U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

INTERNATIONAL TRADE ADMINISTRATION

DORSEY™
always ahead

WELCOME

DORSEY™
always ahead

To do business with Europe
Protect Personal Data!

The new EU 'General Data Protection Regulation' (GDPR)

and the EU-U.S. Privacy Shield

Isabelle Roccia

Isabelle Roccia is a Senior Policy Advisor with the U.S. Foreign Commercial Service since 2013. Based at the U.S. Mission to the EU in Brussels, she works on digital policy and digital economy, including data flows, data privacy and cyber-security. In this role she advises U.S. Government agencies and private sector on EU decision-making process, policies and their potential impact on business models and companies' regulatory compliance.
Previously, Isabelle worked in EU affairs consultancies where she advised U.S. and European companies on EU policies related to ICT and international trade, as well as on EU funding opportunities. She is a law graduate from the University of Paris II – Assas and holds a Master on Defense Industry and geo-strategies.

Michelle Sylvester-Jose

Michelle Sylvester-Jose is a Policy Advisor with the Data Flows and Privacy Team at the U.S. International Trade Administration. In this position, she works to promote policy frameworks to facilitate cross-border data flows to support trade. Since joining ITA in 2014, she has focused on working with small-and-medium sized enterprises to export overseas. She serves as part of the Department of Commerce's Privacy Shield Team, and works on the APEC Cross Border Privacy Rules (CBPR) System.
Prior to joining the Department of Commerce, Michelle has several year of experience working with non-profit organizations on program management and development. Michelle has a master's degree in International Relations with a focus on Conflict Resolution and Negotiations from New York University, she also received her bachelor's degree in International Relations from the University of California Davis.

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Why the European Union matters for U.S. exporters

GDPR: what it is and what it means for U.S. companies

International data flows & Privacy Shield

How to get started…

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Why the European Union matters for U.S. exporters

Basic facts about the European Union

Economic and political partnership between 28 countries

508 million inhabitants

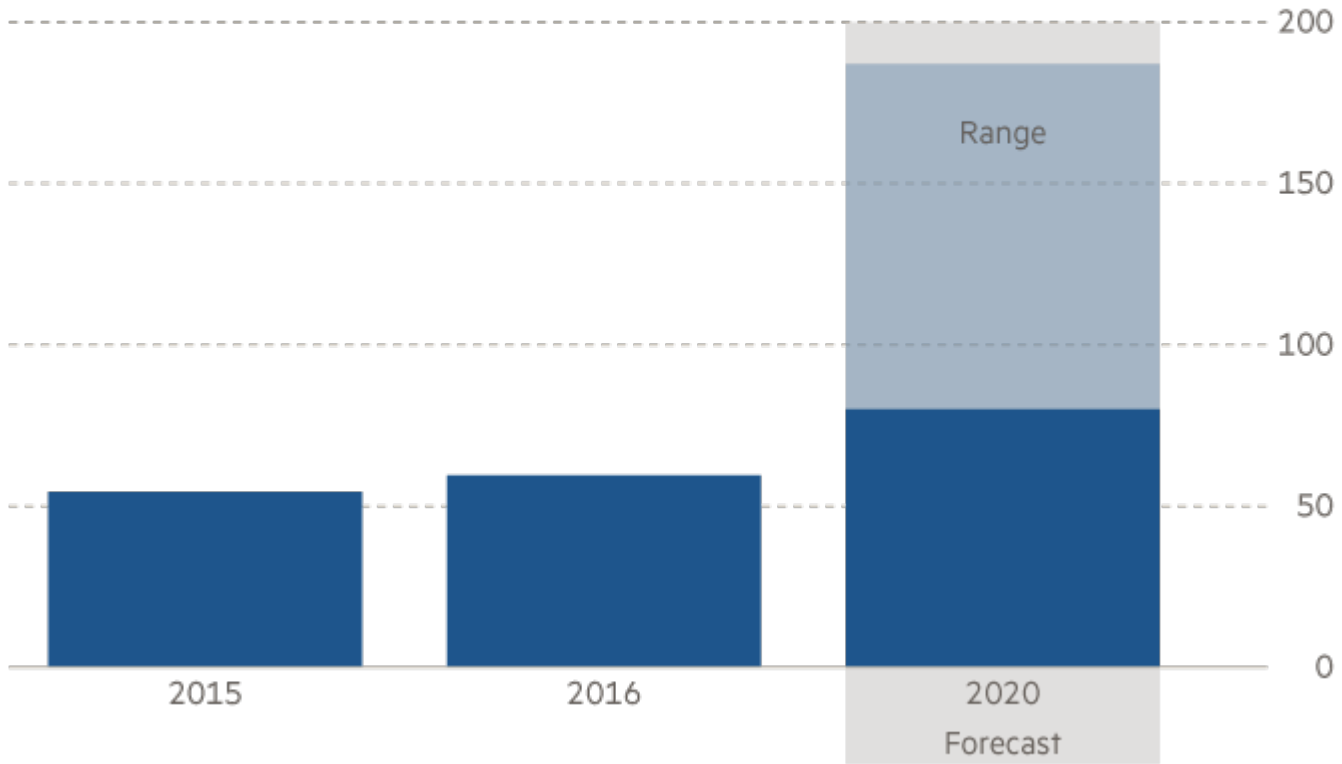
GDP per capita: $32,384 (2016)

24 official languages

U.S. COMMERCIAL SERVICE
United States of America Department of Commerce

European data market

Value of sales (€b)



Source: EU Data Market study

© FT

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

European Commission

Sole initiator of legislation, manager of the EU budget, enforcer of EU law

Represents the European Community – internally and externally

28 Commissioners (1/member state) Rotates every 5 years ➡ 2019

DG Enterprise, Internal Market, Trade, Connect, Health, Environment

Council of Ministers

Main decision-making body, representing Member States

Can't initiate legislation but can amend, Co-decision with European Parliament

Rotating 6-month Presidency

Permanent Representations in Brussels

European Parliament

750 Members of European Parliament representing EU citizens

Increased powers as a result of the Lisbon Treaty

Can't initiate but can amend, Co-decision with Council

Multiple Political Parties (Green, Socialists, Liberals, EPP, etc.)

