

8 November 2023

EU Privacy + Security Law Workshop

Nik Theodorakis
Wilson Sonsini

Nicole Beranek Zanon
Härting Law

Rohan Massey
Ropes & Gray



**Nik
Theodorakis**

Of Counsel
Wilson Sonsini



Nicole Beranek Zanon

Partner
HÄRTING Attorneys-at-Law Ltd.
(Switzerland)



Rohan Massey

Partner
Ropes & Gray (UK)

HÄRTING 

- 1. Cross-Atlantic Transfer**
- 2. Emerging Technology + Regulation**
 - 1. Regulatory Enforcement + Fine Trends**

Cross-Atlantic Transfers

The New EU-US Data Privacy Framework

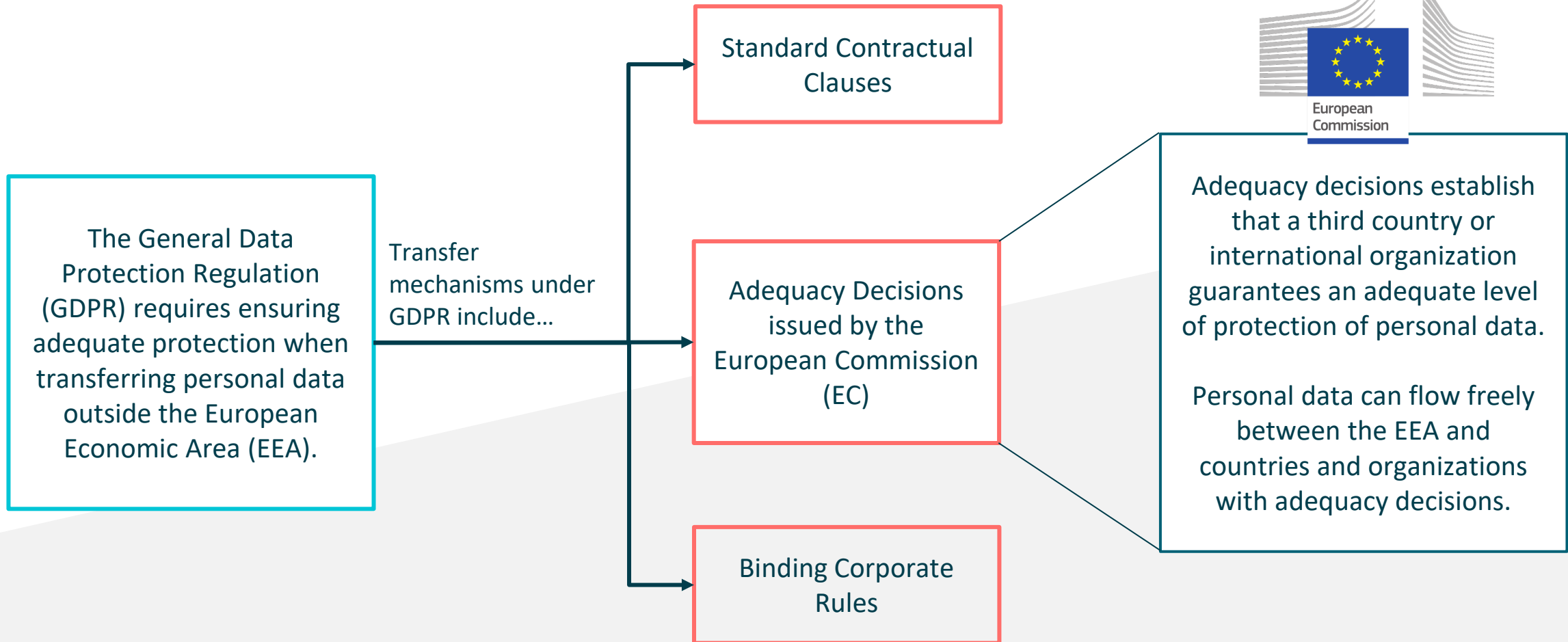
Nik Theodorakis
Of Counsel
Wilson Sonsini

Agenda

1. *Background*
2. *Practical aspects of certification*
3. *What's next*

Background

Background: International Data Transfers



Thousands of U.S. companies relied on Privacy Shield

- Over 5,000 U.S. companies relied on the Privacy Shield adequacy decision for transfers, until the Court of Justice of the EU (CJEU) invalidated it in 2020 in the “*Schrems II*” case.



Schrems II invalidated the Privacy Shield in July 2020

Main reasons for invalidation:

- Lack of adequate protection to individuals’ data protection rights in light of potential for broad disclosures of personal data to U.S. intelligence services/public authorities; and
- Lack of a suitable judicial redress mechanism for individuals in the EU whose personal data was transferred to the U.S.



DPF finalized and adequacy agreement adopted

- On July 10, 2023, the EC adopted an adequacy decision in relation to the DPF. This paves the way for organizations to certify to the DPF, reducing friction for transfers of personal data from the EU to the U.S.



Key steps of the process

- **March 25, 2022** - President von der Leyen and President Biden announced an agreement in principle on a new EU-U.S. Data Privacy Framework.
- **October 7, 2022** - President Biden signed an Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities.
- **December 13, 2022** - European Commission published a draft adequacy decision on the level of protection of personal data under the EU-U.S. Data Privacy Framework.
- **February 28, 2023** - EDPB adopted opinion on draft adequacy decision; called for clarifications on several points.
- **July 10, 2023** – European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework.



Some companies remain Privacy Shield certified (and implemented SCCs).



New definition for “data transfer”: B2C companies in the U.S. may not even need a data transfer mechanism when collecting personal data directly from their users in the EU.



Companies using SCCs often struggle with the new obligation to carry out Data Transfer Impact Assessments (DTIAs).



Data flows to the U.S. are under scrutiny from Supervisory Authorities.



Practical aspects of certification

Public Commitment to Principles



- Companies must publicly disclose commitments to comply with the EU-U.S. Data Privacy Framework (DPF) Principles.



- Principles keep the same headings as under Privacy Shield.
- The substance of some of the supplemental principles has been slightly altered

Voluntary Self-Certification



- Voluntary self-certification mechanism, subject to annual review.

Enforced by the FTC (or DoT)



- The Federal Trade Commission will ensure companies comply with the Data Privacy Framework Principles.



- Department of Commerce maintains a list of certified companies and a list of formerly certified companies (together with reasons for removal).

The EU-U.S. Data Privacy Framework ("DPF") Principles

7 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

Complemented by 16 Supplemental Principles:

1. Sensitive data
2. Journalistic Exceptions
3. Secondary Liability
4. Performing Due Diligence and Conducting Audits
5. The Role of Data Protection Authorities
6. Self-Certification
7. Verification
8. Access
9. HR Data
10. Obligatory Contracts for Onward Transfers
11. Dispute Resolution and Enforcement
12. Choice – Timing of Opt-Out
13. Travel Information
14. Pharmaceutical and Medical Products
15. Public Record and Publicly Available Information
16. Access Requests by Public Authorities

EU Commission has obligations to monitor the DPF:

