# Response by the Centre for Information Policy Leadership to U.S. Department of Justice Advance Notice of Proposed Rulemaking on *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*

Submitted April 19, 2024

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the U.S. Department of Justice (DoJ) Advance Notice of Proposed Rulemaking on *Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern* ("the ANPRM").

CIPL commends DoJ for the commitment expressed in the ANPRM to "Data Free Flow with Trust" and for emphasizing that the proposed rule is not intended to be a generalized data-localization requirement. CIPL has published research on the importance of cross-border data flows for securing a wide range of economic and social benefits.[2] Any measures to address national security concerns associated with international transfers of Americans' personal data should be carefully designed to address the concerns without placing the broader benefits from data flows at risk.

CIPL recommends that DoJ provide greater clarity around several concepts addressed in the ANPRM, especially those oriented toward ensuring the ability to continue normal business operations of multinational organizations, and the ability to fulfil regulatory requirements in areas such as financial services, pharmaceuticals, and technology. We have included our suggestions in response to specific questions below.

**Responses to Specific Questions**

*Section B. Bulk U.S. Sensitive Personal Data*

1. In what ways, if any should the Department of Justice elaborate or amend the definition of *bulk U.S. sensitive personal data? If the definition should be elaborated or amended, why?*

   CIPL commends DoJ for stating that the bulk thresholds "would be set based on a risk-based assessment" that accounts for the context of specific, proposed transactions. However, setting

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective data protection and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] CIPL, "The Real Life Harms of Data Localization Policies," March 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf.

thresholds in the rigid manner proposed by the table in Section B is inconsistent with a context-specific, risk-based approach. We recommend DoJ clarify that any threshold guidance will be treated as suggestive rather than prescriptive, and thresholds will be rebuttable based on the specific context of the proposed transaction.

Setting a threshold of 1,000 U.S. persons for transfers of personal health data may be especially problematic for low-risk transactions associated with health research. Organizations doing pharmaceutical research abide by international principles that call for sharing safety and efficacy data with regulators in every country that is part of a clinical trial or is a location where the drug will be marketed, irrespective of where the data were collected. If the bulk transfer thresholds are too low, pharmaceutical developers may need to limit the scale of clinical research taking place in the United States.[3] For this reason, it will be important for DoJ to consult closely with the Food and Drug Administration (FDA) on the design of any thresholds associated with pharmaceutical research. CIPL also recommends consulting with FDA and other sectoral experts to ensure that the definition of covered genetic data is appropriately nuanced to reflect the fact that some datasets may contain specific genetic elements (e.g., variations in specific genes) rather than the entire genetic sequence of individuals, and to ensure that present and potential future directions of clinical research are not unintentionally hindered.

In addition, DoJ should seek to align the definition of "sensitive personal data" with statutes in effect in U.S. states' comprehensive privacy laws. Doing so will facilitate compliance by organizations that have already structured operations to meet obligations consistent with these laws.

Finally, consistent with our response to Question 2 below, we recommend that anonymized data be excluded from the definition of sensitive personal data as it is, by definition, data in a format that has rendered an individual unidentifiable.[4] Similarly, we recommend that encrypted data be excluded from the definition in circumstances where covered persons would have no access to the encryption keys, as such data would not be accessible and "exploitable by a country of concern" – one of the criteria identified by DoJ for classification of data as "covered personal identifiers."

---

[3] In the case of China, there is also the possibility that China may impose reciprocal restrictions on sharing of clinical trial data, pursuant to Article 43 of China's Personal Information Protection Law (PIPL): "Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt reciprocal measures against said country or region on the basis of actual circumstances." (Translation source: Digichina, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/).

[4] CIPL recommends that DoJ refer to the standard that the Federal Trade Commission articulated in its 2012 report *Protecting Consumer Privacy in an Era of Rapid Change*. The report posits that data is not "reasonably linkable" to a specific consumer, computer, or other device to the extent that a company: "(1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." (https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, p. iv.

2. Should the Department of Justice treat data that is anonymized, pseudonymized, de-identified, or encrypted differently? If so, why?

