COSMOS
Navigate the Compliance Universe

Compliance Today - September 2023

**Leslie M. Howes** (lhowes@hsph.harvard.edu, linkedin.com/in/leslie-howes/) is Director, Office of Regulatory Affairs and Research Compliance, at Harvard T.H. Chan School of Public Health, Boston, MA.

**Emmelyn Kim** (ekim@northwell.edu, linkedin.com/in/emmelynkim/) is Vice President, Research Compliance & Privacy Officer, at The Feinstein Institutes for Medical Research, Northwell Health, Lake Success, NY.

**Julie K. Moore** (julie.moore@advarra.com, linkedin.com/in/julie-moore-j-d-m-s-pa-cip-93683353/) is Managing Director, at Advarra Consulting, Columbia, MD.

# Navigating GDPR and other international data privacy regulations in research

by Leslie M. Howes, MPH, CIP; Emmelyn Kim, MA, MPH, MJ, CHRC; and Julie K. Moore, JD, MS, PA, CIP

The landscape of international data privacy regulations has changed markedly in the past decade and is still evolving. The European Union's (EU) General Data Protection Regulation (GDPR), implemented in 2018, ushered in a new era of more robust, restrictive privacy regulations. The United Nations Conference on Trade and Development estimates that 71% of countries currently have data privacy laws in effect, while an additional 9% have draft legislation pending.[1] As clinical research becomes increasingly global, resulting in more cross-border transfers of data and biospecimens, organizations engaged in research should understand the risks associated with conducting international research and have policies, procedures, and processes in place to ensure compliance with international data privacy regulations.

## Applicability of the GDPR

Many international data privacy regulations are modeled after the GDPR, so understanding the GDPR's terminology and applicability provides a foundation for analyzing similar legislation implemented in other countries. The GDPR establishes broad protection of personal data of individuals in the European Economic Area (EEA); importantly, the GDPR can impact clinical research being conducted by US-based organizations if the research involves personal data of individuals located in the EU, regardless of individuals' citizenship.[2] The GDPR regulates the processing of personal data and defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')"[3] and "processing" as any operation performed on personal data. It's vital to note that the GDPR applies to pseudonymized data (i.e., data that can no longer be attributed to a specific data subject without the use of additional information, such as a code). Thus, the GDPR applies even when personal data has been stripped of identifiers and coded.

The GDPR provides additional protections for certain categories of personal data called "special categories," which include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union

membership, and the processing of genetic data, biometric data uniquely identifying a natural person, and data concerning health or a natural person's sex life or sexual orientation. Unless an enumerated exception applies, the GDPR expressly prohibits the processing of special categories of personal data.[4]

## GDPR analysis: Territorial scope

The first step in analyzing whether the GDPR applies is to consider the law's territorial scope or jurisdiction. One of the most impactful aspects of the GDPR is its broad applicability to organizations outside of the EU. The regulation applies to organizations located outside the EU in three situations. First, if a data controller or processor is "established" in the EU, they are likely subject to the GDPR.[5] Although established is not defined in the articles of the regulation, Recital 22 provides some insight, stating that "establishment implies the effective and real exercise of activity through stable arrangements."[6]

The regulation can also apply to an organization outside the EU when a controller or processor offers goods or services to data subjects in the EU.[7] The test for determining whether an entity is offering goods or services to data subjects in the EU is whether it's "apparent that the entity envisages" offering such goods or services.[8] Here again, the Recitals provide some insight into how to interpret and apply this test. The mere fact that a controller's or processor's website is available to EU data subjects is not sufficient to demonstrate intent to offer goods or services to data subjects; however, if the website provides data subjects the option of ordering goods or services in an EU member state language, or mentions other "customers or users" within the EU, that may demonstrate that the controller or processor envisages offering goods or services to data subjects in the EU.[9]

The third scenario in which an organization located outside the EU may become subject to the GDPR is when it monitors the behavior of data subjects in the EU.[10] The regulation specifies that the test for determining whether data processing activities include monitoring the behavior of data subjects within the EU is if "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person," particularly when such activities are undertaken to analyze or predict personal preferences, behaviors, or attitudes.[11]

