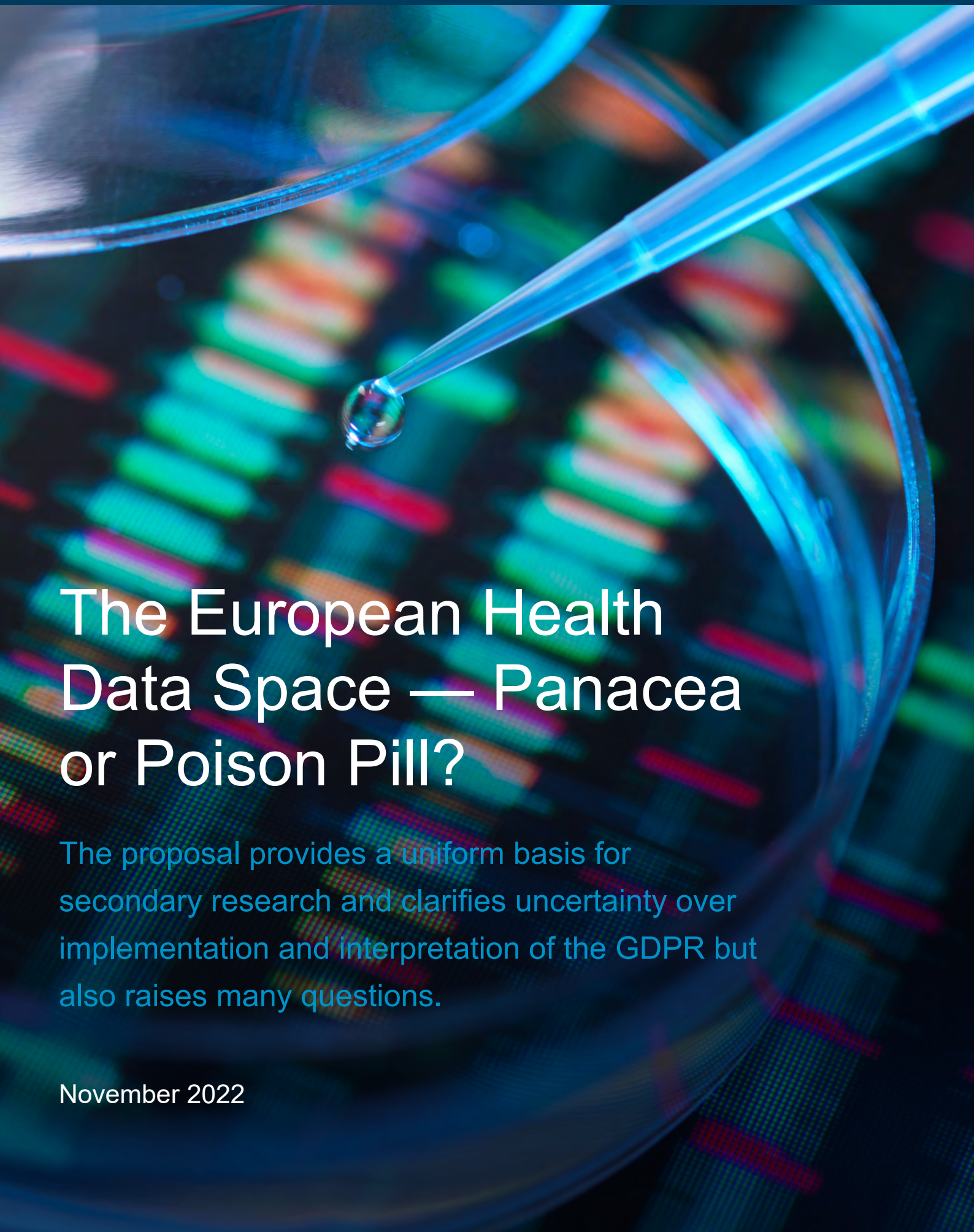
LATHAM & WATKINS LLP



The European Health Data Space — Panacea or Poison Pill?

The proposal provides a uniform basis for secondary research and clarifies uncertainty over implementation and interpretation of the GDPR but also raises many questions.

November 2022

LATHAM & WATKINS LLP

Contents

Introduction

On 3 May 2022, the European Commission launched its proposal for a Regulation for the European Health Data Space to "unleash the full potential of health data". However, questions arise as to whether this proposal is a welcome facilitator of innovation or another burden for research-focussed businesses.

The stated goals of the Regulation are threefold:

- supporting individuals in taking control of their own health data;
- supporting the use of health data for better healthcare delivery, research, innovation, and policy-making; and
- enabling the EU to make full use of the potential from a safe and secure exchange, use and reuse of health data.