20+ Committees including Industry, Trade, Environment

U.S. COMMERCIAL SERVICE
United States *of* America
Department *of* Commerce

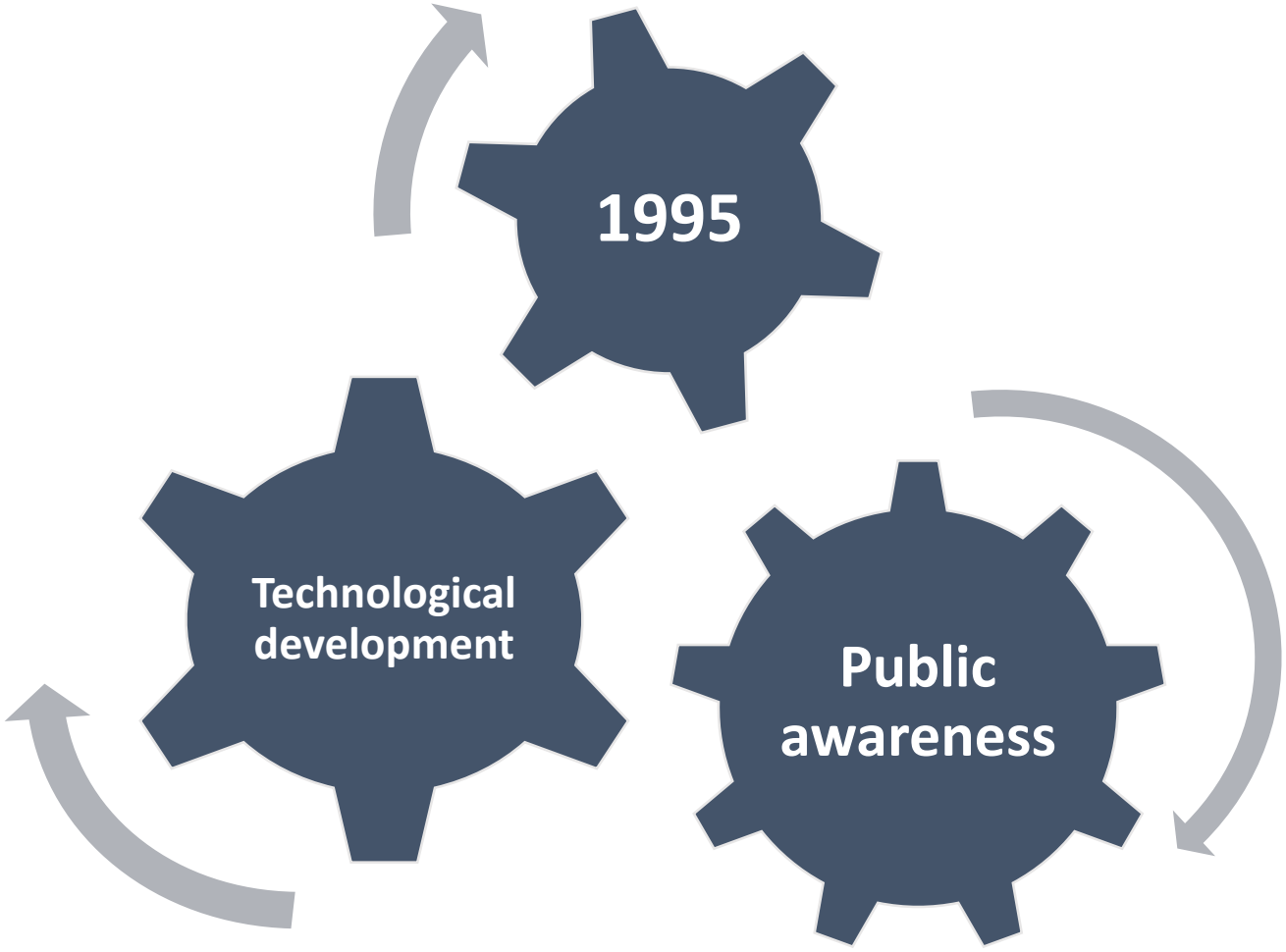

GDPR

29 March 2019

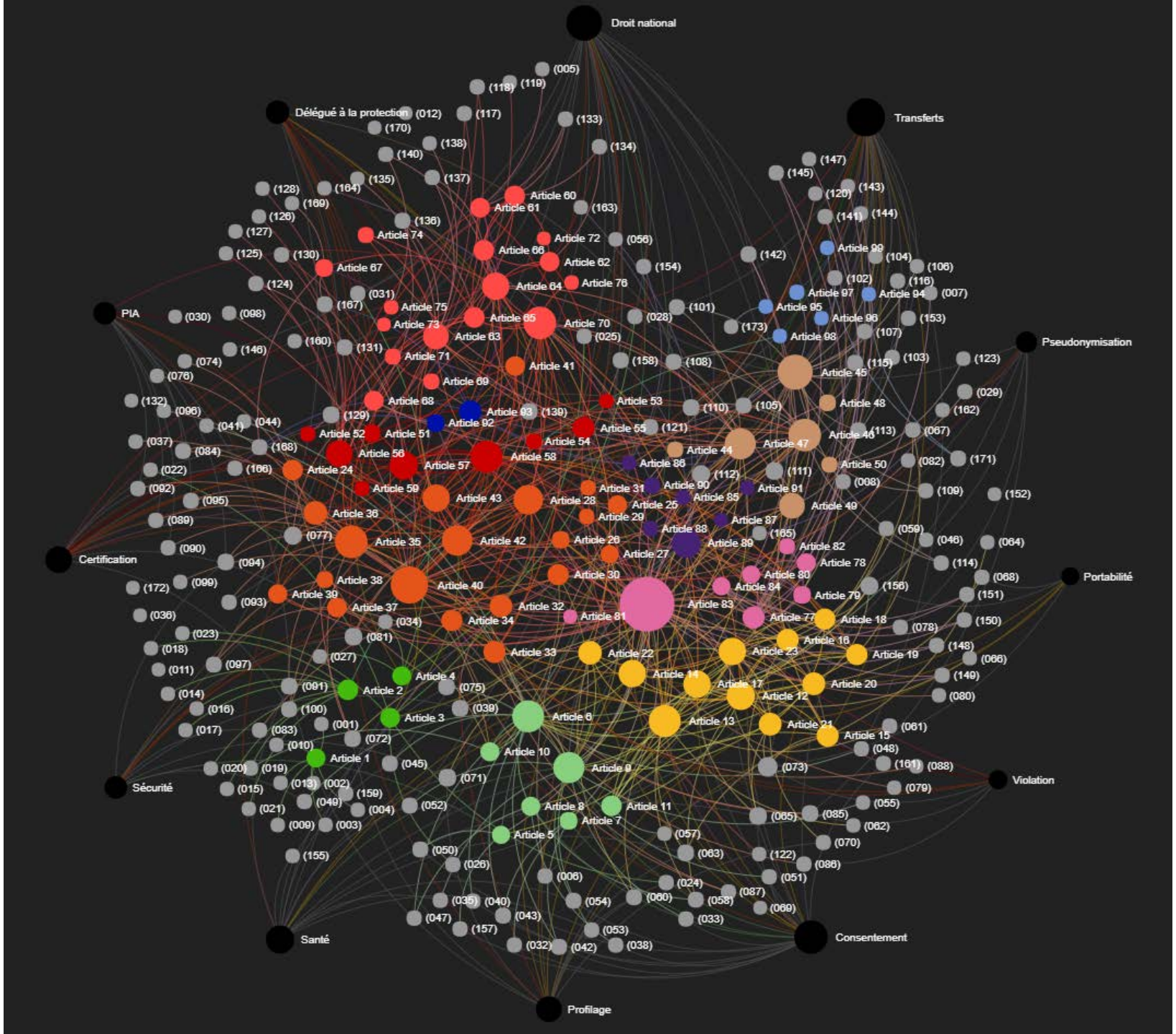
ICELAND
LIECHTENSTEIN
NORWAY
eea

U.S.
COMMERCIAL
SERVICE
United States *of* America
Department *of* Commerce

Genesis



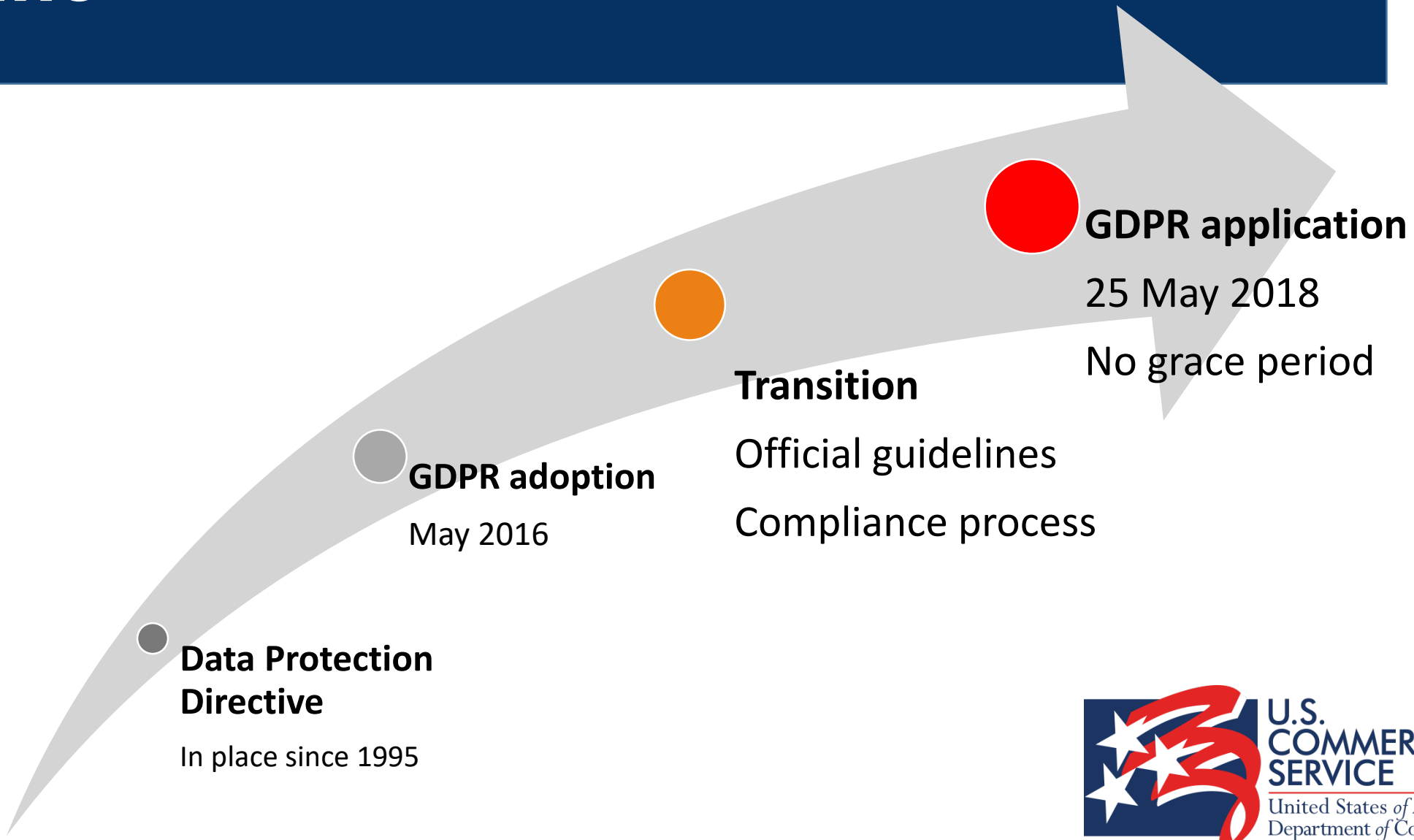
U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce



https://www.cnil.fr/fr/reglement-europeen-protection-donnees/dataviz

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Timeline



Data Protection Directive

In place since 1995

GDPR adoption

May 2016

Transition

Official guidelines

Compliance process

GDPR application

25 May 2018

No grace period

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Top line facts

Data Protection is a fundamental right in Europe.

Builds on existing EU Directive (1995)

Harmonizing legislation…

Principles and concepts remain the same
Similar principles in the U.S.

Becomes applicable on 25 May 2018

Omnibus, legislation vs. sectoral regulations

…but not fully

Expanded scope & definitions
New/stricter requirements

Transition phase

Things to watch:
DPA Guidelines
Member States legislation

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

What GDPR means for U.S. companies*

* non-exhaustive

A few key definitions…

Key definitions

Article 4 (1): *'**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

*'**Processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

Scope: Does GDPR apply to my organization?

Key definitions

GDPR applies to businesses that meet at least one of these criteria:

- ❑ Your company offers goods or services to individuals in the EU;
- ❑ Your company monitors individuals' behavior;
- ❑ Your company processes personal data of EU individuals on behalf of other businesses.

Regardless of a presence in the EU => extraterritoriality

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Controller/Processor

Key definitions

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data;

Processor: a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller.**

→ *No major change of definition but…*

Responsibilities can be different

Terms of contracts will change

An organization can be one or both

U.S. COMMERCIAL SERVICE
United States *of* America
Department *of* Commerce

Key definitions

Impact on contracts (Controller/processor relationship)

Is this new? Partly

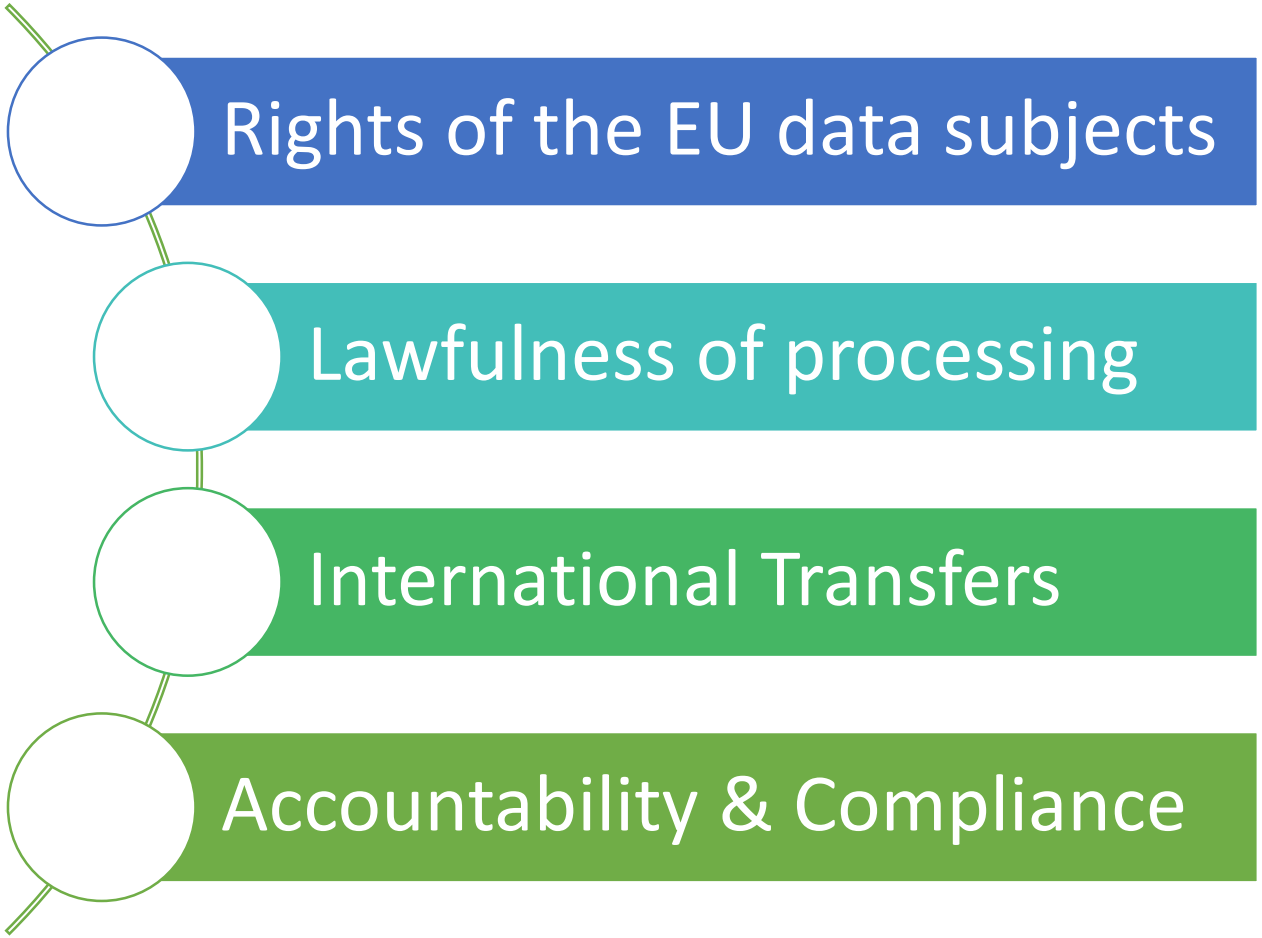
Key points

1. The contract must also contain a number of mandatory terms(article 28) include :
- The subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller;
- Stipulation that the data processor will only process personal data on the documented instructions of the data controller;
- The processor makes available to the controller all information necessary to demonstrate compliance;
- On controller's direction, either return or destroy the personal data at the end of the relationship;

To do Review contractual agreements against new GDPR specifications, **even pre-existing ones**

Main Requirements*

* Not exhaustive



U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Rights of the EU data subjects

- Information notices
- Rights to access, rectification, portability, erasure, restriction of processing, to opt-out of direct marketing
- Profiling and automated decision-taking

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Rights of the EU data subjects

Information notices

Is this new?

