

Post-Brexit divergence from GDPR: Implications for data access and scientific research in the UK

Summary note of a workshop held on 6 February 2023

Background

This note provides a summary of discussions at a workshop, held on 6 February 2023, exploring the scientific research implications of the United Kingdom diverging from the European Union's General Data Protection Regulation (GDPR). The workshop was hosted by the Royal Society and chaired by Sir Nigel Shadbolt FREng FRS. The workshop was held with an expectation that a new version of the UK Government's Data Protection and Digital Information Bill would be introduced in 2023. A prior version of the Bill had gone through first reading in Parliament in July 2022, but was later withdrawn and replaced with the Data Protection and Digital Information (No.2) Bill on 8 March 2023¹.

The workshop convened scientific researchers; data protection experts; industry representatives; and privacy campaigners to explore the implications for scientific research and innovation of replacing the current UK GDPR with a new data protection regime. Participants were asked to consider the risk of losing adequacy with the European Union, the potential changes to the definition of scientific research, and how GDPR could be improved to better support scientific research.

This note serves as a summary of themes that emerged from the discussions. This note is not intended as a verbatim record of discussions and does not represent the views or positions of all participants or organisations who took part. The note was drafted by staff at the Royal Society, considering comments, feedback, and references submitted by workshop participants.

1. House of Commons Library. 2023 The Data Protection and Digital Information Bill 2022-23. See: The Data Protection and Digital Information Bill 2022-23 - House of Commons Library (parliament.uk) (accessed 11 April 2023).

Introduction

Following the UK's exit from the European Union (EU), the UK retained GDPR in domestic law as the 'UK GDPR'². The adoption of the UK GDPR, which is almost identical to the EU GDPR, allowed adequacy with the EU as it provided an 'essentially equivalent' level of data protection to that which exists in the EU³. Obtaining adequacy guarantees the free and uninterrupted flow of data between the EU and the country that has obtained adequacy. Aside from the UK, only 13 countries in the world have obtained adequacy: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Korea, Switzerland, and Uruguay.

In July 2022, the UK Government introduced the Data Protection and Digital Information Bill to improve on GDPR. As any change to data protection legislation could potentially lead to the loss of adequacy with the EU, the Bill carried significant implications for scientists who rely on data sharing between the UK and the EU. In addition, the Bill also set out a new definition of scientific research, differing from the definition included in GDPR.

For these reasons, the Royal Society has been closely monitoring the development of the Bill.

The legislative process was paused in September 2022, following the first reading. The Royal Society therefore set out to convene a group of scientists, representatives from industry, data protection experts and data practitioners to understand their needs and expectations when it comes to data protection regulations. The objectives of the workshop were to:

- assess what aspects of GDPR may have supported scientific research and what aspects could be improved on under a new data protection regime.
- understand the importance of adequacy with the EU and the impact on scientific research if the UK were to lose adequacy.
- inform the Royal Society's response to the upcoming Data Protection and Digital Information Bill

On 8 March 2023, the UK Government re-introduced a new version of the Bill, entitled Data Protection and Digital Information Bill (No.2).

Summary of key discussion points

- Losing adequacy with the EU would be damaging for scientific research in the UK, creating new costs and barriers for UK-EU research collaborations. This was acknowledged by all participants, with some considering this to be a likely risk should the UK diverge from GDPR in a manner which weakens data protections for EU citizens' data.
- Should adequacy be retained, there are concerns that this decision could be reversed in future due to legal challenges by EU citizens or as a result of the UK expanding data sharing agreements with countries with weaker data protection frameworks. The uncertainty that this would create could negatively affect the UK's research and innovation landscape.
- There is a need for better data protection guidance in the UK, especially with regards to existing scientific research exemptions. Some participants suggested that the lack of sufficient guidance has created a tendency towards overcompliance from universities and businesses.
- Improved, scenario-specific, guidance could be an alternative way to address issues with GDPR, without the uncertainty that new legislation may bring with regards to adequacy.

2. Information Commissioner's Office. The UK GDPR. See: <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr/> (accessed 11 April 2023).

3. European Commission. 2021 Data Protection: Commission adopts adequacy decisions for the UK. See: https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183 (accessed 11 April 2023).

Protecting adequacy with the EU

The consensus of participants was that guaranteeing and protecting adequacy with the European Union was a key priority. The UK Government also considers this to be a priority and has stated their commitment to ensuring existing data adequacy decisions can remain in place. However, some expressed concerns that the initial Bill presented enough divergence from GDPR to risk adequacy, as it reduced the rights of data subjects (eg by making subject access requests more difficult) and could therefore be considered as ‘anti-innovation’.

Participants also had concerns over so-called ‘Henry VIII clauses’ throughout the Bill, giving the Secretary of State discretionary power to amend the Act through secondary legislation with limited or no parliamentary scrutiny. These clauses were perceived a risk to adequacy as the EU could consider the legislation to be unstable, with some suggesting there were more than 30 such clauses in the Bill. These amendments could also be seen as threatening the independence of the data protection authority.

