May 8, 2025

A glimpse into the future of cross-border data regulation

Brian Hengesbaugh
Global Chair of Data & Cyber
Baker McKenzie

Maria Merrill Hilsmier
Associate VP, Assistant General Counsel, Digital Sustainability Regional Attorney Lead (Privacy)
Eli Lilly

Suzan Su
Director, Americas Head of Data Legal and Cybersecurity Legal
UBS

Privacy+ Security Forum

Speakers

Brian Hengesbaugh

Global Chair of Data & Cyber
Baker McKenzie

Suzan Su

Director, Americas Head of
Data Legal and
Cybersecurity Legal
UBS

Maria Merrill Hilsmier

Associate VP, Assistant General
Counsel, Digital Sustainability
Regional Attorney Lead
Eli Lilly

Agenda

1. Various and divergent cross-border regulations
2. Data protection: EU-US Data Protection Framework
3. National security: US DOJ outbound covered data transaction rule
4. China: Cyber, data security, and privacy regulations
5. EU digital rulebook
6. The road ahead

1. Various and divergent cross-border regulations

Various and divergent cross-border regulations

- Diminished effectiveness of the World Trade Organization (WTO) and multilateral trading rules
- Broad range of drivers for cross-border regulation: individual privacy rights, national security, cyber, geopolitical rivalries, competition, and more
- Divergent restrictions on outbound transfer, data localization, compelled data disclosure, and more
- Wide application to personal data, non-personal data, important information, and other company data

2. Data protection: EU-US Data Protection Framework

EU-US Data Privacy Framework (DPF)

- Addresses EU, UK, and Swiss data protection restrictions as applied to cross-border data transfers to US
- Third iteration of TransAtlantic data transfer vehicle (Safe Harbor, Privacy Shield)
- Participating US companies comply with DPF privacy principles, certify to US Dept of Commerce, and are subject to Federal Trade Commission (FTC) enforcement
- 2,800 US companies participate
- DPF underpins $2 trillion in trade in services between EU and US
- Approved privacy controls for government surveillance all EU to US transfers (e.g., DPF + standard contractual clauses, and binding corporate rules) and thereby assist with “Schrems II” transfer impact assessments (TIAs)

Privacy controls for US government surveillance

- EO 14086 (Enhancing Safeguards for US Signals Intelligence)
- Privacy principles for US agencies on signals intelligence
- Data Protection Review Court
- Privacy and Civil Liberties Oversight Board (PCLOB) annual review of redress on complaints

3. National security: US DOJ outbound covered data transaction rule

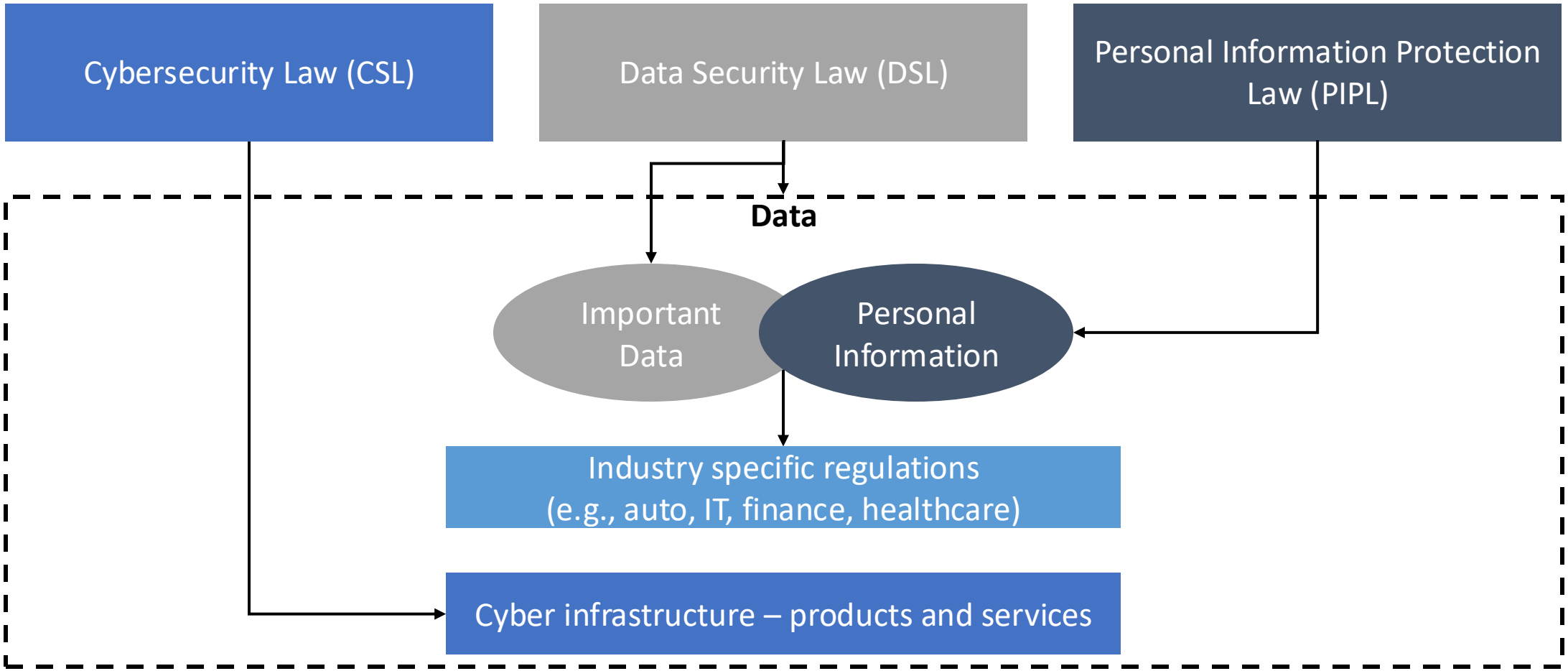
US DOJ Final Rule on protecting Americans' sensitive data from foreign adversaries