Partly

Key points

Information notice must be concise but include more information…
what data is collected, why, how can the individual get a copy, contact details of the controller, details of data transfers outside the EU, complaints, etc.

To do

- Update exiting notices
- Inform individuals (e.g. emails, icons, videos, dashboard…)
- Use plain language; use local language

U.S. COMMERCIAL SERVICE
United States *of* America
Department *of* Commerce

Rights of the EU data subjects

Access, rectification, portability, erasure, restriction of processing, opt-out

Is this new?

Largely

Key points

1. Be able to provide a copy of the data set on request of the data subject;
2. Ensure data can be ported to the individual within one month after the request;
3. Data subjects can require the controller to restrict the processing of their data if there is a complaint (e.g. accuracy issue, processing is unlawful, withdraw consent…);
4. Right to erasure ('right to be forgotten')
5. Rights to opt out of direct marketing, object to processing for statistical/research purposes (not absolute in case of public interest);

To do

- Assess how these new rights may affect your business model
- Set up processes/procedure in case your organization receives one of these requests (e.g. portability: easily readable format)
- One month to comply with a request

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Rights of the EU data subjects

Profiling and automated decision-taking

Is this new? Partly

Key points

1. Automated processing can be used if necessary for a contract (e.g. travel booking), if there is explicit consent, if it is authorized by a Member State law;
2. Restrictions on profiling: if the decision produces legal effect (e.g. credit rating, e-recruiting); for sensitive data and for children;
3. Profiling for marketing purposes;

To do

- For automated processing of sensitive data, ensure explicit consent (e.g. children data)

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Lawfulness of processing

Lawfulness of processing and further processing

- **Legitimate interests**
- **Consent**
- Contract
- Legal obligation
- Vital interest
- Public interest

Special cases

Sensitive data

Children

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Lawful processing

Legitimate interest

Is this new?

Partly (guidance under previous legislation)

Key points

Examples of legitimate interest (not exhaustive list):

1. Fraud detection (incl. credit checks, anti-money laundering)
2. Compliance with law enforcement, court/regulators requirements
3. Industry watch lists (barred customers, non-payment lists…)
4. Cyber security/IP protection/trade secrets protection
5. Employment data processing (e.g. background checks, internal websites, time keeping…)
6. Direct marketing

To do

- Clarify which legal basis your organization relies on.

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Lawful processing

Consent

Is this new? Largely (important difference between EU and U.S. concept)

Key points

1. Consent is active, specific, informed and unambiguous (may mean that consent notice must be in local language);
2. Consent must be explicit for sensitive data processing or transfers outside the EU;
3. Cannot be bundled for various uses;
4. Should be easy to withdraw consent at any time;
5. Not valid if clear imbalance between controller and data subject (e.g. employer/employee);
6. Children (<16yrs or <13yrs) : consent only valid if authorized by a parent (for online services);
7. Greater obligation to identify third party with whom data may be shared.
8. Record keeping obligations.

To do

- Consider other legal basis?
- Avoid pre-ticked boxes
- Rephrase language (in particular if audience are children or non-native English speakers)

Lawful processing

Sensitive personal data

Is this new?

Largely

Key points

1. Sensitive personal data ("special categories of data" – art. 9) are defined more broadly to incl. health data, political opinion, trade union, sexual orientation, genetic, biometric, racial/ethnic origin etc.;

2. Processing of sensitive data is prohibited unless (incl.)…:
- Explicit consent to processing;
- Employment or social security or social protection obligations of the controller;
- Protection of the vital interest of the data subject (if no consent can be given);
- Data manifestly made public by the data subject;

To do

If relying on consent to process and/or transfer, ensure it is explicit.
If large scale processing of sensitive data, DPO/representative is mandatory.
Record of processing activity obligation.
Data protection impact assessment is required.

Lawful processing

Children data

Is this new?

Partly

Key points

Consent from a child only valid if authorized by a parent - under 16 y. old (down to 13 years old for some MS) – for online services only;
Legitimate interest: need balancing test (documentation and risk assessment);

To do

Information notices: clear and easy to understand language drafted with children in mind.
Check the legal basis used

International Transfers

Transfers outside of Europe are forbidden unless authorized.
The protection travels with the data.

Mechanisms available:

- Authorization from a DPA
- Model Contractual Clauses
- Binding Corporate Rules
- **EU-U.S. Privacy Shield** www.privacyshield.gov/

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Privacy Shield Framework

U.S. COMMERCIAL SERVICE
United States *of* America
Department *of* Commerce

Accountability & Compliance

- Accountability & Privacy-by-design and by-default
- Data Protection Officer/Representative in the EU
- Security of processing/Personal data breach

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Accountability & Compliance

Data governance & Privacy-by-design

Is this new?

Largely – for the controller

Key points

1. Be compliant AND be able to demonstrate it (e.g. if you are using a cloud providers: be able to demonstrate the trustworthiness of your data transfers using valid EU tools)
2. Be compliant in the long-run: GDPR compliance is not a one-off; has to be sustained over time (new processes in place, new services offered, etc.)

To do

- Set up a team and set aside budget for compliance activity;
- Establishes processes for recording of activities, reporting, auditing, training, etc.
- Integrate privacy into product development, new relations, organization's restructuring etc.

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Accountability & Compliance

Data Protection Officer or Representative in the EU

Is this new? Yes

Key points Organization fitting certain criteria must appoint a Data Protection Officer. DPO's responsibilities include:
- Inform and advise the organization and its employees of their obligations;
- Monitor compliance with GDPR (incl. training, audits);
- Advise on data privacy impact assessments;
- Acts as the point person for the regulators.

Representative in the EU: Possible exemption for processing occasional, small-scale and no sensitive personal data involved

To do
- Determine whether you must appoint a DPO;
- If you don't, assess whether it is important for you to do so nonetheless.

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Accountability & Compliance

Security of processing/Personal data breach

Is this new? Largely

Key points

1. Organizations must implement technical and administrative measures to protect personal data (criteria: state of the art technology; nature/scope/context/purpose of processing; Likelihood and severity of risks to the rights of the individuals);
2. Processor must notify controller of all breaches without undue delay (see WP29 guideline);
3. Controller must notify supervisory authorities within 72 hours of becoming aware of a data breach (not required if breach is unlikely to result in a risk for data subject);
4. Controller must notify the data subject (unless there is no high risk for data subject; protections were in place.

To do

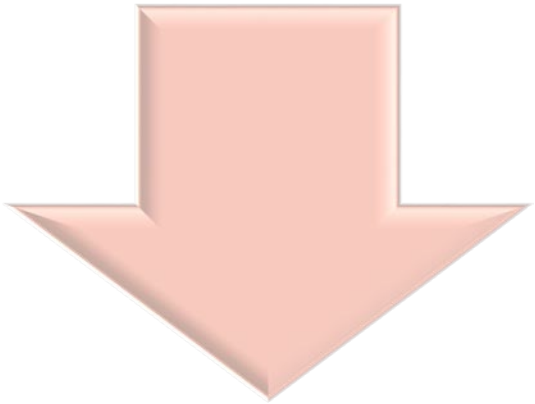
- Develop/update internal breach notification procedures;
- Implement protective measures with your IT security team

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Fines & Sanctions

Up to 4% of annual revenue or $22 million (whichever is higher)

e.g. processing without legal basis, breach of data subjects rights, international transfers…



Up to 2% of annual revenue or $11 million (whichever is higher)

e.g. Failure to notify a data breach, not having a representative in the EU, not maintaining written records…

DPAs can also…

Carry audits, issue warnings, issue a ban on processing.

Data subjects can sue for compensation.

Reputational risk

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce


Where to Start…

Some questions to start with…

What EU personal data does my company have?

Are my European partners aware of GDPR?

Who in my company will deal with these issues? (Compliance/Legal/IT team?)

What new requirements apply to me?

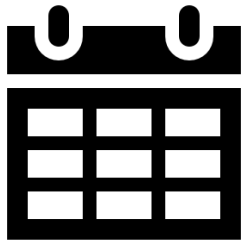
Who is my lead Data Protection Authority (DPA)?

How much getting compliant will cost to my company?

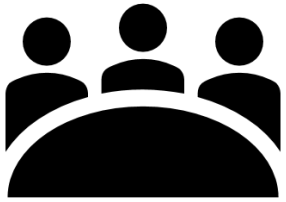
Should I seek external legal counsel specialized in European data privacy?

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

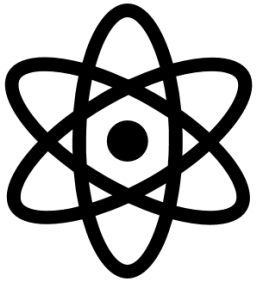
Additional factors



D-Day + 1



Integrate privacy



Eco-system:
Is everyone doing the right thing?

Impact on your business model

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Identify project lead and team members

Core team:
IT (CIO/CISO)
CTO - COO
Compliance
Legal

Establish working methods and decision process
Get management support (resources and funding)

2nd circle – Dissemination & adoption
Communications
Customer relations
Accountability
HR
Etc.

From compliance to product development to marketing/sales

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Complete a data mapping

- Identify the data that the organization has and put that in a *dynamic* mapping document;
- Look at personal data from contractors, vendors, employees, suppliers etc.;
- Look at your contractual agreements;
- Involve all the business units in your organization

U.S. COMMERCIAL SERVICE
United States *of* America
Department *of* Commerce

Determine whether you need to appoint a DPO

Do your core activities consist of processing which requires **regular and systematic monitoring of individuals on a large scale**?

Yes → DPO mandatory

No → DPO not required* → Are you subject to other laws that could require a DPO (e.g. member state legislation)?

Do your core activities consist of processing which is about **special categories of data on a large scale**?