It was noted that adequacy also depends on the UK’s continued commitment to the European Convention on Human Rights. Although the UK is a signatory to Convention 108+ (relating to the protection of individuals with regards to the processing of personal data), some expressed concern that it not yet been ratified into UK law⁴. The European Commission encourages third party countries to adopt the Convention⁵ and participants therefore felt that the UK Government should consider its ratification as a matter of priority.

If the UK were to lose adequacy, participants said this would counteract the proposed aims of the Government’s reforms, which are to accelerate business development in the UK and promote economic growth. Although standard contractual agreements could be used in case of adequacy loss, it was raised that law firms were likely to advise investors against setting up business in countries which do not have adequacy in order to reduce the legal burden. While participants agreed that GDPR is imperfect, it was still generally considered to be the ‘gold standard’ for privacy legislation.

Some participants discussed a need for the UK to ‘unambiguously’ define its position between two conflicting international systems: on the one hand the Asia Pacific Economic Cooperation⁶, with their Cross-Border Privacy Rules (a voluntary self-certified system for which businesses are the ones accountable), and on the other hand, GDPR, a legal framework countries outside of the EU are adopting so as to gain adequacy.

It was considered likely that the UK could retain adequacy in the short-term, however there was debate over the medium to long-term risk. The risk emanates from the potential of the UK becoming a destination for ‘laundering’ data from the EU to countries without adequacy and with weaker data protections in place. Linked to this is the risk that EU citizens could legally challenge the adequacy decision on the basis of their data rights being diluted. This eventuality was considered to be highly likely by some participants in attendance.

The questions surrounding adequacy and the risk that any decision could be overturned present a potential climate of uncertainty in the UK. Should this occur, some companies and researchers may instead decide to base themselves in nearby EU countries (eg the Netherlands or the Republic of Ireland), in order to benefit from a more stable data protection regime.

4. Council of Europe. Chart of signatures and ratifications of Treaty 223. See: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223> (accessed 11 April 2023).

5. EUR-Lex. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Exchanging and Protecting Personal Data in a Globalised World See: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN> (accessed on 11 April 2023)

6. Asia-Pacific Economic Cooperation. What is the Cross-Border Privacy Rules System? See: <https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system> (accessed 11 April 2023).

Definition of scientific research

The initial version of the Data Protection and Digital Information Bill attempted to clarify the definition of scientific research given in GDPR and provide examples of what could be considered scientific research. Scientific research in GDPR is defined in Recital 159 as followed:

The processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes.

It was noted that this definition is broad and open to interpretation. Although the Government is seeking a definition similar to GDPR, a key concern raised was that any attempt to amend the definition of scientific research may lead to broader questions about what is scientific, as science is an evolving landscape and its methods change. The challenge for a clarification of scientific research would for it to be sufficiently encompassing whilst ensuring that it is not exploited by companies and individuals who do not follow ethical research practices.

The issue of data profiling on social media was mentioned, as the Cambridge Analytica scandal illustrated how data purportedly collected for scientific research could be reused for controversial purposes⁷.

Beyond the question of what scientific research is, the question of who can be considered a scientist was also raised. A broader definition which allows individuals and organisations to self-assess their work as scientific research could lead to questions related to the place of citizen science, data collection by non-scientists, and the challenges of private, closed commercial research. If applied loosely, without clear guidance, a broader scope for scientific research could lead to more scandals occurring and risk undermining public trust in data sharing for public benefit research.

Participants felt there was a need for clear guidance (with examples) related to the use and reuse of data collected for scientific research purposes.

Improving GDPR

One of the group discussions was focused on potential improvements to GDPR which could benefit the UK research and innovation landscape. Similar to the group discussion on the definition of scientific research, participants in this group also highlighted the need for a clearer definition as well as guidance on the legitimate interests bases for processing personal data⁸. It was considered particularly important for small and medium-sized enterprises who may be undertaking scientific research without articulating it as such.

Participants stressed the different approaches to risk on the part of data users. Universities, for example, have a lower capacity to absorb the risks, whereas large technology companies have greater legal power and monetary capacity to cover potential fines. This provides an advantage to large technology companies, as GDPR overcompliance and risk aversion can prevent smaller competitors from entering the market. However, some participants suggested that the problem of overcompliance could be addressed with better guidance.

Guidance was generally perceived as a better alternative to new legislation by participants who feared the UK would be moving away from European principles of rights-based data protection. They noted that for both EU GDPR and UK GDPR, the underlying principle is rights-based regulation which is unaffected by specific technologies. Concerns were raised that the direction in the UK appears to instead be shifting towards a US-style consumer rights approach.

7. The Guardian. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. See: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (accessed 11 April 2023).

8. Information Commissioner's Office. What is the 'legitimate interests' basis? See: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> (accessed 30 March 2023).

Some participants said that when conducting research on lessons that could be learnt from data use during the COVID-19 pandemic, the underlying problems that emerged were around the quality of data and interoperability, rather than GDPR. They also noted that public attitudes were in favour of greater data protections. This was exemplified during the pandemic by expert discourse on the COVID-19 contact-tracing app and the recommendation by the Ada Lovelace Institute⁹ for 'strict purpose, access and time limitations' as well as the public backlash to the General Practice Data for Planning and Research scheme¹⁰.