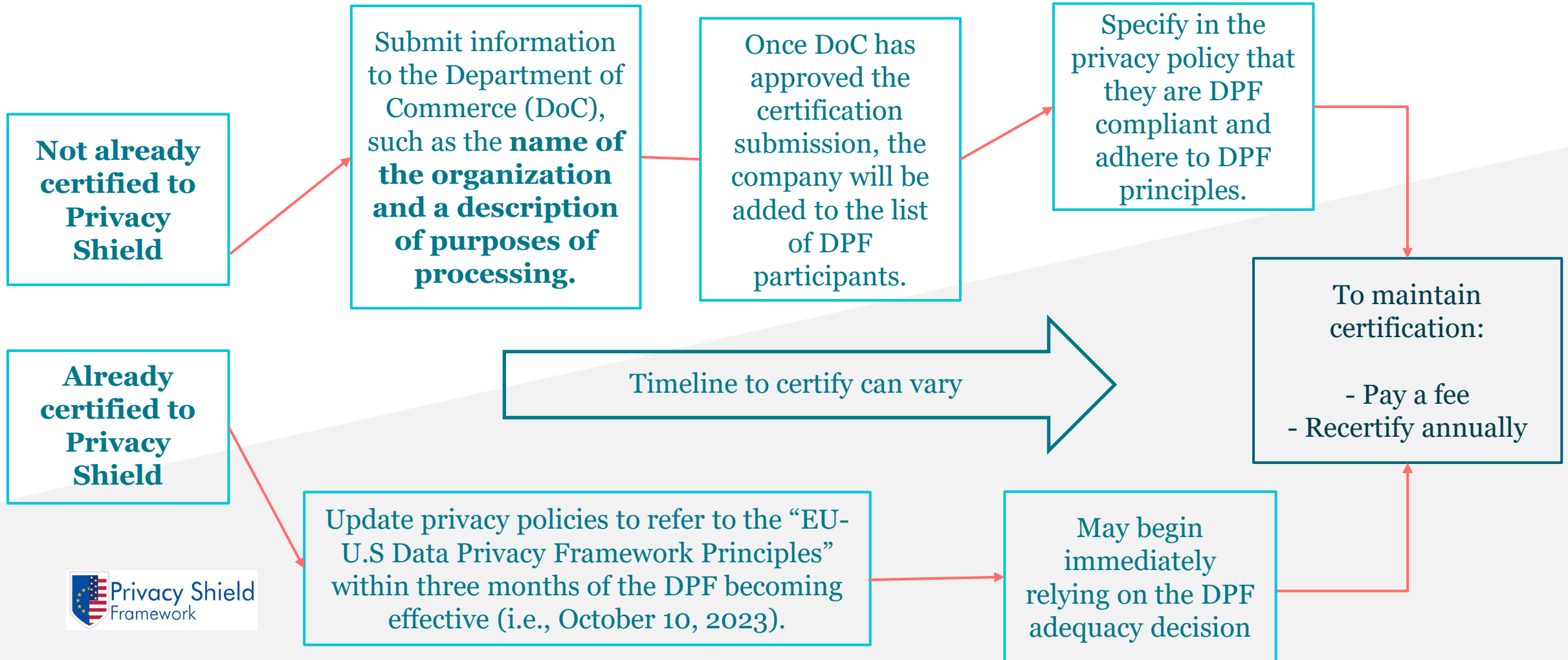
- Periodic factual & legal checks.
- Continuous monitoring of the overall functioning of the DPF, and compliance by U.S. authorities with their representations and commitments.

The EU and the U.S. will conduct a periodic joint review:

- Covering the functioning of all aspects of the DPF, including national security, and involving all relevant stakeholders (e.g., U.S. national intelligence experts, EU DPAs, NGOs through the participation at a public conference).
- Taking into account the U.S. government commitments and transparency reports published (voluntarily) by companies.
- The result will be presented to EU Parliament and Council of the EU.

If the U.S. does not fulfill its commitments, the DPF may be suspended by EU Commission.

How to get certified



Steps to join the DPF for the first time

1. Confirm your organization's eligibility to participate in the DPF
2. Develop a DPF-compliant privacy policy
3. Ensure that your organization has in place an appropriate independent recourse mechanism for each type of personal data covered by its self-certification
4. Make the required contribution for the Annex I binding arbitration mechanism
5. Ensure that your organization's verification mechanism is in place
6. Designate a contact within your organization regarding DPF compliance
7. Review the information required to self-certify (including adhering to the DPF principles)
8. Submit your organization's self-certification to the DoC

What if I previously self-certified but want to withdraw

- Organizations that self-certified to the Privacy Shield, but do not wish to participate in the DPF must follow the International Trade Administration (ITA) withdrawal process.
- The withdrawal process involves notifying the DoC of the withdrawal in advance and telling the DoC what the company intends to do with the personal data that it received in reliance on the Privacy Shield and the DPF:
 - Delete the data,
 - Return the data, or
 - Retain the data, in which case it must either:
 - Affirm to the Department on an annual basis its commitment to continue to apply the Principles to the data, or
 - Provide “adequate” protection for the data by another authorized means (e.g., using SCCs).
- An organization that withdraws must also remove from its privacy policy any references to the Privacy Shield and the DPF.

Only U.S. legal entities subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DoT) are eligible to participate

- The FTC and the DoT are the US bodies charged with enforcing US companies' compliance with the DPF Principles.
- In order to certify with the DPF, an organization must be subject to the **investigatory and enforcement powers of one of these statutory bodies.**
- FTC has jurisdiction over a broad range of entities, subject to a few exemptions:
 - Status-based exemptions
 - Activities-based exemptions



How about Enforcement and Dispute Resolution?

- **The Recourse, Enforcement and Liability Principles'** requirements are additional to the requirement that self regulatory efforts must be enforceable under Section 5 of the FTC Act (15 U.S.C. § 45) prohibiting unfair or deceptive acts.
- FTC will give **priority consideration** to referrals of non-compliance with the Principles from the Department of Commerce and EU Data Protection Authorities.
- If the FTC has reasons to believe Section 5 has been violated, it may:
 - Resolve the matter by seeking an **administrative cease and desist order** prohibiting the challenged practices or by **filing a complaint in a federal district court**, which if successful could result in a federal court order to same effect.
 - Obtain **civil penalties** for violations of an administrative cease and desist order and may pursue **civil or criminal contempt** for violation of a federal court order.



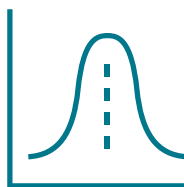
Two main differences between the Privacy Shield and the DPF in this area:

1. U.S. intelligence agencies will only access European data to the extent such access is **necessary and proportionate** to protect national security.
2. The Privacy Shield Ombudsperson, an official charged with reviewing queries from European citizens regarding U.S. intelligence authorities' access to personal data, has been replaced with a newly created **Data Protection Review Court**, which will independently investigate complaints from European citizens, offering an avenue for redress.



Depends on:

• Size



- Companies of all sizes could benefit, and even more so SMEs since compliance requirements and documentation is clearly laid out, and relatively cost-effective.

• Geography



- Businesses with heavy European reach (e.g., EU-based vendors, partners, customers) will greatly benefit.

• Business offering



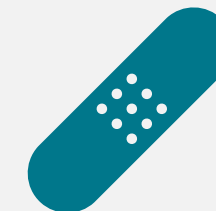
- Industries such as online services, technology, retail, marketing, and healthcare will likely benefit.

• B2B or B2C?



- Many Privacy Shield companies in the past collected data directly from individuals.
- B2C businesses will likely benefit more, but DPF still useful for B2B businesses (including both HR and non-HR data)

• Collecting sensitive data?



- If an organization collects sensitive data, it may be more efficient to rely on the DPF for data flows

- *Do I need to complete DTIAs if I certify with the DPF?*
- *Do my vendors also need to be DPF certified?*
- *What if I am using SCCs- does it make sense to certify with the DPF?*
- *Do I still need a DTIA if I'm using SCCs?*

What's Next

Will the DPF survive?

- No one knows for sure- even if invalidated, it may take 3-4 years before we get there (Privacy Shield was invalidated in exactly 4 years).
- In the meantime, it will provide flexibility to US businesses that want to seamlessly receive data from EU -> e.g. no DTIAs to the US needed
- Max Schrems' privacy organization, NOYB, has already announced that it plans to challenge the validity of the decision, given that it is based on the Executive Order which they believe will not satisfy the CJEU.
- However, the EC has stated that the DPF introduces *“significant improvements compared to the mechanism that existed under the Privacy Shield”*.



The New Swiss-US Data Privacy Framework

Nicole Beranek Zanon
Partner
HÄRTING Attorneys-at-
Law Ltd.