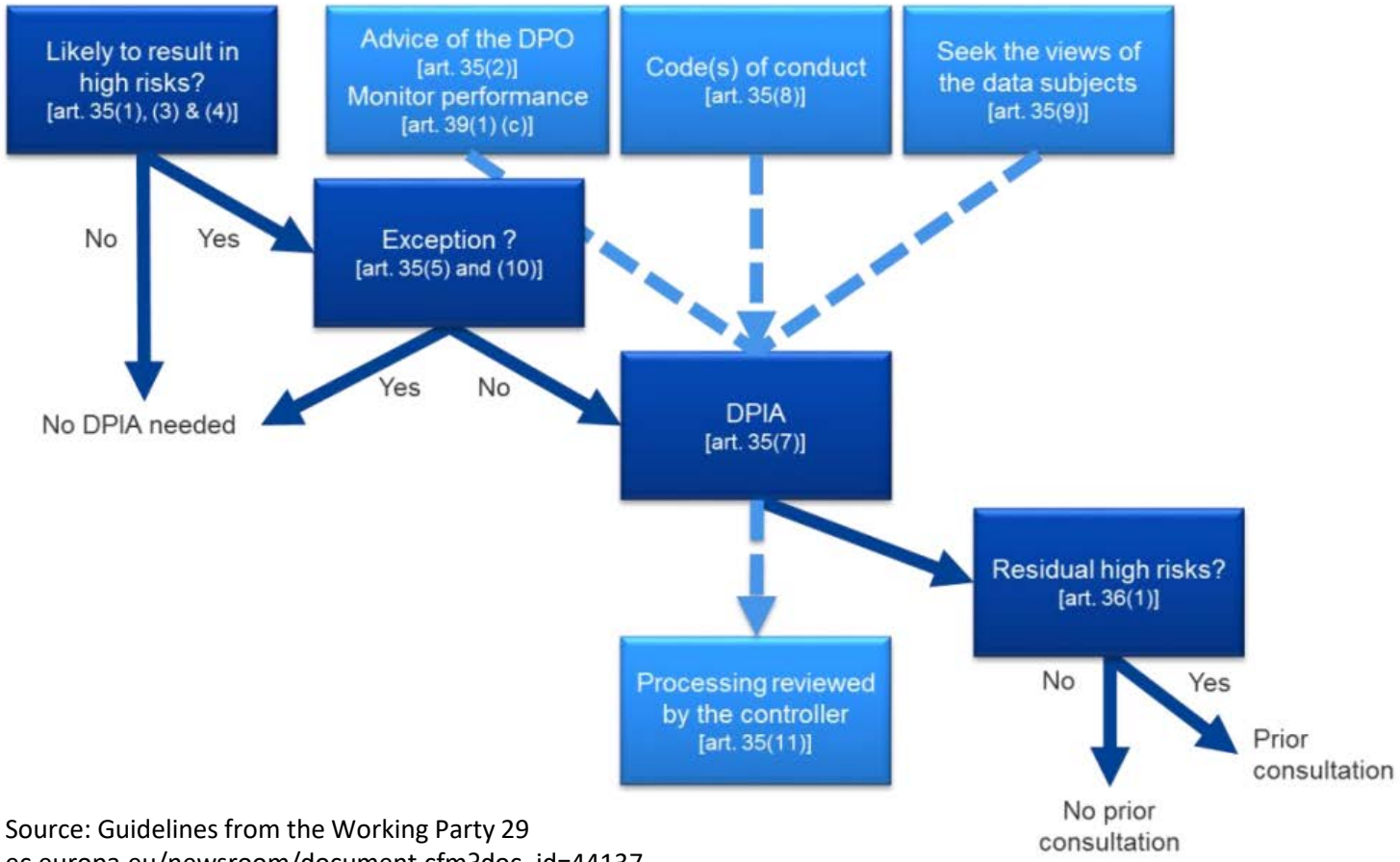
Yes → DPO mandatory

No → DPO not required* → Are you subject to other laws that could require a DPO (e.g. member state legislation)?

Even if the appointment of a DPO is not mandatory for your organization, you may still want to consider a voluntary appointment of a DPO (accountability).

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Run a Privacy Impact Assessment (PIA) ?



Source: Guidelines from the Working Party 29
ec.europa.eu/newsroom/document.cfm?doc_id=44137

Indicative check-list:

- Develop a standing procedure;
- Ensure a PIA is carried out when a new process is put in place within the organization;

U.S. COMMERCIAL SERVICE
United States of America Department of Commerce

Assess your international data transfers

Key questions to ask:

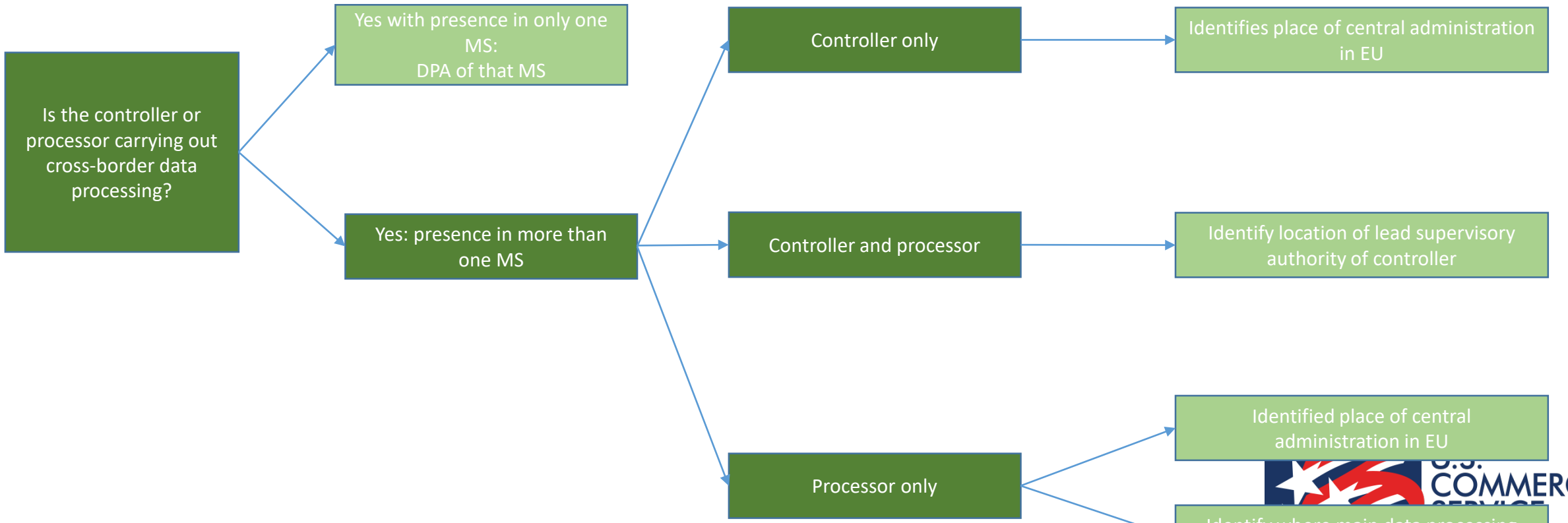
What type of data transfers are you doing? (e.g. HR, customer data?)
What mechanism are you using? Is your certification up-to-date?
Are you transferring European personal data to the U.S. and onwards?

Indicative check-list:

- You have the right legal basis to use that mechanism;
- You are meeting the necessary commitments (e.g. language in contractual agreements, privacy policy on your website);
- You are up-to-date on regulatory and legal developments in key jurisdictions;

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Identifying your DPA (for U.S. organizations with a physical presence in the EU)



U.S. COMMERCIAL SERVICE

of America
Commerce


Resources

USEACs & Foreign Commercial Service offices & market intelligence
https://www.export.gov/welcome

European Commission guidance:
http://ec.europa.eu/justice/smedataprotect/index_en.htm
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

DPA guidelines:
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360

U.S.-EU Privacy Shield:
https://www.privacyshield.gov/welcome

Find your DPA:
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

Keep an eye out for new guidance and national legislation…

U.S. COMMERCIAL SERVICE
United States *of* America
Department *of* Commerce

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Legal basis for processing personal data

You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 Consent

You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 Children

You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 International

If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico.
Information Commissioner's Office

ico.org.uk

Example of DPA guidance
(This does not constitute endorsement)

Source: UK DPA

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Questionnaire for GDPR implementation on 25 May 2018

Company/Controller	Receipt stamp Bavarian DPA

I. Structure and responsibility in the company

1. Is there an awareness in the company that data protection is management responsibility, e.g. by
   - Existence of data protection guidelines
   - Description of the data protection goals
   - Regulation of responsibilities
   - Awareness of data protection risks
   - Transparency of conflicts of objectives (e.g. between the marketing and the legal department)

2. Does your company have a data protection officer?
   - If not, why not?
   - If yes, is it clear in which cases he will be involved by whom?
   - If yes, has he already been reported to the competent supervisory authority according to Art. 37 para. 7 GDPR?

II. Overview of processing activities

1. Do you have records of your processing activities according to Art. 30 GDPR?
   - If not, why not? Is this documented?
   - How did you ensure that data protection issues are taken into account within your company upon commencement or modification of each processing activity (Privacy by Design – Art. 25 GDPR)?

III. Involvement of third parties

1. Do you engage third parties for the execution of your activities (processors)?
   - If yes, do you have an overview of your processors?
   - If yes, have you entered into the necessary agreements containing the minimum content of Art. 28 para. 3 GDPR with all your processors?

IV. Transparency, information duties and assurance of data subject rights

1. Have you adapted your texts providing information regarding data protection for data subjects in the course of data collection to the requirements of Art. 13 and 14 GDPR?
   - If not, why not?

2. Have you recently included in particular the following information, provided it had not been included before:
   - Contact details of the data protection officer
   - Legal basis for processing of personal data
   - If the purpose for processing data on your behalf or on behalf of third parties lies on legitimate interests: specify the legitimate interests
   - If you transfer data to third countries: the appropriate safeguards for the protection of the data applied by you (e.g. standard data protection clauses)
   - Retention period; if impossible to provide, specify the determination of the storage period.
   - Existence of the data subject's rights to access, to rectify, to erase, to restrict processing, to object on grounds of the particular situation of the data subject, and to data portability
   - If the legal basis for processing is consent: does the data subject has the right to withdraw the consent at any time
   - Right to lodge a complaint with a supervisory authority
   - Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract
   - If relevant: the execution of automated decision making, including profiling, and, in this case, information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Questionnaire for GDPR implementation on 25 May 2018

   - If you have not obtained personal data from the data subject: from which source the personal data originates, and if applicable, if it comes from publicly accessible sources
   - Have you adapted your marketing consents for customers, prospective customers etc. to the requirements of Art. 7 and Art. 13 GDPR (in particular: extended information duties, also regarding the right to withdraw the consent at any time)?

3. Have you established a procedure in order to promptly and completely satisfy requests for access to the personal data by the data subject according to Art. 15 GDPR (Art. 12 para. 1 GDPR)?

