Asia-Pacific
Economic Cooperation

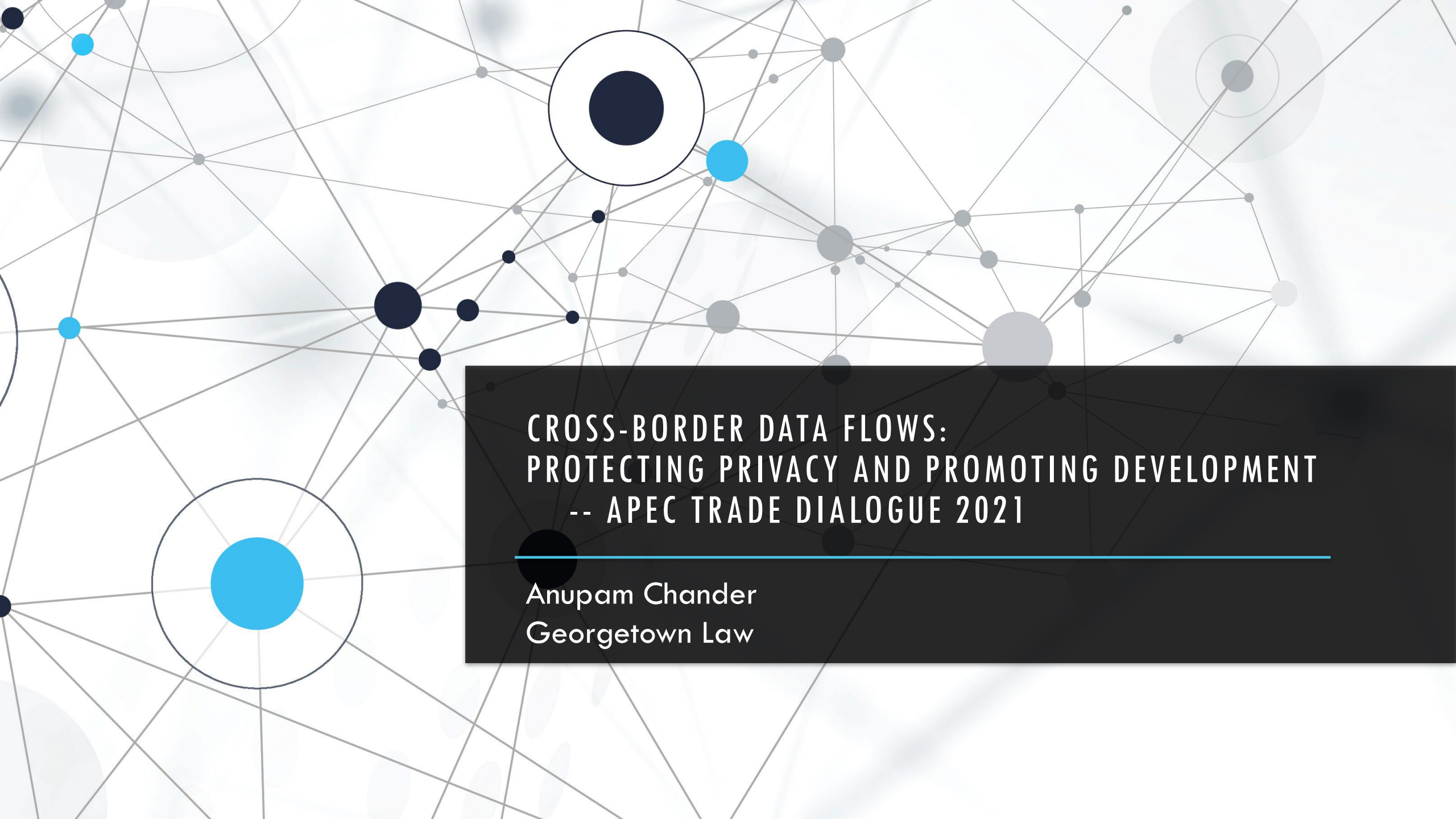
2021/SOM2/CTI/TPD/006
Session: 2

Cross-Border Data Flows: Protecting Privacy and Promoting Development

Submitted by: Georgetown University

NEW ZEALAND
APEC 2021
ASIA-PACIFIC ECONOMIC COOPERATION 2021

Digital Trade Policy Dialogue
18 May 2021



CROSS-BORDER DATA FLOWS: PROTECTING PRIVACY AND PROMOTING DEVELOPMENT -- APEC TRADE DIALOGUE 2021

Anupam Chander
Georgetown Law

OUTLINE

- IMPORTANCE OF CROSS-BORDER FLOWS
- Mechanisms for Cross-Border Transfer
- COMPLIANCE COSTS
- ENFORCEMENT COSTS
- RECOMMENDATIONS

CROSS-BORDER DATA FLOWS CRITICAL TO NEW TECHNOLOGIES

Cloud computing	The Internet of Things	App Economy	Outsourcing of Services
E-commerce	World Wide Web	Big data	Digital products and streaming services
The sharing economy	Artificial Intelligence	FinTech	Smart Cities

Fire in a Samsung building in Gwacheon, Korea interrupts Samsung smart TVs worldwide (2014)

GDPR – TRANSFER MECHANISMS

Adequacy	Only a few European territories and Argentina, Canada, Israel, Japan, New Zealand, Switzerland, Uruguay ~~and the United States (under the Privacy Shield framework)~~. Korea coming.
Standard Contractual Clauses	Made difficult by Schrems II (CJEU 2020)
Binding Corporate Rules –	Only within corporate group; not intra-corporate group even if both have BCRs
Certification	Largely theoretical
Codes of Conduct	Largely theoretical
Ad hoc contractual clauses	Too risky
Derogations	Limited availability

COMPLIANCE

AVERAGE EXPENDITURE FOR GDPR COMPLIANCE

The different results suggest the great variation in expenditures for compliance, depending on firm size, industry, types of activities, geography, perceived risks of operations, and risk tolerance.

$1 million

- A study conducted in 2019 by the International Association of Privacy Professionals (IAPP) in conjunction with Ernst & Young, a global professional service network, found mean privacy expenditures for the companies at which its survey respondents worked to be $1 million in 2018, the year the GDPR first went into effect, and $622,000 in 2019.

$13.2 million

- Research conducted by the Ponemon Institute in 2019 on behalf of international law firm McDermott Will & Emery (MW&E) found substantially higher figures: an average 2019 budget of $13.6 million for GDPR activities, a slight increase from $13.2 million in 2018.