The Regulation aims to meet the first goal by correcting perceived deficiencies in the implementation of the Cross Border Healthcare Directive (Directive 2011/24/EU). For the second and third goals, it both clarifies uncertainty around secondary research using health data following the significant differences in implementation and interpretation of the General Data Protection Regulation (GDPR) and facilitates the creation of a legal and technical environment to support the development of innovative medicinal products, vaccines, medical devices, and in vitro diagnostics.

The Regulation covers three main areas:

1. **Data portability and patient control:** It requires Member States to ensure the systematic digitisation of health records in common formats and participate in a common digital infrastructure established by the Commission for cross-border exchange of health records.
2. **Electronic health record systems:** It introduces a system of self-certification and CE marking for manufacturers of electronic health record systems.
3. **Secondary use of research data:** It facilitates secondary use of clinical data for research purposes by requiring "data holders" to make data available and enabling "data users" to access that data in secure processing environments and based on permits issued by "health data access bodies".

This article focuses on the third area — secondary processing and the issues that the Commission's proposals raise.

Background

At the outset, it is helpful to understand the current status of secondary research under the GDPR and the problems the Commission is trying to solve with the introduction of a European Health Data Space.

Legal Basis

Under the GDPR, a controller must have an appropriate legal basis to process personal data taken from a finite list set out in Article 6. For clinical research, the most appropriate legal bases are consent of the data subject (Article 6(1)(a)) or processing that is necessary for the controller's legitimate interests (Article 6(1)(f)). (Note that these are the most appropriate legal bases for the research elements of the data processing. For other activities, for example, safety data reporting, other legal bases may be applicable such as processing necessary for compliance with a legal obligation (Article 6(1)(c))).

If the data processing involves a special category of personal data such as health data, as will be the case for clinical research, the controller can only process such data if one of the conditions listed in Article 9 of the GDPR apply. When it comes to processing data in the context of clinical trials, the most likely conditions are:

- explicit consent of the data subject (Article 9(2)(a));
- processing necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or pursuant to contract with a health professional who is subject to the obligation of professional secrecy (Article 9(2)(h));
- processing necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Article 9(2)(i)); or
- processing necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on EU 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 (Article 9(2)(j)).

Article 9(2)(h), which is directed at "preventive or occupational medicine", is unlikely to apply to research activities and may only cover the medical treatment activities of the trial. Article 9(2)(i), which is directed at public health, cross-border threats to health, and safety standards, may apply to some public sector research or safety reporting, but may not apply to all types of commercial research.

Most commercial sponsors of clinical research must therefore look to either Article 9(2)(a) (explicit consent) or Article 9(2)(j) (scientific research). The problem, however, with these two conditions is that they have been unevenly applied throughout the EU. As the European Data Protection Board (EDPB) points out in its response to the request for clarifications on the consistent application of the GDPR with regard to health research, Member State or EU law is required in order to rely on Article 9(2)(j) (scientific research). In other words, there needs to be a national law or an EU law that implements this conditions and enables data processing on this ground, and these laws may diverge. As Member States have introduced national laws to implement Article 9(2)(j) and introduced different requirements for the relevant scientific research, "choices made in Member States' law can have a serious impact on the level of harmonisation that can be achieved under GDPR in the domain of processing personal health data for scientific research purposes" and "considerable differences can be found".

In addition, the EDPB in its Opinion 3/2019 on the interplay between the Clinical Trials Regulation and the GDPR casts doubt on whether explicit consent is the appropriate conditions, noting that "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller" and "[d]epending on the circumstances of the clinical trial, situations of imbalance of power between the sponsor/investigator and participants may occur". The EDPB gives the examples of a participant who is not in good health, participants belonging to an economically or socially disadvantaged group, or participants in any situation of institutional or hierarchical dependency. These examples illustrate circumstances in which the participant may not have alternative options, and therefore their consent may not be considered "freely given". The EDPB concludes that "consent will not be the appropriate legal basis in most cases, and other legal bases than consent must be relied upon".

In its response to the request for clarifications, the EDPB rowed back on this position somewhat by saying that "Opinion 3/2019 does not exclude the possibility for the data controller to rely on explicit consent as a legal basis for the processing of data from patients" but rather "Explicit consent as a legal basis can still be relied on in medical research projects where it can be established that no imbalance of power between data subjects and researchers exists and the requirements for explicit consent in GDPR can be met. However, this will require a careful assessment on a case-by-case basis".

Regulators and research institutions across the EU have also been taking divergent views on whether consent is an appropriate legal basis. For example, the UK's Health Research Authority in its pre-Brexit GDPR guidance says, "For the purposes of the GDPR, the legal basis for processing data for health and social care research should NOT be consent." Conversely, in countries such as Hungary, the participant's explicit consent is the only accepted legal basis for data processing in the context of a clinical trial. Similarly, in Portugal, consent must be used as a legal basis other than in exceptional circumstances. In most EU countries, however, there is no mandated legal basis for clinical trials, and there is a lack of clarity as to which is the most appropriate.