4. Have you established procedures in order to satisfy requests for data portability by the data subject (Art. 20 GDPR)?

V. Accountability, risk management

1. Is there information about each processing activity which serves to prove the lawfulness of processing, e.g. concerning purposes, categories of personal data, recipients and/or deletion periods (Art. 5 para. 2 GDPR)?
   - Have you assessed if the consents on which your processing is based still complies with the requirements of Art. 7 and/or Art. 8 GDPR??
   - Can you demonstrate that consent has been given?

2. Have you installed a data protection management system in order to ensure and be able to prove that your processing is in compliance with the GDPR (Art. 24 para.1 GDPR)?

3. Have you adapted your existing security review processes to the new requirements of Art. 32 GDPR?
   - Have you, in particular, replaced existing checklists for the selection of technical and organisational measures with a risk-oriented approach based on the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms?
   - Is an appropriate management system implemented for the regular review, assessment and improvement of security measures?
   - Are protective measures implemented such as pseudonymisation and the use of cryptographic procedures for the protection against unauthorised or unlawful processing done by both external and internal "attackers"?

4. Have you prepared for the possible necessity to conduct a data protection impact assessment?
   - Have you established an appropriate method in your enterprise for determining if a data protection impact assessment has to be conducted?
   - Have you established an appropriate risk method in your enterprise for the conduct of a data protection impact assessment? Have you chosen a process for the data protection impact assessment; have you already tested it?

VI. Data breaches

1. Have you ensured that the notification of a personal data breach to the supervisory authority can be performed within 72 hours according to Art. 33 GDPR?
   - Have you ensured in particular that data breaches in your enterprise can be identified? Have you established an appropriate method in your enterprise to determine a risk or a high risk?
   - Have you established a process on how to handle potential breaches internally?
   - Have you determined who communicates when and how with the supervisory authority?

Correctness of information provided above is confirmed		
Date	Management	Data protection officer (if applicable)

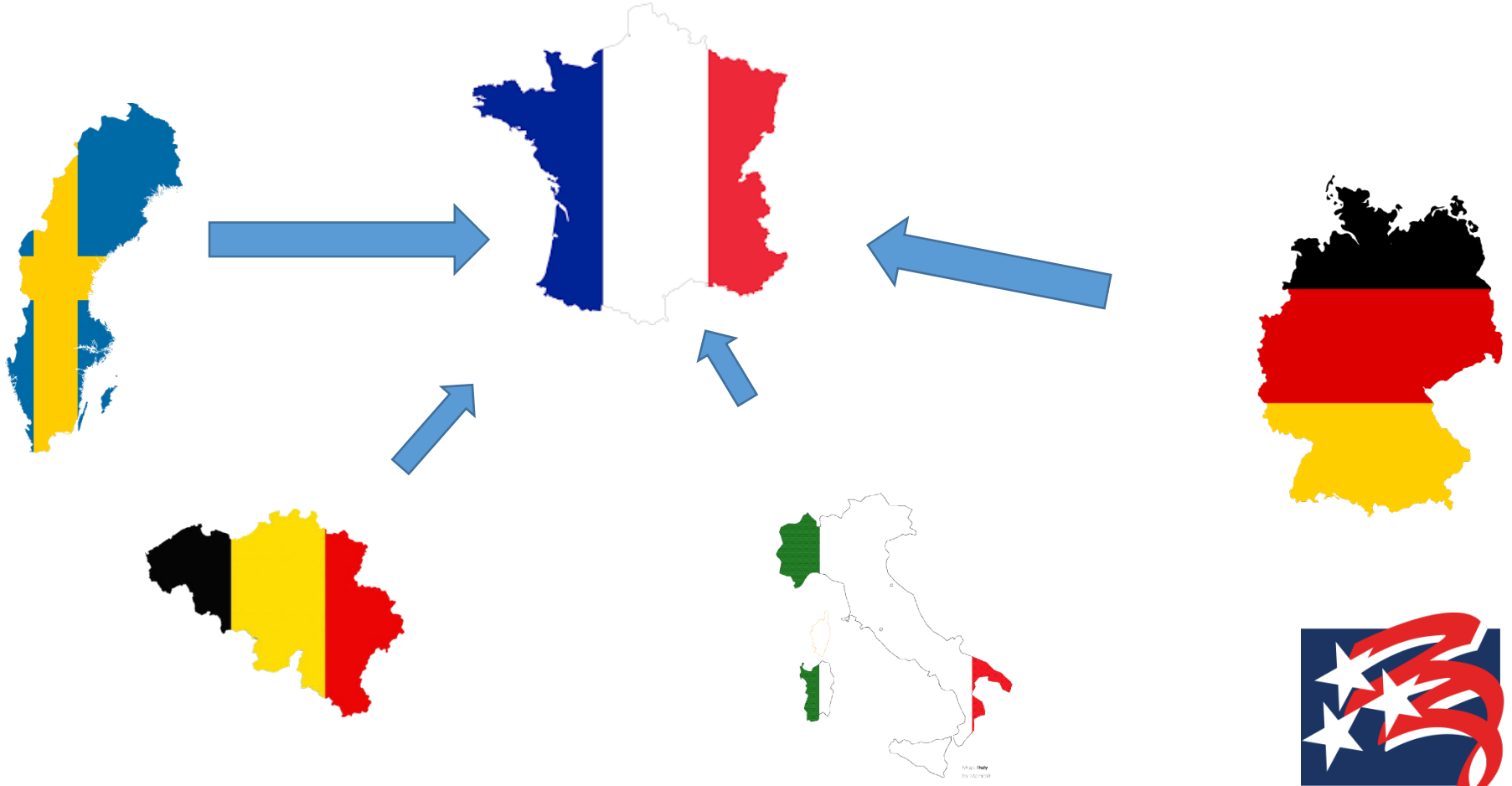
Example of DPA guidance
(This does not constitute endorsement)

Source: DPA Bavaria

U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

Back-up slides

One-Stop-Shop (aka Consistency Mechanism)
example



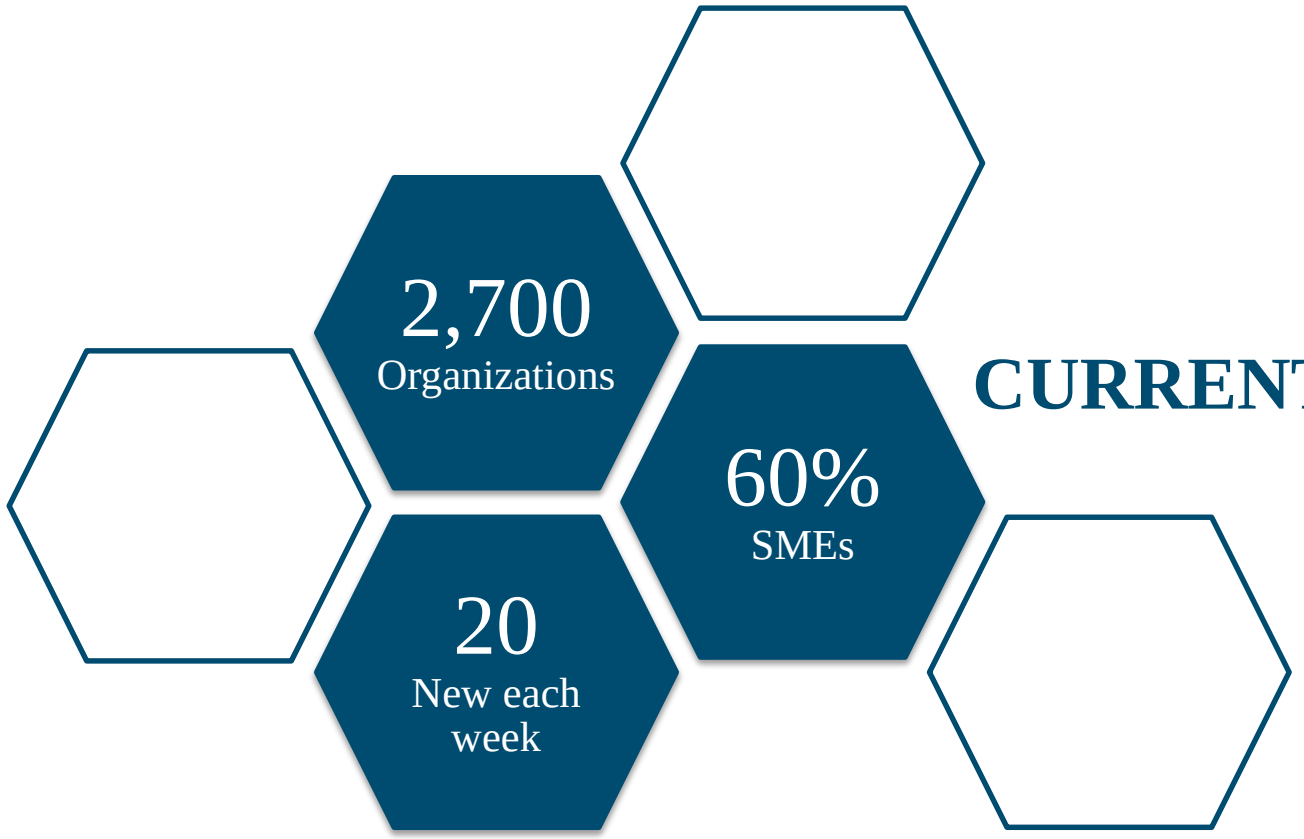
U.S. COMMERCIAL SERVICE
United States of America
Department of Commerce