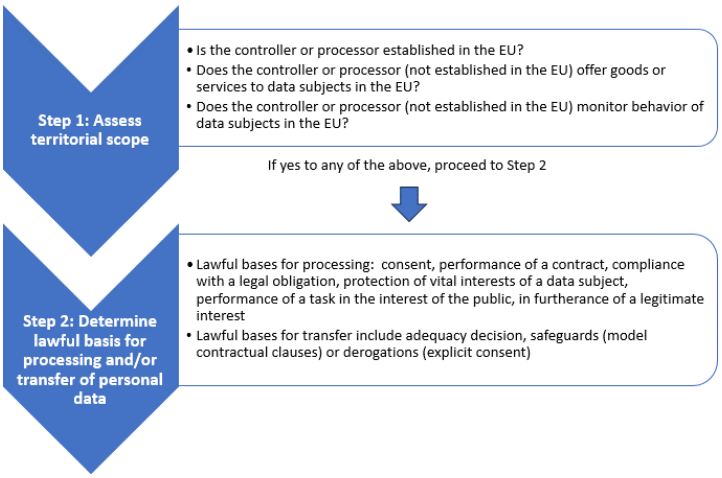
## GDPR analysis: Lawful basis for processing and transfer

Once it's been determined that the GDPR applies, the second step in the analysis is to determine whether there is a lawful basis for processing and transferring personal data. The regulation clearly states that processing is only allowable if at least one of six enumerated bases applies: consent, performance of a contract, compliance with a legal obligation, protecting the vital interests of a data subject, performing a task in the interest of the public, or furtherance of a legitimate interest.[12]

The European Data Protection Board (EDPB) has provided some insight into the legal bases for processing personal data in the context of clinical trials. In its January 2019 opinion, the EDPB specified that processing personal data from a clinical trial can generally be split into two types: the protection of health and conducting research activities—each with its own legal basis.[13] The EDPB opinion states that processing clinical trial data for the protection of health (e.g., to ensure reliability and safety) is a legal obligation; thus, the basis for processing is compliance with the legal obligation.[14] By contrast, processing data for the purpose of conducting research activities is not a legal obligation; as such, it requires a different basis for processing. Per the EDPB, the lawful basis for conducting research activities may be the data subject's explicit consent, a task carried out in the public interest, or in furtherance of a legitimate interest, based on the facts and the circumstances of the particular clinical trial.[15]

The regulation also enumerates several legitimate bases for transferring personal data to third-party countries. First, the transfer of personal data outside the EU is allowed if the EU Commission has determined that the recipient country ensures an adequate level of protection.[16] The effect of such an "adequacy decision" is that personal data can flow from the EU to the third country without any additional protections. If personal data is to be transferred to a third country for which the EU Commission has not made an adequacy decision, another basis of transfer must be identified to ensure appropriate safeguards are in place to protect the data.[17] Secondly, transfer of personal data can be legitimate if the data subject has provided explicit consent.[18] Finally, the transfer can be legitimate if completed pursuant to model contractual clauses, which are preapproved by the EU Commission.[19]

Figure 1: GDPR Analysis Steps




## China's Personal Information Protection Law

In the wake of the GDPR, China adopted the Personal Information Protection Law (PIPL) in 2021. The PIPL regulates the processing of "personal information," defined as any kind of information related to identified or identifiable natural persons, not including anonymized information.[20] The PIPL has many similarities to the GDPR, including that it regulates the processing of personal information within China but can also apply to organizations outside of China. Specifically, an organization outside of China may be subject to the PIPL when the purpose of an activity is to provide products or services to natural persons inside China's borders or to analyze or assess activities of persons within China's borders.

Like the GDPR, once a determination has been made that your organization is subject to the jurisdiction of the regulation, the PIPL requires an analysis to determine whether there is a lawful basis for the processing or transfer of personal information. There are seven lawful bases for processing personal information under the PIPL: consent, contractual obligations, statutory obligations, public health emergency or to protect natural persons' life and health, news reporting and other activities in the public interest, personal information already disclosed by persons themselves or otherwise lawfully, and where otherwise permitted by laws and regulations.[21]

