Processing health data for scientific research purposes in the EU and the UK

Sarah Tedstone, **Nuria Pastor** and **Alex Beresford** of Fieldfisher look across the legislative landscape, and identify challenges and common elements for a multi-jurisdictional model.

There is no doubt that scientific research is important to our society, but it often requires a large amount of protected special category personal data. This article explains the current legal landscape for scientific research activities under data protection law in the UK and the EU and how the forthcoming European Health Data Space (EHDS) and UK plans may change it.

Recently, the EU has created a draft European Health Data Space[1]. The final version is expected to be formally adopted by the EU Council this coming autumn. The primary purpose of the EHDS is to allow individuals to take control of their health data and facilitate data sharing within healthcare systems across the EU. However, the EHDS also aims to provide a "consistent, trustworthy, and efficient system for ensuring health data for research, innovation, policy-making and regulatory activities"[2]. The aim is to benefit individuals, health professionals and researchers but generally also the industry, which should have greater availability of electronic health data for research use. The UK also has future plans to improve research conditions including within the new draft Data Protection and Digital Information Bill.

EU AND UK GDPR PROVISIONS ON SCIENTIFIC RESEARCH

Data protection laws recognise the importance of scientific research and contain specific provisions to ensure that the restrictions on data processing do not inhibit innovation and advancement. They permit a softening of some of the GDPR requirements when personal data is to be used for scientific purposes.

The relevant EU and UK GDPR provisions are currently similar. While the term "scientific research" is not defined, Recital 159 helpfully explains that scientific research purposes should be viewed broadly and that they include technological development and demonstration, fundamental research, applied research and privately funded research. Scientific research purposes include studies carried out in the public interest in the area of public health.

Regulatory guidance provides further support. For example, UK ICO guidance explains that research in a commercial setting would be included and also gives a non-exhaustive list of activities and features that are indicative of this kind of processing enjoying exemptions. Examples from the list of activities include formulating hypotheses, isolating variables, designing experiments, sampling populations, integrating and analysing data as well as publication of findings. We await updates to the ICO guidance on this point. The PHG Foundation paper dated May 2020 dealing with data protection issues in the health research space[3] highlighted some of the grey areas requiring clarification from the ICO.

The softening to the standard rules, that is available within the research provisions, can be summarised into three main areas of focus:

- **Exceptions within the data protection principles**: For example, the "storage limitation" principle notes you can keep personal data indefinitely for research purposes and research is identified as a secondary purpose compatible with primary purposes.
- **Exemptions and exceptions to individual rights**: The GDPR provides individuals with a number of data subject rights. There are a number of exceptions and exemptions that can be applied when responding to a request to exercise these rights which involve processing for scientific research purposes. For example, there is an exception for research built into the right to be informed[4] but they can be derived in different ways under varying national legislation.
- **Conditions for processing special category personal data and criminal offence data**: There is a specific condition allowing the use of special category personal data or criminal offence data for research purposes. In addition, consent for scientific research is allowed to be broader with less specificity.

All of these provisions are underpinned by Article 89 GDPR which requires appropriate safeguards to be in place as a condition of processing personal data for scientific research purposes. These safeguards take the form of technical and organisational measures and might include, where possible, anonymising or pseudonymising data.

LEGAL BASIS FOR PROCESSING HEALTH DATA FOR RESEARCH

There is no specific lawful basis under Article 6 GDPR for processing personal data in a scientific research context. However, for commercial organisations, "legitimate interests" is the most likely lawful basis for processing.

Consent in this area can be problematic. It is important to note that the lawful basis for processing personal data under data protection law is distinct from obtaining consent for separate ethical reasons or under another legal obligation. Obtaining consent from a patient as a lawful basis under data protection law can be challenging as it can be withdrawn (with no exception for research). The specificity required can still be challenging when inevitably research may

take the processing in new and unexpected directions. In the UK, there is ICO guidance and also guidance from the Health Research Authority[5]. It specifically recommends avoiding reliance on consent as a lawful basis supported by the PHG Foundation paper which highlights numerous difficulties, not least that of explaining the differences between consent under the GDPR and consent to research more broadly.

