MAYER | BROWN

All the Buzz:

The Latest Developments for Emerging & Tech Companies

Recent Developments with the EU and UK GDPR: What Utah Tech Companies Need to Know

September 12, 2023

Agenda

All the Buzz

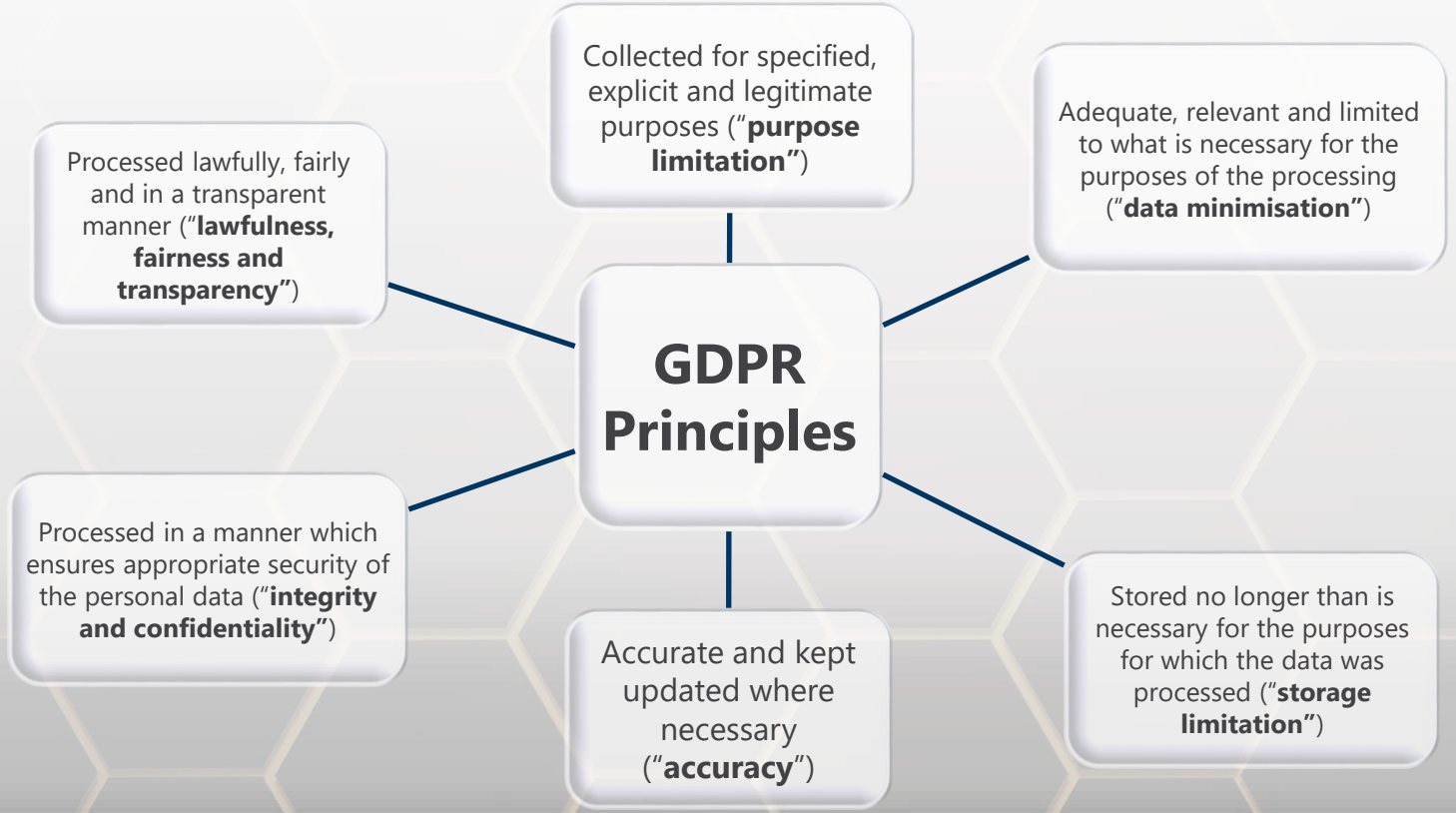
- The EU/UK GDPR: Overview and How it Impacts Utah Tech Companies
- Recent Enforcement Trends
- Impact of the new EU/US Trans-Atlantic Data Privacy Framework
- Other EU and UK Privacy-related Laws Relevant to Utah Tech Companies
  - EU Digital Markets and Data Developments
  - Draft EU AI Act and UK AI Developments