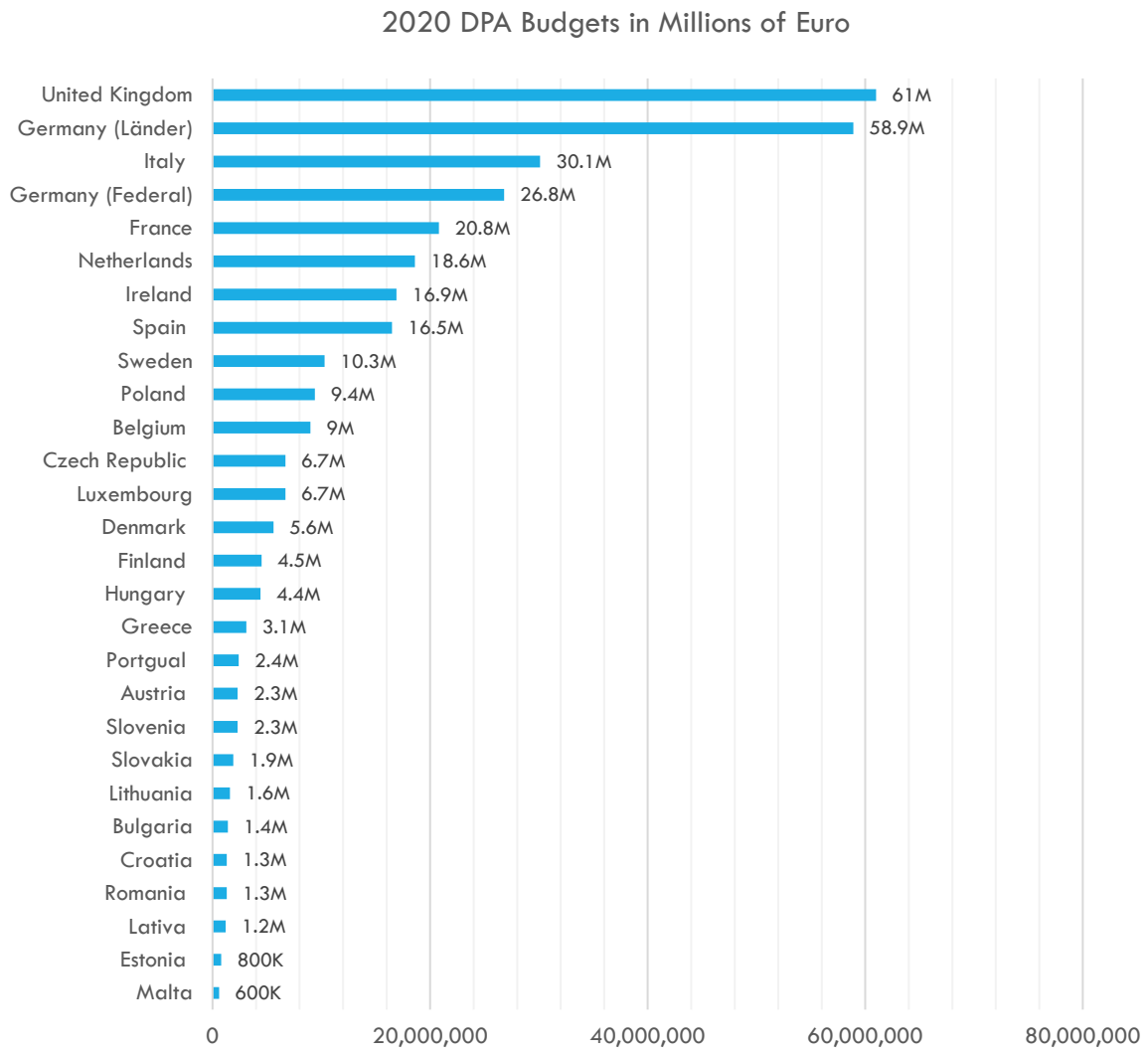
ENFORCEMENT

EU ENFORCEMENT

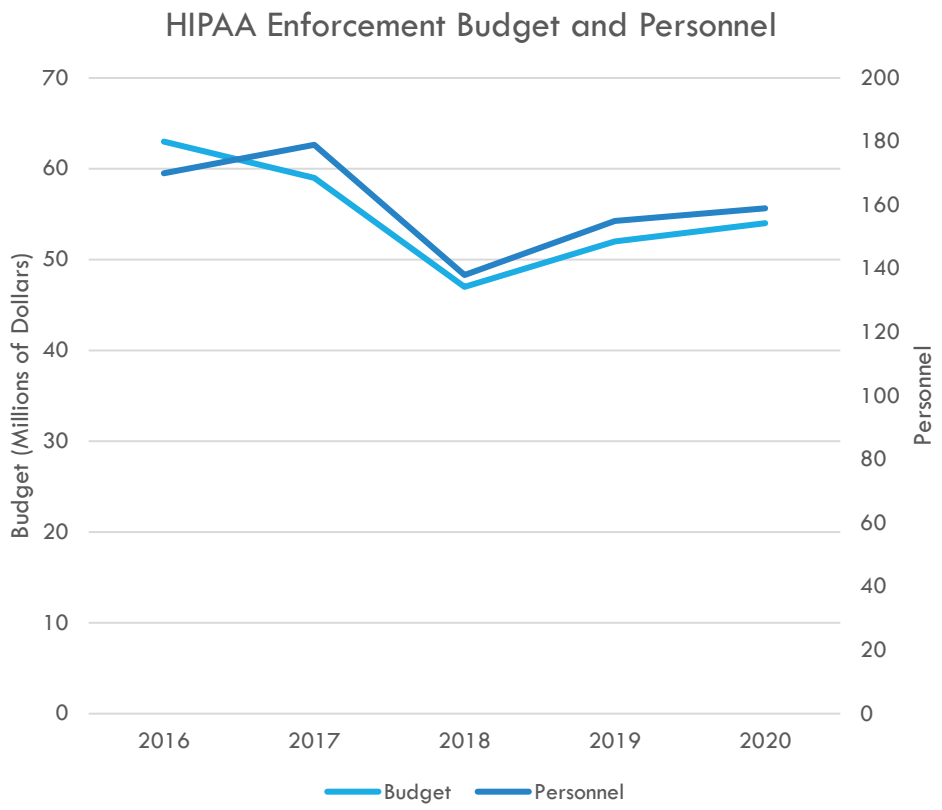
On average, the European Union member states and the UK allocated €12.1 million to each of their data protection authorities in 2020.