As health data is special category personal data, as well as an Article 6 lawful basis, organisations will be required to identify an additional condition for processing in compliance with Article 9. Others may apply depending on the circumstances but there is a specific Article 9 GDPR condition - Article 9 (2) (j) which can be relied on for processing health data for scientific research purposes.

The above is supported by European Data Protection Board's (EDPB) guidance on the interplay between Clinical Trials Regulations and the GDPR[6], which specifically considers the combination between legitimate interest and Article 9 (2) (j) as one of the viable combinations of lawful bases for processing clinical trial personal data for secondary research purposes. Furthermore, the EDPB re-iterates the challenge of obtaining valid consent from a patient in the context of a clinical trial given the possible imbalance between the individual and the controller. It cautions that imbalances of power can also be indicated more generally where there is a public body involved or where a participant is not in good health, or when they belong to economically or socially disadvantaged groups. This means that consent may be an inappropriate legal basis for significant amounts of health research.

Fragmentation of the conditions for processing

The GDPR enables EU member states (which at the time of implementation included the UK) to introduce further conditions with regard to the processing of health data for research purposes. These local law requirements will apply in addition to the GDPR condition but may be variable per location.

For the UK, the Data Protection Act 2018 (DPA 2018) introduces additional requirements. Section 19 and Schedule 1 paragraph 4 of the DPA 2018 state that you can process special category including health personal data for research-related purposes, but only if the processing is:

- necessary for that purpose (i.e. it is a reasonable and proportionate way of achieving your purpose, and you must not have more data than you need);
- subject to appropriate safeguards for people's rights and freedoms;
- not likely to cause someone substantial damage or substantial distress;
- not used for measures or decisions about particular people, except for approved medical research; and
- in the public interest (i.e. a clear and positive public benefit is likely to arise from the research).

The fragmented legislative landscape in EU member states in relation to the requirement for additional conditions for the processing of health data for research purposes leaves a patchwork of requirements that organisations must navigate through, involving some risk in trying to adopt one multi-jurisdictional model. There are however some common themes which are relevant in various member states, including the requirements of:

- ensuring that the processing of personal data is 'necessary' with de-identifying or coding (if anonymisation is not viable) where possible;
- implementing security measures to protect the information, including measures to restrict access to the same;
- restricting the dissemination of the personal data processed and to have contracts in place with the third parties from where you source the information;
- keeping certain records regarding your research processing activities in addition to your GDPR Article 30 records;
- carrying out risk assessments in relation to these processing activities, including data protection risk assessments (DPIAs) where applicable;
- appointing a data protection officer (DPO) or, if you already have one in place, to involve the DPO in the relevant risk assessments carried out regarding your research activities;
- having governance structures in place and appropriate policy documents;
- involving a health practitioner who is subject to professional confidentiality requirements in the processing activities; and
- obtaining a permit from the local Data Protection Authority (or liaising with the local data protection authority by means of a consultation) before you carry out the research activities.

The future: The new EHDS in the EU, and UK initiatives

Potentially, the new EHDS in the EU, will provide another way to access health data in order to use it for research purposes.

The EHDS regulation sets out that "data holders" shall make certain categories of health data available for secondary processing purposes. This may be personal or non-personal data as it may be shared in an anonymised form.

These types of data include electronic health records, pathogen genomic data, person generated electronic data, including those generated via medical devices or wellness and digital health applications. These data categories may have been obtained for different purposes (e.g. the provision of health care or for public health, research, policy-making purposes) and by a variety of stakeholders in the public and private sector.

Data holders (also present in the recently adopted EU Data Act[7]) are organisations as a public or private entity with the risk or obligation to make available, provide, restrict access or exchange certain data.

The data holders will provide the data to a "data user" (again, defined broadly, as a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use). The data user will have access to such data via a "data permit", which will be issued by "health data access bodies" only for certain intended purposes. These include the processing of personal data for a number of health-related purposes including (Art. 34):

(e) scientific research related to health or care sectors;
(f) development and innovation activities for products or services

contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;

(g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices.

There are prohibited secondary purposes for which the data accessed cannot be used which include advertising or marketing activities towards health professionals, individuals, or corporates.