EU and UK GDPR: Overview and How it Impacts Utah Tech Companies

Legal Framework – EU/UK GDPR

- **EU GDPR:** primary law regulating personal data processing in the European Economic Area ("EEA")
- **UK GDPR =** version of the GDPR retained in the UK post-Brexit
  - UK GDPR contains the same **general data protection obligations** as EU GDPR
- **Broad definition of personal data:** Any information relating to an identified or identifiable individual
  - GDPR applies to pseudonymized data, but not to anonymized data
- **Fines:** greater of:
  - EUR 20 million / £17.5 million; or
  - 4% of previous annual global turnover.

Legal Framework – EU/UK GDPR (cont.)



How can Utah Tech Companies be Impacted by the EU/UK GDPR?

All the Buzz

Direct applicability: The EU/UK GDPR is extra-territorial:

- *Processing in the context of activities of an "establishment" in the EEA / UK*
- *Monitoring data subjects in the EEA / UK*
- *Offering goods / services to individuals in the EEA / UK*

Situations where a Utah entity's processing may be directly subject to GDPR

If directly applicable, Utah entities must comply with the EU/UK GDPR for all of the applicable processing → Need to implement GDPR-compliant documentation, security processes and data breach response obligations

How can Utah Tech Companies be Impacted by the EU/UK GDPR? (cont.)

All the Buzz

Indirect applicability: contractual obligations with EEA/UK-based customers:

- Provisions in **data processing agreements**:
  - Mandatory provisions in controller-to-processor clauses
  - Mandatory joint controller arrangements
  - Controller-to-controller data sharing agreements (not mandatory)
- **Data breach** response obligations:
  - EEA/UK organisations have data breach notification obligations
  - 72hr timeframe to notify data protection authorities and/or individuals
  - Controllers to pass down provisions to Utah-based processors
- International **data transfers**:
  - EEA/UK entities are subject to international data transfer obligations
  - Utah entities should expect to be asked to enter into these arrangements