INTERNATIONAL TRADE ADMINISTRATION

The Privacy Shield

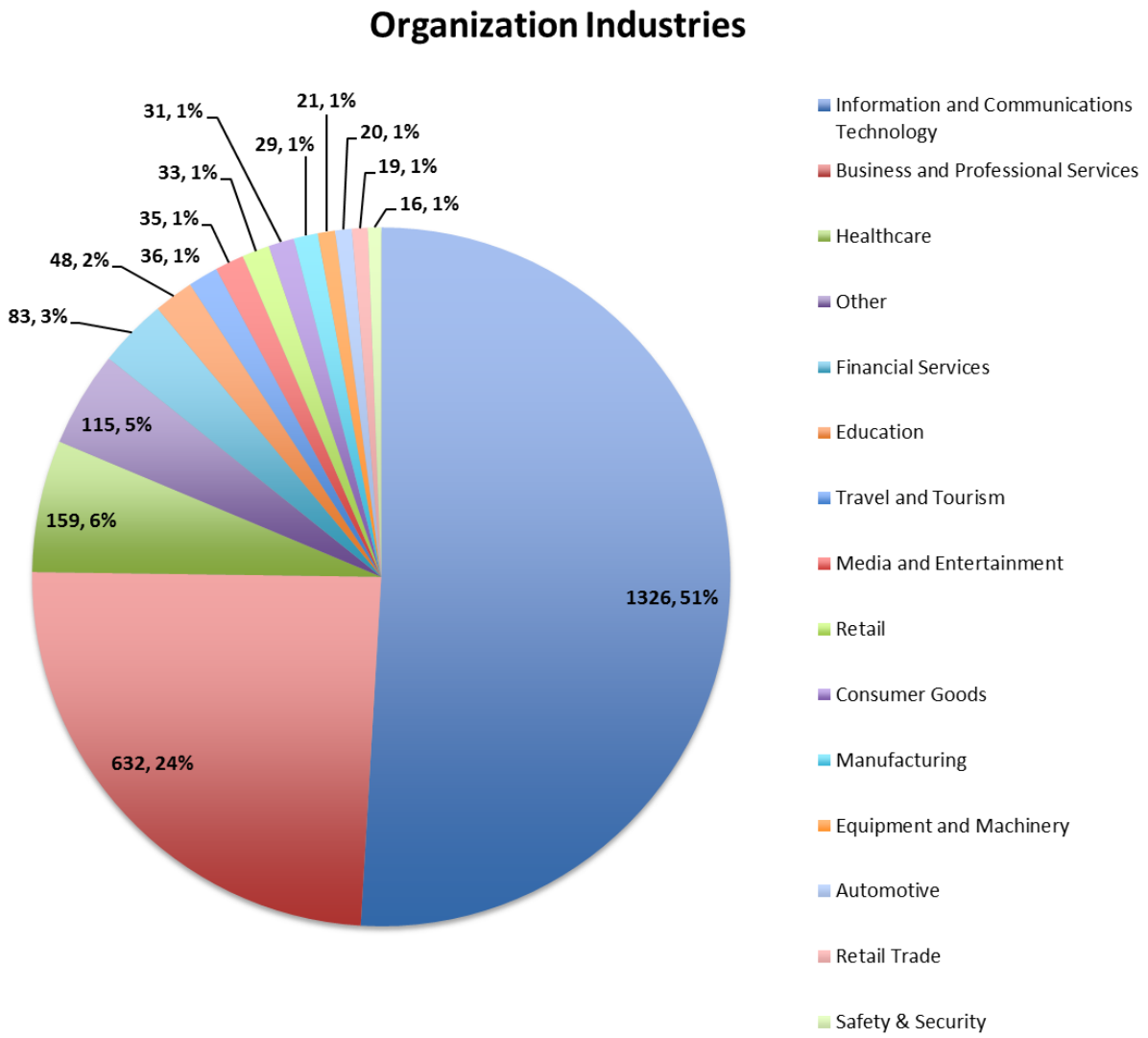

$400B
in digitally-deliverable services exported from U.S.
Services exports accounts for
1/6
of U.S. goods and services exports
3.2B
connected to the internet worldwide

PRIVACY SHIELD: Overview



CURRENT STATISTICS

PRIVACY SHIELD: Overview



PRIVACY SHIELD: How to Prepare

New Website and Resources: www.privacyshield.gov

- Resources Available:
  - Privacy Policy FAQ
  - New Requirements FAQ
  - Webinars
  - Payment Information

PRIVACY SHIELD: Principles

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement, and Liability

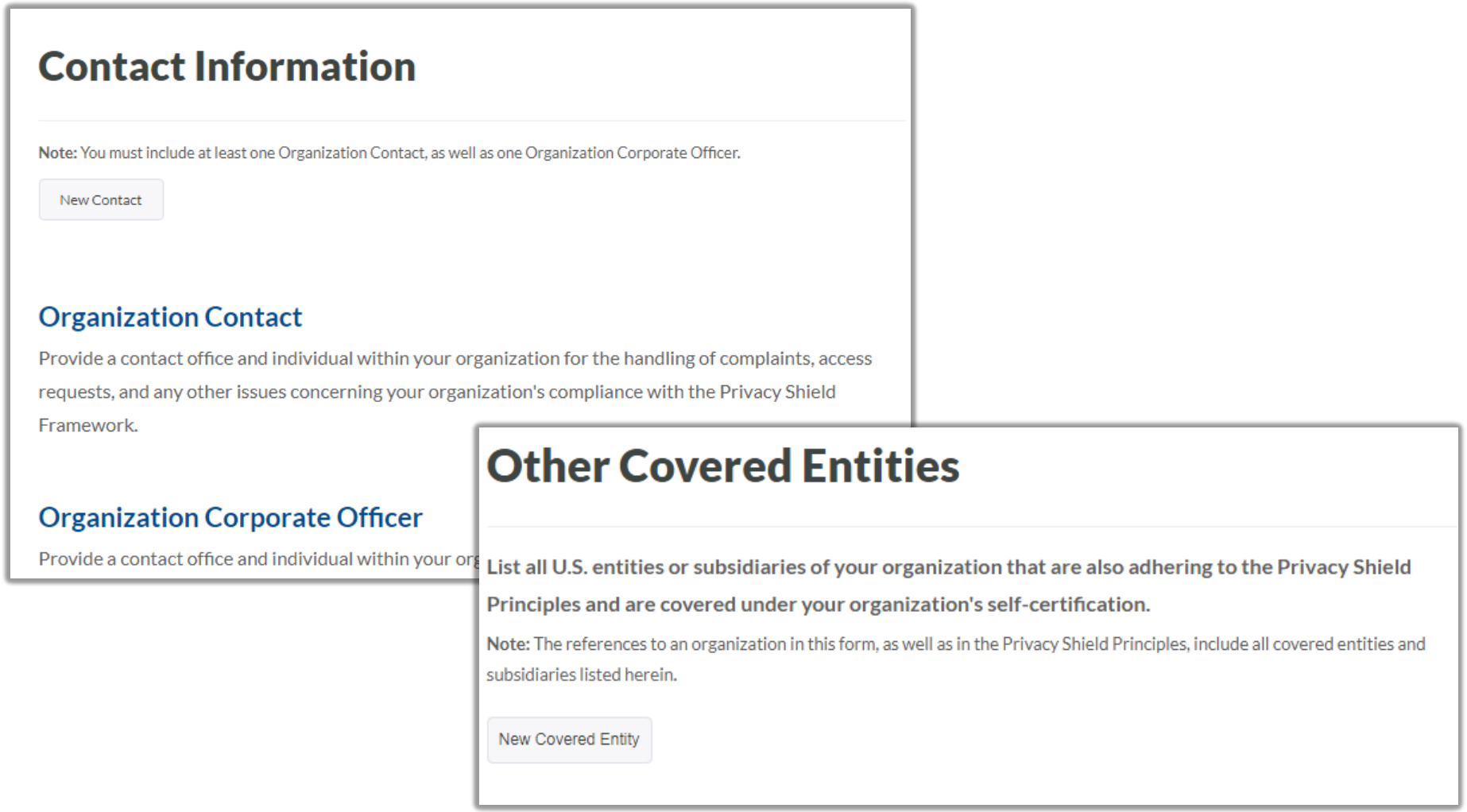
PRIVACY SHIELD: Notice Principle

1. NOTICE

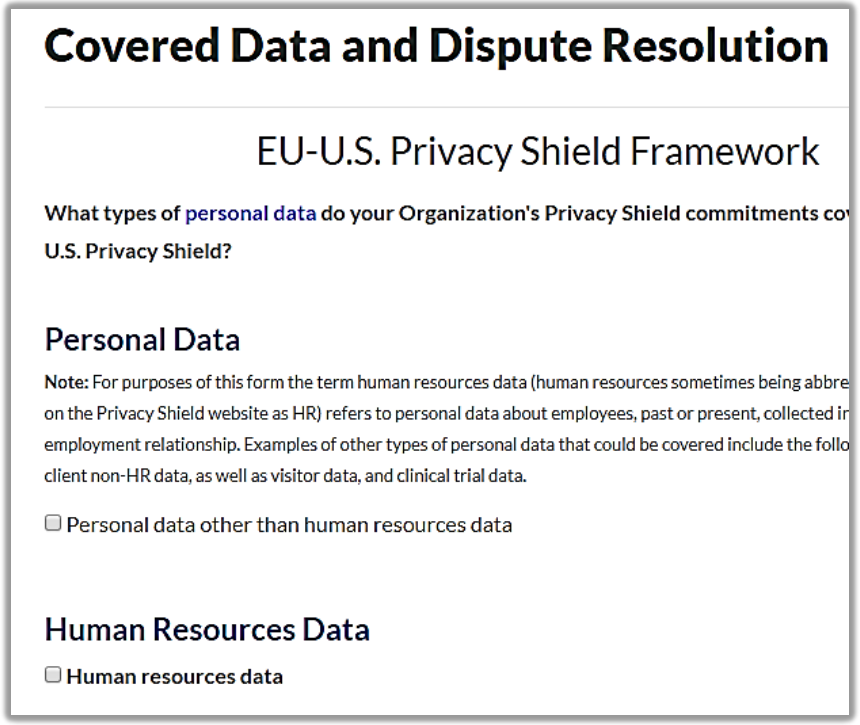
a. An organization must inform individuals about:

- i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,
- ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,
- iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,
- iv. the purposes for which it collects and uses personal information about them,
- v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,
- vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

PRIVACY SHIELD: Application Overview



PRIVACY SHIELD: Application Overview



Covered Data and Dispute Resolution

EU-U.S. Privacy Shield Framework

What types of personal data do your Organization's Privacy Shield commitments co
U.S. Privacy Shield?

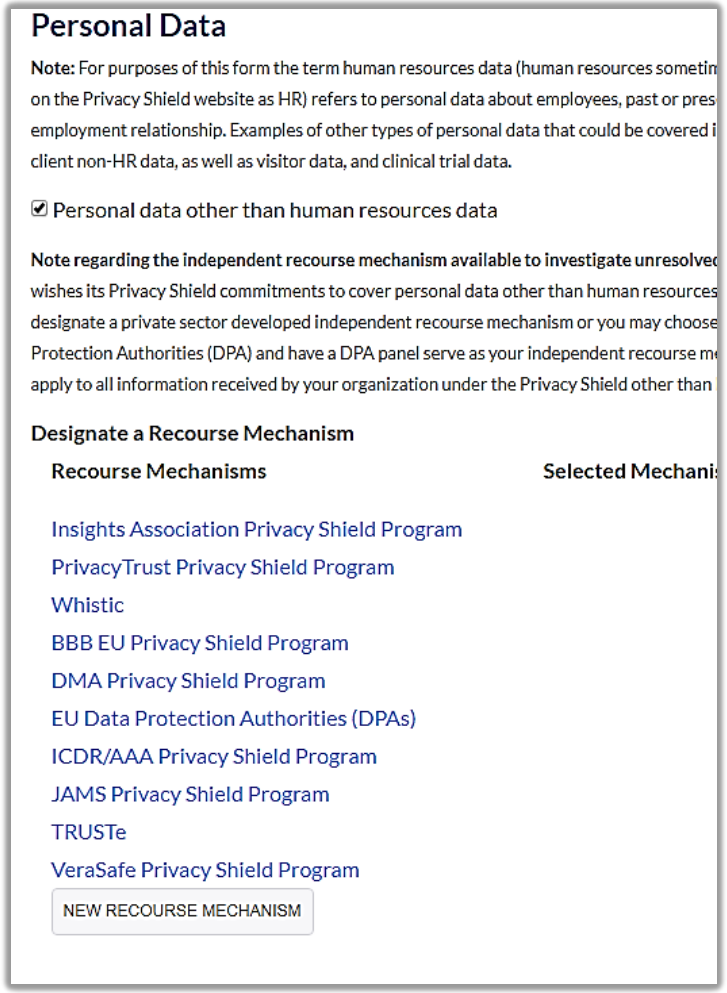
Personal Data

Note: For purposes of this form the term human resources data (human resources sometimes being abbre
on the Privacy Shield website as HR) refers to personal data about employees, past or present, collected ir
employment relationship. Examples of other types of personal data that could be covered include the follo
client non-HR data, as well as visitor data, and clinical trial data.

