U.S. Data Security Program

Cheat Sheet

The U.S. Department of Justice's final rule on protecting Americans' sensitive data took effect on 8 April 2025. The Data Security Program was adopted pursuant to Executive Order 14117 and is implemented by the DOJ's National Security Division. The DSP establishes controls to prevent foreign adversaries, and those subject to their control and direction, from accessing bulk U.S. sensitive personal data and U.S. government-related data.

Scope

The Data Security Program applies to any U.S. person that engages in transactions involving U.S. sensitive personal data or U.S. government-related data when there is a potential for access by covered persons or countries of concern.

A **transaction** is within the scope of the rule if:

✓ It involves any access by a country of concern or covered person to any bulk U.S. sensitive personal data or government-related data.

✓ It involves:

- Data brokerage
- Vendor agreements
- Employment agreements
- Investment agreements

Access means 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.

Currently, there are six designated **countries of concern:**

1. China (including Hong Kong and Macau)
2. Cuba
3. Iran
4. North Korea
5. Russia
6. Venezuela

Selected definitions

A U.S. person is anyone who is a U.S. citizen, national, or lawful permanent resident, i.e., green card holder; any individual admitted to the U.S. as a refugee or granted asylum; any individual or entity physically present in the U.S., regardless of citizenship or immigration status; and any entity organized solely under the laws of the U.S., including the foreign branches of such entities.

A covered person is a foreign entity with its principal place of business in, or organized under the laws of, a country of concern or that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or other covered persons; a foreign individual that is an employee or contractor of a country of concern or of an entity that is a covered person; or a foreign individual primarily resident in a country of concern. In addition, anyone the U.S. attorney general determines to meet certain specified criteria, such as acting on behalf of, being controlled by, or being subject to the jurisdiction of a country of concern or a covered person.

A country of concern is a foreign nation that has shown a long-term pattern or serious instances of conduct significantly harmful to U.S. national security or the safety of its citizens and poses a significant risk of exploiting sensitive U.S. personal data or government-related data in ways that could harm the U.S.

Bulk U.S. sensitive personal data means a collection or set of sensitive personal data relating to U.S. persons, where the volume of such data meets or exceeds the threshold specified in the rule for the particular type of data. Whether the data qualifies as "bulk" depends on volume thresholds over a 12-month period.

Government-related data is

- Any precise geolocation data, regardless of volume, that relates to areas identified on the DOJ's Government-Related Location Data List, including but not limited to military installations, intelligence facilities or worksites of national security employees.
- Any sensitive personal data, regardless of volume, that is marketed as being linked or linkable to current or recent federal employees or contractors, or former senior officials of the U.S. government, including the military and intelligence community.

Data brokerage refers to the sale of data, licensing of access to data or similar commercial transactions where the recipient did not directly collect or process the data from the individuals to whom it relates. This definition excludes employment, investment and vendor agreements, but it includes both first-party, or primary, data brokers who collect and sell information from their own customers and third-party data brokers who purchase and resell data they did not collect in the first instance.

Transaction types

A **covered data transaction** is any transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data and that involves data brokerage, a vendor agreement, an employment agreement or an investment agreement.

Prohibited transactions are

- Any data brokerage transaction that involves any access by a country of concern or covered person to any government-related data or bulk U.S. sensitive personal data;
- Any data brokerage transaction with a foreign person who is not a covered person unless the U.S. person contractually requires that the foreign person refrain from onward sale with a country of concern or covered person and reports any known or suspected violations of that contractual requirement; and
- Any covered data transactions with countries of concern or covered persons involving access to bulk human `omic data or human biospecimens from which bulk human `omic data could be derived.

Evasions, attempts, causing violations and conspiracies to violate the DSP are also prohibited.

Restricted transactions are covered data transactions involving a vendor agreement, employment agreement or investment agreement with a country of concern or covered person. See Subpart D of the rule.

Legal authority: 50 U.S.C. § 1701 et seq.; Executive Order 14117

Implementing regulation: 28 C.F.R. Part 202

Effective date: 8 April 2025

Thresholds for bulk data

Sensitive personal data means human genomic and other human `omic data, biometric identifiers, precise geolocation data, personal financial data, personal health data, covered personal identifiers or any combination thereof. "Bulk" sensitive personal data is defined by numerical thresholds. The thresholds apply over any 12-month period and may be met through a single transaction or multiple related transactions.

Type	Bulk threshold
Human genomic data	More than 100 U.S. persons
Human `omic data (§ 202.224)	More than 1,000 U.S. persons
Biometric identifiers (§ 202.204)	More than 1,000 U.S. persons
Precise geolocation data (§ 202.242)	More than 1,000 U.S. devices
Personal financial data (§ 202.240)	More than 10,000 U.S. persons
Personal health data (§ 202.241)	More than 10,000 U.S. persons
Covered personal identifiers (§ 202.212)	More than 100,000 U.S. persons
Combined data (§ 202.205(g))	Aggregate for the lowest number of U.S. persons or U.S. devices in that category of data

Exemptions

Several categories of transactions are exempt from all or parts of the DSP. Notable exemptions include:

- Personal communications, such as email or phone calls, not involving the transfer of anything of value (§ 202.501).
- The import or export of information or informational materials (§ 202.502).
- Activities conducted on behalf of the U.S. government or required by federal law (§§ 202.504, 202.507).
- Data transactions ordinarily incident to and part of the provision of financial services (§ 202.505) or telecommunications service (§ 202.509).
- Corporate group transactions (§ 202.506).
- Investment agreements subject to a Committee on Foreign Investment in the United States action (§ 202.508).
- Drug, biological product and medical device authorizations (§ 202.510).
- Medical research or clinical trials that fall under certain regulatory frameworks (§§ 202.510–511).

Compliance, recordkeeping and reporting obligations

U.S. persons engaging in restricted transactions must implement robust compliance measures including:

- Due diligence (§ 202.1001).
- Audits (§ 202.1002).
- Recordkeeping and reporting (§§ 202.1101–1104).

U.S. persons must maintain detailed records of restricted and prohibited transactions, internal controls and due diligence efforts. U.S. persons must also:

- Submit annual reports to the DOJ summarizing covered transactions (§ 202.1103).
- Report if they have received and affirmatively rejected any offer from another person to engage in a prohibited transaction involving data brokerage (§ 202.1104).
- Provide additional documentation if requested by the DOJ (§ 202.1102).

Licensing

The DOJ provides two mechanisms for permitting otherwise restricted transactions:

1. General licenses, which authorize a broad class of transactions, may be published by the DOJ (§ 202.801).
2. A specific license applies to a particular transaction and must be requested by submitting an application to the DOJ (§ 202.802).

Enforcement

The DOJ is responsible for enforcing this rule and may take action through:

1. Civil penalties, including fines up to USD368,136 or twice the amount of the transaction that is the basis of the violation, whichever is greater.
2. Criminal penalties: up to 20 years' imprisonment and a fine of up to USD1 million for a person who willfully commits, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of a violation.

Published July 2025.

iapp.org