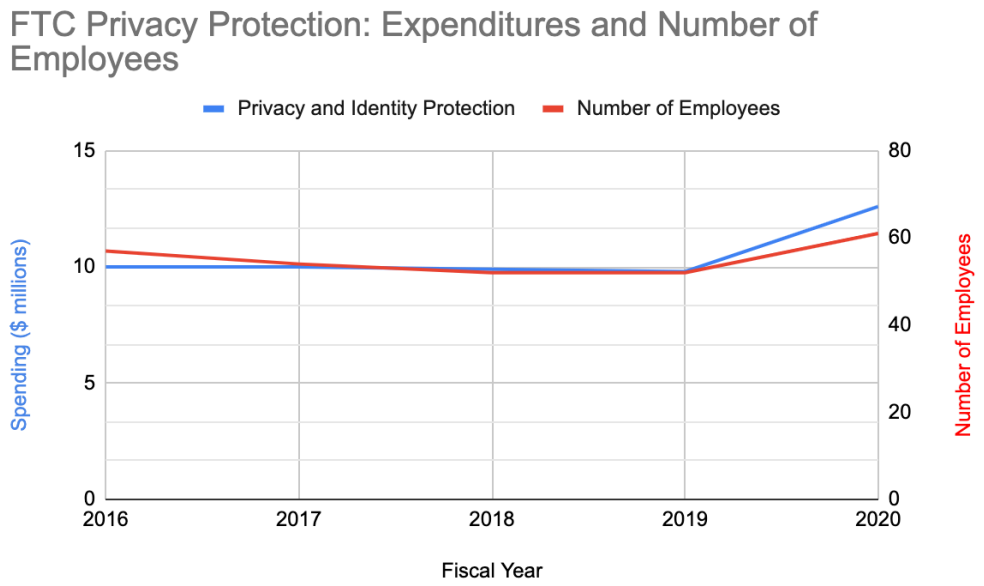
At the high end, Germany allocated €85.7 million among both its federal and state data protection authorities, while Cyprus, Malta, and Estonia, allocated just €0.5 million, €0.6 million, and €0.8 million for the latest year available.