*Yes.* These techniques significantly lower the likelihood that personal data could be linked to individuals and used in ways to harm them. CIPL documented the role of privacy-enhancing technologies (PETs) in rendering data secure and private while enabling a range of beneficial uses in its white paper Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age.[5] DoJ is correct to incentivize the use of PETs by proposing that "restricted covered data transactions" could proceed if data minimization, masking technologies, or privacy-enhancing technologies are employed. More detailed guidance on deployment of these techniques for various use cases would be useful. In this guidance, DoJ should clarify how it will distinguish among the concepts of anonymization, pseudonymization, de-identification, and encryption, and how obligations will vary accordingly.

As noted under Question 1, CIPL recommends that DoJ exclude anonymized data from the definition of "U.S. bulk sensitive data" given that it has, by definition, been rendered such that individuals are unidentifiable. Anonymization enables beneficial uses of data while protecting individuals' privacy; the ANPR implicitly recognizes these benefits by proposing to exclude from the definition of sensitive personal data any public or non-public data that does not relate to an individual. The ANPR's proposal to include anonymized data within the definition of bulk U.S. sensitive personal data would be inconsistent with this approach. Instead, anonymized data should be fully and consistently excluded from the definition of U.S. bulk sensitive data. In addition, and for clarity, DoJ should specify that data that has been aggregated in a manner that does not enable linkage back to individuals should not be covered by the Rule.

Also as per our response to Question 1, we recommend that DoJ remove encrypted data from the definition of "U.S. bulk sensitive data" where covered persons would have no access to the encryption keys. Without access to encryption keys, encrypted data is unavailable and unexploitable, and therefore does not pose a national security risk. Inclusion of encrypted data under the definition may also disincentivize the use of privacy-enhancing technologies such as homomorphic encryption which rely on cryptographic techniques. Section I (Security Requirements for Restricted Transactions) of the ANPR identifies homomorphic encryption as a potential mechanism to enable transactions that would otherwise be restricted. This proposal is consistent with the proposed definition of "access," which includes ''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-technology systems, cloud-computing platforms, networks, security systems, equipment, or software.'' If data is encrypted in such a way that the Covered Person does not have access to encryption keys, such data should not be regarded as accessible.

[5] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf.

Finally, it will be important to understand how the use of PETs would affect an entity's calculation of its holdings of sensitive personal data vis-à-vis the bulk volume thresholds specified in the ANPRM. From a practical perspective, it may not be possible to "count" the data once they have been encrypted, anonymized, or otherwise de-identified.

11. Should the Department of Justice consider changing any of the categorical exclusions to the definition of sensitive personal data? How should the program define the exclusion for data that is lawfully a matter of public record, particularly considering data that is scraped from the internet or data points that are themselves public but whose linkage to the same individual is not public? What types of data are generally available to the public through open-access repositories?

DoJ could address the concern around de-identified data that are public but whose linkage to particular individuals is not public—e.g., epidemiological statistics for a certain geographic area—by introducing into the rule the concept of foreseeability of future linkage with data that would enable reidentification. The data should not be considered sensitive personal data unless it would be reasonably foreseeable by the party disclosing the data that the linkage would be made.

16. How should the Department define information or informational materials? What factors should the Department take into account in its definition? What relevant precedents from other IEEPA-based programs should the Department take into account when defining the term?

The Department should take care to avoid unintended consequences on Internet traffic that is expressive in nature, with due consideration of existing U.S. law on this topic.

*Section C: Government-Related Data*

17. In what ways, if any, should the Department of Justice elaborate or amend the definition of *government-related data,* including with respect to "recent former" employees or contractors, and "former senior officials"?

DoJ should establish clear criteria to define "recent former" and "former senior officials," including thresholds for seniority and a clear time period for "recent."

*Section D: Covered Transactions*

22. What modifications to enhance clarity, if any, should be made to the definitions under consideration for *data brokerage, vendor agreements, employment agreements, and investment agreements?*

The definition should clarify that *data brokerage* does **not** include:

- Intra-corporate transfers, including transfers of data of multinational companies' parent entities with their foreign affiliates or branches, or among such affiliates and branches, for the purposes of internal operations, such as human resources information, as well as data

necessary for research, development, production and delivery of products and services. For example, pharmaceutical organizations should be able to exchange clinical trial data across borders within their organizations as needed for research and development. If pharmaceutical companies are unable to transfer clinical trial and drug safety ("pharmacovigilance") data, drug development costs and timelines could be affected.