CH: Evolution of cross Atlantic data transfer

Schrems II

- Ruling → **EU-US Privacy Shield** invalid → Federal Data Protection and Information Commissioner (FDPIC) qualified the Swiss-US Privacy Shield as inadequate
- USA was no longer a third country with an adequate level of data protection

Art. 16 DSG

- Data transfer must fulfil the requirements of Art. 16 FADP

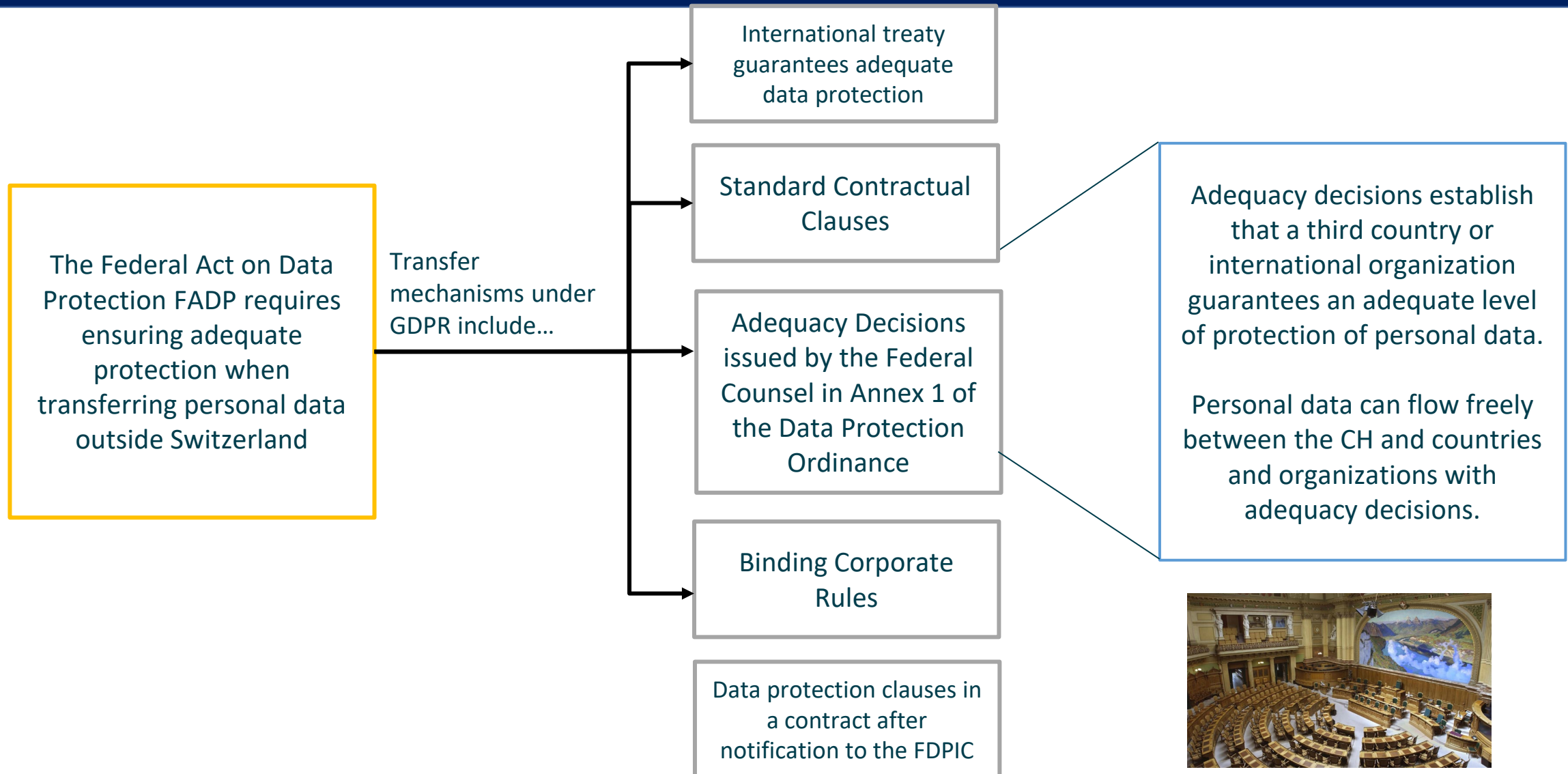
Executive Order

- President Biden signed executive order for Swiss-US Data Privacy Framework in 2022

Swiss-US Data
Privacy
Framework

- Swiss-US Data Privacy Framework already exists but the Federal Council's adequacy decision is missing and set for 2023/early 2024

Background: International Data Transfers (Art. 16 FADP)



- SCC must have a Swiss finish
- Applicable law depending on the transfer or onward transfer (CH or EU or both)
- Change of Authorities
- Articles of GDPR mutatis mutandis to Swiss Law
- Definitions must be amended
- Ev. Exclusion of Liability-Clause
- Free SCC Generator with EU/CH rules:
<https://shop.haerting.ch/scc-generator/>

- U.S. companies can certify under the Swiss-US DPF commit to comply with Swiss-U.S. DPF Principles
- **Principles identical to the EU-US DPF**
 - 7 Principle & 16 Supplemental Principles
- + Advantages
 - + Access by the American intelligence service to Swiss personal data limited to a necessary and proportionate extent
 - + Creation of the **Data Protection Review Court (DPRC)**, to which Swiss citizens can appeal.

- **Principles compared to FADP**

DPF Principle	Article FADP
Notice	Art. 19
Choice	Art. 31 para. 1
Accountability onwards transfer	Art. 16
Security	Art. 8
Data Integrity and purpose limitation	Art. 6 para. 3
Access	Art. 25
Recourse, Enforcement	Art. 32 para. 2

Problem areas

New agreement to be treated with caution

EU-US DPF to be referred to ECJ for review

If ECJ considers EU-US DFA inadequate, Federal Council will most likely follow this ruling

Appeal procedure does not comply with European principles

US intelligence agencies still have access to personal data of foreigners

The New UK-US Data Bridge

Rohan Massey
Partner
Robes & Grey

UK: Evolution of the UK-US Data Bridge

What?

- Data bridge with the United States of America through the UK Extension to the EU-US Data Privacy Framework.
- UK is using data bridges more – i.e. South Korea (Nov 2022)

Why ?

- Part of the Atlantic Declaration between UK and US – and aligns with EU
- Reduces need for TIA, SCCs or other transfer mechanisms
- Leverages EU-US mechanism and access to the newly established redress mechanism

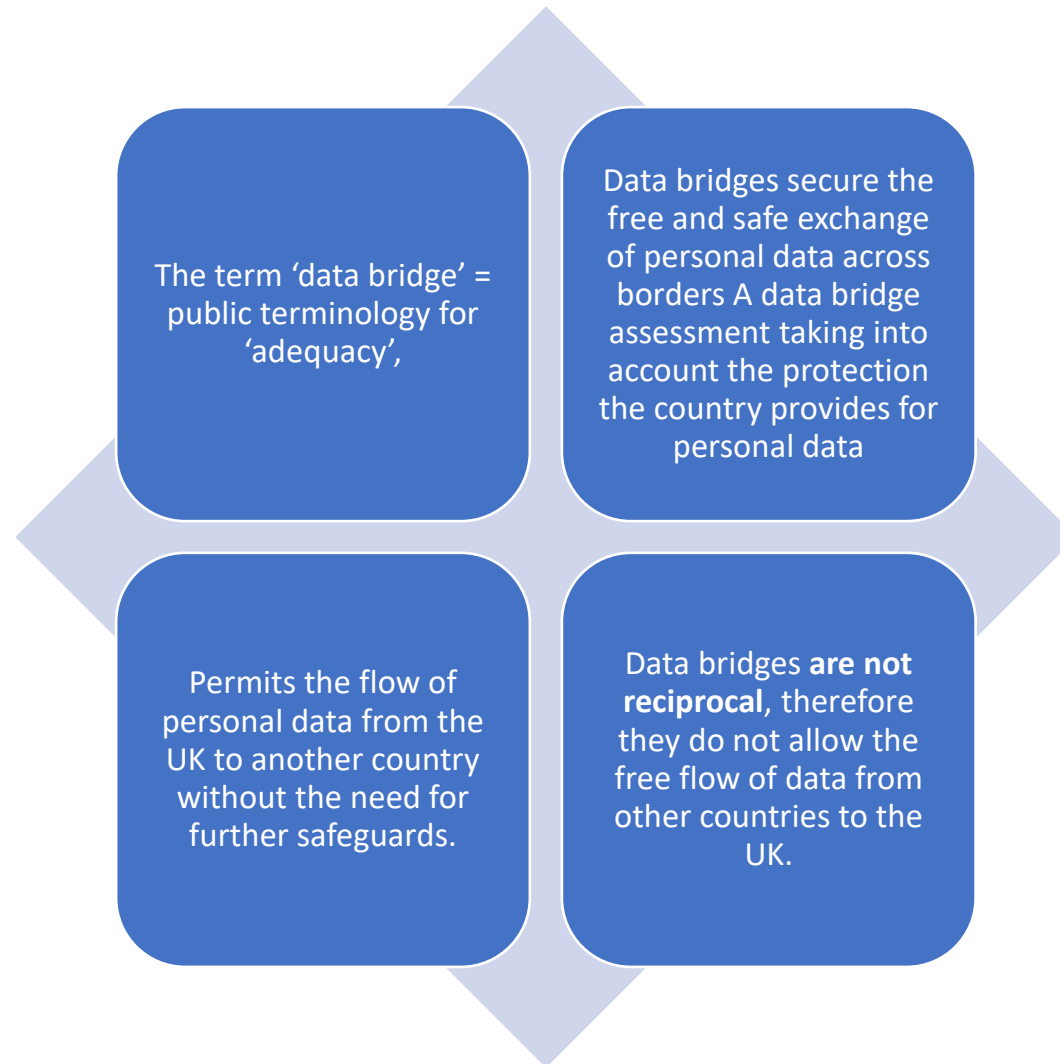
When?

- 8 June 2023, the UK Government announced that it had reached a commitment in principle
- Enforceable from 12 October 2023

Enforcement

- ICO will oversee
- Department for Science, Innovation and Technology will monitor all data bridges under UK Data Privacy Framework

What is a Data Bridge?



Aims

- (i) strengthen the rights and safeguards of UK individuals;
 - (ii) ensure robust and reliable data flows; and #
 - (iii) reduce burdens on businesses.
-
- In addition, the strengthening of individual's rights and safeguards is a clear response to wide ambit of U.S. signal intelligence activities identified in *Schrems II*

Challenges within the Data Bridge

- The UK Information Commissioner's Office & EU privacy activists have commented critically
- Data Bridge does not contain all UK GDPR rights: there is no
 - (i) right to be forgotten
 - (ii) right to withdraw consent
 - (iii) right to obtain a review of an automated decision by a human.
- As a result, UK data subjects might not have the same level of control over their data as they do under UK GDPR.
- 'sensitive information' does not include all 'special categories of personal data' in UK GDPR but broad 'umbrella' concept providing that sensitive information can be any data regarded as sensitive by the transferring entity.
- UK businesses will have to clearly label certain types of data as 'sensitive' when transferring to a US organisation certified under the UK Extension to ensure adequate protection.
- For data on criminal offenses, the ICO highlights potential vulnerabilities, even when tagged as sensitive.

Emerging Technology + Regulation

Upcoming EU AI Act: practical implications for businesses and interplay with the GDPR

AI regulatory landscape

Existing laws
(GDPR, etc.)

Local enforcement
(e.g., Italy bans
ChatGPT)

Sectoral laws &
product liability

*EU AI Act**

Pro-innovation
approach in UK

AI legislative
proposals globally

EU AI Act – current state

Commission

April 2021

Commission proposed
the AI Act (EC Proposal)

Council

December 2022

Council adopted its
Common Position

Parliament

June 2023

Parliament adopted its
amendments

Trilogue & Final Approvals

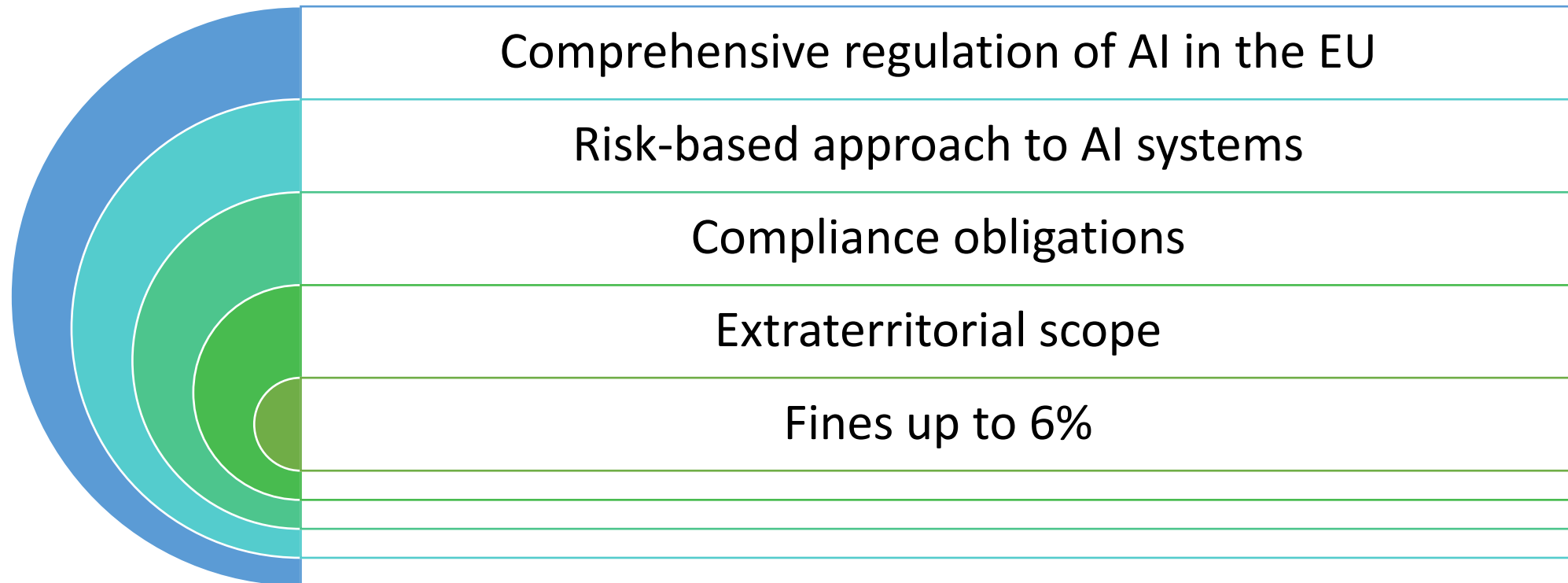
Ongoing | Enforcement date



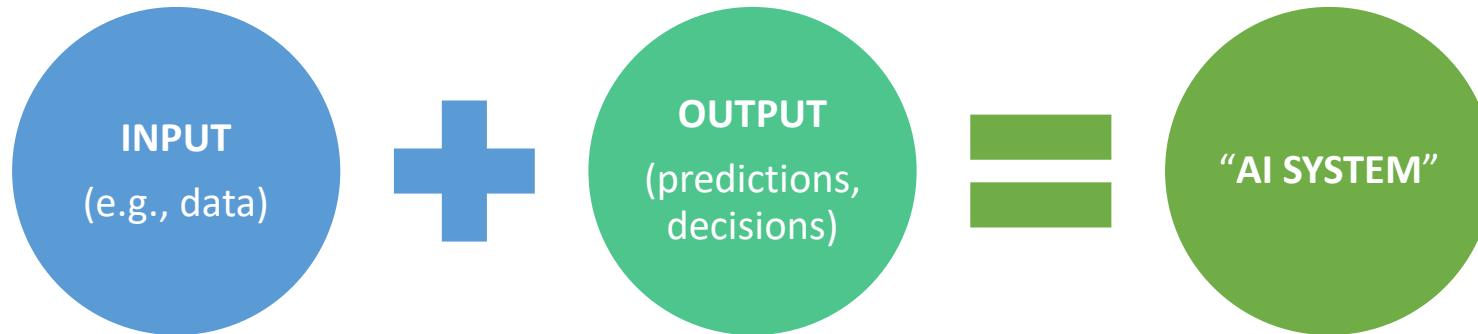
Application

Two years after the adoption

EU AI Act – key points



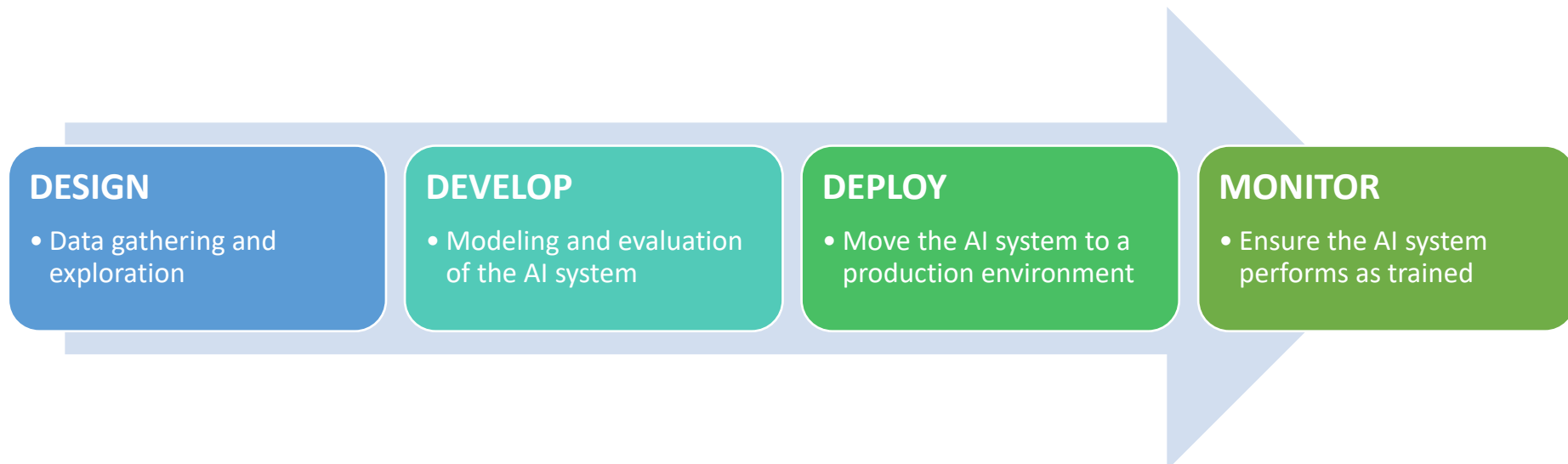
Key terminology



AI systems

- Engineered or machine-based system
- For a given set of objectives
- Generate outputs such as content, predictions, recommendations
- Varying levels of autonomy

AI system lifecycle



EU AI Act – risk-based approach

The cornerstone of the AI Act is a **classification system** that determines the level of risk an AI system could pose to the health and safety or fundamental rights of a person

Minimal or Limited Risk

- *Examples:* chatbots, spam filters, video games, etc. -> **Some transparency**



High Risk

- AI systems in certain areas: employment and worker management, critical infrastructure, law enforcement, etc. and safety components of regulated products* -> **Strict obligations**

Unacceptable Risk

- Social scoring, real-time facial recognition in public (and private*) spaces, subliminal techniques, etc. -> **Prohibited uses**

EU AI Act – general purpose AI

General Purpose AI (GPAI)

*An AI system that can be used in and adapted to a **wide range of applications** for which it was not intentionally and specifically designed*

[NEW] Obligations toward downstream providers
GPAI will be treated as a high-risk system

Foundational Models

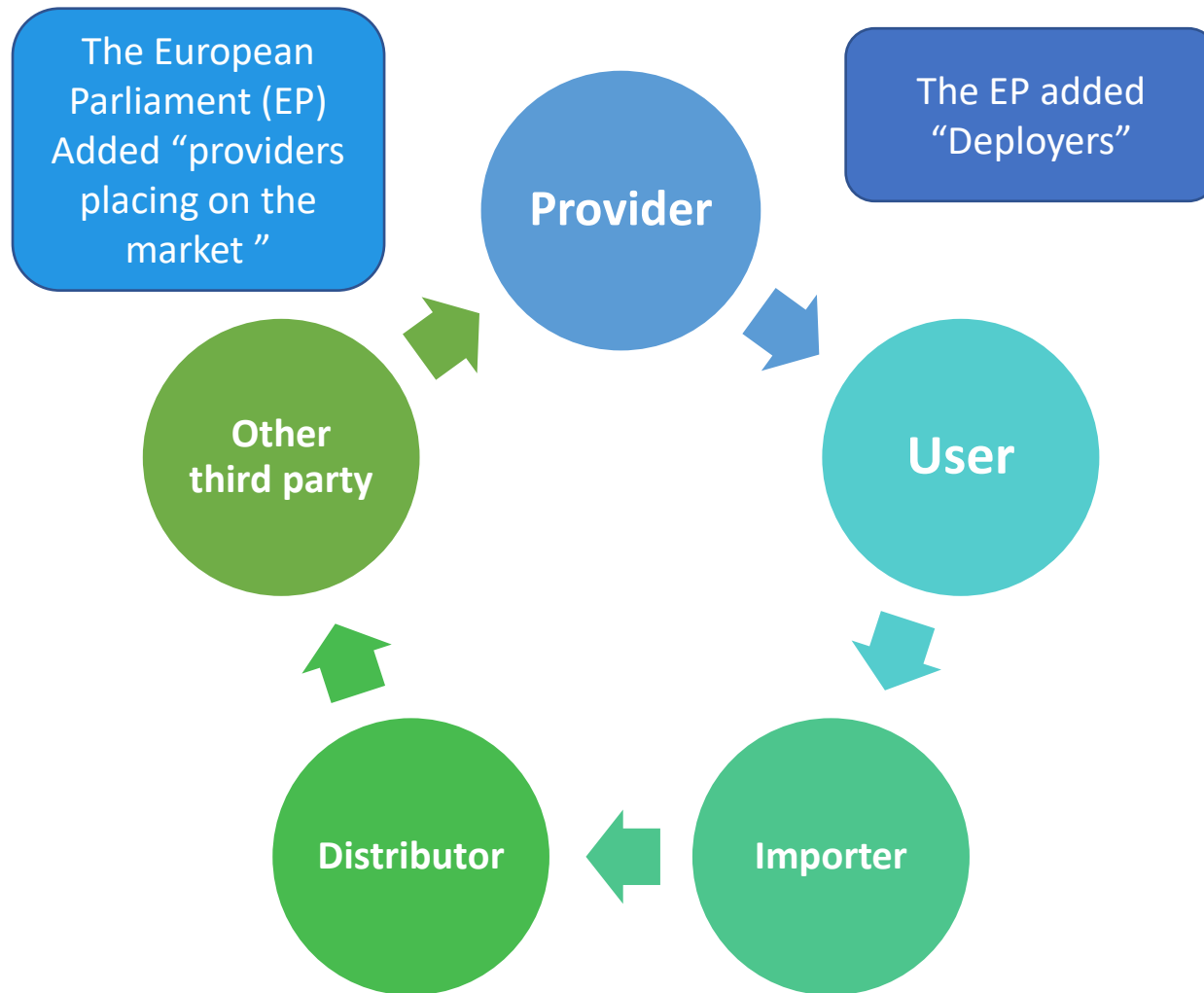
*Subset of GPAI specifically characterised by being trained on **broad data at scale***

[NEW] Independent assessment? Energy consumption considerations

Generative AI

AI intended to generate text, images, audio, or video content with some degree of autonomy

[NEW] Further transparency obligations and specific requirements re: **copyrighted materials**



Article 28. Obligations of distributors, importers, users or any other third-party

1. Any distributor, importer, user or other third-party shall be considered a **provider** for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

- a) they place on the market or **put into service** a high-risk AI system under their name or trademark;
- b) they modify **the intended purpose** of a high-risk AI system already placed on the market or put into service;
- c) they make a **substantial modification** to the high-risk AI system.

Provider Obligation (HRAIS)

- Conduct a **prior conformity assessment** before placing AI systems on the market
- Set up a **risk management system*** that documents and manages risks across the AI system's entire lifecycle
- Other **essential requirements** related to data and data governance; technical documentation; record-keeping; *transparency* and provision of information to users; human oversight; and robustness, accuracy and cybersecurity
- Conduct **post-market monitoring**

User Obligation

- Operate AI system in accordance with **instructions of use**
- Ensure **human oversight** when using AI system
- Monitor operation for **possible risks**
- **Inform** the provider or distributor about any serious incident or any malfunctioning
- **Existing legal obligations** continue to apply (e.g., DPIA requirements under GDPR)

The European Parliament added a fundamental rights impact assessment

EU AI Act – preparations

Buy-in from senior leadership

Create a **cross-functional team** or leverage existing programmatic resources (e.g., privacy program)

Develop and maintain a **register of AI/ML use cases**

Data/Input: Establish **guardrails and review processes** for data acquisition and data use for AI/ML

Model/Output: Develop **checkpoints and assessments** for model evaluation – technical expertise is needed

UK – A different perspective

“A pro-innovation approach to AI regulation”

- Proposal **does not target specific technologies** and focuses on context instead to avoid stifling innovation or placing undue burdens on businesses.
- **Principles-based regulatory regime** overseen by existing regulators.
- **No new laws or sanctions**
- **Sector-specific guidance** for organisations (e.g. ICO Guidance on AI and Data Protection, issued on 15 March 2023)

Five overarching principles:

- Safety, security and robustness;
- Transparency and explainability;
- Fairness;
- Accountability and governance;
- Contestability and redress (note that there will be **no new rights or routes to redress**).

1. Identify the role of the party in relation to the personal data:

- Independent Controller
- Processor
- Joint Controller

2. Consider legal basis for using the personal data

- The use of personal data to develop, train and deploy AI systems requires a legal basis
- Appropriate legal basis depends on lifecycle stage
- The use of an AI system also requires a legal basis

3. Identify how to comply with GDPR transparency requirements

- “*concise, understandable, and easily accessible*”
- Ensure the information can be provided within a reasonable timeframe

4. Consider how to comply with all GDPR data subject rights

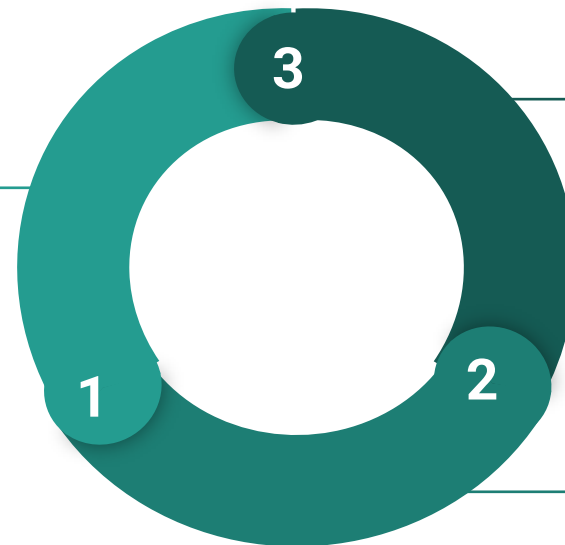
- Obtain **access** to data (e.g., confirmation of processing, receive a copy of the data)
- Data **portability** (e.g., transmit the data to another company)
- **Rectify** outdated or wrong data
- Request **deletion** of data (“right to be forgotten”)
- **Object** to processing (e.g., based on LI) or **restrict** processing

Automated Decision Making (“ADM”)

- Individuals’ right to not be subject to solely automated decisions significantly affecting them
- Broad interpretation of ‘ADM’ (see AG opinion in C-634/21, *Schufa I*)

High-Level Controls:

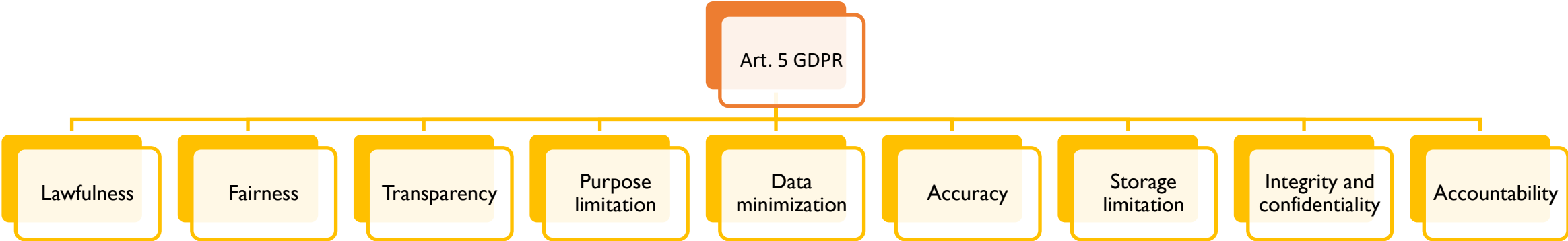
Legal Basis for ADM?



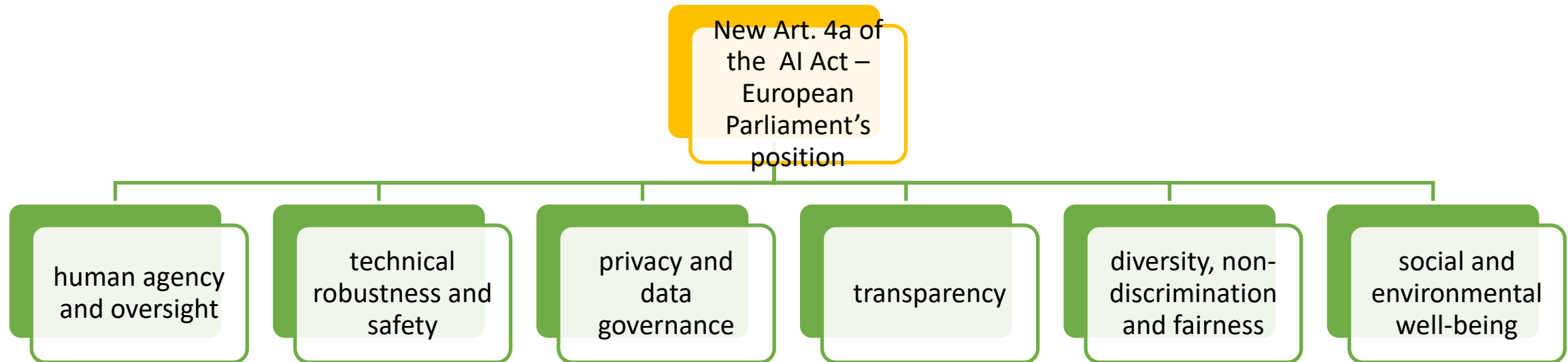
Are individuals informed about ADM?

Can individuals challenge decision or request human intervention?

GDPR principles



General trustworthy AI principles



GDPR

Art. 5(1)(a) general principle

Article 13

Article 14

Article 12

AI ACT

Art. 51 and 60 AIA

Art. 13 AIA

Art. 52 AIA

Art. 29 (6a)
EP position

Art. 69
c new:
added
by the
EP

Governance and Enforcement of the AI Act



Any upcoming Regulation in Switzerland?

Nicole Beranek Zanon

Partner

HÄRTING Attorneys-at-Law Ltd.

Profiling: Art. 21 FADP

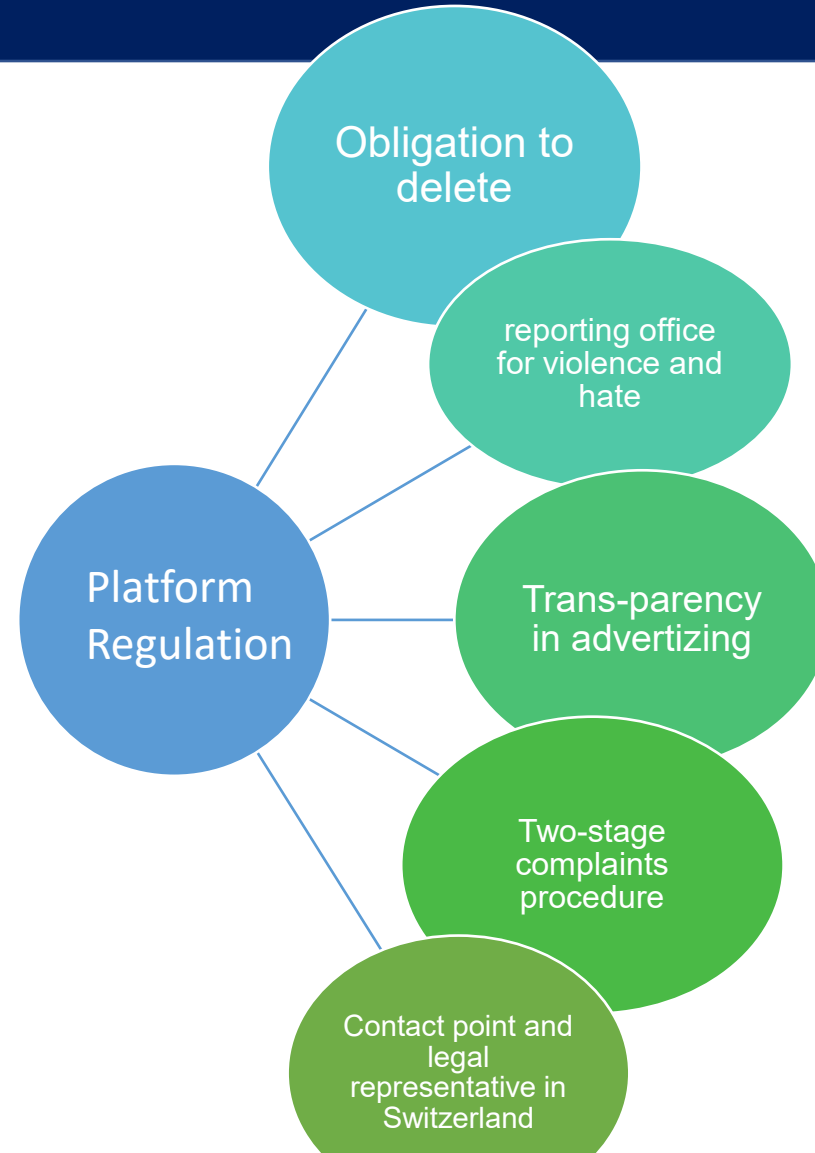
- Duty to inform regarding automated individual decisions exclusively based on automated processing
- Must be associated with a legal consequence or significantly affect data subject

Does not apply, if (Art. 21 para. 3 FADP):

- a. the automated individual decision is directly connected with the conclusion or the processing of a contract between the controller and the data subject and the data subject's request is granted; or
 - b. the data subject has explicitly consented to the decision being automated.
- Under Art. 6 Abs. 7 FADP consent is a pre-requisite for lawful (high-risk) profiling by private person or federal body

Digital Services Act for Switzerland?

