PEPPERDINE UNIVERSITY

**Office of the General Counsel**

# Memorandum

Date: January 9, 2025

To: Katy Carr

From: Tom Knudsen and Angela McHale, Office of the General Counsel

Subject: Compliance Memo: DOJ Data Security Program (Bulk Sensitive Data)

---

**CONFIDENTIAL AND ATTORNEY-CLIENT PRIVILEGED**

1. Regulatory Context

Under Executive Order 14117, the U.S. Department of Justice (DOJ) has established a new regulatory framework titled "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons." The primary objective is to safeguard national security by restricting the transfer of large-scale personal information to foreign adversaries. **These regulations function similarly to export controls and apply to any university member engaged in international data sharing, foreign research collaborations, or third-party vendor agreements**.

2. Geographies of Concern

The DOJ currently identifies the following as Countries of Concern:

- China (including Hong Kong and Macau)
- Russia
- Iran
- North Korea
- Cuba
- Venezuela

Covered Persons include entities headquartered in these nations, individuals acting as their contractors or employees, and foreign citizens residing primarily in these countries.

3. Data Categories & Bulk Thresholds

The rule applies when data transfers meet or exceed specific volume thresholds within a 12-month rolling period. These categories include:

| Data Type | Threshold (U.S. Persons/Devices) |
|---|---|
| Human Genomic Data | 100+ individuals |
| Biometric Identifiers | 1,000+ individuals |
| Precise Geolocation | 1,000+ devices |
| Human 'Omic Data | 1,000+ individuals |
| Personal Health Data | 10,000+ individuals |
| Financial Data | 10,000+ individuals |
| Personal Identifiers | 100,000+ individuals |

*Note: For "Government-Related Data" (e.g., location data near sensitive federal sites), there is no minimum threshold; any amount is subject to the rule.*

4. Restricted vs. Prohibited Transactions

- Prohibited: Generally includes the direct sale or brokerage of bulk sensitive data to a Country of Concern or Covered Person.
- Restricted: Includes vendor, employment, or investment agreements that involve data access. These are only permitted if specific cybersecurity safeguards (mandated by CISA) and auditing procedures are in place.

5. Institutional Compliance Requirements

To remain in compliance, researchers and administrators must:

1. Conduct Due Diligence: Evaluate any international collaboration for potential "Covered Person" status.
2. Screen Data Flows: Audit whether research datasets involve "Bulk" thresholds before initiating a transfer.
3. Implement Security Controls: For restricted transactions, ensure data is protected by approved access controls and encryption standards.
4. Adhere to Recordkeeping: Maintain documentation of risk assessments and data-sharing agreements for federal review.

6. Consequences of Non-Compliance

The DOJ enforces these rules with significant penalties:

- Civil: Fines exceeding $360,000 or twice the transaction value.
- Criminal: Willful violations can lead to fines up to $1,000,000 and imprisonment for up to 20 years.

7. Internal Support

If you believe your project involves bulk data or collaborators from a Country of Concern, please contact the Office of General Counsel before proceeding with any data transfer.