- Data transfers required to complete delivery of financial services or payment transactions, including activities of payment providers in countries of concern, and services provided to them by vendors that are vital for their operations (see additional discussion below).
- Submission of data to government entities as required to fulfil government regulatory requirements, e.g., for financial or pharmaceutical regulation. In the case of pharmaceuticals, if biomedical researchers, pharmaceutical partners, and regulators are unable to access or share certain types of health data—with appropriate controls and limitations—biomedical research and development may be hampered and patients' access to new treatments may be delayed.

Under *vendor agreements,* the rules on cloud computing services should not prevent U.S. providers from offering services to customers within countries of concern and processing data of U.S. individuals who may be resident in those countries (e.g., human resources data about U.S. nationals working for a multinational company operating in the country).

More generally, CIPL recommends that the rules on vendor agreements recognize that organizations may depend upon relationships with vendors in Countries of Concern that offer specialized products and services that may be difficult to find elsewhere (e.g., certain specialized testing services for research). Organizations should have the ability to contract with vendors in such circumstances if the vendors have put in place demonstratable, verifiable programs to ensure that data are protected. DoJ could consider establishing a program akin to Standard Contractual Clauses (SCCs) in the EU, whereby transfers could take place provided certain pre-approved contractual conditions are in place.

In particular, DoJ should exempt from the scope of vendor agreements those situations in which: (i) the vendor is providing product research, development, or improvement services for a U.S. person; (ii) any sensitive personal data is processed by the vendor only in ways ordinarily incident to and part of that product research, development, or improvement; (iii) the U.S. person directs and controls the manner of processing the data; and (iv) the vendor is contractually bound by the U.S. person to maintain the privacy and security of the data.

*Employment agreements* should not lead to a blanket restriction on the ability of U.S. organizations to employ individuals in countries of concern in activities that involve handling of U.S. sensitive personal data. Furthermore, DoJ should take care to ensure that restrictions do not create potential employment law issues for U.S. organizations that currently employ individuals from and in countries of concern. Data security has long been a priority of many multinational organizations; consistent with a risk-based approach, DoJ should enable organizations to employ individuals in such roles where the organizations have taken demonstrable and documented steps to ensure that data is secure.

*Section H.* Exempt Transactions

43. What modifications, if any, should be made to the proposed definitions above [on exemptions] to enhance clarity?

It is important that the rules not unintentionally impede legitimate business and research activities of multinational organizations. DoJ states that it:

*is considering exempting from this program: data transactions involving certain kinds of data; official business transactions; financial-services, payment-processing, and regulatory-compliance-related transactions; intra-entity transactions incident to business operations; and transactions required or authorized by Federal law or international agreements.*

These exemptions are critical for maintaining the ability of organizations to continue doing normal international business and research across a range of sectors. We recommend that "incident to" be expanded to "intra-entity transactions incident or integral to" to clarify that the exemption is meant to enable transactions that are vital for maintaining normal business functions of multinational organizations (see discussion under Section D above).

We also recommend that DoJ incorporate into the rule a distinction between controllers (those who determine the purposes and means of processing personal data) and processors (those who process data on behalf of controllers), and clarify that "intra-company transactions" includes the processing of data by processors on behalf of controllers. For example, routine business transactions that a service provider might complete on behalf of a controller should be clearly covered by the exemption. Examples include the processing of human resources, payroll, and recruiting data; communications services such as email and videoconferencing; document management and collaboration systems; pricing systems and billing; and business intelligence tools. If such activities are not included within the exemption, multinational organizations could be forced to perform these tasks in-house or establish redundant organizational infrastructure in ways that may not be feasible or sustainable.

With respect to "financial-services, payment-processing, and regulatory-compliance-related transactions," we welcome DoJ's exemption of banking and payment services but recommend that it provide greater clarity on the activities to be covered by the rules. Activities such as payments processing involve numerous subordinate and ancillary activities (e.g., business-to-person funds transfers, payor authentication, tokenization, and fraud detection) and the rules should make clear that these activities are covered by the exemption, as these are critical to ensure the safety, security and resilience of transactions in the financial and payment ecosystem.

Furthermore, we recommend that the examples of regulatory requirements for which data transfers could be permitted be expanded beyond financial services to also include other sectors, such as technology and pharmaceuticals (see discussion under Question 22 above).