☐ Personal data other than human resources data

Human Resources Data

☐ **Human resources data**



Personal Data

Note: For purposes of this form the term human resources data (human resources sometim
on the Privacy Shield website as HR) refers to personal data about employees, past or pres
employment relationship. Examples of other types of personal data that could be covered i
client non-HR data, as well as visitor data, and clinical trial data.

☑ Personal data other than human resources data

Note regarding the independent recourse mechanism available to investigate unresolved
wishes its Privacy Shield commitments to cover personal data other than human resources
designate a private sector developed independent recourse mechanism or you may choose
Protection Authorities (DPA) and have a DPA panel serve as your independent recourse m
apply to all information received by your organization under the Privacy Shield other than

Designate a Recourse Mechanism

Recourse Mechanisms **Selected Mechani**

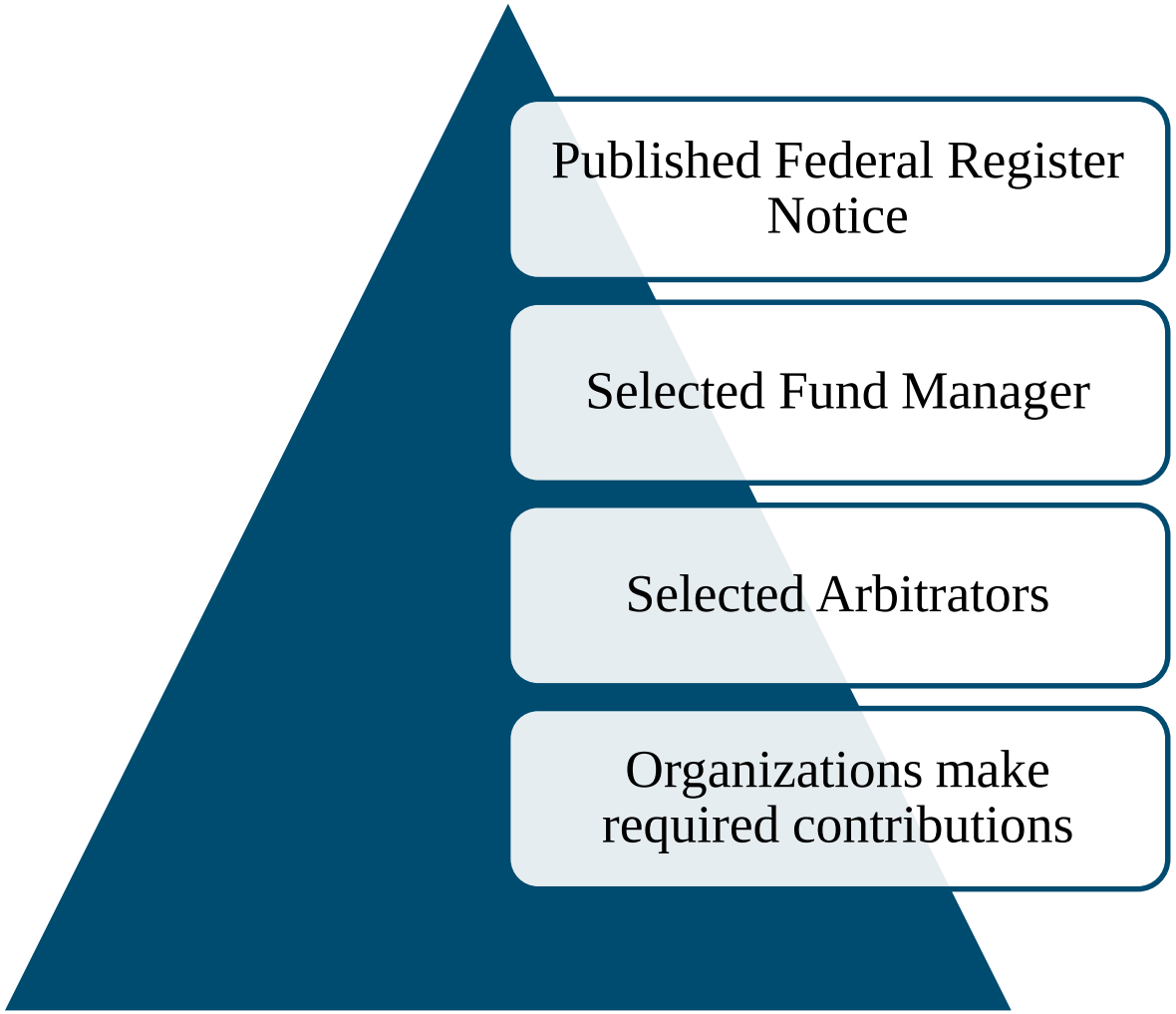
Insights Association Privacy Shield Program
PrivacyTrust Privacy Shield Program
Whistic
BBB EU Privacy Shield Program
DMA Privacy Shield Program
EU Data Protection Authorities (DPAs)
ICDR/AAA Privacy Shield Program
JAMS Privacy Shield Program
TRUSTe
VeraSafe Privacy Shield Program

NEW RECOURSE MECHANISM

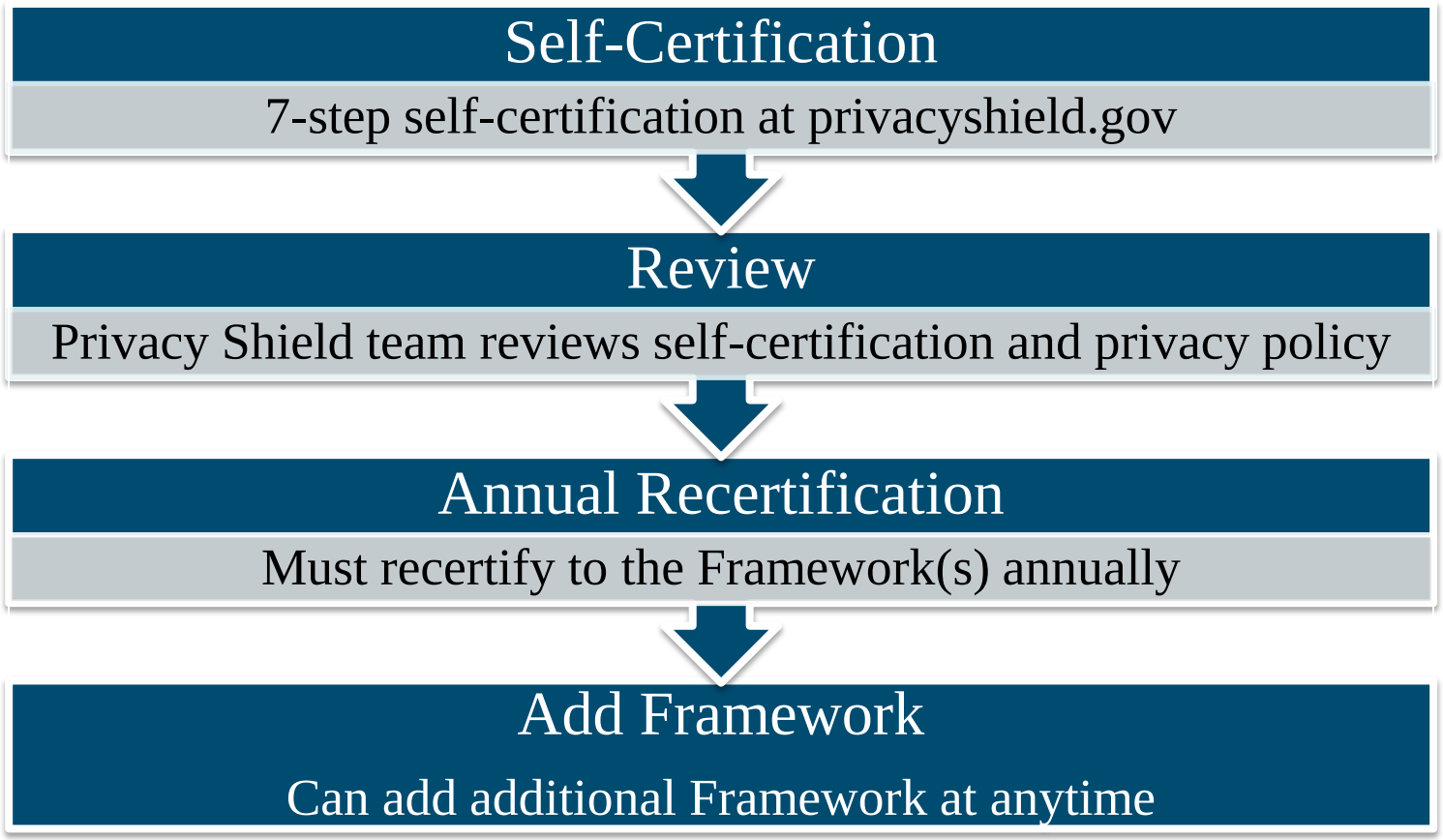
PRIVACY SHIELD: Self-Certification Fees

Organization's Annual Revenue:	Single Framework/Both Frameworks:
$0 to $5 million	$250/$375
Over $5 million to $25 million	$650/$975
Over $25 million to $500 million	$1,000/$1,500
Over $500 million to $5 billion	$2,500/$3,750
Over $5 billion	$3,250/$4,875

PRIVACY SHIELD: Annex 1



PRIVACY SHIELD: Review Process



PRIVACY SHIELD: Public List

Participation

EU-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE

Original Certification Date: 11/6/2017

Next Certification Due Date: 11/6/2018

Data Collected: HR, NON-HR

Dispute Resolution

QUESTIONS OR COMPLAINTS?

If you have a question or complaint regarding the covered data, please contact Test Organization at:

First Name Last Name
Organization Contact
Test Organization
123 Main Street
Whoville, Florida 34711

email@email.com
Phone: (202) 555-8585

Privacy Shield organizations must respond within 45 days of receiving a complaint.