In addition to granting permits for the secondary use of health data, health data access bodies will monitor the activities of data users and data holders and may issue penalties for non-compliance with their obligations.

The heath data access bodies will be appointed in each member state and they will manage the application process for data permits. Where the data required contains personal data, the applicant data user will have to provide information regarding the legal basis for processing and an assessment of the ethical aspects of the processing. The data permit will contain a number of conditions applicable to the data users regarding their ability to use the data, for instance, in relation to the format of the health data accessed, the purposes for which it is made available, the duration of the permit etc.

In the UK, the Goldacre review, the government's Data for Research and Development Programme, the recently-formed national institute of the Health Data Research UK and UK Health Data Research Alliance, all have broad aims of improving the environment for health data research for the public good. Furthermore, the new Data Protection and Digital Information Bill going through the UK Parliament has the aim of reducing burdens on researchers and giving organisations greater confidence about the circumstances in which they can process personal data without consent by allowing the re-use of personal data for the purpose of:

1. longer term research studies,
2. clarifying what amounts to "scientific research",
3. easing the consent requirements where it may not be possible to identify fully the purposes at the outset of scientific research, and
4. the requirement to provide privacy notices in certain cases for research.

There is currently no direct equivalent of the EHDS or Data Act in the UK.

Conclusion

While the GDPR recognises the importance of scientific research and, accordingly, softens some of its requirements when personal data is to be used for these purposes, the fragmented legislative framework in the UK and EU is a challenge for organisations that wish to carry out such activities on a transborder basis. In practice, different approaches and multi-layers of regulation regarding the legal basis for processing create difficulties and may stifle research and innovation.

The forthcoming EU EHDS seeks, amongst other purposes, to set out a framework for the sharing of health data for scientific research purposes. This may be a step in the direction of improving the sharing of data for the purpose of the advancement of society, in particular, in relation to scientific research, without seemingly opening it up to commercial exploitation. This is in line with other recent initiatives of the European Union, such as the Data Act. The UK also has intentions to make some changes to improve the conditions for research which will be reviewed keenly by the industry.

It seems there is still an impetus to develop the improved ways of working, established during the recent pandemic, for research generally.

AUTHORS

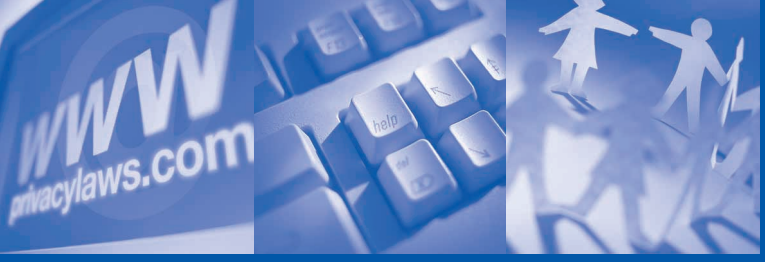
Sarah Tedstone is a Partner, Nuria Pastor a Director and Alex Beresford an Associate at Fieldfisher's Privacy & Data team in London.
Emails:
sarah.tedstone@fieldfisher.com
nuria.pastor@fieldfisher.com
alex.beresford@fieldfisher.com

INFORMATION

There are several health related sessions at *PL&B's* 37th Annual International Conference 1-3 July at St. John's College, Cambridge.
www.privacylaws.com/plb2024

REFERENCES

1 European Health Data Space - European Commission (europa.eu) health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en
2 European Health Data Space - European Commission (europa.eu).
3 PHG Foundation report: The GDPR and genomic data - the impact of the GDPR and DPA 2018 on genomic healthcare and research. PHG Foundation is a charity and part of the University of Cambridge.
4 Article 14(5)(b) GDPR gdpr-info.eu/art-14-gdpr/
5 www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/
6 EDPB Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)). Adopted on 23 January 2019 www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf
7 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (europa.eu) eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_20232854



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The current status of Brazil's Artificial Intelligence (AI) Bill

Brazil's legislature is currently examining a comprehensive AI bill which was proposed in February. **Juliana Müller** of Brazil's Data Protection Authority (ANPD) reports.

