US imposes restrictions on certain transactions involving sensitive personal data

'Countries of concern' include China (and Hong Kong) Russia, Iran and Venezuela.

By **Nicholas Shepherd**, **Ingrid Price**, **Libbie Canter**, and **Jonathan Wakely** of Covington.

On January 8, 2025, the US Department of Justice (DOJ) issued a Final Rule[1] to implement Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the EO).[2] The Final Rule categorically prohibits or restricts US persons from engaging in certain transactions that would result in access by countries of concern or covered persons to bulk US sensitive personal data and government-related data, and is reflective of the US government's broader efforts to strategically decouple from China. The Final Rule will have broad implications for US companies across a range of sectors, as it relates to both internal operations and third-party transactions. The Final Rule largely takes effect on April 8, 2025, with certain compliance requirements entering into force on October 6, 2025.

To be clear, the Final Rule is a national security law at its core, intended to protect US national security interests – it is not a privacy law designed to ensure privacy or safeguard individual rights. That said, the Final Rule does impose prohibitions and restrictions on the transfer of, or access to, certain data originating in the US in a way that is comparable in some respects to cross-border transfer restrictions under other regimes' privacy laws. Accordingly, there are obligations in the Final Rule for which covered organizations can likely leverage aspects of their existing data privacy and security compliance programs to address. Notably, US companies should bear in mind that violations of the Final Rule are punishable by both civil and criminal penalties, up to and including potential imprisonment for major violations.

In this article, we provide an overview of key aspects of the Final Rule, explain their relevance to data privacy and security compliance programs, and identify some potential next steps for organizations to consider in order to address compliance requirements under the Final Rule.

Overview of key terms and requirements

The Final Rule prohibits or restricts US persons (e.g. US entities) from engaging in certain "covered data transactions." Here, a "transaction" refers to "any access by a country of concern or covered person to any government-related data or bulk US sensitive personal data" which involves (1) data brokerage; (2) vendor agreements; (3) employment agreements; or (4) investment agreements. Notably, "access" is defined broadly to include not just actual access to the relevant data, but also captures, for example, the "ability to" read, obtain, or otherwise receive such data. Under the Final Rule, certain covered data transactions are outright prohibited (unless DOJ gives a special authorization), including any data brokerage transaction, any transaction involving bulk human 'omic data, and any transaction designed for purposes of avoiding application of the Final Rule. By contrast, certain investment, employment, and vendor agreements will be restricted, meaning such transactions may be lawfully carried out if the security requirements issued by the Cybersecurity and Infrastructure Security Agency ("CISA") and other requirements for restricted transactions in the Final Rule are implemented.

Six categories of US "sensitive personal data" are regulated if such data meets the corresponding bulk thresholds in the Final Rule. These categories include US covered personal identifiers, precise geolocation data, biometric identifiers, "human 'omic" data (i.e., human genomic data, as well as human epigenomic/ proteomic/ transcriptomic data), personal health data, personal financial data.[3] The volume-based thresholds that define the concept of "bulk" vary based on the type of sensitive personal data. (For example, a transaction involving access by a covered person to precise geolocation data relating to over 1,000 US persons or devices would meet the bulk threshold, whereas a transaction involving access to personal health data would be covered if access involved data of over 10,000 US persons).

"Countries of concern" include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. Further, a "covered person" is defined very broadly to include any of the following:

- a non-US entity which is 50 percent or more owned, directly or indirectly, *individually or in the aggregate*, by one or more countries of concern, or by another covered person (entity or individual) as defined below;
- a non-US entity which is organized or chartered under the laws of, or has its principal place of business in, a country of concern;
- a non US individual who is primarily resident in the territorial jurisdiction of a country of concern;
- a non-US individual who is an employee or contractor of a country of concern or of any of the entities listed above;
- a non-US person (entity or individual), wherever located, that is designated as a covered person by the US Attorney General; or

- a non-US entity which is 50 percent or more owned, directly or indirectly, individually or in the aggregate, by one or more of the persons (entity or individual) set out in any the bullet points above.

Consequently, the Final Rule's definition of covered person extends not only to, for example, Chinese subsidiaries of non-Chinese companies, but also to any entity that is 50 percent or more owned by a Chinese party, any foreign person who is an employee of such entity, or any foreign person who is primarily resident in China. Further, the Final Rule clarifies that at least two levels of ownership must be reviewed to determine if an entity is a covered person. For instance, if a covered person owns 50 percent of Entity A, and Entity A in turn owns 50 percent of Entity B, Entity B would be considered a covered person. Moreover, the Final Rule makes clear that foreign ownership can also be satisfied in the aggregate. Thus, if in the previous example, Entity A only owns 40 percent of Entity B, but Entity C, which is also a covered person, owns 10 percent of Entity B, the total covered person ownership would be 50 percent, satisfying the Final Rule's definition of covered person.

