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

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

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]

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.