The PIPL provides three bases for transferring personal information outside China's borders. Similar to the GDPR, the PIPL allows transfer based on "pre-approval" if the transferor has applied for and passed a security

assessment by the Cyberspace Administration of China or has obtained Personal Information Protection Certification from an authorized data security assessment organization or authority.[22] There are also standard contractual clauses that may be used to facilitate cross-border transfer of personal information; however, it is notable that these clauses can only be used by processors that meet certain requirements, including that the transferor has not transferred sensitive personal information of more than 10,000 data subjects (in aggregate) since January 1 of the preceding year.[23]

## Organizational processes and business decisions

### Organizational checkpoints

Whether your organization is primarily US-based or has an international presence, it is imperative to assess how international regulations may impact your research through existing or future global engagements. This will largely depend on your research portfolio, researcher community, and international academic programs and collaborations. Privacy and data protection requirements may need to be evaluated and incorporated into work streams. Keep in mind that global business activities, international exchanges, and remote work may have expanded over time and can impact the human resources (HR) or employment space in the research environment. Global data repositories and collaborative data-sharing systems are also more likely to occur in research and academic environments. Data protection requirements may need to be more closely evaluated as part of contracts and agreements. Finally, institutional review board (IRB) and international ethics review committee requirements and approvals need to be considered for research occurring in international settings. Having organizational checkpoints and a framework to assess risks will be essential.

Consider the following actions:

- Identify global activities and touchpoints occurring at your organization through surveys and assessments.
- Perform a gap analysis to ensure processes are working at checkpoints where additional review against international privacy and data protection laws may be required.
- Develop organization-wide policies and procedures to promote awareness, standardize processes, set expectations, and provide contact information for compliance and other stakeholder offices involved in further review.
- Monitor and audit for compliance and assess risks.
- Review and evaluate results with a larger group (such as an international privacy or data protection committee) comprised of stakeholders across the organization.
- Continually monitor new international privacy laws to determine applicability to the research community, implement necessary changes, and provide education.

### Coordination with stakeholders

An organization should identify and consider the applicable compliance groups and stakeholders impacted by the GDPR as it builds an infrastructure to support research affected by the regulation. For example, careful coordination with the IRB will be necessary as international data privacy laws can impact the IRB's decisions. Consider that under the GDPR, waivers of consent and/or consent documentation for prospective studies are not allowed—even if the IRB finds that the human research is exempt. Additionally, an organization's contracts

group is likely responsible for ensuring that the GDPR's contractual clauses are included as applicable. Your organization's stakeholders include the human research protection program, IRB, compliance, negotiating offices such as contracts or legal affairs, IT security, research administration, technology transfer/development, HR, and others. Some of these groups may be gatekeepers or main points of contact.

## Ensuring proper triage

Ensuring an organization establishes a proper mechanism for triaging research activities under international privacy laws is necessary. Such a mechanism requires the oversight group or body to have a sufficiently large scope (see Figure 2). For example, relying primarily on an IRB to identify research that may be subject to international privacy laws is likely to be insufficient. Consider the IRB's scope of review, which is limited to the regulatory definitions of research with human subjects. As a result, it's possible that an international data privacy law like the GDPR could apply in the absence of any requirement for IRB review and approval. We know this to be the case given the previous discussion of "pseudonymized data." Specifically, under the GDPR, such use may not meet the regulatory definitions of research with human subjects; however, this type of data is still considered "personal data" under the GDPR even in the absence of a crosswalk or coding system that links data to individual participants.[24] GDPR may also apply in circumstances where the organization provides services as a processor on behalf of a controller but is not considered engaged in human subjects research. Certain GDPR obligations may subsequently appear in contracts or agreements that the appropriate offices should evaluate. Proper triage is also essential when considering research with "special categories" under the GDPR.

Figure 2: An example of an organizational workflow relying on a group with broad compliance scope for GDPR/international data privacy regulations triage


## Implementing security measures

Another business decision worth exploring is the security measures required for personal data processing activities to ensure appropriate technical and organizational controls. For example, end-to-end encryption, multifactor authentication, and role-based access controls. Specifically, an organization may find it appropriate to require that an investigator provide an attestation that such measures are in place. Alternatively, an organization might instead rely on an independent third party for this verification. For instance, an organization's internal information security group might fulfill this role. While there are advantages and disadvantages related to each option, either could be appropriate for an organization. And the decision will likely be informed by an organization's current compliance culture and expectations.

## Offering goods or services

As previously described, the GDPR governs data controllers and processors established outside the EU if they either (1) offer goods or services to individuals in the EU (regardless of whether payment is required); or (2) monitor individuals' behavior there. A business "offers goods or services" to individuals in the EU if it "envisages" offering goods or services in the EU.[25] This is a facts and circumstances test. Further, this is an important business decision for an organization to consider specifically to analyze whether it is "offering goods or services" and/or "monitoring individuals' behavior." As part of its analysis, an organization may wish to engage its legal department and, more broadly, consider the resources and infrastructure such a decision may warrant.

## Remain flexible to evolving landscape

To date, many organizations have focused their attention on meeting GDPR requirements. As additional international data privacy laws continue to come into the regulatory landscape, organizations now need to pivot to address this growing body of rules. For instance, if an organization developed policies and procedures specific to the GDPR, they likely now need to revisit these resources to accommodate the broader regulatory and still evolving landscape. Instead of creating a particular policy and/or resources for each international data privacy law, another approach may be to have a single policy that sets forth the strictest standard yet retains the ability for flexibility depending on the specific applicable regulation.

## Conclusion

An organization should be cognizant of how international privacy laws, including GDPR and PIPL, apply to its operations to best anticipate critical implementation considerations. To that end, there are some business decisions, policies, and processes an organization will need to consider, including identifying its stakeholders, implementing checkpoints, and establishing proper triage. Other considerations, such as implementing security controls and resources needed to support research activities that require compliance with GDPR obligations, are essential. Organizations must remain flexible while continuing to monitor business activities against regulatory changes. Fortunately, GDPR has established a global data privacy framework that organizations may consider when responding to the broader international data privacy landscape.

*The views expressed in this article are the authors' own and do not necessarily reflect the views of their organizations.*

## Takeaways

- Describe how data privacy laws have shifted globally and have become more relevant in the research environment.
- Analyze how the General Data Protection Regulation (GDPR) may apply to proposed research activities.
- Develop checkpoints and a framework for evaluating international activity essential to assessing privacy and data protection risk.
- Evaluate how GDPR and other international data privacy laws apply to organizational operations to anticipate implementation and security considerations.
- Coordinate with key organizational stakeholders that have different roles and responsibilities.

**1** United Nations Conference on Trade and Development, "Data Protection and Privacy Legislation Worldwide,"

accessed May 11, 2023, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
2 Note that because the United Kingdom left the European Union in 2021, it is not directly regulated under the European General Data Protection Regulation. However, pursuant to the European Union (Withdrawal) Act of 2018, the European General Data Protection Regulation was adopted as UK domestic law.
3 Regulation (EU) 2016/679 of the European Parliament and of the Council, "On the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation)," April 27, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.
4 General Data Protection Regulation, Article 9, https://gdpr.eu/tag/gdpr/.
5 General Data Protection Regulation, Article 3.
6 General Data Protection Regulation, Recital 22, https://gdpr.eu/recital-22-processing-by-an-establishment/,
7 General Data Protection Regulation, Article 3.
8 General Data Protection Regulation, Recital 23.
9 General Data Protection Regulation, Recital 23.
10 General Data Protection Regulation, Article 3.
11 General Data Protection Regulation, Recital 24.
12 General Data Protection Regulation, Article 6.
13 European Data Protection Board, "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 January 23, 2019,
https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf.
14 European Data Protection Board, 4.
15 European Data Protection Board, 5.
16 General Data Protection Regulation, Article 45.
17 General Data Protection Regulation, Article 46.
18 General Data Protection Regulation, Article 49.
19 General Data Protection Regulation, Article 46.
20 Rogier Creemers and Graham Webster, "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021," Digichina (Stanford University), last revision September 7, 2021,
https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.
21 Personal Information Protection Law of the People's Republic of China, Article 13, accessed June 27, 2023,
http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.
22 Personal Information Protection Law of the People's Republic of China, Article 38.
23 Barbara Li, "A look at what's in China's new SCCs," International Association of Privacy Professionals, February 23, 2023, https://iapp.org/news/a/a-look-at-whats-in-chinas-new-sccs/.
24 45 C.F.R. § 46.102 , https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/revised-common-rule-regulatory-text/index.html#46.102.
25 General Data Protection Regulation, Recital 23.