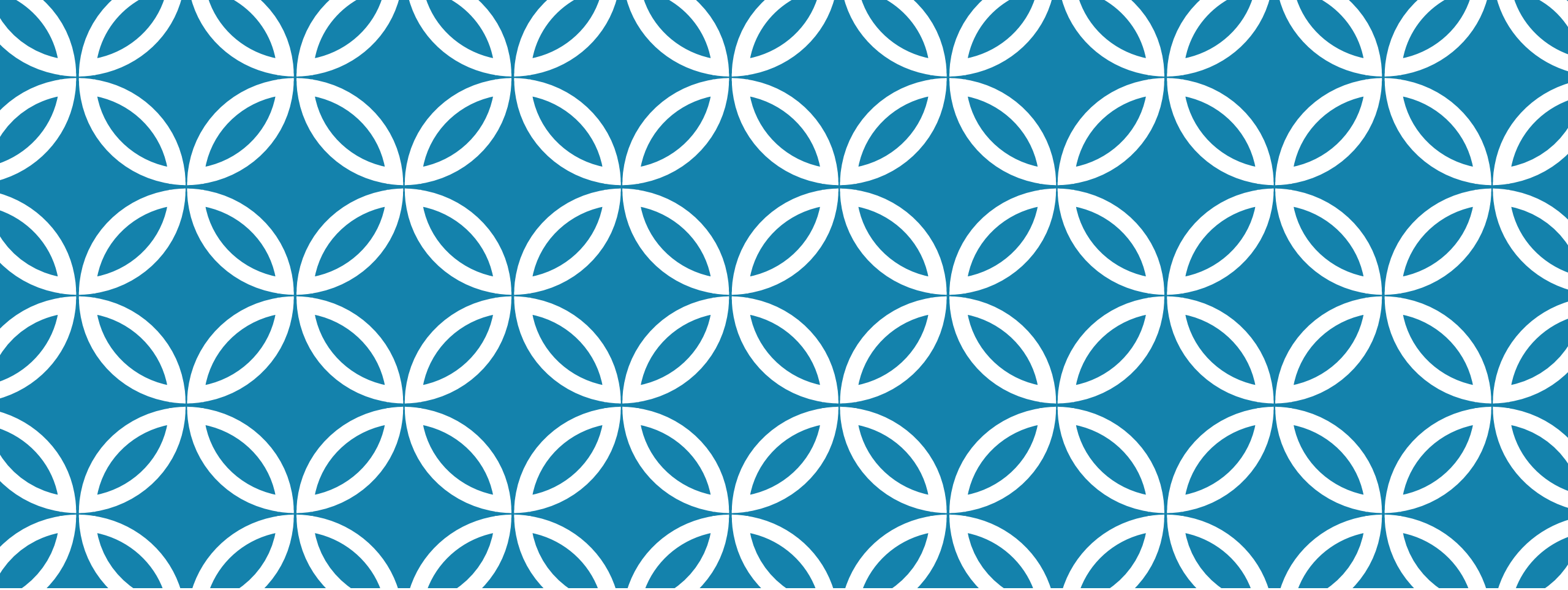
Collectively, in 2020, the EU member states and the UK expended €326 million to enforce data privacy rules governing some 513 million people—**less than a euro (or a dollar) per person for the year.**



US ENFORCEMENT







RECOMMENDATIONS

MICRO, SMALL, AND MEDIUM-SIZED ENTERPRISES

GDPR applies to a sole proprietorship to a large business, though some of its responsibilities are risk-based.

California Consumer Privacy Act only applies if:

- annual gross revenues of $25 million;
- annually buy, sell, receive, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices (CPRA raises this to 100,000 consumers); or
- derive 50 percent or more of its annual revenues from selling consumers' personal information.

EU-US PRIVACY SHIELD AS MODEL FOR INTEROPERABILITY

Opt-in to Interoperability

Creates interoperability between systems by allowing corporations to commit to legally-enforceable obligations when dealing with data from EU.

European Court of Justice 2020 *Schrems II* ruling focuses on inadequacy of legal rights against government surveillance—a broad problem which will require substantial work by all economies to fix.

Key Features

Notice

Choice

Accountability for Onward Transfer

Security

Data Integrity and Purpose Limitation

Access

Resources, Enforcement and Liability

EU-JAPAN ADEQUACY AS MODEL FOR INTEROPERABILITY

Additional safeguards:

- For sensitive data
- conditions under which EU data can be further transferred from Japan to another third economy
- individual rights to access and rectification.

Access of Japanese public authorities for criminal law enforcement and domestic security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms.

A complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities.