23 November 2024

EU Privacy + Security Law

Workshop

Privacy+ Security Forum

Speakers

Nikolaos Theodorakis

Partner
Wilson Sonsini - Brussels

Dr. Kai Westerwelle

Partner
CMS Law – Silicon Valley

23 November 2024

EU Privacy + Security Law

EU AI Act – Nik Theodorakis

Cross Border Data Transfer – Kai Westerwelle

Privacy+ Security Forum

Interactive

Privacy+ Security Forum

- ✓ We will make this **INTERACTIVE**
- ✓ We will do **CASES**
- ✓ We will initiate **DISCUSSSIONS**
- ✓ Please ask **QUESTIONS**

23 November 2024

EU Privacy + Security Law

EU AI Act – Nik Theodorakis

Cross Border Data Transfer – Kai Westerwelle

Privacy+ Security Forum

Agenda

1. EU AI Act
2. UK Approach to Regulating AI
3. Discussion

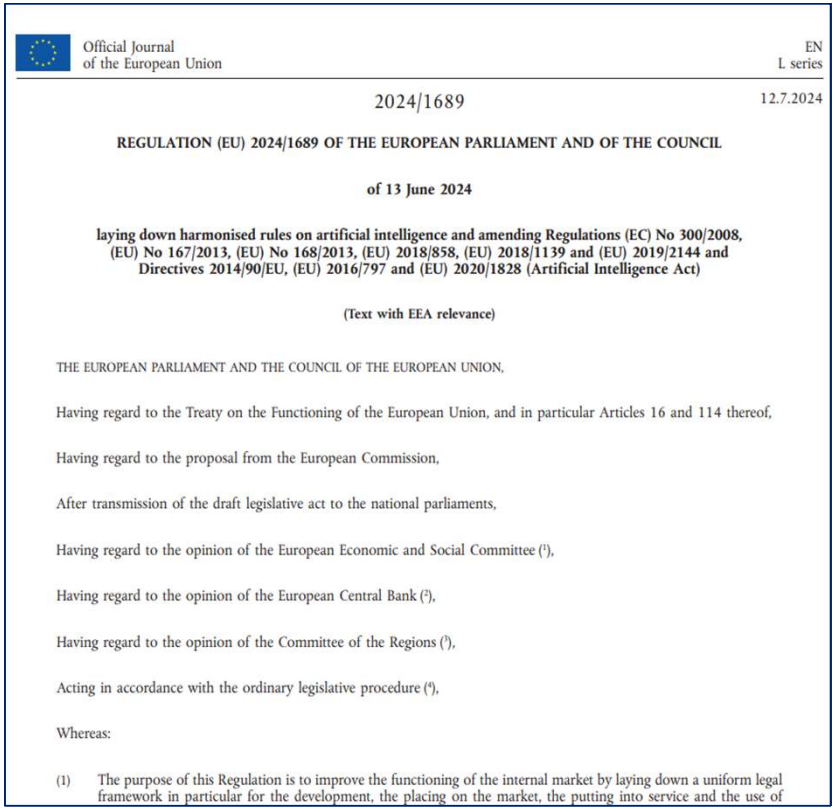
EU AI Act

Privacy+ Security Forum

What is the EU AI Act?

Privacy+ Security Forum

- The AI Act is a **regulation for artificial intelligence** in the EU.
- It is a **risk-based horizontal framework** and its scope. **encompasses all sectors**, and all types of AI.
- It has an **extra-territorial** scope of application.
- The requirements are modelled on **EU product safety law**.
- The AI Act entered into force on August 12, 2024. Requirements will start to apply in phases, primarily over the next 3 years.



Official Journal of the European Union — EN L series

2024/1689 — 12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the European Central Bank [2],

Having regard to the opinion of the Committee of the Regions [3],

Acting in accordance with the ordinary legislative procedure [4],

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of

EU AI Act : 8 Key Points to Know

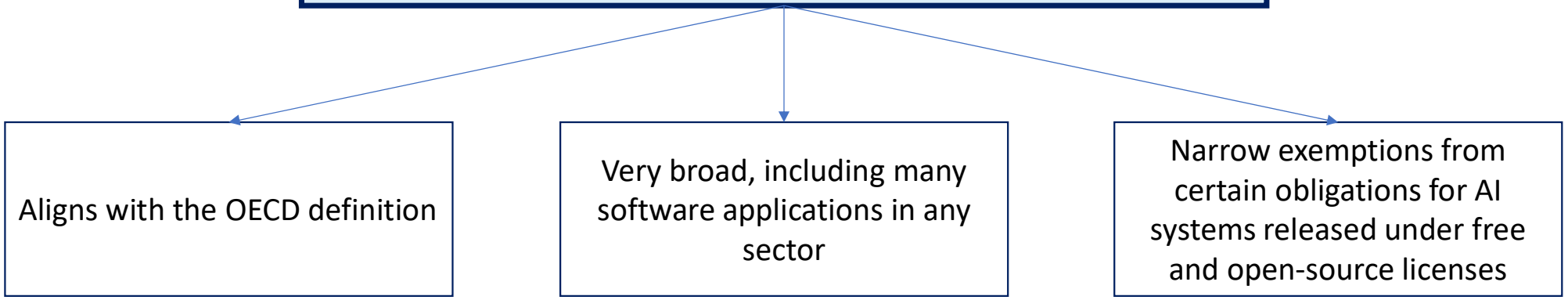
Privacy+ Security Forum

1. Broad, extra-territorial scope
2. Does not apply to areas outside of EU law
3. Applies to actors throughout the AI supply chain
4. Horizontal / cross-sector approach
5. Bans certain applications of AI
6. Majority of obligations focused on high-risk applications of AI
7. Transparency obligations for AI that poses specific risks
8. Separate obligations for providers of general purpose AI

What is an AI System?

Privacy+ Security Forum

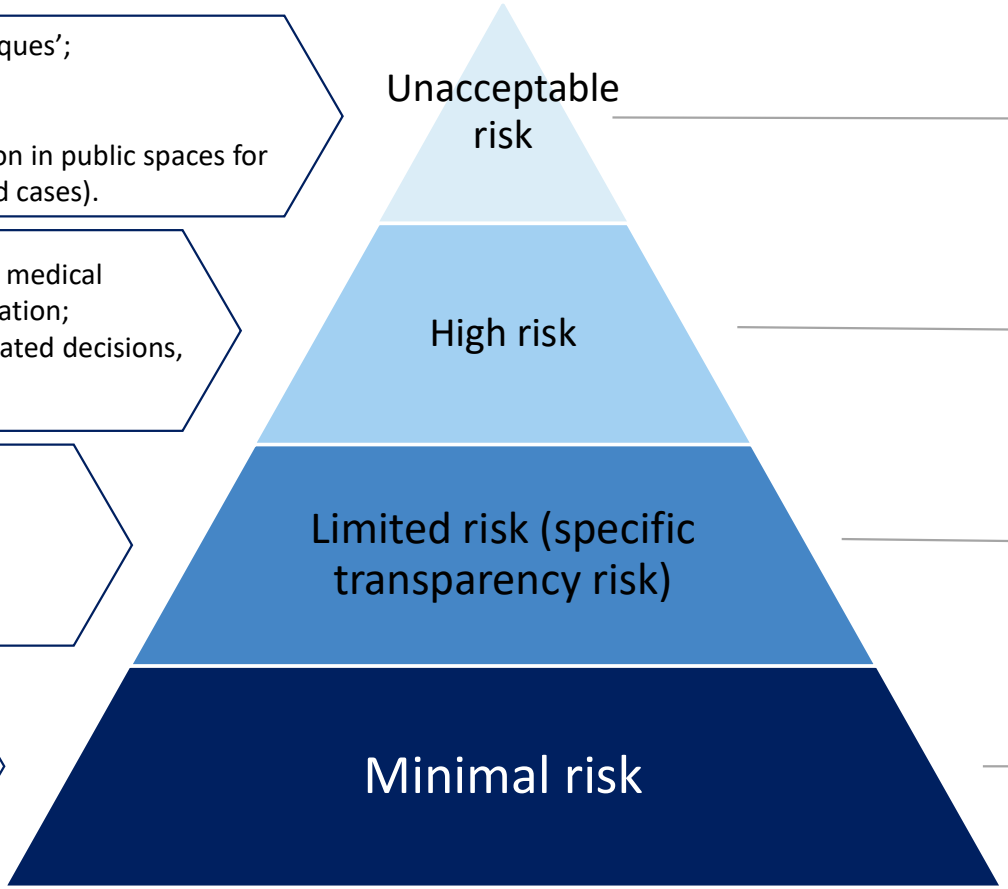
'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments; *(Art. 3(1) AI Act)*



AI Act Risk-Based Approach

Privacy+ Security Forum

- Harmful manipulative ‘subliminal techniques’;
- Exploit specific vulnerable groups;
- Social scoring;
- Real-time’ remote biometric identification in public spaces for law enforcement (allowed in very limited cases).



Banned

- Products with health or safety risks e.g., medical devices, radio equipment, cars, toys, aviation;
- AI for assessing creditworthiness, HR related decisions, remote biometric identification, etc.

Documentation and internal processes

- Chatbots, deep fakes, emotion recognition (that is not prohibited).

Transparency

- Video games, spam filters.

No obligations under the AI Act

Tiered Rules for GPAI

General Purpose AI (GPAI)	*Systemic Risk GPAI*
Models trained with large amounts of data, that display significant generality (presumed if +1B parameters) which can be integrated in a variety of downstream systems.	GPAI models that have "high impact capabilities" (presumed if trained using a total computing power of more than 10^25 FLOPs). Unless there are no foreseeable risks to health, safety, security etc. The AI Office may specify other criteria for systemic risk GPAI. E.g., OpenAI's Chat GPT 4 or likely Google DeepMind's Gemini.

Transparency obligations apply to all GPAI (excl. open source) and systemic risk GPAI (inc. open source):

- Draw up technical documentation;
- Share documentation with companies who integrate the GPAI into their systems;
- Comply with EU copyright law;
- Publish detailed summaries of content used for training.

Example additional measures that only apply to systemic risk GPAI:

- Assess systemic risks at EU level;
- Incident reporting;
- Red-teaming;
- Cybersecurity requirements;
- Reporting on the model's energy consumption.

Prohibited AI Systems

Privacy+ Security Forum

AI systems that **manipulate or exploit individuals' vulnerabilities**

AI systems that perform **social scoring**

Untargeted scraping of facial images from the internet or CCTV footage

Emotion recognition systems used at the **workplace or in educational institutions** (excl. for medical or safety reasons)

Biometric systems that categorize people to infer sensitive data, such as sexual orientation or religious beliefs

Certain applications of **predictive policing**

Facial recognition for law enforcement purposes in publicly accessible areas (allowed in very narrow cases, e.g., to prevent terrorist attacks, subject to additional safeguards)

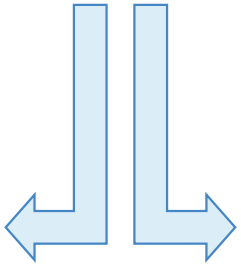
High-Risk AI Systems

Privacy+ Security Forum

Two ways for an AI system to qualify as “high-risk”:

The **AI System is (integrated into) a safety product, that is subject to other EU safety legislation**, for example:

- Medical devices
- In vitro medical devices
- Components of lifts
- Radio equipment
- Civil aviation
- Agricultural and forestry equipment



The **AI system is intended to be used for a defined “high-risk application”**, such as:

- ‘Real-time’ and ‘post’ remote biometric identification systems e.g., airport security or fingerprint recognition for smartphone access
- Safety component in management and operation of critical infrastructure e.g., autonomous traffic management system for smart cities
- To determine access to education e.g., making decisions about university admission
- For recruitment e.g., placing targeted job ads
- Emotion recognition e.g., voice analysis
- Border control management e.g., assessing security risk of incoming travelers

Requirements for High-Risk AI Systems

Privacy+ Security Forum

Accuracy, Robustness and Cybersecurity

Implement reasonable accuracy, robustness and cybersecurity safeguards.

Human Oversight

Implement controls to ensure that humans can oversee the AI systems.

Transparency to Deployers

Ensure the AI system is designed and developed in a way that makes its functioning transparent and allows deployers to use it appropriately.

Registration

Register a high-risk AI system before it is released in the EU.

Risk Management System

Establish and maintain a comprehensive risk management system.

Technical Documentation

Draft technical documentation of the AI system before it is released and update it as necessary.

Data & Data Governance

Training data must comply with quality criteria in the AI Act. There must be a data governance and management approach to training data.

Record Keeping

Ensure that the AI system automatically records logs.

Obligations for Providers and Deployers of High-Risk AI Systems

Providers and deployers of AI must comply with certain obligations when developing or using high-risk AI.

Providers are individuals or entities that develop an AI system and place it on the market or into service under their own name or trademark.

- Obligations for providers include:
  - Establish and maintain quality management system;
  - Conduct conformity assessment;
  - Document retention;
  - Incident notification;
  - Post-market monitoring.

Deployers are individuals or entities that use AI systems (exception for personal non-professional use).

- Obligations for deployers include:
  - Use the AI system in accordance with its instructions;
  - Notify serious incidents to providers;
  - Where the deployer controls data input, they must ensure that the data is relevant and sufficiently representative;
  - Monitor the functioning of the AI system.

Specific Transparency Risk Obligations

Deep fakes and other AI-generated content must be labelled as such.

Individuals must be informed when biometric categorization or emotion recognition is being used.

Synthetic audio, text, video and image content will need to be marked in a machine-readable format and be detectable as artificially generated or manipulated.

Transparency obligations for generative AI e.g., chatbots.

Conformity Assessments for High-Risk AI

Privacy+ Security Forum

What is it?	• The process of **demonstrating that a high-risk AI system fulfils the requirements** for high-risk AI systems in the AI Act.
Who is subject to it?	• **Providers of high-risk AI** i.e., individuals or companies that develop a high-risk AI system and place it on the market or into service in the EU under their own name or trademark.
When does it need to be performed?	• **Before the AI system is placed on the market or put it into service in the EU.** • **Must be repeated before making a "substantial change"** to the AI system e.g., change of operating system or software architecture.

Who conducts the assessment?	• Depending on the context of the AI system:
	  • The provider conducts the conformity assessment **internally**.
	  • A **third-party body** designated by the national regulator.

What is being assessed?	• The **quality management system and technical documentation** for the AI system.

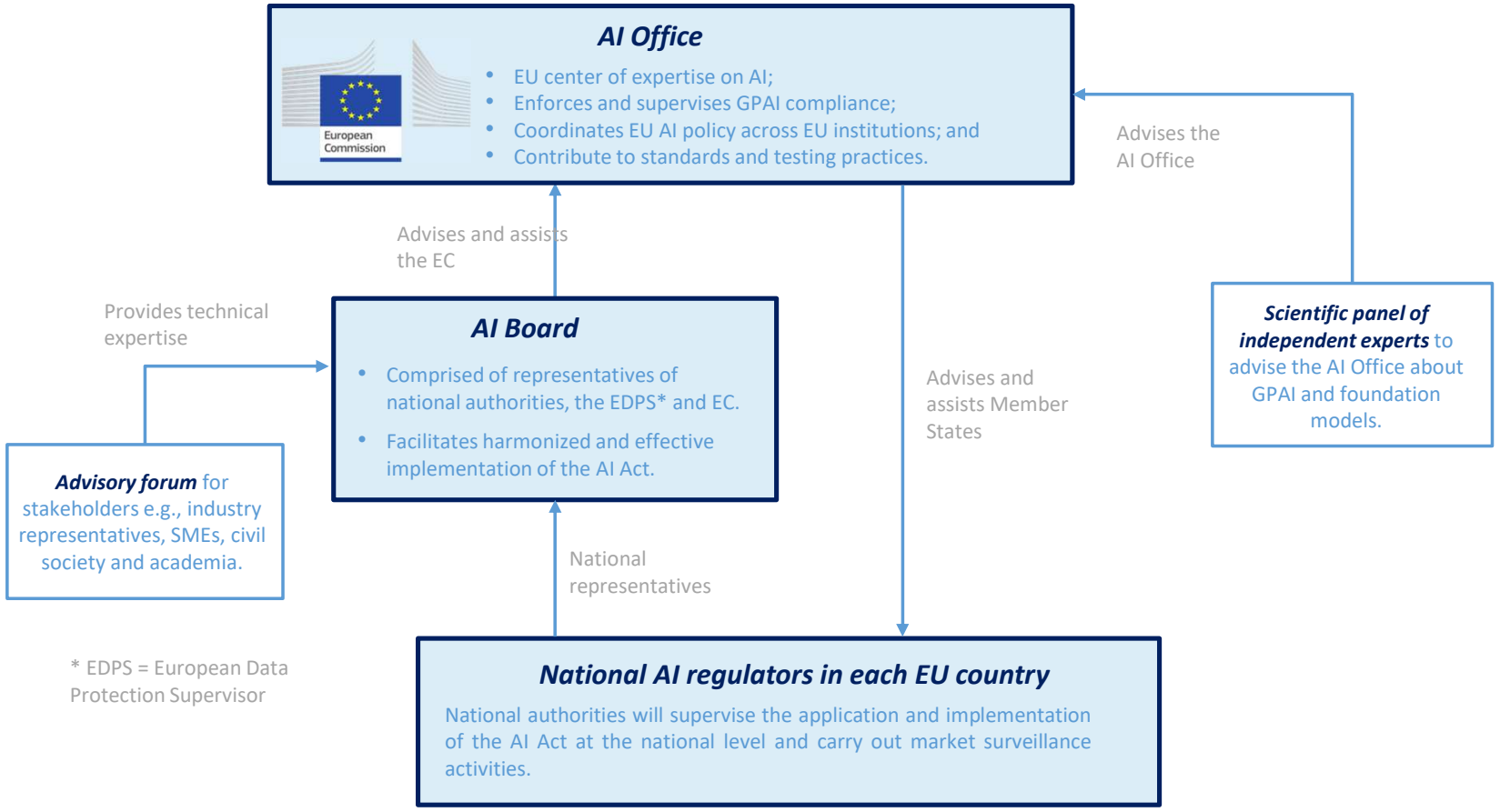
Conformity Assessments for High-Risk AI

Privacy+ Security Forum

High Penalties

Up to **EUR 35 mil. or 7% total worldwide annual turnover** for preceding financial year (for violations of banned AI provisions).

Up to **EUR 15 mil. or 3% total worldwide annual turnover** for preceding financial year (for violations of all other AI provisions).



Timeline for Phased Application of the AI Act

Privacy+ Security Forum

AUGUST 1 2024	FEBRUARY 2 2025	AUGUST 2 2025	AUGUST 2 2026	AUGUST 2 2027	AUGUST 2 2030
EU AI Act entered into force	Prohibition of certain AI systems + AI literacy requirements	Requirements for new GPAI models	Requirements for some high-risk AI systems + Requirements for AI systems with specific transparency risk	Requirements for existing GPAI models and high-risk AI systems subject to EU health and safety laws	Requirements for existing high-risk AI systems intended to be used by public authorities
					

UK Approach to AI

Privacy+ Security Forum

UK Approach to AI Regulation: 4 Key Points

Privacy+ Security Forum

Flexible, non-legislative approach	Key regulators have published their strategic approach to AI
In 2023, the UK Government published its AI Regulation White Paper which outlined a **principles-based and non-legislative approach to regulating AI**.	In April 2024, **key sectoral regulators** including the data protection regulator (ICO), Financial Conduct Authority (FCA) and the Medicines and Healthcare products and Regulatory Agency, were **tasked to present their own strategic approach to AI**.
Cross-sector collaboration between regulators is central	**Potential for AI legislation in the future**
The **Digital Regulation Cooperation forum brings together the ICO, Ofcom (online safety), FCA and the Competition Markets Authority**. AI is one of its focus areas for collaboration.	The **UK Government is monitoring the landscape, and may will introduce legislation** to regulate the largest AI models. To date no firm proposals or draft legislation has been introduced.

EU and UK: Comparing Approaches

Privacy+ Security Forum

	EU	UK
Legally binding?	Legally binding, **legislative** approach	Non-binding, and **principles based** – regulators are expected to develop non-binding guidance
Horizontal or vertical?	Horizontal, **cross-sectoral** application	Vertical, **sectoral** guidelines with cross-sector collaboration between regulators
Focus of the regulation	**Risk-based** and focused on the highest-risk applications of AI and development AI models	Focused on **proportionate** requirements that do **not inhibit innovation**
Institution responsible for AI safety and international cooperation	**EU AI Office** is responsible for monitoring the most advanced AI models and international cooperation for AI safety. Many national-level regulators are involved	**AI Safety Institute** established to focus on systemic risks posed by AI and international cooperation

Discussion

Privacy+ Security Forum

Questions for Discussion

Privacy+ Security Forum

- How can companies build on existing AI governance programs to comply with the AI Act?
- What are the first steps companies should take to approach complying with a new law with no existing guidance or precedent?
- Which requirements stand out as potentially the most challenging to comply with? How can companies approach these requirements?

Questions

Privacy+ Security Forum

23 November 2024

EU Privacy + Security Law

EU AI Act – Nik Theodorakis

Cross Border Data Transfer – Kai Westerwelle

Privacy+ Security Forum

Cross Border Data Transfer

Background: Data Transfers from Europe / UK
Consent
Standard Contractual Clauses
Binding Corporate Rules
Data Privacy Framework
Increasing Localization Requirements
Enforcements

Privacy+ Security Forum

Let's Play

Privacy+ Security Forum

International Data Transfer?

Privacy+ Security Forum

Do the following scenarios constitute Cross-Border Transfer of Personal Data?

1. Consumer Kai in Germany purchases a T-Shirt from the US based platform "Golf US". Golf US is an English language (only) website. Kai pays in EURO with no VAT added.

2. Student Nik from Belgium attends a virtual MBA program in Brussels. Speakers include experts lecturing from the US and Singapore.

3. Canadian company CCS offers "EU based" cloud services. The service is run on EU based servers with first level support in Ireland. 2nd level support is provided from CCS' HQ in Canada.

4. Company SPA (B2B only) in Spain is raising its series C. It offers customer and employee data for the due diligence of possible investors. A data room has been created by the international law firm L in Madrid. LawCloud Inc, the worldwide cloud service provider of L, has its servers in the US and Canada.

Cross Border Data Transfer

Background: Data Transfers from Europe / UK

Consent

Standard Contractual Clauses

Binding Corporate Rules

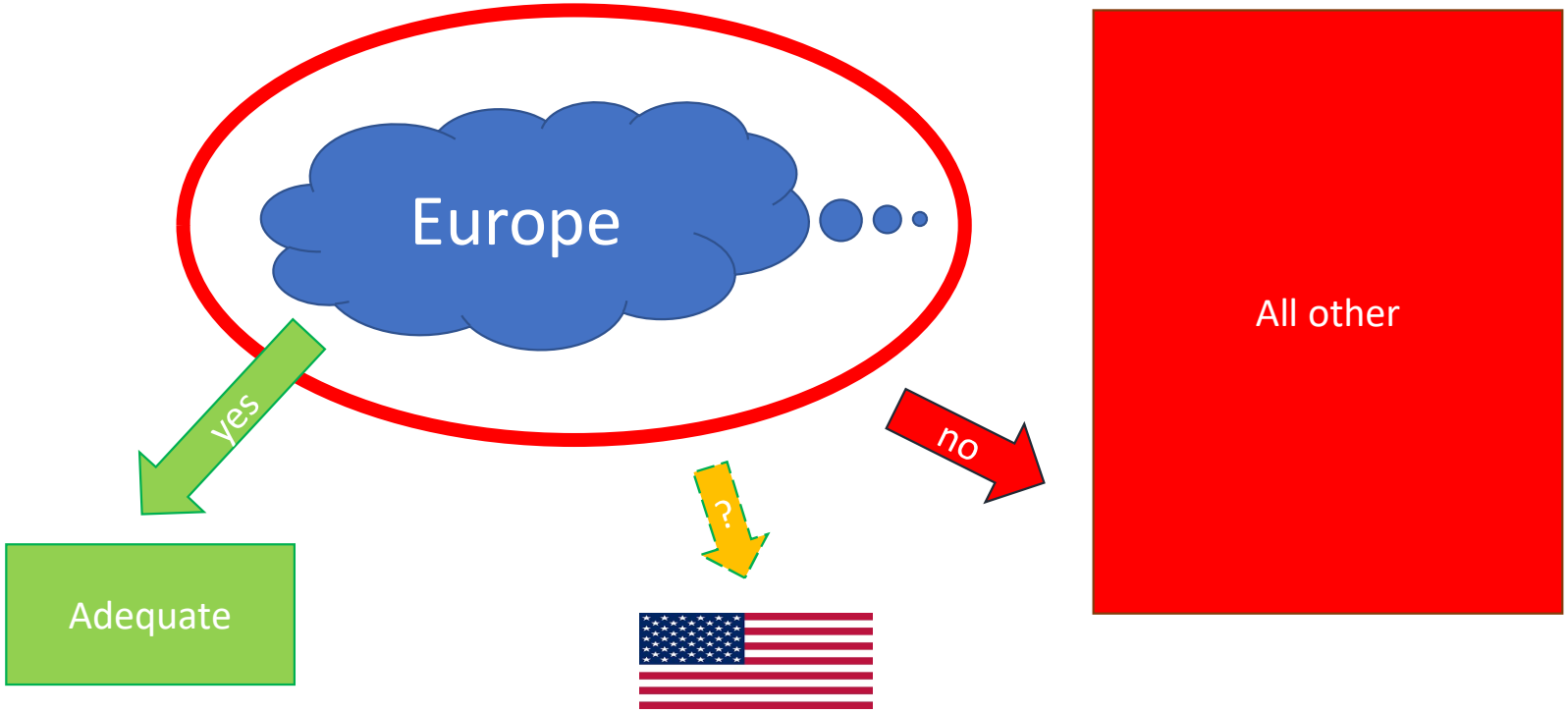
Data Privacy Framework

Increasing Localization Requirements

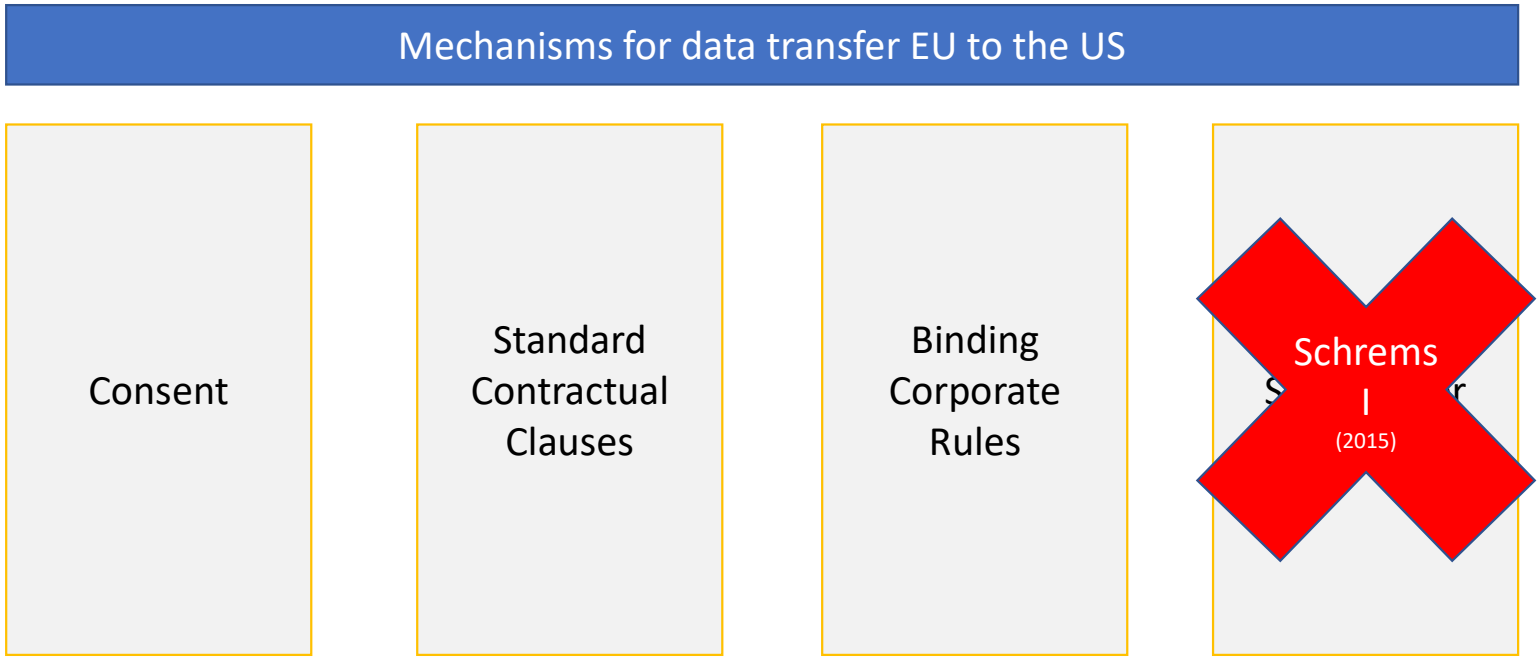
Enforcements

Privacy+ Security Forum

Data Transfers from Europe / UK



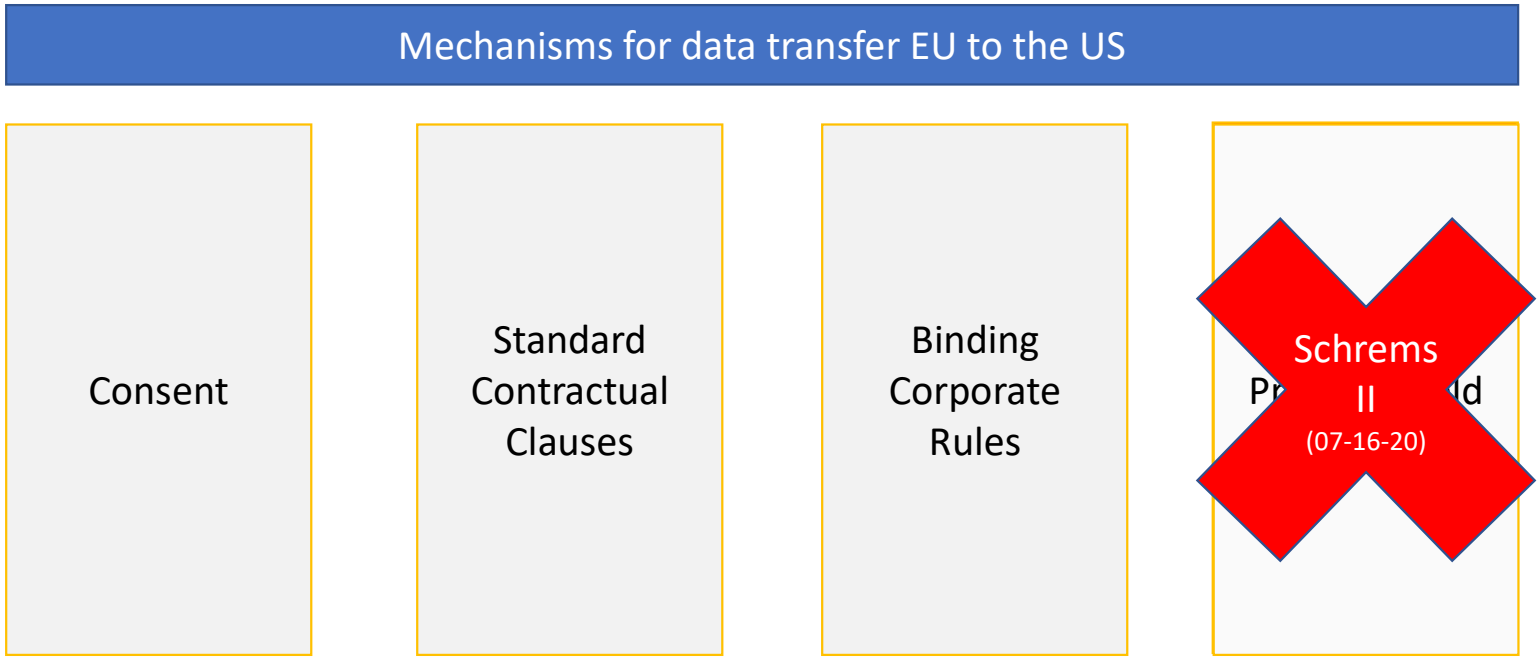
Data Transfers from Europe / UK



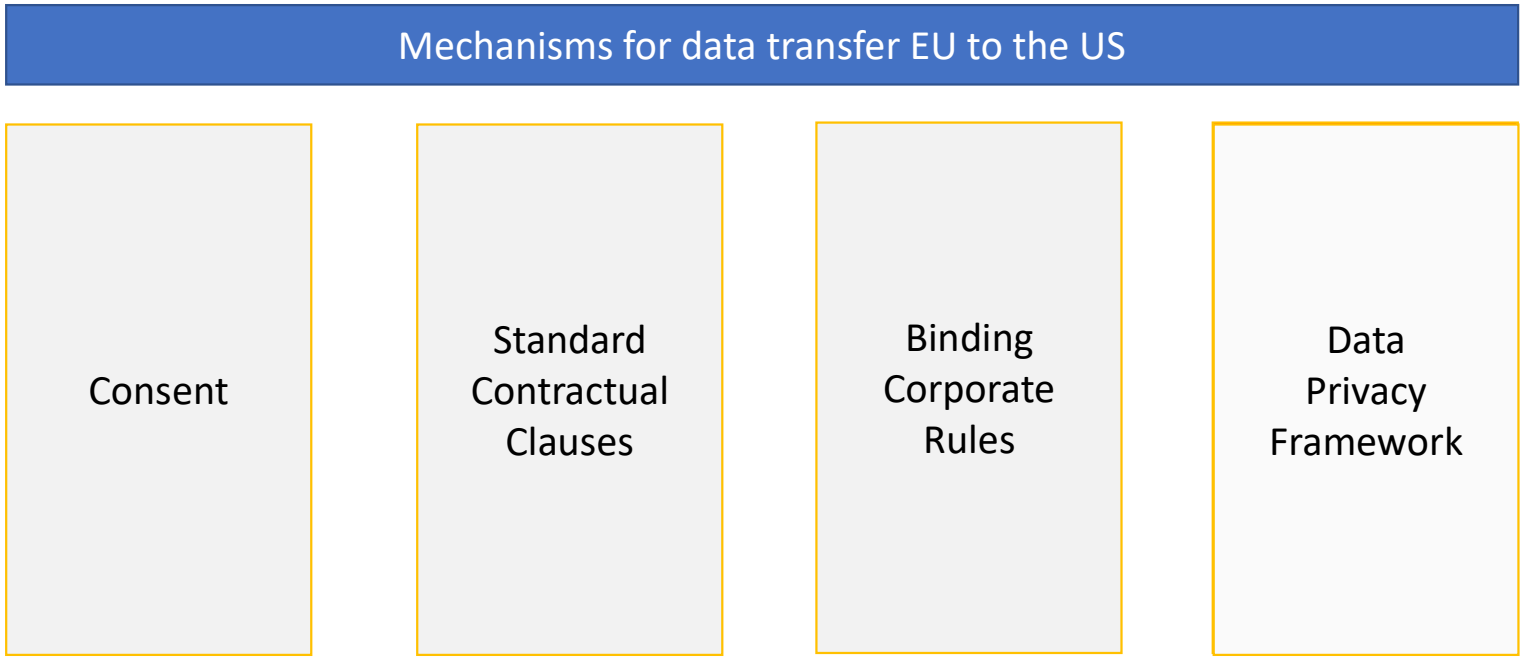
Data Transfers from Europe / UK

- US Authorities can access personal data (intelligence)
- No supervision
- No legal means for EU data subjects to claim their rights in the US

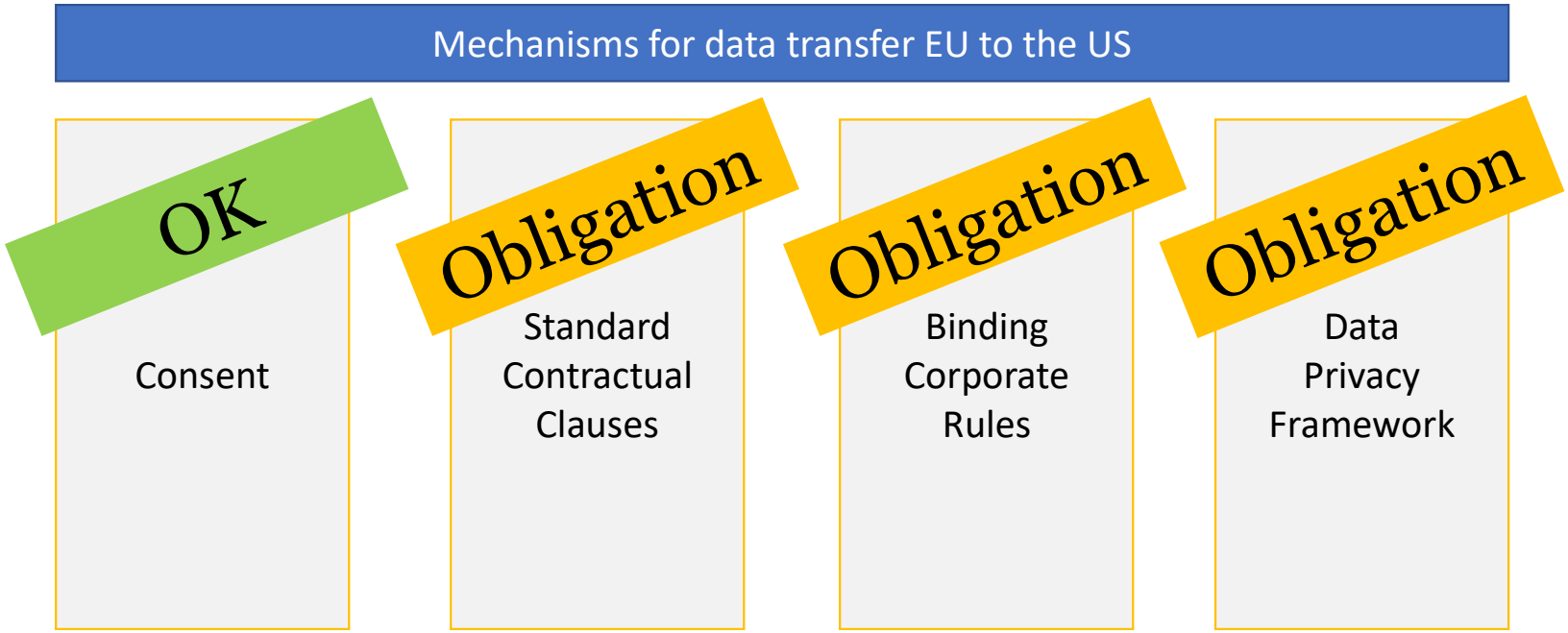
Data Transfers from Europe / UK



Data Transfers from Europe / UK



Data Transfers from Europe / UK



Cross Border Data Transfer

Background: Data Transfers from Europe / UK

Consent

Standard Contractual Clauses

Binding Corporate Rules

Data Privacy Framework

Increasing Localization Requirements

Enforcements

Privacy+ Security Forum

Data Transfers from Europe / UK

Privacy+ Security Forum

Mechanisms for data transfer EU to the US

Consent

- By the Data Subject
- Clear and affirmative action
- Fully informed on data processing
- Freely given
- Can be withdrawn any time

• Easy Set-up • Safe if correct • Sustainable	• Individual Solution • Ltd use for B2B • Employment issue

Consent

Art. 4(11)

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Art. 7 ('further conditions')

- ✓ keeping records to demonstrate consent
- ✓ prominence and clarity of consent requests
- ✓ the right to withdraw consent easily and at any time
- ✓ freely given consent if a contract is conditional on consent

EDPB

Guidelines 05/2020 on Consent under Regulation 2ß16/679

Consent

Let's Play

Privacy+ Security Forum

Let's Play

Privacy+ Security Forum

1. Frankfurt Fair
2. German Sub
3. CRM Germany
4. CRM USA

1. Consent?
2. PII to CRM?
3. Use of PII?
4. What to do?

Cross Border Data Transfer

Background: Data Transfers from Europe / UK
Consent
Standard Contractual Clauses
Binding Corporate Rules
Data Privacy Framework
Increasing Localization Requirements
Enforcements

Privacy+ Security Forum

Standard Contractual Clauses

Privacy+ Security Forum

Mechanisms for data transfer EU to the US

Standard Contractual Clauses

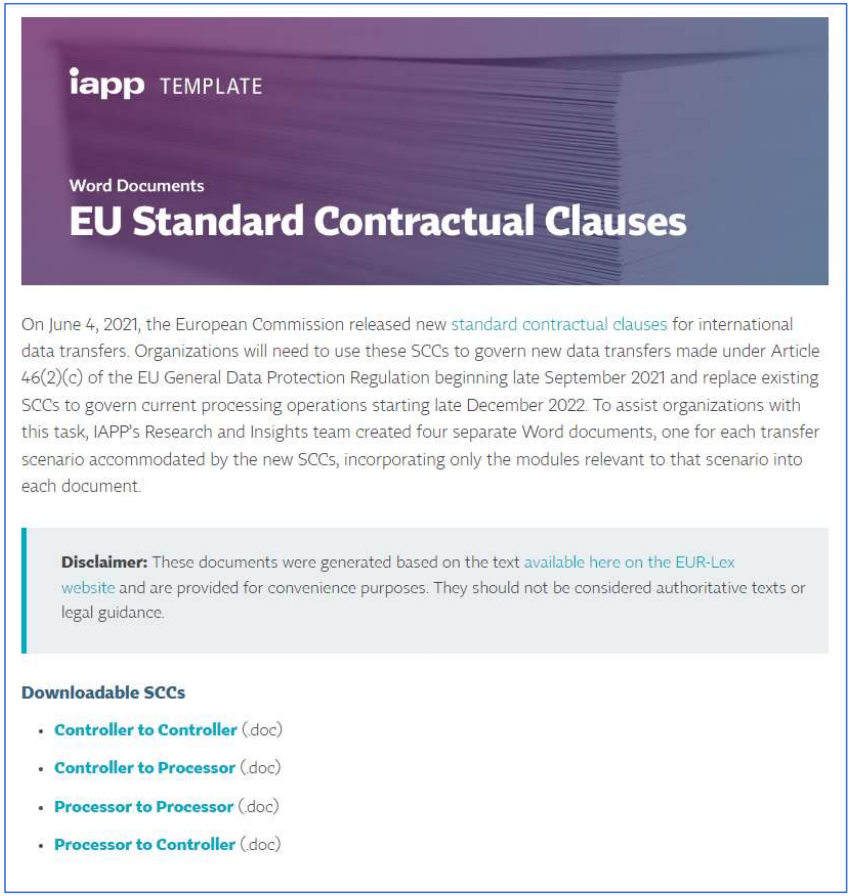
- EU Standard contract (different sets)
- Between data exporter and data importer
- Importer to comply with EU standards
- Easy, fast, and cheap solution
- "The" standard for data transfer

• Easy set-up • No DPA approval • Worldwide	• Not negotiable • Negative add-ons • Liability

Standard Contractual Clauses

Privacy+ Security Forum

- Standardized
- Pre-approved
- Can be incorporated (but shall not be contradicted)
- Do not modify (except where offered
- Fill in the annexes
- Docking clause
- Transfer Impact Assessment



Main mistakes

- Wrong set of clauses
- Contradictions by separate DPA (not needed!)
- Sub-processors (Module 3)
- Data Transfer into the EEA

Standard Contractual Clauses

Privacy+ Security Forum

Substantial obligations for the parties of the SCC contact after Schrems !

- Ensure "appropriate protection" – SCCs are just part of this
- Consider the law of importing country (DPF standards)
- Additional safeguards (clauses or other safeguards) may be required
- Importer (US) must notify exporter if it cannot meet obligations
- If exporter still transfers data, it must send notification to DPA

Standard Contractual Clauses

Privacy+ Security Forum

Standard contractual clauses for the transfer of data to third country controllers and processors subject to the GDPR

Have your say - Public Consultations and Feedback > Published initiatives >

Standard contractual clauses for the transfer of data to third country controllers and processors subject to the GDPR

In preparation

UPCOMING

Public consultation

Planned for

Fourth quarter 2024

FEEDBACK: UPCOMING

Draft act

FEEDBACK: UPCOMING

Commission adoption

Planned for

Second quarter 2025

About this initiative

Summary	Standard contractual clauses are model data protection clauses EU data exporters can incorporate into their contracts to transfer personal data to data importers in third countries in line with the requirements of the General Data Protection Regulation (GDPR). These clauses are for the specific case where a data importer is located in a third country but is directly subject to the GDPR. They complement the existing clauses, for data transfers to third country importers not subject to the GDPR.
Topic	Justice and fundamental rights
Type of act	Implementing decision
Committee	C49000

Public consultation

FEEDBACK: UPCOMING

Planned for

Fourth quarter 2024

Let's Play

Privacy+ Security Forum

Let's Play

Privacy+ Security Forum

Cross Border Data Transfer

Background: Data Transfers from Europe / UK
Consent
Standard Contractual Clauses
Binding Corporate Rules
Data Privacy Framework
Increasing Localization Requirements
Enforcements

Privacy+ Security Forum

Binding Corporate Rules

Privacy+ Security Forum

Mechanisms for data transfer EU to the US

- All companies apply same standard
- Comprehensive process
- Need to be DPA approved
- Very expensive and burdensome
- Not for small to midsize companies

• Full coverage • DPA Approved • Sustainable	• Expensive • Difficult set-up • EU backlog

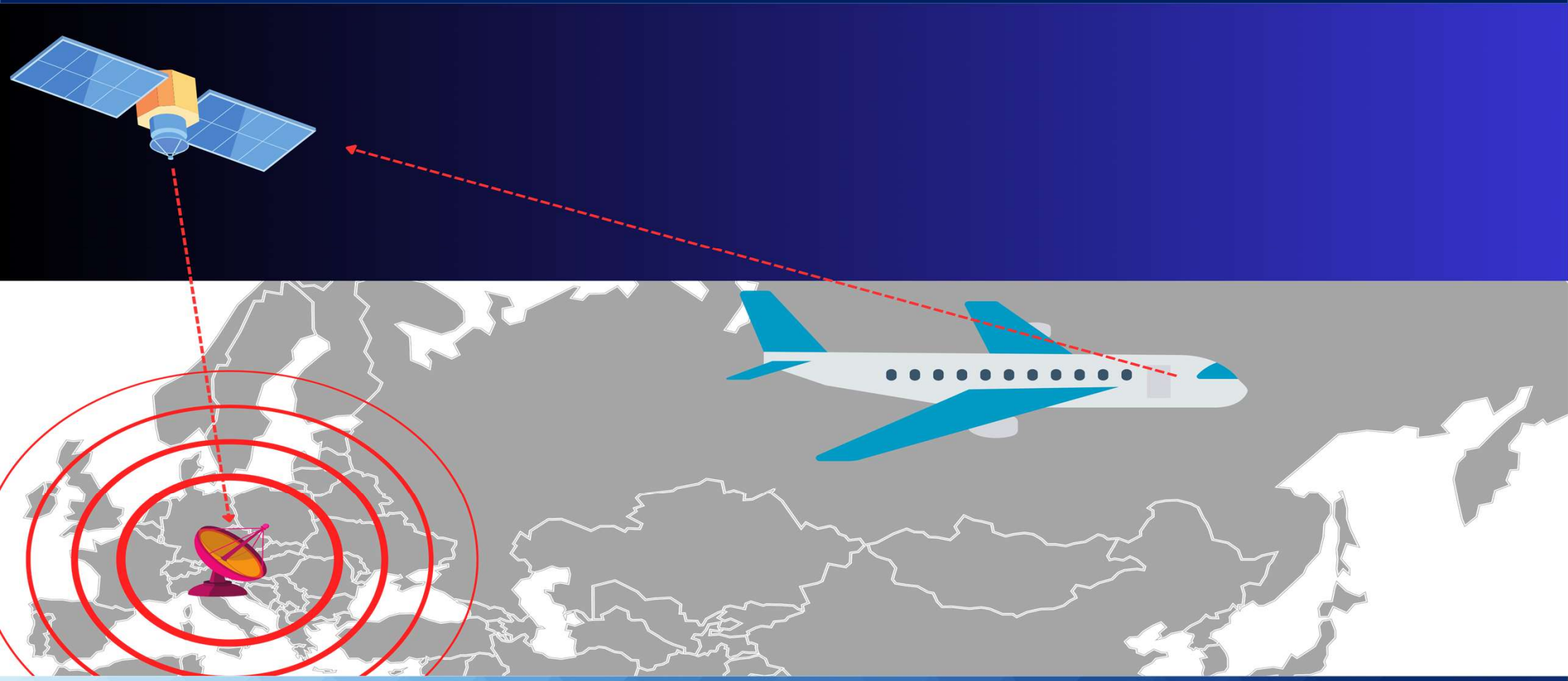
Binding Corporate Rules

Let's Play

Privacy+ Security Forum

Flying to Russia

Privacy+ Security Forum



Cross-Border Data Transfer

Background: Data Transfers from Europe / UK
Consent
Standard Contractual Clauses
Binding Corporate Rules
Data Privacy Framework
Increasing Localization Requirements
Enforcements

Privacy+ Security Forum

Data Privacy Framework

Privacy+ Security Forum

Mechanisms for data transfer EU to the US

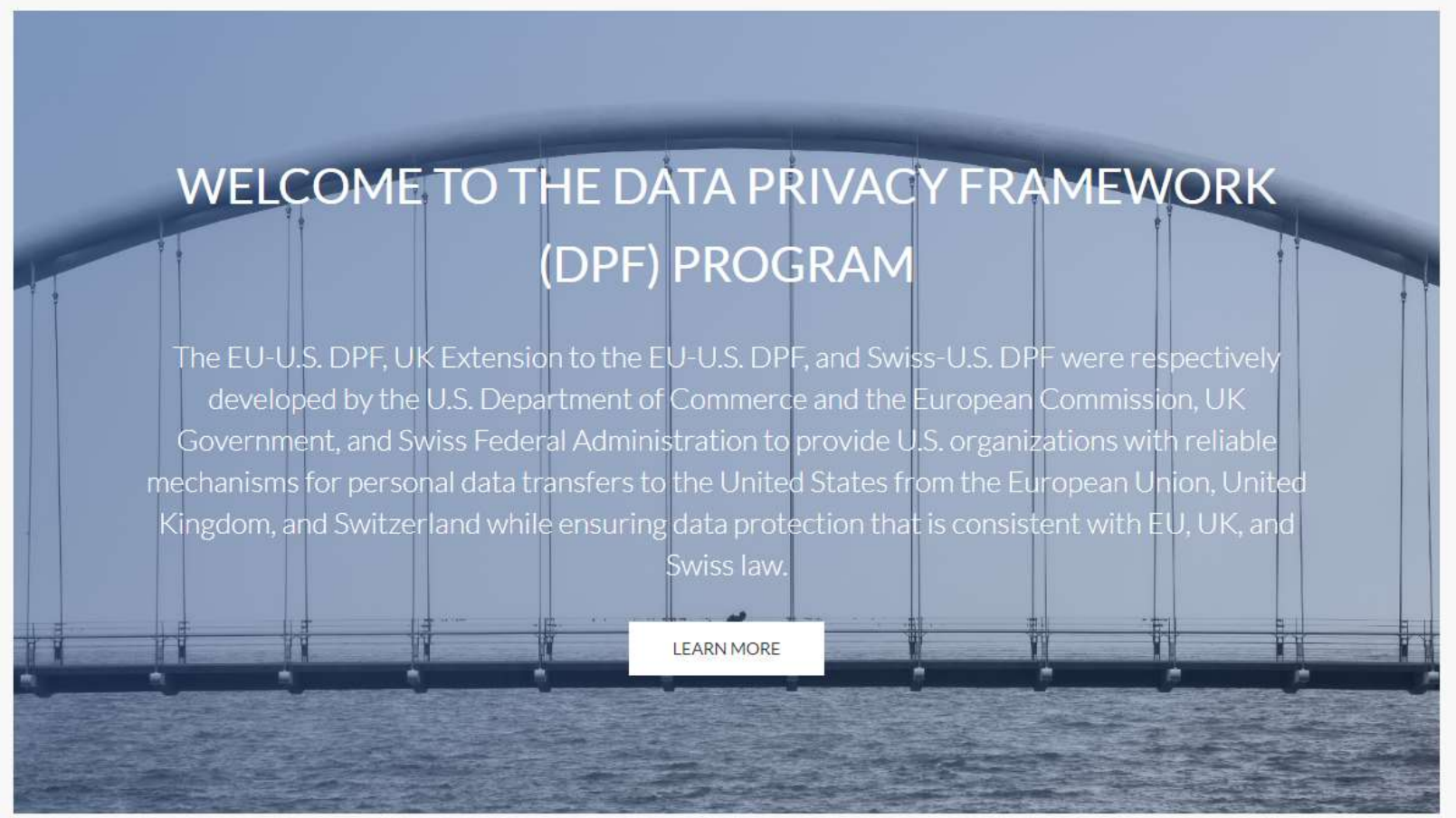
- New since 10 July 2023
- US only (!)
- High importance for US companies
- Easy, fast and cheap solution
- UK-U.S. Data Bridge / Switzerland

• Easy set-up • No DPA approval • No audits • 2,800+ enterprises • 70% SMEs	• EU to US only • Needs registration • Yearly Review • DP Review Court

Data Privacy Framwork

Data Privacy Framework

Privacy+ Security Forum



Data Privacy Framework

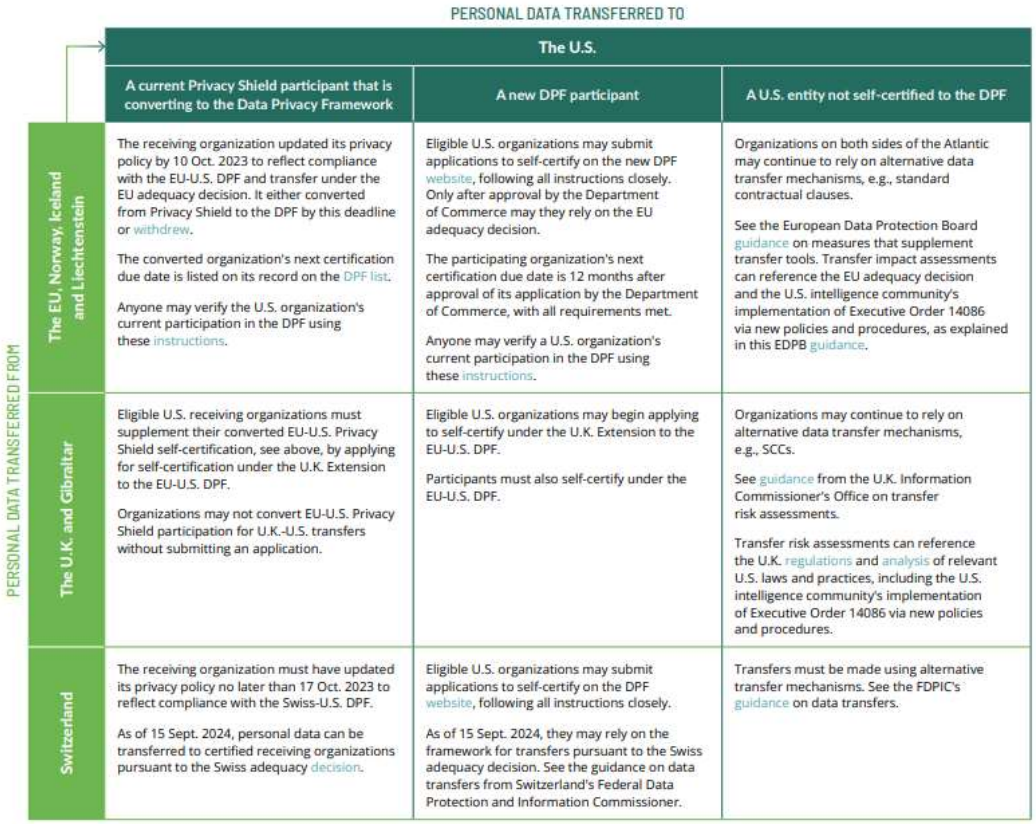
Privacy+ Security Forum

- ✓ **EU-U.S. Data Privacy Framework** (July 10, 2023)
- ✓ **UK Extension to the EU-U.S. Framework** – Data Bridge (October 12, 2023)
- ✓ **Swiss-U.S. Data Privacy Framework** (September 15, 2024 – recognition of adequacy)

- ➢ **International Trade Administration** (US Department of Commerce)
- ➢ **Self-Certification with the ITA** (DPF program website)
- ➢ **Publicly commit to the DPF priciples** (enforceable under US Law)
- ➢ **Annual Re-Certification**

Data Privacy Framework

Privacy+ Security Forum



PERSONAL DATA TRANSFERRED TO

PERSONAL DATA TRANSFERRED FROM	The U.S.		
	A current Privacy Shield participant that is converting to the Data Privacy Framework	A new DPF participant	A U.S. entity not self-certified to the DPF
The EU, Norway, Iceland and Liechtenstein	The receiving organization updated its privacy policy by 10 Oct. 2023 to reflect compliance with the EU-U.S. DPF and transfer under the EU adequacy decision. It either converted from Privacy Shield to the DPF by this deadline or withdrew. The converted organization's next certification due date is listed on its record on the DPF list. Anyone may verify the U.S. organization's current participation in the DPF using these instructions.	Eligible U.S. organizations may submit applications to self-certify on the new DPF website, following all instructions closely. Only after approval by the Department of Commerce may they rely on the EU adequacy decision. The participating organization's next certification due date is 12 months after approval of its application by the Department of Commerce, with all requirements met. Anyone may verify a U.S. organization's current participation in the DPF using these instructions.	Organizations on both sides of the Atlantic may continue to rely on alternative data transfer mechanisms, e.g., standard contractual clauses. See the European Data Protection Board guidance on measures that supplement transfer tools. Transfer impact assessments can reference the EU adequacy decision and the U.S. intelligence community's implementation of Executive Order 14086 via new policies and procedures, as explained in this EDPB guidance.
The U.K. and Gibraltar	Eligible U.S. receiving organizations must supplement their converted EU-U.S. Privacy Shield self-certification, see above, by applying for self-certification under the U.K. Extension to the EU-U.S. DPF. Organizations may not convert EU-U.S. Privacy Shield participation for U.K.-U.S. transfers without submitting an application.	Eligible U.S. organizations may begin applying to self-certify under the U.K. Extension to the EU-U.S. DPF. Participants must also self-certify under the EU-U.S. DPF.	Organizations may continue to rely on alternative data transfer mechanisms, e.g., SCCs. See guidance from the U.K. Information Commissioner's Office on transfer risk assessments. Transfer risk assessments can reference the U.K. regulations and analysis of relevant U.S. laws and practices, including the U.S. intelligence community's implementation of Executive Order 14086 via new policies and procedures.
Switzerland	The receiving organization must have updated its privacy policy no later than 17 Oct. 2023 to reflect compliance with the Swiss-U.S. DPF. As of 15 Sept. 2024, personal data can be transferred to certified receiving organizations pursuant to the Swiss adequacy decision.	Eligible U.S. organizations may submit applications to self-certify on the DPF website, following all instructions closely. As of 15 Sept. 2024, they may rely on the framework for transfers pursuant to the Swiss adequacy decision. See the guidance on data transfers from Switzerland's Federal Data Protection and Information Commissioner.	Transfers must be made using alternative transfer mechanisms. See the FDPIC's guidance on data transfers.

*https://iapp.org/resources/article/ilmplementing-trans-Atlantic-transfer/

How to Join the Data Privacy Framework (DPF) Program (part–1)

Guide to Self-Certification

The decision by a U.S.-based organization to join the Data Privacy Framework (DPF) program is entirely voluntary. However, once an eligible U.S.-based organization self-certifies to the U.S. Department of Commerce's International Trade Administration (ITA) and publicly declares its commitment to adhere to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) Principles and/or the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) Principles that commitment is enforceable under U.S. law by the relevant enforcement authority (i.e., by the Federal Trade Commission (FTC), the U.S. Department of Transportation (DOT), or other relevant government body).

To be entitled to the benefits of participating in the DPF program, an organization must initially self-certify and then annually re-certify to the ITA that it adheres to the DPF Principles, including the Supplemental Principles that collectively consist of a detailed set of requirements based on privacy principles. To initially self-certify or subsequently re-certify for the relevant part(s) of the

*https://www.dataprivacyframework.gov/program-articles/how-to-join-the-data-privacy-framework-(DPF)-program

Data Privacy Framework

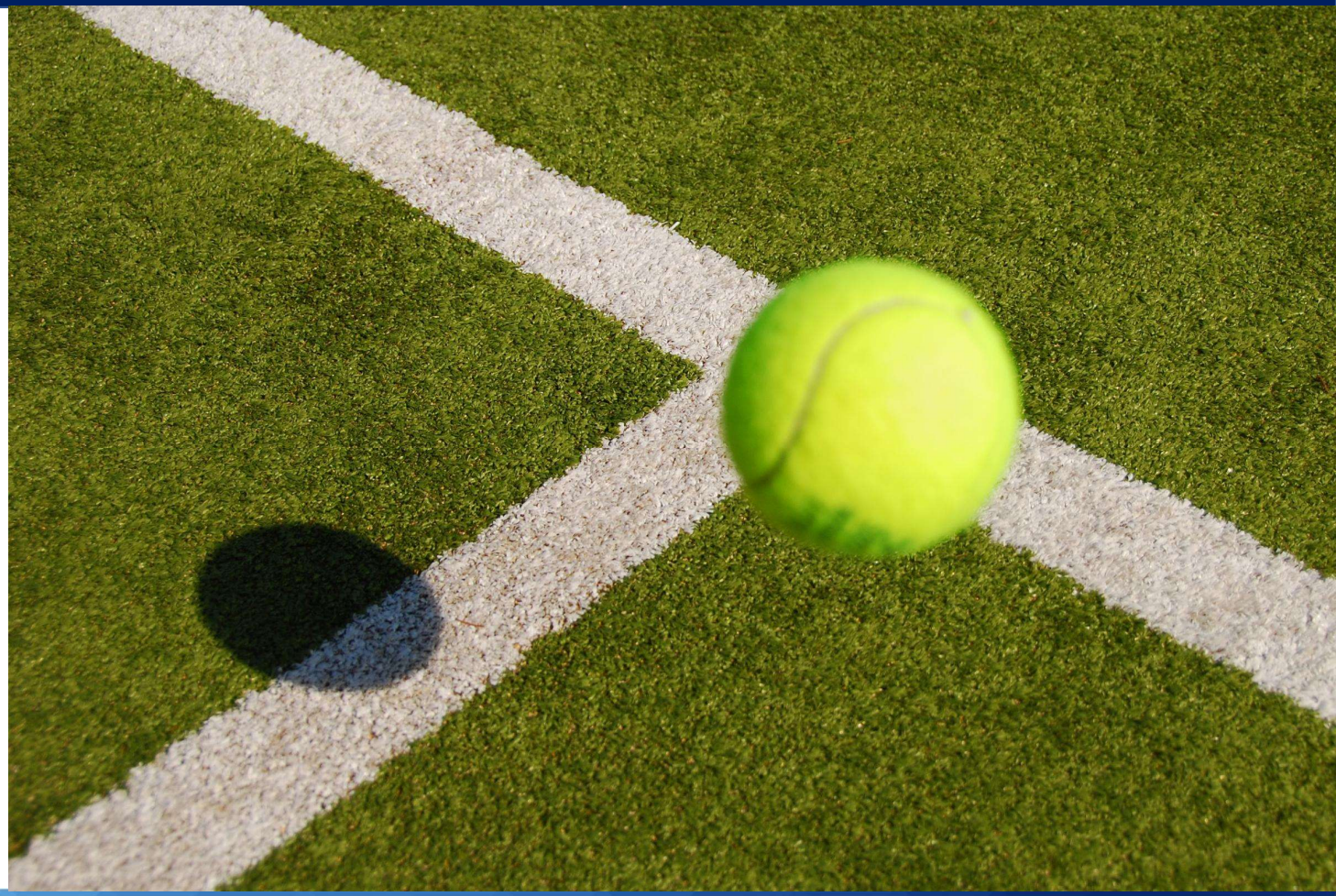
Privacy+ Security Forum

Guide to join the DPF-Program

1. Confirm eligibility to participate in the DPF program (only US legal entities subject to FTC or DOT)
2. Have a DPF-compliant Privacy Policy Statement (with references and links; quite comprehensive)
3. Have an appropriate independent recourse mechanism for each type of Personal Data covered (Recourse, Enforcement, and Liability Principle: investigate unresolved complaints, recourse free of charge to affected individuals)
4. Make the required contribution for the Annex I Binding Arbitration Mechanism
5. Ensure that your organization's Verification Mechanism is in place (self-assessment or outside compliance review)
6. Designate a Contact within your organization regarding DPF compliance (complaints, access requests, etc.)
7. Review the information required to self-certify
8. Submit self-certification to the ITA (and pay the fee; initiates the review)

Let's Play

Privacy+ Security Forum



Dutch Uber Case 08/2024

Privacy+ Security Forum

AUTORITEIT PERSOONSGEGEVENS

What are you looking for?

Report data breach | File a complaint

Home | Themes | Current | Documents | Contact | DPO

Home > Current >

Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US

26 August 2024 Themes: Transfer within and outside the EEA, Personal data

The Dutch Data Protection Authority (DPA) imposes a fine of 290 million euros on Uber. The Dutch DPA found that Uber transferred personal data of European taxi drivers to the United States (US) and failed to appropriately safeguard the data with regard to these transfers. According to the Dutch DPA, this constitutes a serious violation of the General Data Protection Regulation (GDPR). In the meantime, Uber has ended the violation.

"In Europe, the GDPR protects the fundamental rights of people, by requiring businesses and governments to handle personal data with due care", Dutch DPA chairman Aleid Wolfsen says. "But sadly, this is not self-evident outside Europe. Think of governments that can tap data on a large scale. That is why businesses are usually obliged to take additional measures if they store personal data of Europeans outside the European Union. Uber did not meet the requirements of the GDPR to ensure the level of protection to the data with regard to transfers to the US. That is very serious."

Dutch Uber Case 08/2024

Uber: “This flawed decision and extraordinary fine are completely unjustified. Uber’s cross-border data transfer process was compliant with GDPR during a 3-year period of immense uncertainty between the EU and US. We will appeal and remain confident that common sense will prevail.”

The company claims it sought guidance from the AP during the period where there was no high-level EU-U.S. data transfer deal, but says the regulator did not provide it with any clarity that there were problems with its processes.

Data Privacy Framework

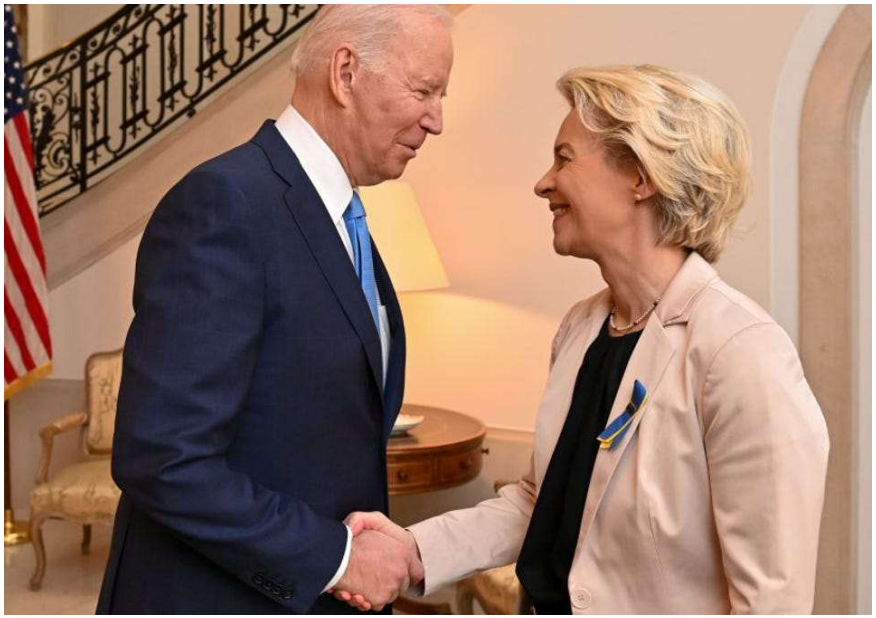
Privacy+ Security Forum

Data Privacy Framework

Executive Order

Schrems III

Data Privacy Framework



- July 10, 2023 EU adopts EU-US DPF
- Principles: notice, choice, accountability for onward transfers, security, data integrity and purpose limitation, access and recourse, enforcement
- New: controls to mitigate deficiencies
- New: better rights for individuals to redress claims (Data Protection Review Court)

Data Privacy Framework

Privacy+ Security Forum

- ✓ Adds further safeguards for U.S. intelligence activities (i.a. Civil Liberties Protection Officer)
- ✓ Mandates handling requirements for personal information
- ✓ Creates multi-layer mechanism for individuals to redress claims (Data Protection Review Court)

Data Privacy Framework


BRIEFING

European Parliament

Reaching the EU-US Data Privacy Framework:
First reactions to Executive Order 14086

… "Moreover, the interplay between the executive order and the Cloud Act remains uncertain. Furthermore, the Baden-WürttembergDPA pinpoints discrepancies between EU and US interpretations of 'proportionality', pointing out that the permission of bulk surveillance does not meet CJEU standards. Finally, it criticises that lodging a complaint with the CLPO is subject to the fulfilment of substantial requirements, which may present a means of preventing 'unwelcome' complaints; that the order envisages the DPRC as being part of the executive branch, which runs contrary to judicial independence; and that the neither-confirm nor-deny principle hampers effective redress. …"

Data Privacy Framework

Privacy+ Security Forum

- November 2022 (IAPP EU DP Congress): going to CJEU re DPF
  - DPF still allows for data collection by US intelligence agencies, and what constitutes as “necessary and proportionate” is open to interpretation
  - The Data Protection Review Court (DPRC) may not meet the standards of independence, transparency, and impartiality required under EU law
  - The DPF doesn’t address onward transfers of data from the US to third countries, which may pose additional risks to EU individuals’ data
- noyb (none of your business) on it

Data Privacy Framework


POLITICO

Enter keyword

EXPLORE

NEWSLETTERS & PODCASTS

POLITICO PRO

French lawmaker challenges transatlantic data deal before EU court

MP Philippe Latombe launches the latest round of legal fighting.

Latombe filed two challenges, he told POLITICO: one to suspend the agreement immediately and another on the text's content | Joel Saget/AFP via Getty Images

- September 7th 2023
- Challenging the DPF at the CJEU:

  "The text resulting from these negotiations violates the Union's Charter of Fundamental Rights, due to insufficient guarantees of respect for private and family life with regard to bulk collection of personal data, and the General Data Protection Regulation (GDPR),"

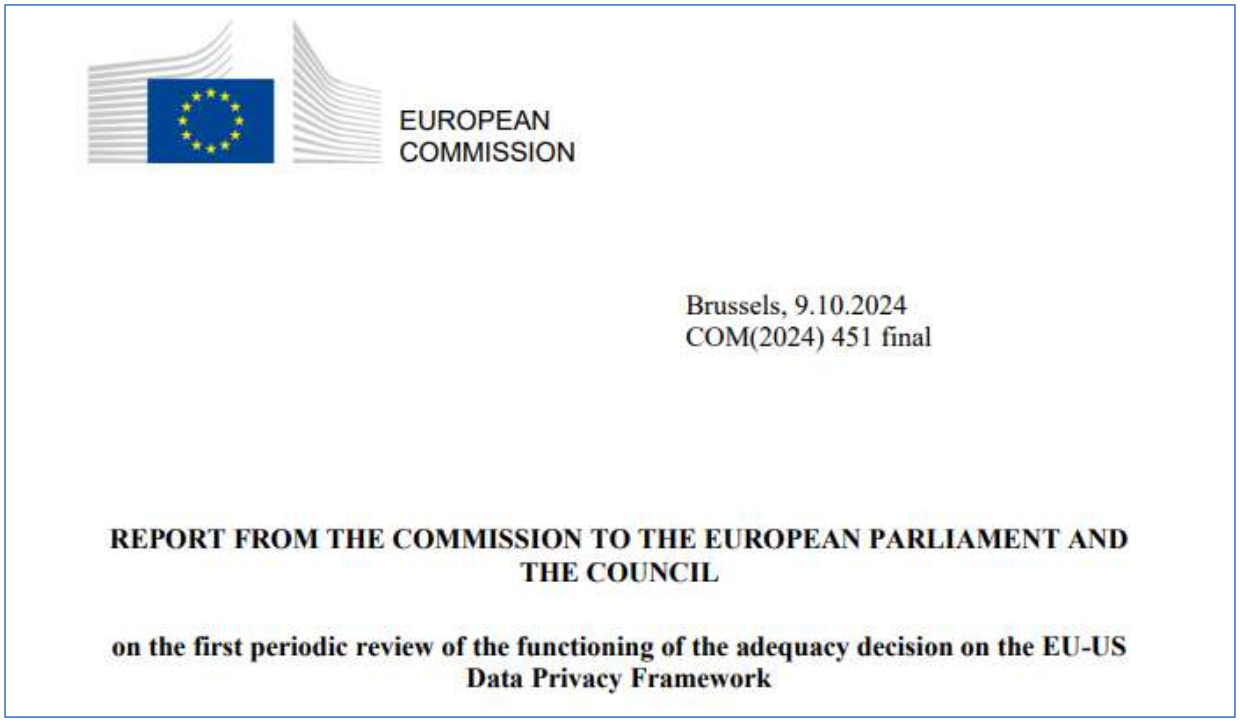
- October 12, 2023 - CJEU denies Interim Measures

Data Privacy Framework

Landesbeauftragter Dr. Lutz Hasse

„Unternehmen etwa sollten vor diesem Hintergrund abwägen, ob sie sensible Daten – auch Kundendaten – in die USA transferieren oder bis zur Entscheidung des EuGH vorsorglich nicht. Denn die Wahrscheinlichkeit, dass der Europäische Gerichtshof den Adäquanzbeschluss aufheben wird, ist danach recht hoch.

Data Privacy Framework



EUROPEAN
COMMISSION

Brussels, 9.10.2024
COM(2024) 451 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework

"Based on the information gathered during this first review, the Commission concludes that the U.S. authorities have put in place the necessary structures and procedures to ensure that the Data Privacy Framework functions effectively. In this context, the Commission very much values the very good cooperation with the U.S. authorities to conduct the review."

Data Privacy Framwork

Privacy+ Security Forum

Mechanisms for data transfer EU to the US

Consent	Standard Contractual Clauses	Binding Corporate Rules	~~Safe Harbor~~ ~~Privacy Shield~~ Schrems III (???)

Let's Ask

Privacy+ Security Forum

Poll

How long will the Data Privacy Framework last?

1. Less than 2 years
2. 2 – 3 years
3. 3 – 5 years
4. Forever

Poll

Given the uncertainty, will you advocate the self-certification under the DPF in your company?

1. We are already in the process of self-certifying under the DPF.
2. I will not advocate the self-certification of my company.
3. I will advocate the self-certification of my company.
4. I am not sure / still evaluating.

Group Work

Would anyone share the reasons for their answer with the group?

Cross-Border Data Transfer

Background: Data Transfers from Europe / UK
Consent
Standard Contractual Clauses
Binding Corporate Rules
Data Privacy Framework
Increasing Localization Requirements
Enforcements

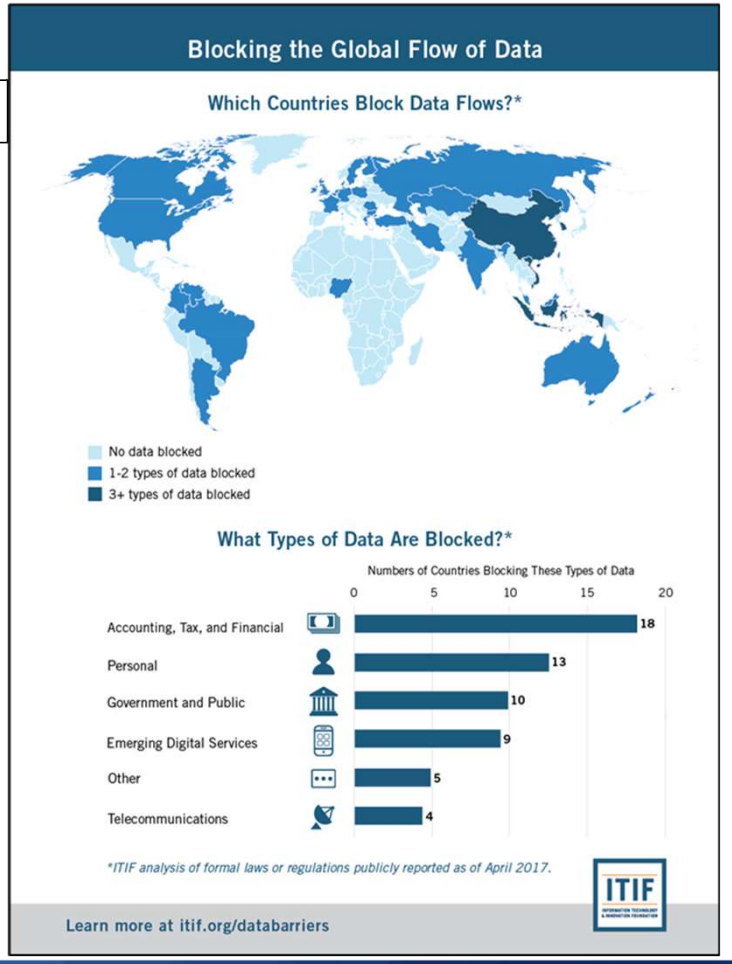
Privacy+ Security Forum

Localization Requirements

Privacy+ Security Forum

https://incountry.com/blog/data-residency-laws-by-country-overview/

Source: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/



Localization Requirements - Variations

Privacy+ Security Forum

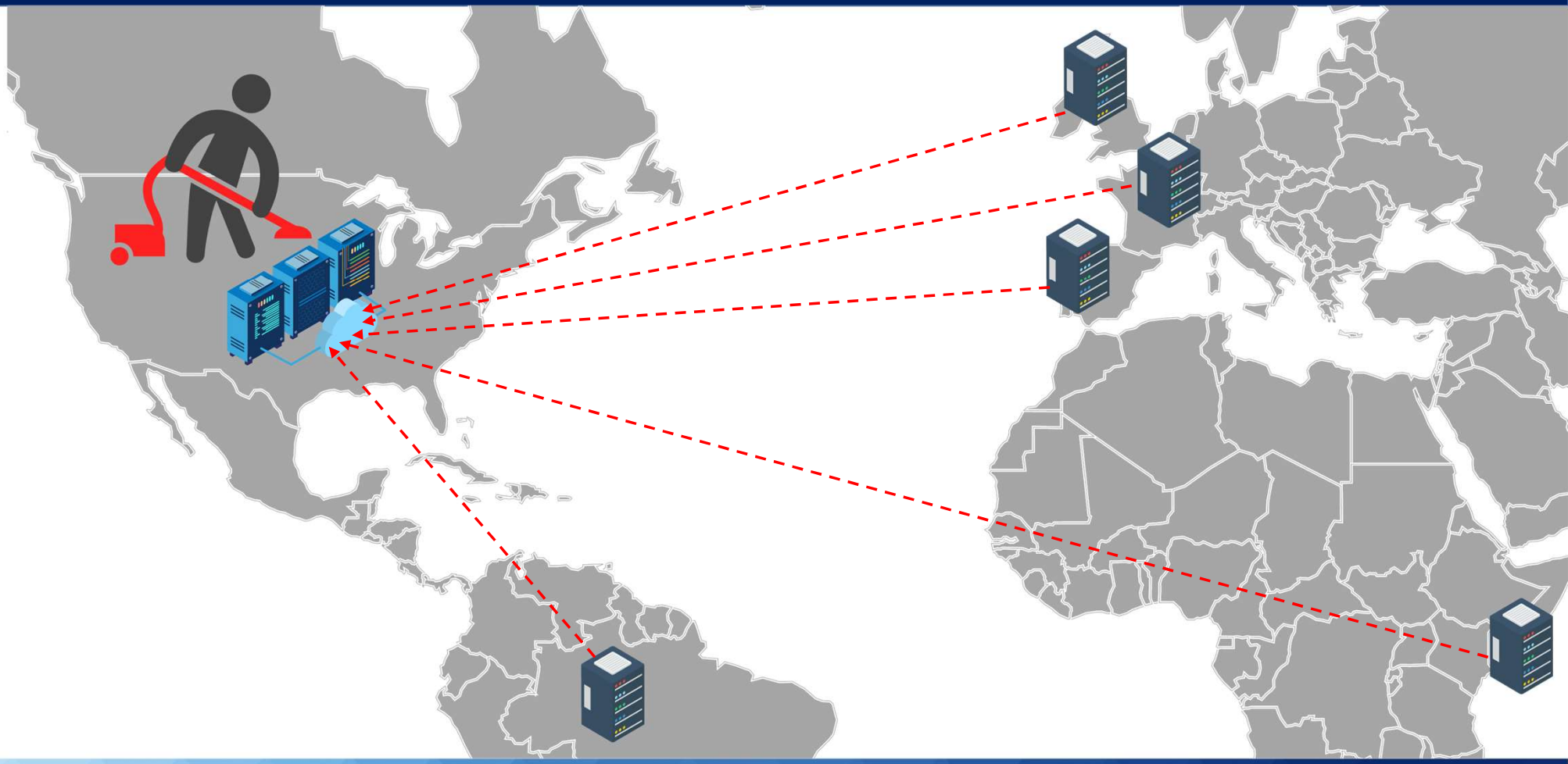
Universal Data Sovereignty	• Personal Data to be stored in the country
Partial Data Sovereignty	• Some Personal Data stored in the country (category, industry)
Data Replication	• Copy of Personal Data to be stored in the country
Controlled Localization	• Restrictions apply (mainly privacy)

Let's Play

Privacy+ Security Forum

Group Work

Privacy+ Security Forum



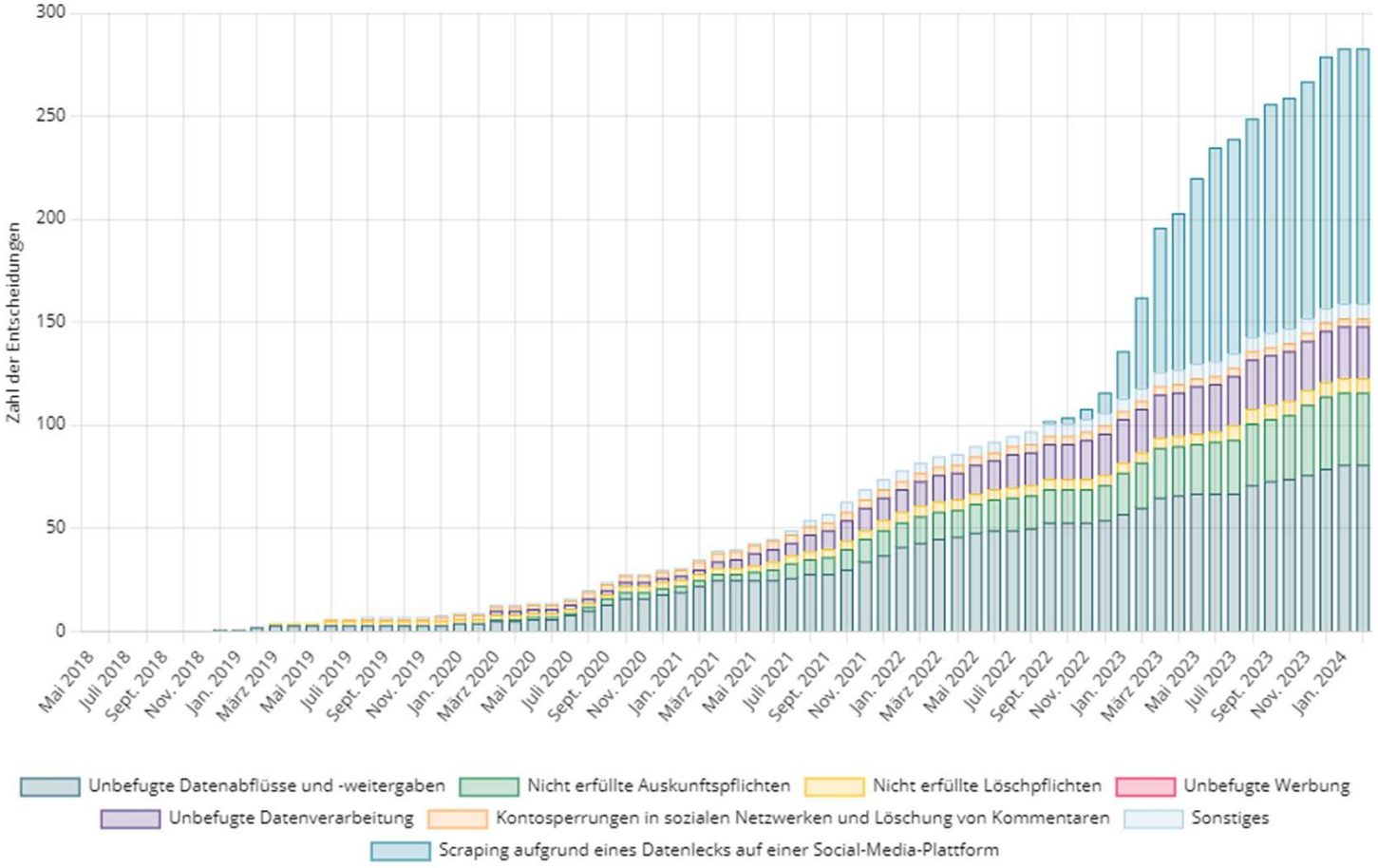
Cross-Border Data Transfer

Background: Data Transfers from Europe / UK
Consent
Standard Contractual Clauses
Binding Corporate Rules
Data Privacy Framework
Increasing Localization Requirements
Enforcements

Privacy+ Security Forum

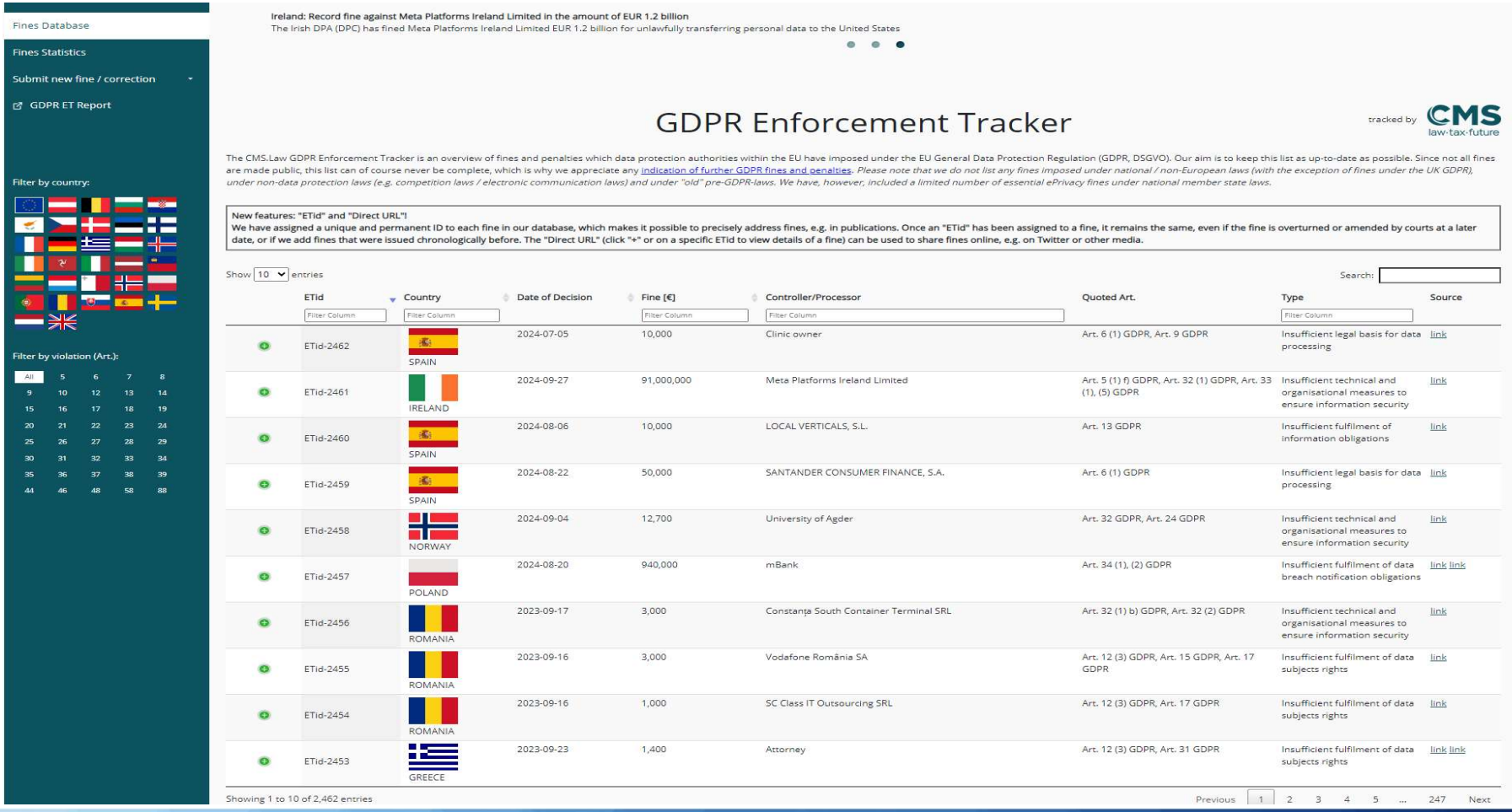
Litigation

Number of Court Decisions referring to GDPR damage claims



Fines

Privacy+ Security Forum



Fines Database

Fines Statistics

Submit new fine / correction

GDPR ET Report

Filter by country:

Filter by violation (Art.):

All 5 6 7 8
9 10 12 13 14
15 16 17 18 19
20 21 22 23 24
25 26 27 28 29
30 31 32 33 34
35 36 37 38 39
44 46 48 58 88

Ireland: Record fine against Meta Platforms Ireland Limited in the amount of EUR 1.2 billion
The Irish DPA (DPC) has fined Meta Platforms Ireland Limited EUR 1.2 billion for unlawfully transferring personal data to the United States

GDPR Enforcement Tracker

tracked by CMS law·tax·future

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties. *Please note that we do not list any fines imposed under national / non-European laws (with the exception of fines under the UK GDPR), under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws. We have, however, included a limited number of essential ePrivacy fines under national member state laws.*

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 10 entries Search:

	ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
		Filter Column		Filter Column	Filter Column		Filter Column	
+	ETid-2462	SPAIN	2024-07-05	10,000	Clinic owner	Art. 6 (1) GDPR, Art. 9 GDPR	Insufficient legal basis for data processing	link
+	ETid-2461	IRELAND	2024-09-27	91,000,000	Meta Platforms Ireland Limited	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR, Art. 33 (1), (5) GDPR	Insufficient technical and organisational measures to ensure information security	link
+	ETid-2460	SPAIN	2024-08-06	10,000	LOCAL VERTICALS, S.L.	Art. 13 GDPR	Insufficient fulfilment of information obligations	link
+	ETid-2459	SPAIN	2024-08-22	50,000	SANTANDER CONSUMER FINANCE, S.A.	Art. 6 (1) GDPR	Insufficient legal basis for data processing	link
+	ETid-2458	NORWAY	2024-09-04	12,700	University of Agder	Art. 32 GDPR, Art. 24 GDPR	Insufficient technical and organisational measures to ensure information security	link
+	ETid-2457	POLAND	2024-08-20	940,000	mBank	Art. 34 (1), (2) GDPR	Insufficient fulfilment of data breach notification obligations	link link
+	ETid-2456	ROMANIA	2023-09-17	3,000	Constanța South Container Terminal SRL	Art. 32 (1) b) GDPR, Art. 32 (2) GDPR	Insufficient technical and organisational measures to ensure information security	link
+	ETid-2455	ROMANIA	2023-09-16	3,000	Vodafone România SA	Art. 12 (3) GDPR, Art. 15 GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects rights	link
+	ETid-2454	ROMANIA	2023-09-16	1,000	SC Class IT Outsourcing SRL	Art. 12 (3) GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects rights	link
+	ETid-2453	GREECE	2023-09-23	1,400	Attorney	Art. 12 (3) GDPR, Art. 31 GDPR	Insufficient fulfilment of data subjects rights	link link

Showing 1 to 10 of 2,462 entries Previous 1 2 3 4 5 ... 247 Next

Fines

- To March 2024 – 2,086 fines
- Total amount of fines around EUR 4,48 billion (2018 – 2023)
- Average fine around EUR 2,14 million
- Highest fine: 1,2 billion (Meta)

Fines

- Ireland on Meta ref. data transfer to the US
- DPC found that Meta violated Art. 46 GDPR after Schrems II
- U.S. law doesn’t provide level of protection / SSCs not sufficient
- Meta used SCCs + additional safeguards
- DPC: additional measures did not compensate for inadequate protections provided by U.S. law
- EDPB: DPC fine proposal not sufficient (upon objections of other DPAs and dispute)

Questions

Privacy+ Security Forum

See you !

Privacy+ Security Forum

Contacts

Nikolaos Theodorakis

Partner
Wilson Sonsini
ntheodorakis@wsgr.com

Dr. Kai Westerwelle

Partner
CMS US Representative Office
kai.westerwelle@cms-hs.com

23 November 2024

EU Privacy + Security Law

Material

Privacy+ Security Forum

Data Transfers from Europe / UK

Privacy+ Security Forum

GDPR – CHAPTER V: Transfers of personal data to third countries or international organizations

- Article 44: General principle for transfers
- Article 45: Transfers on the basis of an adequacy decision
- Article 46: Transfers subject to appropriate safeguards
- Article 47: Binding corporate rules
- Article 48: Transfers or disclosures not authorized by Union law
- Article 49: Derogations for specific situations
- Article 50: International cooperation for the protection of personal data

Article 44: General principle for transfers

Privacy+ Security Forum

"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. **All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."**

Article 45: Transfers on the basis of adequacy

Recital 104: " (…) The third country should offer guarantees ensuring an adequate level of protection **essentially equivalent to that ensured within the Union**, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress."

<u>Nations with adequacy:</u>
Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, UK, Uruguay, and the United States (for members of the Data Privacy Framework).

Article 46: Appropriate Safeguards

Privacy+ Security Forum

To transfer data to a non-adequate country, **without DPA approval**, a transferor must rely on one of:

a) legally binding and enforceable instrument between public authorities or bodies;
b) Binding Corporate Rules (BCRs) adopted by the European Commission
d) Standard Contract Clauses (SCCs) adopted by the EU Commission
c) SCCs adopted by a DPA and approved by EU Commission
e) A Code of Conduct recognized by the EU Commission
f) A certification mechanism recognized by the EU Commission

Appropriate safeguards with prior authorization by a DPA:
a) ad-hoc clauses
b) administrative arrangements between public authorities

Article 49: Derogations for Specific Situations

Alternatively, **without adequacy OR one of the Article 46 methods**, a controller may still transfer data if:

a) The controller has explicit consent, after data subject is informed of risks
b) The transfer is necessary for the performance of a contract (data subject – controller)
c) The transfer is necessary for the performance of a contract (controller – third party, but in the benefit of the data subject)
d) The transfer serves important reasons of public interest
e) The transfer is for establishment, exercise and defense of legal claims
f) The transfer is for the vital interests if the data subject