Legal context
Biden administration declared national emergency under "IEEPA" regarding access to US sensitive personal data and government-related data by **Countries of Concern** (i.e., China, incl. Hong Kong and Macau, Cuba, Iran, North Korea, Russia and Venezuela) and **Covered Persons** (>50% owned and primary CoC residents)
US DOJ published Final Rule in Federal Register on January 8, 2025. Effective date April 8, 2025, and limited enforcement policy expires on July 8, 2025
Drafted by national security (not privacy) professionals
US DOJ to lead criminal and civil enforcement
New type of combined privacy and trade/sanctions rule

Application
Covered Data Transactions (i.e., data brokerage (1st party data), vendor, employment, and investment agreements)
Prohibited transactions (i.e., data brokerage with CoC and covered persons, and bulk human 'omic data and human biospecimens)
Exempt transactions (e.g., financial services, corporate group, drug/ biological product/ medical device authorizations)
Exclusion from covered personal identifiers (e.g., name and email that is not linked to other data)
Restricted transactions (strict CISA security requirements)
Key practical issues: shared service centers, cloud vendors, back-office processing, global databases, group operations
Cross-functional collaboration needed (privacy + trade/sanctions)

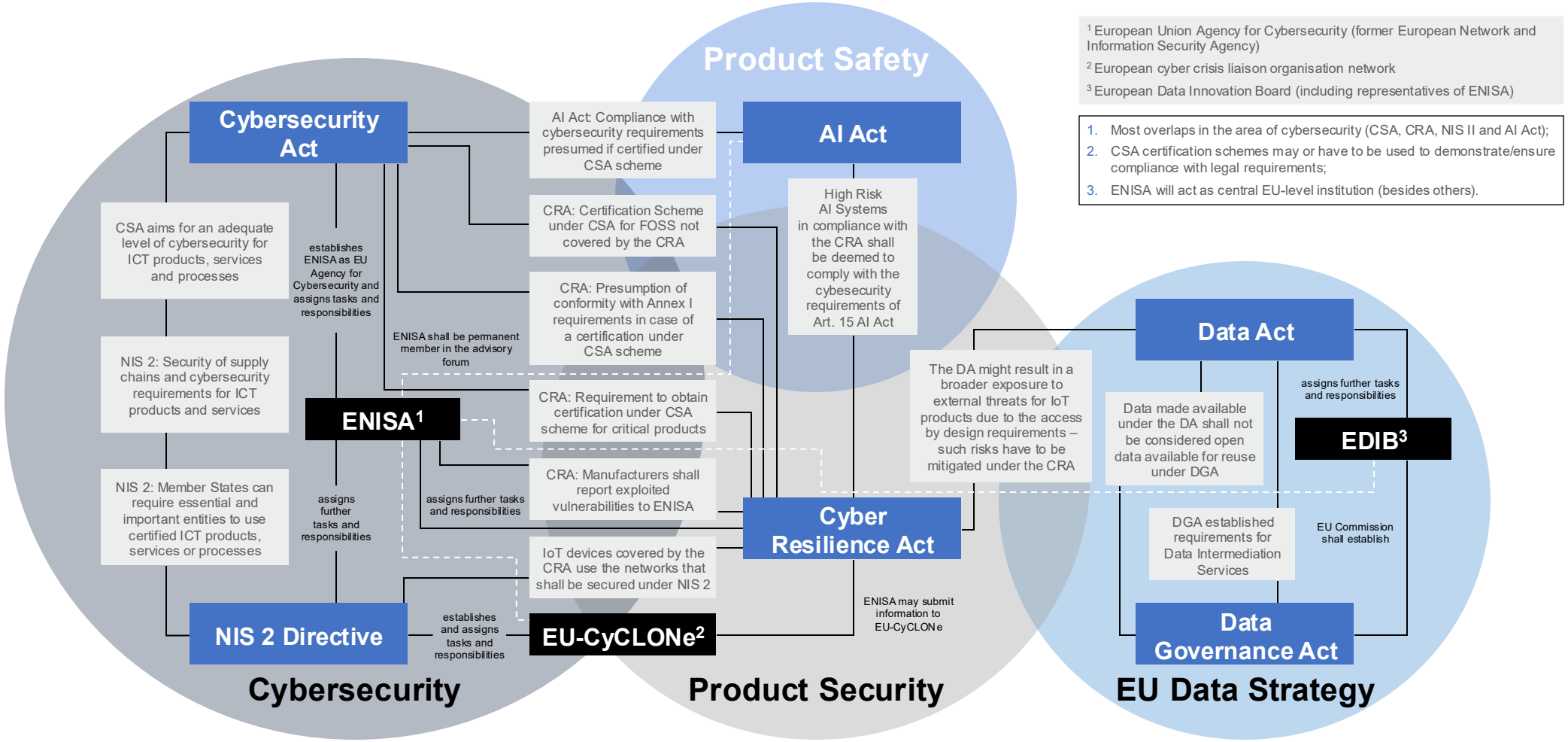
4. China: Cyber, data security, and privacy regulations

China Cyber/Data Security/Privacy Laws



5. EU digital rulebook

EU digital rulebook



[1] European Union Agency for Cybersecurity (former European Network and Information Security Agency)

[2] European cyber crisis liaison organisation network

[3] European Data Innovation Board (including representatives of ENISA)

1. Most overlaps in the area of cybersecurity (CSA, CRA, NIS II and AI Act);
2. CSA certification schemes may or have to be used to demonstrate/ensure compliance with legal requirements;