If you have not received a timely or satisfactory response from Test Organization to your question or complaint, please contact the independent recourse mechanism listed below

HR RECOURSE MECHANISM

EU Data Protection Authorities (DPAs)

NON-HR RECOURSE MECHANISM

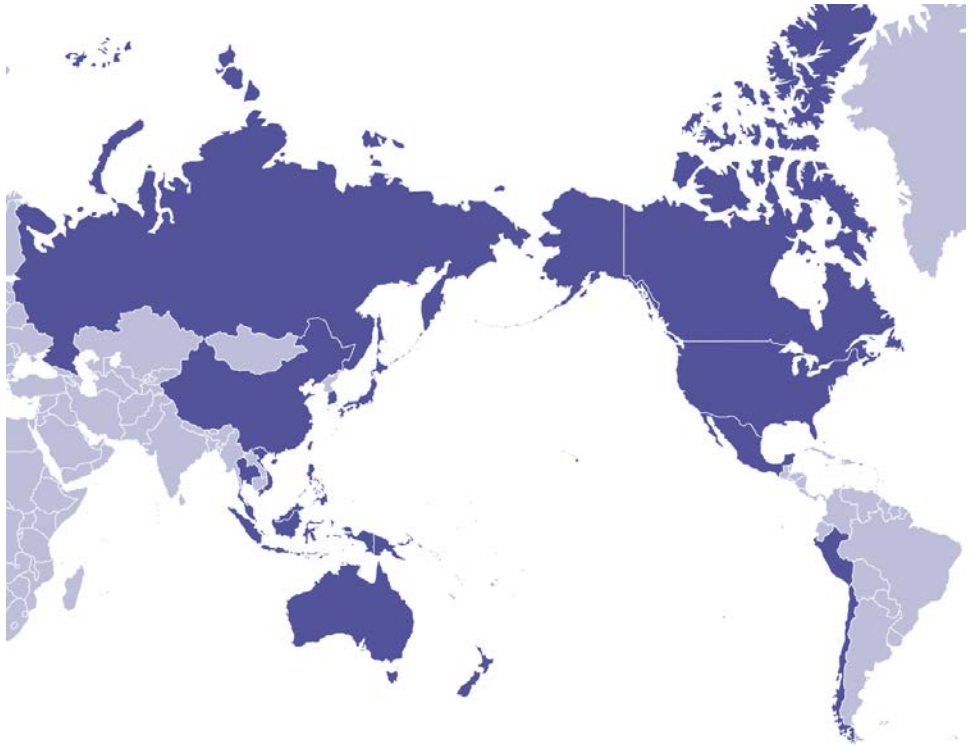
BBB EU Privacy Shield Program

Appropriate statutory body with jurisdiction to investigate any claims against Test Organization regarding possible unfair or deceptive practices and violations of laws or regulations covering privacy Department of Transportation

PRIVACY SHIELD: Updates

- The GDPR
  - Designed with an eye to GDPR
  - Continuity of adequacy determinations under the Directive
- Annual Review
  - End of September 2017

APEC CBPR: Overview



- Endorsed in 2011 by all 21 APEC Economies:

Australia	New Zealand
Brunei Darussalam	Papua New Guinea
Canada	Peru
Chile	Republic of Korea
China	Russia
Chinese Taipei	Singapore
Hong Kong	Thailand
Indonesia	The Philippines
Japan	The United States
Malaysia	Viet Nam
Mexico	

APEC CBPR: Overview

Current Participants

- **Six Participating Economies:**
  - United States, Canada, Mexico, Singapore, Republic of Korea, and Japan

Accountability Agents

- United States: TRUSTe
- Japan: JIPDEC

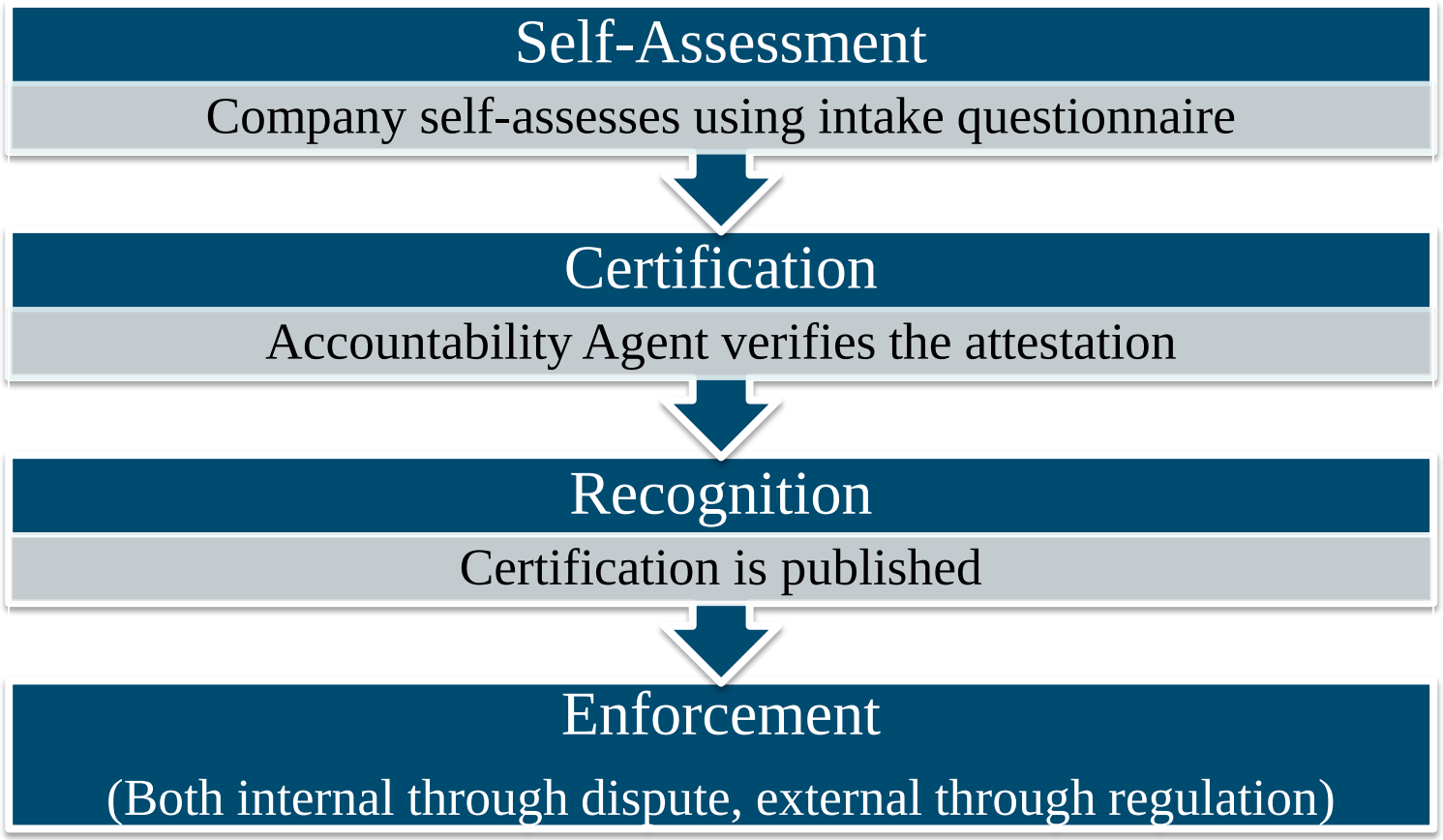
Next Steps

- Australia, Chinese Taipei, the Philippines noted intent to participate
- APEC CBPR – EU GDPR Interoperability

APEC CBPR: Privacy Framework

1. Preventing Harm
2. Notice
3. Collection Limitation
4. Uses of Personal Information
5. Choice
6. Integrity of Personal Information
7. Security Safeguards
8. Access and Correction
9. Accountability

APEC CBPR: Certification Process



THANK YOU!

CONTACT

Michelle Sylvester-Jose | michelle.sylvester-jose@trade.gov | 202-482-0396

RELEVANT WEBSITES

privacyshield.gov

cbprs.org

DORSEY™
always ahead

GDPR Challenges (and Opportunities!)
Some Practical Perspectives and Tips

Robert E. Cattanach, Partner
Dorsey & Whitney

Friday, March 23, 2018

Document Your Actions – Thoughtfully
EU Regulators' First Question: show us your plan

- **Acknowledge potential impact to your company**
- **Identify the right stakeholders to develop the plan to assess**
  - **It can't be just IT**
- **Consider benefits of protecting what follows through privilege**
  - **how GDPR impacts the company's data governance**
  - **what needs to be done to comply, and the priorities**
  - **who in management has been informed**
  - **how are you going to demonstrate compliance**

DORSEY™
always ahead

Be Careful Not to Create an Enforcement Road Map

- **Slide 49 questionnaire very helpful, but potentially also very dangerous**
- **Assume you will receive something like this sometime**
  - **be prepared to explain the “why not” answers**
  - **don’t memorialize other than through counsel**
- **Key exception: legal basis justification**
  - **collection**
  - **processing**

DORSEY™
always ahead

Questionnaire for Compliance (Slide 49)

- **Basic questions:**
  - **Awareness**
  - **Responsibility**
    - **DPO**
- **Disclosures and Consents**
- **Data subjects rights and requests**
- **Processing**
- **Third parties**
- **Data protection impact assessment**
- **Ability to demonstrate compliance**
- **Data breach preparedness**

DORSEY™
always ahead

Remember:
Significant Cultural and Structural Differences
Regulators Less Encumbered or Accountable

- **Checks and balances more muted in the EU than in US**
- **Only EU Parliament directly elected**
- **Culturally, very different balance between free enterprise and privacy**
- **Consequence: difficult to counterbalance natural tendency to regulate – Working Party 29 (enforcement regulators) has the last word as a practical matter**

DORSEY™
always ahead

GDPR Is Not the Unification Device It Originally Promised to Be

- **40 derogations (exceptions) - but generally only if more strict**
- **Enormous authority to Data Processing Authorities/Supervisory Authorities**
  - **Need to select based on criteria - can't forum-shop**
  - **Emerging as the "unsupervised" enforcer of GDPR in many instances**
- **Unknown impact: Working Party 29, to be replaced by European Data Protection Board (EDPB) on May 25th – *two months from now***
- **EDPB (Supervisors) fully independent versus WP 29 representatives representing each member state**
- **Member state DPAs remain powerful *in their respective member states***

DORSEY™
always ahead

What's the Future Look Like? Pendulum Is Still Swinging

- **Cambridge Analytica is gas on the fire powered by a blowtorch**
- **Being treated as a 'breach' even though no systems compromised**
- **Sensitive data definition of 'political opinion' could be expanded**
- **Crowd sourcing to fund test cases**
- **Expect harsh treatment of Facebook abroad *and at home* (Facebook made significant commitments 2011 FTC consent decree)**
- **Trickle down impact on all other companies collecting or processing personal data**
- **Continued erosion of trust by consumers**

DORSEY™
always ahead

GDPR Not Always Easily Reconciled with US law

- **One example: Breach notification**
- **GDPR requires 72 hours "unless unlikely to result in a risk to the rights and freedoms of natural persons"**
- **Demonstrates lack of any meaningful experience of EU regulators in breach responses**
- **It is IMPOSSIBLE to know whether the exception applies until more detailed forensics have been performed – typically takes *60 days***
  - **expect over-notifications**
  - **1000 in the first month of the Netherlands regulation becoming effective**
  - **Delaying notification in the US after notifying in the EU will invite regulatory scrutiny**
  - **Practical result is that the Supervisory Authority will assume control of the breach investigation process - turns the US model (and frankly common sense) on its head**

DORSEY™
always ahead

Where Are These So-Called Opportunities?

- **Ultimately, GDPR is simply good information governance**
  - **Knowing your data, where it flows, and who has access is no longer an option**
  - **As the 'risk flavor of the day', GDPR provides a compelling justification for much-needed compliance resources**
- **GDPR compliance will serve companies well going forward**
  - **Third-party vendor management challenges (up and down supply chain)**
  - **Cyberinsurance underwriting is becoming increasingly more robust**
- **Privacy by design, the heart of GDPR, reduces your risk**

DORSEY™
always ahead

Questions

Please contact:

Bob Cattanach
(612) 340-2873
cattanach.robert@dorsey.com

DORSEY™
always ahead