While the Final Rule is significantly broad in scope, it also contains certain exemptions, including for: personal communications; information or informational materials; travel; official business of the US government; transactions "ordinarily incident to and part of the provision of financial services" (which is somewhat broad in scope, including e-commerce transactions); corporate group transactions; transactions required or authorized by US federal law or international agreements or necessary to comply with US federal law; investment agreements subject to an action by the Committee on Foreign Investment in the United States (CFIUS); transactions "ordinarily incident to and part of the provision of telecommunications services"; "drug, biological product, and medical device authorizations"; and "other clinical investigations and post-market surveillance data[4]."

Given the significant breadth of the Final Rule, it will be important for organizations to evaluate how best to implement and scale compliance. To that end, we offer the following high-level steps to consider in connection with developing remediation work-plans.

Step 1: Understand the scope and impact on your operations

As a first step, US companies – regardless of industry – will need to evaluate their affiliates, partners, vendors, employees, potential investors, and commercial counterparties, and their corresponding data sharing with those parties, to determine whether the Company engages in any covered data transactions. To carry out this assessment, many companies may be able to leverage their existing data governance strategies to address privacy and security requirements under laws like the EU General Data Protection Regulation (GDPR) and/or the comprehensive state privacy laws emerging across the US.

However, existing personal data inventories may not be sufficient in certain respects. In particular, it is important to bear in mind that:

1. "Sensitive personal data" that has been de-identified, anonymized, encrypted, or pseudonymized will also be caught by the Final Rule, subject to a few narrow exceptions. Accordingly, to the extent US companies have focused on any existing data mapping efforts on inventorying *identifiable* personal data, they may need to take a more fulsome view of data sets to determine if they contain de-identified, anonymized, pseudonymized or encrypted data that was "sensitive personal data" at collection.
2. As noted above, the term "access" to sensitive personal data is broadly defined to include "logical *or* physical access, including *the ability* to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud computing platforms, networks, security systems, equipment, or software." This means companies will need to consider not only the sensitive personal data that internal or external parties actually access, but also identify which individuals *could* access such data based on other factors, such as their access privileges, other rights or accounts they could use, or their authority / seniority within the organization.
3. Any existing data mapping will not address whether employees, vendors, and others with access to sensitive personal data are "covered persons" under the Final Rule, which is a concept more akin to blocked parties found in export control laws and cross-border sanctions regimes. Thus, privacy and data security professionals may need to coordinate with counterparties who regularly work on these other topics (e.g. in Risk and/or Compliance functions), and leverage tools used by those colleagues, to fully examine this point in depth.

Each of these variables holds new challenges, and will require privacy and security professionals to adapt and effectively communicate across a range of functions.

Step 2: Identify any prohibited data broker transactions or restricted transactions

Prohibited Data Transactions: Even companies that do not operate as traditional data brokers may engage in "data brokerage transactions," because of how broadly the Final Rule defines data brokerage. Some striking examples of a data brokerage in the Final Rule include the automated collection and transmission of data to a country of concern or covered person via third-party cookies, pixels, and software development kits (SDKs), including where this involves:

1. provision of data by a website or mobile app operator to a social media app via the knowing installation or approval of tracking pixels or software development kits into the website or mobile app;
2. provision of data by an online publisher to an advertising exchange;
3. provision of data by an advertising exchange to advertisers; and
4. provision of data to an affiliated company to help develop artificial intelligence technology and machine learning capabilities.

The Final Rule also imposes certain requirements on any data brokerage transaction involving a foreign person, regardless of whether the foreign

person is a "covered person." Specifically, if a US company sells, licenses, or engages in a similar commercial arrangement with a foreign person that is not a covered person, the US company is required to secure contractual commitments that the foreign person will not engage in an onward transfer of such data to a covered person and report any known or suspected violations of this obligation. Absent such contractual commitments, the transaction is a prohibited data brokerage under the Final Rule.