- Platform Regulation
 - Oriented at European Data Services Act (EU-DSA)
 - Set for 2024



**Any upcoming Regulation in
UK?**

Aims

- reduce compliance costs in the sector and reduce the amount of paperwork that organisations need to complete to demonstrate compliance
- reduce burdens by enabling businesses to continue to use their existing cross-border transfer mechanisms if they are already compliant.
- give organisations greater confidence about the circumstances in which they can progress personal data without consent.
- increase public and business confidence in AI technologies.

Are you a local business working only in the UK?

- Yes – then its good news!
- No – then read on...

Is your business international? Do you work in / with the EU?

- Then GDPR still applies and so you might as well keep your compliance program as-is

Key issues

- Legal basis of processing
- Direct Marketing
- Cookie exemptions and consents

Scope

- (i) the living individual is identifiable by the controller or processor by “reasonable means at the time of the processing”; or
- (ii) the controller or processor “knows or ought to know” that a third party “will or is likely to be able to identify the person as a result of its data processing”
- If not = anonymized and outside scope of UK GDPR

Legitimate Interests

- “recognised” legitimate interests for which no balancing test is required
- processing for direct marketing purposes is legitimate interest BUT (along with any general commercial purpose) is not “recognised legitimate interest”, so subject to a balancing test against user’s rights
- Opposition fears this, as unlike consent legitimate interests do not require “easy” mechanism for opt-out

ROPA

- only for “high risk” – ICO to publish list (will not help those one still subject to GDPR)

Cookies - Key Changes

“strictly necessary” cookies can be used without consent.

DPDI “strictly necessary” is wider the current PECR definition and includes

- Improving the website or service
- Adapting the appearance or user preferences of the website or service
- Enhancing the software functionality
- Updating security
- Statistical analysis

Data captured CANNOT BE shared, save to make improvements etc

All use requires clear and comprehensive transparency notices

All require functionality for user to object

Looks like cookie banners are here to stay (is this yet another broken promise?)

Regulatory Enforcement + Fine Trends

Regulatory Enforcement + Fine Trends in the EU (+UK)

GDPR enforcement is often focused on the financial penalties: non-compliant organisations face fines of up to the higher of €20 million or 4% worldwide annual turnover.

Initial observations - Current statistics and objectives

Compliance

- 72 guidelines and 8 recommendations in 5 years. The most recent guidelines on: *calculation of administrative fines under the GDPR, on the application of Article 65(1)(a) GDPR, use of facial recognition technology in the area of law enforcement, and on identifying a controller or processor's lead supervisory authority.*

Enforcement

- *Fines in 2023 - 1.2 billion EUR fine for Facebook as a result of an EDPB binding decision (almost the same amount as the total amount of the previous year). 500-600 OSS cases per year.*

GDPR Sanctions – Current Landscape

- **Non-financial penalties received less publicity but can be just as significant:**
 1. **Reprimands and warnings issued by the DPA:**
 - i. **UK Home Office was reprimanded in October 2022 by the ICO for losing sensitive documents relating to terrorism in a public location. The personal data in the documents included a foreign visa applicant's details and details of two Metropolitan Police officers.**
 2. **Temporary or permanent ban on data processing:**
 - i. **In July 2022, the Danish municipality of Helsingør was ordered to temporarily stop processing data via Google Analytics after a Danish decision ruled that Google Analytics' transfers of personal data could not be afforded GDPR-like protections.**
 3. **Order of rectification, restriction or erasure of personal data:**
 - i. **Tends to be enforced by individuals exercising their rights under Articles 16, 17 and/or 18 GDPR.**
 4. **Suspension of transfers of personal data to third countries:**
 - i. **In April 2021, Portuguese National Institute for Statistics' transfers of personal data to Cloudflare, Inc. in the US were based on the SCCs. Portuguese DPO ordered the National Institute for Statistics to stop processing the data and suspend the transfers.**
 - ii. **Even if SCCs are in place, there may still be no guarantee that the personal data transferred will be adequately protected in the third country.**

Key Trends between Fines and Other Sanctions

- **Frequency of fines: up to October 2023, an additional 493 GDPR fines were issued as compared to the previous year (avg is close to 500 p.a).**
- **Total € 4,414,051,564**
- **Average quantum of fines during the period 2018-2022 was €1,533,910 across the EU. Note that this is distorted due to large fines against global technology companies, including:**
 1. **Meta, fined over €2 billion in total by the Irish DPC;**
 2. **Amazon, which was fined €746 million by the Luxembourg DPA;**
 3. **Tik Tok, which was fined €345 million by the Irish DPC;**
 4. **Google, which was fined €150 million by the French DPA.**
- **What about the frequency of non-financial penalties?**
 1. **UK ICO issued 24 reprimands during the period April 2021 – March 2022, compared with 4 fines with an aggregate value of £740,800 during the same period.**
 2. **French CNIL carried out 18 enforcement actions in 2021, only two of which resulted in solely non-financial penalties.**
- **DPAs often mix financial penalties with non-financial penalties:**
 - **Stop processing or remediation orders**

Business Impacts of Non-Financial Penalties

- **Businesses should consider the following impacts:**
 1. **Cost of third-party advisors to bring their data protection compliance programme up to the GDPR's standards.**
 2. **Operational cost of reviewing IT systems and implementing a new, GDPR-compliant, data processing infrastructure in the business.**
 3. **Reputational damage for the business if issued with a public reprimand and order to stop processing.**

- **Priority of the DPA is to ensure individuals are protected from poor data protection practices.**

- **Engagement of senior management to ensure data protection remains a priority:**
 1. **Is there a tension between innovation by senior executives and data protection compliance?**
 2. **Conduct diligence into third-party partners' GDPR compliance.**
 3. **Do the business and its partners have reputable certifications such as ISO, SOC and CMMI?**

EDPB Strategy 2021-2023 (new strategy 2023-2026 to be adopted soon?)

- **Key action 1:** encourage and facilitate **use of the full range of cooperation tools** enshrined in Chapter VII of the GDPR.

EDPB Statement on Enforcement Cooperation (28 April 2022) (“**Vienna Declaration**”): *“EDPB will facilitate the use of all instruments provided for in the GDPR, including Article 62 joint investigations ... The EDPB will also streamline the use of Article 65 dispute resolution mechanism and Article 66 urgency procedures by DPAs.”*

- **Key action 2:** implement a **Coordinated Enforcement framework** (CEF).

Within CEF priority for 2024: implementation of the right of access by controllers. In a CEF, the EDPB prioritizes a certain topic for data protection authorities (DPAs) to work on at national level. The results of these national actions are then bundled and analyzed, generating deeper insight into the topic and allowing for targeted follow-up on both the national and the EU level.

- **Key action 3:** establish a **Support Pool of Experts** (SPE) on the basis of a pilot project.

SPE launched on 21 February 2022, a list of experts has been drawn up on 23 June 2022. applications are still open, and the list will be valid until 10 February 2026.



EDPB adopted the Guidelines 04/2022 on the calculation of administrative fines under the GDPR in June 2023.

New EDPB Guidelines offer a 5-step method of calculating a fine to be used by all DPAs across the EEA.



Overview of the methodology

- Step 1** Identifying the processing operations in the case and evaluating the application of Article 83(3) GDPR.
(Chapter 3)
- Step 2** Finding the starting point for further calculation based on an evaluation of (Chapter 4)
 - a) the classification in Article 83(4)–(6) GDPR;
 - b) the seriousness of the infringement pursuant to Article 83(2)(a), (b) and (g) GDPR;
 - c) the turnover of the undertaking as one relevant element to take into consideration with a view to imposing an effective, dissuasive and proportionate fine, pursuant to Article 83(1) GDPR.
- Step 3** Evaluating aggravating and mitigating circumstances related to past or present behaviour of the controller/processor and increasing or decreasing the fine accordingly.
(Chapter 5)
- Step 4** Identifying the relevant legal maximums for the different processing operations. Increases applied in previous or next steps cannot exceed this amount.
(Chapter 6)
- Step 5** Analysing whether the final amount of the calculated fine meets the requirements of effectiveness, dissuasiveness and proportionality, as required by Article 83(1) GDPR, and increasing or decreasing the fine accordingly.
(Chapter 7)



CNIL.