The final regulations should also clarify whether "transactions required or authorized by Federal law or international agreements", as discussed under Example 56, includes transactions pursuant to agreements focused on facilitating international commercial data flows, such as the EU-US Data Privacy Framework[6], the Global Cross-Border Privacy Rules (G-CBPR) and the Global Privacy

[6] https://www.dataprivacyframework.gov/s/

Recognition for Processors (G-PRP) of the Global Cross-Border Privacy Rules Forum (Global CBPR Forum)[7], and the APEC Cross-Border Privacy Rules and APEC Privacy Recognition for Processers, which were the prototypes for the G-CBPR and G-PRP.[8] The US played and continues to play a substantial leadership role in the development, implementation and operation of the APEC and Global CBPR/PRP systems. Significantly, the United States-Mexico-Canada Agreement (USMCA) recognizes the APEC CBPR system as a valid privacy and data transfer mechanism.[9]

*Section I: Security Requirements for Restricted Transactions*

While DoJ does not ask questions about the proposed security requirements for restricted transactions discussed in Section I and notes that the Department of Homeland Security (DHS) will request comments on the proposed requirements through a separate process, CIPL notes the importance of these requirements being carefully designed to avoid restrictions to legitimate, cross-border business activities. We urge DoJ and CISA to take a risk-based approach to the design of these requirements and to recognize that pursuit of "zero risk" could lead to loss of benefits and greater harms while yielding only marginal security improvements.[10]

*Section J. Licensing*

We recommend that any new licensing regime be designed to minimize unnecessary burdens on businesses, with transparent requirements and clear guidance to facilitate understanding of the criteria.

46. Would general and specific licenses be useful to regulated parties? Why or why not?

*Yes.* It would be useful for there to be licenses that cover commonly occurring scenarios that may apply to a broad range of applicants, as well as specific licenses to account for unique circumstances. For example, a license for scientific research could strike a reasonable balance between the need to protect sensitive personal information and "suppor[t] open scientific data and sample sharing to accelerate research and development through international cooperation and collaboration."[11]

---

[7] https://www.globalcbpr.org/
[8] https://cbprs.org/
[9] https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between at Article19.8; *see also* "What Does the USMCA Mean for a Federal Privacy Law?", Centre for Information Policy Leadership, 17 January 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_what_does_the_usmca_mean_for_a_us_federal_privacy_law__01.17.2020__4_.pdf.
[10] See Theodore Christakis, "The Zero Risk Fallacy," February 2024, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/the_zero_risk_fallacy_-_t.christakis_feb24.pdf, and CIPL, "The Real Life Harms of Data Localization Policies," March 2023.
[11] "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," February 28, 2024,

51. What factors should the Department of Justice assess when considering whether to grant or deny a specific license application?

DoJ should consider establishing self-certification regimes whereby applicants could certify to standards for secure data storage or processing and thereby receive expedited consideration for licenses.

*Section K. Interpretive Guidance*

CIPL believes interpretive guidance—made available to the public—and advisory opinions issued at applicants' request would be useful. Both would increase transparency and broaden understanding of the licensing process.

57. Would an advisory opinion process in general be useful? What effect, if any, should the issuance of an advisory opinion have for the party or parties who requested it? For third parties?

*Yes.* Please see text above.

58. Should industry groups or other associations be permitted to request advisory opinions or interpretive guidance on behalf of one or more of their members (noting that such requests would still need to identify all relevant participants in a data *transaction*)?

*Yes.* Responses to such group requests would be more efficient for both DoJ and applicants.

*Section L. Compliance and Enforcement*

CIPL commends DoJ for the objective articulated in Section L to foster broad compliance through a risk-based approach that calls on U.S. entities to develop compliance programs consistent with their risk profiles. CIPL encourages DoJ to strive for greater clarity on compliance obligations, such as reporting requirements, and to create opportunities for entities to leverage compliance programs already in place (e.g., for sanctions and export controls) to meet obligations under the Rule.

*N. Economic Impact*

CIPL commends DoJ for its commitment to ensuring that the program is scoped to minimize unintended economic consequences and encourages DoJ to consult closely with potentially affected parties on potential impacts and strategies to mitigate them.

---

https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.