Bill No. 2338/2023[1], titled "On the Use of Artificial Intelligence", authored by Senator Rodrigo Pacheco, is currently being debated by the Temporary Internal Committee on Artificial Intelligence in Brazil (CTIA, in Portuguese)[2], within the Federal Senate of Brazil.

Throughout 2023, the CTIA held several public hearings[3] with renowned experts to discuss the impacts of artificial intelligence from

Continued on p.3

France's stance on pay or consent after the EDPB Opinion

Nana Botchorichvili of Idea Avocats analyses the key differences in the approach to cookie walls and the controversial issue of behavioral advertising.

On 17 April 2024, the European Data Protection Board (EDPB) published its much awaited Opinion on the lawfulness under the GDPR of the so called "pay or consent" models implemented by large online platforms[1] (hereafter, EDPB Opinion) – i.e., when users of such services are asked either to consent to the processing of their personal data for behavioral advertising purposes to access the service for free,

Continued on p.6

Issue 189 **JUNE 2024**

INTERNATIONAL report

ISSUE NO 189 JUNE 2024

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
g.greenleaf@iinet.net.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Juliana Müller
Formerly Data Protection Authority (ANPD), Brazil

Nana Botchorichvili
IDEA Avocats, France

Fábio Lacaz
ALV Advogados, Brazil

Professor Emeritus Colin J. Bennett
University of Victoria, Canada

Sarah Tedstone, Nuria Pastor and Alex Beresford
Fieldfisher, UK

Robyn Mohr, Chanda Marlowe and Teodoro Shelby
Loeb & Loeb LLP, US

Elena Testa
Independent Consultant, Italy

Professor Emeritus Bertil Cottier
University of Lausanne, Switzerland

Abigail Dubiniecki
Independent Consultant, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

EU AI Act soon in force – global cooperation needed

The EU AI will soon be in force – we await publication in the Official Journal in early June. The Act is groundbreaking and, as Professor Graham Greenleaf writes, will also affect businesses and governments located outside the EU (p.23). Elsewhere, Brazil has an advanced draft (p.1). What is needed now is regulatory interoperability. Apart from the EU, there are many active players: G7 and G20, UNESCO, United Nations, OECD (p.5) and Council of Europe (p.8) to name a few.

While the EU GDPR and the EU AI Act are complementary, it may be that lessons can be learned to some extent from the GDPR 'failures' – one of them being enforcement challenges. The EU GDPR procedural rules regulation, aimed at improving enforcement in cross-border cases, is making progress. Speaking at the CPDP conference in Brussels on 23 May, Karolina Mojzesowicz, Deputy Head of Unit Data Protection, EU Commission, said that the Council is currently forming its position and the Belgian presidency is committed to adopting a general approach soon.

The UK GDPR reform on the other hand is dead for now as the country prepares for a general election on 4 July (p.11). If the Labour party wins, as is expected, there may well be an AI Bill. But it has not announced whether it will revive the Conservative government's Data Protection and Digital Information Bill.

The European Data Protection Board (EDPB) has issued its Opinion on 'pay or consent' but France's previous stance is somewhat different (p.1). The EDPB, the UK ICO and DPAs from other "adequate" jurisdictions met recently to discuss adequacy and data transfers (p.11). The pool of adequate countries is still very small. Canada's renewed adequacy is discussed in this issue by Professor Emeritus Colin J. Bennett who aptly states that "Canada's privacy protection regime passes, but the exam is still on" (p.9).

PL&B's 37th Annual Conference, 1-3 July, will feature 30 sessions including one with Commissioners from Canada, Germany and the UK discussing regulatory cooperation.
See www.privacylaws.com/plb2024

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

"The UK and International *PL&B* Reports have been my 'go to' resource for 20 years despite the wide choice of alternate resources now available. And have you tried the Annual Conference at Cambridge? I have seven IAPP certificates so a big IAPP supporter. But the *PL&B* Cambridge event, each July, still knocks the spots off IAPP and other conferences!"

Derek A Wynne, SVP Privacy & Chief Privacy Officer, Paysafe Group

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.