Priority topics for investigations in 2023: "smart" cameras, mobile apps, bank and medical records



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

1. Regulate consistently and effectively
2. Safeguard Individuals and promote data protection awareness
3. Prioritise the protection of children and other vulnerable groups
4. Bring clarity to stakeholders
5. Support organisations and drive compliance





GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Digital identity, cookies, artificial intelligence
(temporary ban of ChatGPT from Italian DPA)

Enforcement Actions - Largest GDPR Fines To Date (2018-2023)

 IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR
 LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown
 IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR
 IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR
 IRELAND	2023-09-01	345,000,000	TikTok Limited	Art. 5 (1) c), 5 (1) f) GDPR, Art. 12 (1) GDPR, Art. 13 (1) e) GDPR, Art. 24 (1) GDPR, Art. 25 (1), (2) GDPR
 IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR
 IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR

How to Prepare and Engage with Regulators

- **Practical steps to be taken:**
 1. **Maintain and update records of processing.**
 2. **Regularly undertake DPIAs before processing data.**
 3. **Designation of a data protection officer.**
 4. **Registration with the relevant DPA – have the fees and other renewals been made on time?**
- **Timing for action**
 1. **As early as possible and not later than 72 hours after awareness of a personal data breach.**
 2. **Compliance with the requirements of the GDPR should not be an afterthought.**
- **Timeframes for change and its substance. Consequences of no change?**
- **Some example cases:**
 1. **May 2020: Belgian DPA fined a company €50,000 for combining the head of compliance, risk management and audit role with that of a DPO on the grounds that this generates a conflict of interest.**
 2. **October 2020: British Airways' engagement with the ICO in demonstrating mitigating factors led to a 20% reduction in the penalty issued by the ICO.**

Regulatory Enforcement + Fine Trends in Switzerland

Nicole Beranek Zanon

Partner

HÄRTING Attorneys-at-Law Ltd.

Criminal proceedings

Differs significantly from GDPR:

- **Natural persons** can be fined up to **CHF 250'000**
- **Aiding and abetting** is *not punishable*, since the violations are merely transgressions (Art. 25 StGB: "Whoever intentionally provides assistance to a felony or misdemeanor [...]").
- Fines can be issued up to **C-level** or above. (esp. no executive position required)
- **Intention required: Sufficient to take it into consideration**
- Violations are entered in the criminal record if a fine of more than 5000 Swiss francs has been imposed!
- **Legal entities** if fine **under CHF 50'000**

- Art. 61 Violation of duties of care

On complaint, a fine not exceeding 250,000 francs shall be imposed on private persons who wilfully:

- a. disclose personal data abroad in violation of Article 16 paragraphs 1 and 2 without satisfying the requirements of Article 17;
- b. assign the data processing to a processor without satisfying the requirements of Article 9 paragraphs 1 and 2;
- c. fail to comply with the minimum requirements for data security stipulated by the Federal Council in Article 8 paragraph 3.

Criminal proceedings

- Non-Compliance with:
 - Art. 60: Violation of information, disclosure and cooperation obligations
 - Art. 61: Violation of due diligence obligations
 - Art. 62: Violation of the professional duty of confidentiality
 - Art. 63: Disregarding orders

- Art. 61 Violation of duties of care

On complaint, a fine not exceeding 250,000 francs shall be imposed on private persons who wilfully:

- disclose personal data abroad in violation of Article 16 paragraphs 1 and 2 without satisfying the requirements of Article 17;
- assign the data processing to a processor without satisfying the requirements of Article 9 paragraphs 1 and 2;
- fail to comply with the minimum requirements for data security stipulated by the Federal Council in Article 8 paragraph 3.

Criminal proceedings

- Penalty provisions of the new FADP are generally only punished **upon request!**
- **The person entitled to file a criminal complaint** is the person who has been violated by the act (cf. Art. 30 para. 1 StGB) ="person concerned whose relevant rights have been violated"
- **Application deadline** is three months from the date of knowledge of the offender (cf. Art. 31 StGB)

Criminal proceedings

FDPIC can file complaint with prosecution authority and cooperate with them.

-  **Art. 65 Jurisdiction**

¹ The prosecution and the adjudication of criminal acts is a matter for the cantons.

² The FDPIC may file a complaint with the competent prosecution authority and exercise the rights of a private claimant in the proceedings.

Prosecution is subject to statute of limitations of five years.

-  **Art. 66 Statute of limitations for prosecution**

Prosecution is subject to a statute of limitations of five years.

Administrative Procedures

- New authorizations pursuant to Art. 49 ff. FADP
- Binding orders to obtain information (enforcement by force necessary)

Divided into three phases:

- 1. Preliminary clarification:** Preliminary clarification as an informal preliminary review
- 2. Investigation procedure:**
 - preliminary clarification,
 - investigative measures,
 - precautionary and administrative measures
- 3. Appeal procedure:** only applies if the FDPIC issues an order

– Art. 49 Investigation

¹ The FDPIC shall open an investigation into a federal body or a private person ex officio or in response to a report if there are sufficient indications that a data processing activity could violate data protection regulations.

² It may refrain from opening an investigation if the violation of data protection regulations is of minor importance.

³ The federal body or the private person shall provide the FDPIC with all the information and documents that is needed for the investigation. The right to refuse to provide information is governed by the Articles 16 and 17 of the APA¹⁹, unless Article 50 paragraph 2 of this Act provides otherwise.

⁴ If the data subject has filed a report, the FDPIC shall inform them about the steps taken in response and the result of any investigation.

Administrative Proceeding

- New **administrative assistance provisions** in Art. 54 (between Swiss authorities) and Art. 55 (vis-à-vis foreign authorities) new FADP
- FDPIC may exchange information with EU data protection authorities by name, receive information from them and use it for **investigations**
- **Administrative criminal law**, which is why bilateral treaties of international mutual legal assistance in criminal matters do not apply:
- **No mutual enforcement of** coercive measures such as fines between FDPIC and EU data protection authorities
- BUT: FDPIC may allow foreign data protection authorities to **send** rulings **directly to** Switzerland, provided **Switzerland** is granted **reciprocal rights** (cf. Art. 58 para. 3 new FADP)

Administrative Measures

- Art. 51 Administrative measures

¹ If data protection regulations have been violated, the FDPIC may order that the processing be modified, suspended or terminated, wholly or in part, and the personal data deleted or destroyed, wholly or in part.

² It may delay or prohibit disclosure abroad if this violates the requirements of Article 16 or 17 or provisions relating to the disclosure of personal data abroad in other federal acts.

³ It may in particular order that the federal body or the private person:

- a. provide him or her with information in accordance with Articles 16 paragraph 2 letters b and c and 17 paragraph 2;
- b. take the measures in accordance with Articles 7 and 8;
- c. inform the data subjects in accordance with Articles 19 and 21;
- d. conduct a data protection impact assessment in accordance with Article 22;
- e. consult him or her in accordance with Article 23;
- f. provide him or her or, if applicable, the data subject with information in accordance with Article 24;
- g. provide the data subject with the information specified in Article 25.

⁴ It may also order that private controllers with registered office or domicile abroad appoint a representative in accordance with Article 14.

⁵ If the federal body or the private person has taken the required measures during the investigation in order to restore compliance with the data protection regulations, the FDPIC may simply issue an official warning.

Sources EU

<https://www.cnil.fr/en/priority-topics-investigations-2023-smart-cameras-mobile-apps-bank-and-medical-records#:~:text=The%20CNIL%20carries%20out%20checks,health%20files%20and%20mobile%20apps.>

https://www.dataprotection.ie/sites/default/files/uploads/2021-12/DPC_Regulatory%20Strategy_2022-2027.pdf

https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en?f%5B0%5D=opinions_publication_type%3A64

https://edpb.europa.eu/sites/default/files/files/file1/edpb_strategy2021-2023_en.pdf

https://edpb.europa.eu/news/news/2022/call-experts-new-edpb-support-pool-experts_en

<https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/#:~:text=While%20the%20GDPR%20right%20to,in%20situations%20where%20AI%20systems>

<https://www.enforcementtracker.com/>

Sources CH

- Federal Act on Data Protection (FADP) of the 25 September 2020. Retrieved from www.fedlex.admin.ch/eli/cc/2022/491/en
- Ordinance on Data Protection (DPO) of 31 August 2022. Retrieved from <https://www.fedlex.admin.ch/eli/oc/2022/568/de>

Thank you!