A similar theme arose in the Royal Society's public dialogue on data for emergencies and non-emergencies¹¹ with trust in data systems being dependent on 'clarity of purpose', 'transparency in data flows', and 'knowledge of who owns, controls and governs that data'.

Another factor raised by participants questioning the need for a new Bill was the economic cost of transitioning to a new data protection regime, particularly given the recency of the transition to GDPR (which came into effect in May 2018).

A potential benefit of reform, highlighted by some participants, was the opportunity to better embed the principle of explainability¹² for automated decision-making processes into legislation.

Overall, there was an agreement among participants in this group that while some aspects could be updated and legal requirements could be clarified, better guidance should be prioritised over new legislation.

Considerations for the new Data Protection and Digital Information Bill

The Data Protection and Digital Information Bill (No.2) published on 8 March 2023 does not appear to address some of the concerns that participants of the workshop had expressed. In particular, the concerns over a climate of uncertainty, arising from potential future challenges to the UK's adequacy status remain.

There are also concerns that the rights and safeguards of data subjects could be downgraded as a result of the changes proposed in the Bill (eg through lower thresholds for data protection impact assessments and new limitations on subject access requests). This will require careful consideration as a strong, independent, data protection regime is key for fostering trust in data sharing, particularly for scientific research purposes where data can often be highly sensitive^{13,14}.

There will continue to be a need for clearer guidance following the Bill's passage, not least because individuals and organisations may need to abide by two different data protection regimes if they want to maintain operations with EU entities and meet any new UK data protection requirements.

Finally, it was noted that this new Bill should be an opportunity to account for the new systems of data governance enabled by emerging technologies such as privacy enhancing technologies (PETs). An example of where this may become challenging are when PETs obscure the role of controller. To this end, an international sandbox environment for testing PETs solutions could inform up-to-date, scenario-specific guidance for using PETs in cross-border collaboration¹⁵.

9. Ada Lovelace Institute. 2020 Exit through the App Store? A rapid evidence review of the technical considerations and societal implications of using technology to transition from the COVID-19 crisis. See: <https://www.adalovelaceinstitute.org/evidence-review/covid-19-rapid-evidence-review-exit-through-the-app-store/> (accessed 11 April 2023).

10. NHS data grab on hold as millions opt out. The Observer. 22 August 2021. See: <https://www.theguardian.com/society/2021/aug/22/nhs-data-grab-on-hold-as-millions-opt-out> (accessed 11 April 2023).

11. The Royal Society. 2023 Creating resilient and trusted data systems. See: <https://royalsociety.org/topics-policy/projects/data-for-emergencies/> (accessed 11 April 2023).

12. The Royal Society. 2019 Explainable AI: the basics. See: <https://royalsociety.org/topics-policy/projects/explainable-ai/> (accessed 11 April 2023).

13. The Royal Society. 2023 Creating resilient and trusted data systems. See: <https://royalsociety.org/topics-policy/projects/data-for-emergencies/> (accessed 11 April 2023).

14. The British Academy and The Royal Society. 2017 Data management and use: Governance in the 21st century. See: <https://royalsociety.org/topics-policy/projects/data-governance/> (accessed 11 April 2023).

15. The Royal Society. 2023 report: From Privacy to partnership. See <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf> (accessed 11 April 2023)

Annex

The Royal Society would like to thank the following workshop participants who have contributed to the development of this note.

Workshop participants included:	Royal Society staff
Abigail Burke, Open Rights Group	Eva Blum-Dumontet, Senior Policy Adviser, Data
Rachel Coldicutt, Careful Industries	Areeq Chowdhury, Head of Policy, Data
Professor Jon Crowcroft FRS, University of Cambridge	Nicole Mwananshiku, Project Coordinator, Data
Dani Dhiman, techUK	
Alexandra Ebert, MOSTLY AI	
Anna Fielder, EDRi	
Gavin Freeguard, Connected by Data and Open Data Institute	
Tom Harrison, Wellcome Trust	
Ed Humpherson, Office for Statistics Regulation	
Carly Kind, Ada Lovelace Institute	
Konrad Kollnig, University of Oxford	
Alex Lawrence-Archer, AWO	
Professor Carsten Maple, University of Warwick	
Dr Lukasz Olejnik, independent cybersecurity and privacy researcher and consultant	
Jen Persson, Defend Digital Me	
Lori Roussey, Oxfam GB, Oxfam International, and Data Rights	
Professor Rossitza Setchi, Cardiff University	
Sam Smith, MedConfidential	
Pete Stokes, Bennett Institute for Applied Data Science, University of Oxford	

© The Royal Society. Issued: April 2023 DES8497

The text of this work is licensed under the terms of the Creative Commons Attribution License which permits unrestricted use, provided the original author and source are credited. The license is available at: creativecommons.org/licenses/by/4.0