Restricted Transactions: Restricted transactions are any covered data transactions involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person (except those involving human 'omic data, which are also prohibited outright). Again, such restricted transactions will be prohibited *unless* the US person party to the transaction adopts detailed security requirements specified by the Cybersecurity & Infrastructure Security Agency (CISA) in a separate rulemaking, implements a written program to support compliance with these requirements, and conducts annual audits of the program.[5]

CISA's security requirements include numerous organizational-, system-, and data-level measures, some of which are adapted from the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST Privacy Framework, and CISA's Cross-Sector Cybersecurity Performance Goals. Importantly, the data-level security requirements contemplate significant limitations on covered persons' access to covered data in any form that is "linkable, identifiable, unencrypted, or decryptable using commonly available technology," which might require significant changes in day-to-day operations involving these transactions, or could effectively prohibit certain transactions altogether.

Step 3: Remediation and implementation of new processes

Once any prohibited transactions or restricted transactions have been identified, US companies will need to evaluate whether any exemptions apply or remedial action is necessary to ensure compliance with the Final Rule. For prohibited data brokerage transactions, this may include steps such as removing any pixels, SDKs, or similar technologies from company websites or mobile apps that are associated with covered persons or countries of concern. For restricted transactions, this may include either implementing the requisite Security Requirements and compliance obligations, or if not possible, limiting data access or sharing with covered persons.

The EO and Final Rule will also require US companies to consider implementing new due diligence processes going forward, such as:

1. operationalizing a new screening process for employees, vendors, and other parties, to identify any nexus with countries of concern or covered persons that might result in a covered data transaction;
2. updating template agreements with vendors to include representations/warranties that they are not covered persons or in countries of concern, and in the context of data brokerage, prohibit onward transfers to covered persons or countries of concerns (and to reporting the same if identified);
3. updating any intra-company data transfer agreements to clarify that US-originating sensitive data should not be transferred or made accessible to covered persons or countries of concern under the regulations, unless subject to an exemption under the Final Rule; and
4. implementing a documented data compliance plan, which may include establishing policies, Standard Operating Procedures, and other documentation laying out these new due diligence processes, and ensuring whistleblower channels are in place to report any non-compliance.

In sum, the EO and Final Rule set out a unique hybrid of obligations on US companies that will require privacy and data security professionals to leverage and adapt existing data governance resources. While this may require significant time and effort up front, over time these efforts should pay off in the form of efficiencies and streamlined processes.

AUTHORS

Nicholas Shepherd is an Associate, Ingrid Price is a Special Counsel, Libbie Canter is a Partner, and Jonathan Wakely is a Partner at Covington & Burling LLP.
Emails: nshepherd@cov.com
iprice@cov.com
ecanter@cov.com
jwakely@cov.com

REFERENCES

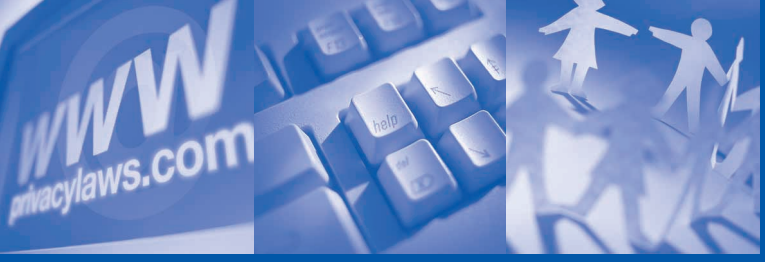
1 See 28 CFR Part 202, "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons." U.S. Dept. of Justice, 27 December 2024. Available at: www.justice.gov/nsd/media/1382521/dl [last accessed 2 February 2025].

2 U.S. Federal Register, Executive Order 14117 of February 28, 2024 ("Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern"). Available at: www.govinfo.gov/content/pkg/FR-2024-03-01/pdf/2024-04573.pdf [last accessed 24 February 2025].

3 While this article focuses on "sensitive personal data," the Final Rule also regulates "government-related data," which is defined to include (among others) "[a]ny sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the [U.S. government], including the military and Intelligence Community." This includes precise geolocation data relating to 736 different latitude/longitude coordinates listed in the Final Rule. So, for example, if a company collects precise geolocation from the device of a U.S. servicemember or contractor who enters a military base, such a scenario may be covered by the Final Rule.

4 Refers to the process of monitoring the safety and performance of medical devices after they have been released to the market.

5 See "Security Requirements for Restricted Transactions." CISA, 3 January 2025. Available at: www.cisa.gov/resources-tools/resources/EO-14117-security-requirements [last accessed 24 February 2025].



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Global data privacy laws 2025: 172 countries, 12 new in 2023/24

Law revisions overtake new laws in importance.