3. ENISA will act as central EU-level institution (besides others).

6. The road ahead

The road ahead

Reasonably anticipate

- More cross-border restrictions based on national security, cyber, and geopolitical risks
- Significant consequences (e.g., criminal) for non-compliance
- Increased tension b/w US and Countries of Concern, including China, and others (e.g., Russia)

Business implications

- More intense risk assessment and strategic decision-making
- Greater focus on empowering senior leadership
- Regional or local applications and infrastructure may prove more durable than global
- Enhanced cross-functional cooperation and alignment will be key
- Third party business partners and vendors will continue to pose risk

Baker McKenzie Resources

Connect on Tech Blog and Podcast Series

Our blog and podcast series covering a broad range of topics such as data privacy and security, cybersecurity, digital innovation and transformation, generative AI and machine learning and other topics.

How Could Trump Administration Actions Affect the EU-US Data Privacy Framework?

A Glimpse into the Future of Cross-Border Data Regulation

What does the DOJ final rule on protecting Americans' sensitive data from foreign adversaries really mean for global business?

Primer on the DOJ final rule on protecting Americans' sensitive data from foreign adversaries

Global Data Privacy & Cybersecurity Handbook

(Updated January 2025)

It has never been easier for companies to collect, copy and transfer personal data around the world. But at the same time, the introduction of a wide range of privacy and security laws worldwide imposes complex and often inconsistent privacy and data protection standards impacting on multinational companies. Our Global Privacy & Cybersecurity Handbook provides detailed overviews of the increasingly complex and sophisticated privacy and data protection standards in over 50 countries.