There is also the risk that withdrawal of consent could affect the ongoing viability of a clinical trial or the integrity of the analyses. In general, data subjects who have consented to the processing of their personal data are entitled to withdraw that consent. If consent is withdrawn, all data processing operations that were based on consent remain lawful, but the controller must stop the processing actions concerned and, if there is no other lawful basis justifying the retention for further processing, the controller must delete the data.

It should be noted here that consent or explicit consent under the GDPR is a different concept from informed consent of the patient to participate in the trial. The latter is required by the Clinical Trials Regulation (Regulation (EU) No 536/2014) (the CTR) and the ethical principles enshrined in the Declaration of Helsinki. While it is defined in the CTR as a subject's "free and voluntary expression of his or her willingness to participate", it is not considered sufficient for the GDPR standard of a "freely given, specific, informed and unambiguous indication".

Compatibility

The above requirements relate to primary processing activities, i.e., processing personal data for the purpose for which it was collected. When it comes to secondary research, the purpose limitation principle in Article 5(1) of the GDPR states that personal data must be collected for "specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". Compatibility is determined taking into account a number of factors, including the link between the original purposes and the further processing, the context in which the data was collected, and the consequences for the data subject. Further processing for scientific research purposes is presumed to be compatible provided that appropriate safeguards are in place to ensure respect for the principle of data minimisation. The compatibility requirement also does not apply if the appropriate legal basis is consent, on the basis that in order for consent to have the requisite specificity, the data subject will have consented to both the primary and the secondary processing.

Transparency

Articles 13 and 14 of the GDPR require a data controller to provide certain information to data subjects regarding the use of their personal data. Such information includes the identity and contact details of the data controller, the purposes of processing, recipients of the data, and information on the data subject's rights. This requirement has always presented a difficulty for secondary research as it may not have been envisaged and covered in the informed consent form or patient information leaflet when the data was collected, and sponsors of secondary research will usually not have access to the relevant data subjects to supplement that information.

European Health Data Space

Data Permits and Secondary Research

The Regulation seeks to address the above problems by creating a compliant environment for secondary research. It provides the appropriate safeguards for secondary researchers to rely on legitimate interests (Article 6(1)(f)) as the relevant legal basis and the relevant "Union law" for the purposes of the scientific research derogation (Article 9(2)(j)). To achieve this, the Regulation introduces the new roles of data holders, health data access bodies, and data users.

A data holder is defined as:

> *"any natural or legal person, which is an entity or a body in the health or care sector, or performing research in relation to these sectors, as well as Union institutions, bodies, offices and agencies who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data, through control of the technical design of a product and related services, the ability to make available, including to register, provide, restrict access or exchange certain data".*

This is an extremely broad definition and captures not only public health systems and hospitals but also private, commercial entities performing research in the health or care sector.

A data user is "a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use".

Health data access bodies are public bodies established by Member States responsible for granting access to electronic health data for secondary use.

Other than microenterprises, which are exempt, Article 33 of the Regulation requires data holders to make certain broad categories of data available for secondary use through a secure processing environment provided by the health data access body, including:

a. electronic health records;

b. data impacting health, including social, environmental, and behavioural determinants of health;

c. relevant pathogen genomic data impacting human health;

d. human genetic, genomic, and proteomic data;

e. population-wide health data registries (public health registries);

f. electronic health data from medical registries for specific diseases;

g. electronic health data from clinical trials;

h. electronic health data from medical devices and from registries for medicinal products and medical devices;

i. research cohorts, questionnaires, and surveys related to health; and

j. electronic health data from biobanks and dedicated databases.

Health data access bodies would then compile and publish a dataset catalogue including details about the source and nature of electronic health data and the conditions for making this available. The underlying data itself is not made public by the health data access body. If a data user wishes to access a particular dataset, it would need to submit an application to the health data access body, including details regarding the intended use, the requested data, whether anonymised or pseudonymised data is required, and a description of the relevant safeguards to be implemented. Health data access bodies would assess the relevant applications and determine whether the requested use is for a permissible purpose. If so, the health data access body would issue a data permit and immediately request access to the data from the data holder. The data permit will specify the type and format of the data, the purpose for which it is to be made available, and the duration. Following the issuance of a data permit, the data holder must make the data available to the health data access body, which in turn will make the data available to the data permit holder through a secure processing environment. The data must be made available by the health data access body to the data user within two months of receipt of the data from the data holder, unless a longer timeframe is specified by the health data access body.