By **Graham Greenleaf**, Honorary Professor, Macquarie University.

This biennial global assessment is the ninth in this publication since 2011. Each assessment has been accompanied by detailed tables listing key features of all the laws assessed (see Eighth Edition, 2023)[1]. The Ninth Edition of the Tables will accompany the next issue.

This is the first assessment to conclude that revisions to existing data privacy laws are now more important than enactment of new laws in countries without such laws. This review is comprehensive in that it covers, for 2023-24: (i) new countries with data privacy laws; (ii) laws

Continued on p.3

The next chapter on the legal requirements for profiling

A balance must be struck between the right of access to personal data and trade secrets in automated decision-making processes. By **Katharina A. Weimer** of Fieldfisher.

Another Court of Justice of the European Union (CJEU) decision on the fine print of handling automated decision-making in credit scoring was handed down recently (C-203/22)[1]. This case originated from Austria and involved an individual person (CK) proceeding against the Magistrat der Stadt Wien (City Council of Vienna – City Council), with further involvement of Dun & Bradstreet Austria.

Continued on p.10

Issue 194 **APRIL 2025**

COMMENT

2 - A different world – also for data protection

NEWS

13 - TikTok moves to enhance data security for its European users

17 - Australia continues to push forward on online safety policy

ANALYSIS

1 - The next chapter on the legal requirements for profiling

25 - Biometrics at the crossroads of the AI Act and the GDPR

LEGISLATION

1 - Global data privacy laws 2025

MANAGEMENT

14 - US imposes restrictions on certain transactions involving sensitive personal data

20 - Ireland's DP Commissioner Dr Des Hogan: We expect more from large tech companies

23 - The EU AI Act's disclosure requirements and legal privilege

27 - Events Diary

NEWS IN BRIEF

12 - Meta settles in UK; ICO says targeted advertising is direct marketing

12 - EU Commission withdraws e-Privacy regulation

12 - Dubai consults on law amendments

19 - Finland's DPA probes health data transfers to China

19 - Italy, South Korea ban DeepSeek

24 - EU delays the review of UK adequacy decisions by six months

INTERNATIONAL report

ISSUE NO 194 APRIL 2025

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
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Graham Greenleaf
Honorary Professor, Macquarie University, Australia

Katharina A. Weimer
Fieldfisher, Germany

Nicholas Shepherd, Ingrid Price, Libbie Canter and Jonathan Wakely
Covington, US

Lizzie O'Shea
Principal Lawyer and Civil Society Advocate, Australia

Frank Madden
IBM, UK

Richard Lawne
Fieldfisher, US

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

A different world – also for data protection

Since US President Donald Trump made changes to the Privacy and Civil Liberties Oversight Board by dismissing the Democrat members, the future of the agreement is in question. The Board is a key part of the EU-US Data Privacy Framework ensuring seamless data transfers.

Michael McGrath, EU Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection has said that the EU is monitoring US developments and any possible complications that may arise for the data transfer deal. No-one wants a new challenge in the Court of Justice of the EU, and the deal benefits businesses on both sides of the Atlantic.

US Vice-President JD Vance has expressed dislike for the EU GDPR and the Digital Services Act. While the EU has been declaring for years that it is not re-opening the GDPR, it may now be considering a stripped-down framework for small and medium sized organisations. The EU is, on the whole, committed to a simplification agenda and better implementation of EU rules to make business easier in Europe.

The situation is different for the UK, now out of the EU but with its own UK-US adequacy arrangement, based on the EU one. A considerable weight rests on these trade deal negotiations with the US. But the UK also has to ensure that it retains its own EU adequacy by the end of 2025 (p.24).

Elsewhere in the world new data protection laws are emerging, often influenced by the GDPR. There are now 172 jurisdictions globally with a data law (p.1).

In Europe, new GDPR interpretations are developing, for example on automated decision-making, profiling and the right of access (p.1). Apart from court decisions, DPAs' opinions from the European Data Protection Board (EDPB) are shaping the landscape. Ireland's DPA is a major player due to the presence of many big tech companies in the country. For example, it initiated the process for obtaining an EDPB Opinion on AI models late last year. Read on p.20 about Ireland's role as an enforcer and influencer.

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 in advance of the free-place deadline. Excludes the Annual Conference. More than one place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> *PL&B* is a reliably useful resource, prompting intelligent questions and offering insightful analysis on many of the data protection and privacy issues that are of interest to us and, more importantly, to our clients.
>
> **Alan Baker, Partner, Farrer & Co.**

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.