Transparency concerns are addressed by making health data access bodies and data users joint controllers for the purpose of the secondary research. The Commission will publish a template joint controllers' arrangement governing such relationship. The Regulation provides for an exception to the general transparency requirements under Article 14 of the GDPR and instead provides for health data access bodies to make publicly available general information concerning the conditions for secondary use, including legal basis, technical and organisational measures, data subject rights, and results or outcomes of the relevant projects.

Limitations on Secondary Use

The right of access to datasets seems far-reaching but would be subject to some limitations. Access to the relevant data is provided only through a secure processing environment provided by the health data access body, from which data users will not be permitted to download personal data.

Access would only be granted to a user for limited purposes, including:

a. activities for reasons of public interest in the area of public and occupational health;

b. education or teaching activities in health or care sectors;

c. scientific research related to health or care sectors;

d. development and innovation activities for products or services contributing to public health;

e. training, testing, and evaluating algorithms, including in medical devices, AI systems, and digital health applications; and

f. providing personalised healthcare.

Certain purposes would be expressly prohibited, namely:

a. taking decisions detrimental to natural persons based on their electronic health data;

b. taking decisions to exclude persons from the benefit of an insurance contract or to modify their contributions and insurance premiums;

c. advertising or marketing activities towards health professionals, health organisations, or natural persons;

d. providing access to, or otherwise making available, the electronic health data to third parties not mentioned in the data permit; and

e. developing products or services that may harm individuals and societies at large, including illicit drugs, alcoholic beverages, tobacco products, or goods or services that are designed or modified in such a way that they contravene public order or morality.

In addition, health data access bodies would need to provide the relevant data in anonymised form if the purposes of processing can be achieved with anonymised data. If the intended purpose cannot be achieved with anonymised data, the health data access bodies may provide the data in pseudonymised format, and the relevant key to reverse the pseudonymisation would be available only to the health data access body.

Benefit or Burden?

While the Regulation is generally permissive and seeks to open up new avenues of research, as drafted it would also introduce onerous obligations on businesses.

From the point of view of data holders, the obligation to make broad categories of data available would introduce an additional burden on any business sponsoring a clinical trial. The data holder also would need to communicate a general description of the dataset it holds and make the underlying data available to the health data access body within two months of request. In addition, if these datasets have been enriched through processing based on a data permit, the original data holder would need to make the new dataset available. While the obligation on public health systems and hospitals to make electronic health records and research analyses available would be a game-changer for research using real-world evidence, given the broad definition of “data holder”, as drafted any clinical trial sponsor would need to make available all “electronic health data from clinical trials”.

It is not clear what level of data would need to be provided and at what point following completion of or even during the trial. Such data may constitute valuable intellectual property and, while health data access bodies would need to take all measures necessary to preserve the confidentiality of intellectual property rights or trade secrets, data holders would remain under an obligation to make such data available notwithstanding the subsistence of such rights. In addition, while the Regulation envisages a data holder being allowed to charge fees for making data available, such fees would need to reflect only the costs for providing such services and, in some cases, fees for the collection of data, and therefore would not fully reflect the commercial value

of such data. If data holders and data users do not agree on the amount of the fees within one month after the data permit is granted, the health data access body may set the fees.

From the point of view of data users seeking to conduct research, the Regulation is a more welcome proposal. However, the health data access body would need to publish details of all data permits, requests, and applications, which should be borne in mind if there is particular sensitivity in the proposed research. In addition, as a quid pro quo, data users would need to make public the results or output of the secondary use of data, including information relevant for the provision of healthcare, no later than 18 months after completion of the processing. Any clinically significant findings that may influence the health status of a data subject included in the dataset would need to be communicated to the health data access body, which may inform the subject or their treating health professional.

Lastly, the Regulation would provide for health data access bodies to issue fines if data holders withheld data with the manifest intention of obstructing the use of the data or did not meet the relevant deadlines for making the data available. The amount of the fines would be established by the relevant health data access body. In the case of repreated breaches, a data holder could be blacklisted and excluded from the European Health Data Space for up to five years.

Conclusion

Opening the door to further research and open data sharing is an important goal in the EU's digital transformation and would create a framework for innovation, in particular using new technologies such as artificial intelligence and machine learning. The Regulation is welcome in providing a uniform basis for secondary research and clarifying much of the uncertainty caused by significant differences in implementation and interpretation of the GDPR. However, the Regulation raises as many questions as it answers, and significant stakeholder discussion and refinement is needed to ensure that the Regulation achieves an appropriate balance between fostering innovation and ensuring protection of proprietary rights and commercial freedoms.

Contacts

Oliver Mobasser
Associate, London
T +44.20.7710.4738
E oliver.mobasser@lw.com

Gail Crawford
Partner, London
T +44.20.7710.3001
E gail.crawford@lw.com