GDPR: Data Processing Roles

All the Buzz

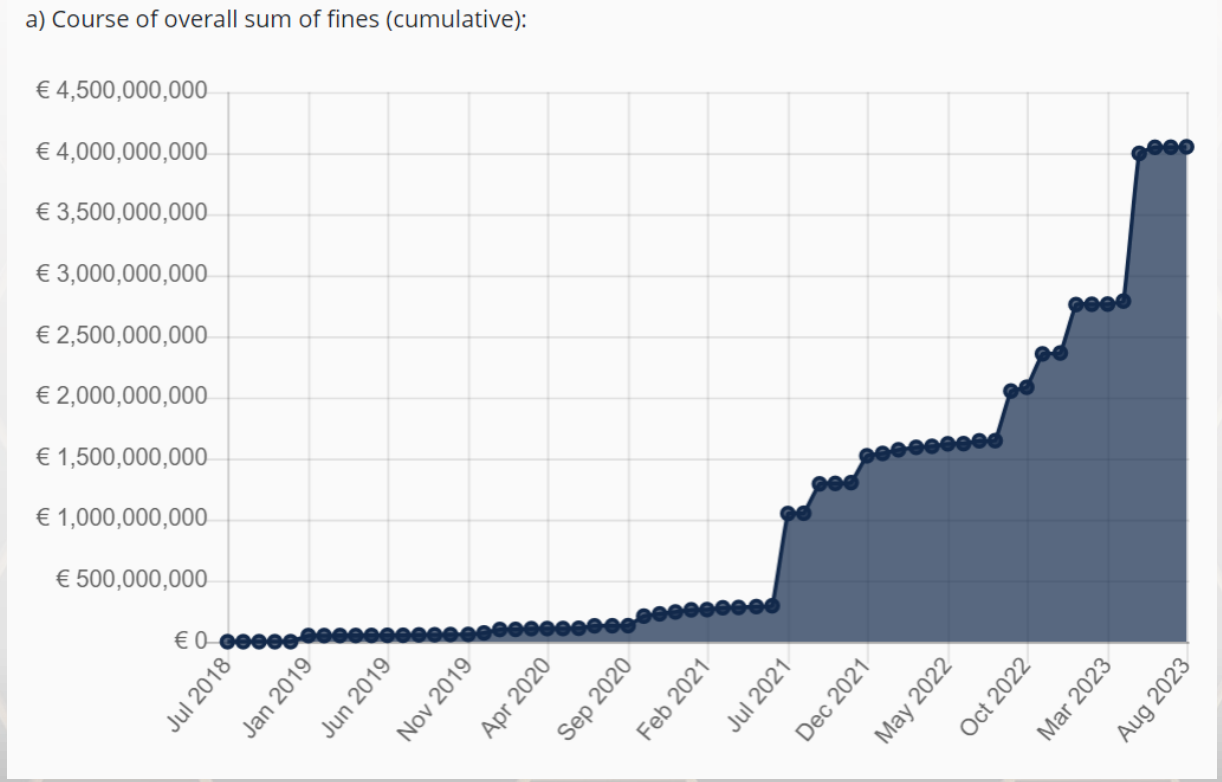
Controller =
An entity that ***determines the purposes and means of the processing of personal data, alone*** *or* ***jointly*** *with others*

Processor =
An entity that processes personal data ***on behalf of the controller***

- **Factual determination** regardless of what a contract between the parties states
  - Who decides why and how the personal data is processed? How much freedom do they have?
- Blurring roles
  - **Not binary** – a party can be a controller with respect to some processing activities and processor with respect to others
  - **Challenging** to determine processing roles in complex data flows or in large corporate groups
  - Expanding definition of **joint controllers** through CJEU case law and European guidance

Recent Enforcement Trends

GDPR Today: Increasing Levels of Fines



Source: GDPR enforcement tracker (August 2023)
https://www.enforcementtracker.com/?insights

GDPR Today: Top Fines

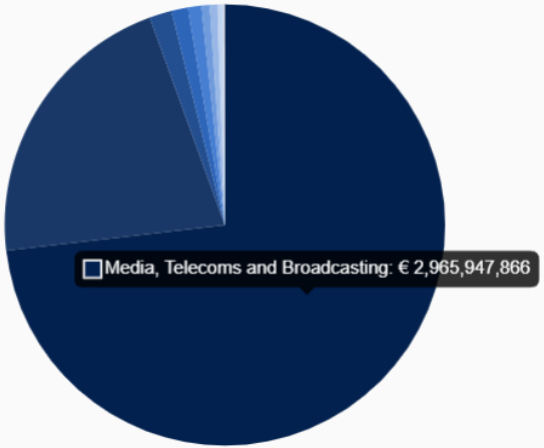
⊕	ETid-1844	 IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing
⊕	ETid-778	 LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown	Non-compliance with general data processing principles
⊕	ETid-1373	 IRELAND	2022-09-05	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	Non-compliance with general data processing principles
⊕	ETid-1543	 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	Non-compliance with general data processing principles
⊕	ETid-1502	 IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
⊕	ETid-820	 IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
⊕	ETid-978	 FRANCE	2021-12-31	90,000,000	Google LLC	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
⊕	ETid-980	 FRANCE	2021-12-31	60,000,000	Facebook Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
⊕	ETid-979	 FRANCE	2021-12-31	60,000,000	Google Ireland Ltd.	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
⊕	ETid-23	 FRANCE	2019-01-21	50,000,000	Google LLC	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing

Source: GDPR enforcement tracker (August 2023)
https://www.enforcementtracker.com/?insights

GDPR Today: Fines by Sector

All the Buzz

1. By total sum of fines:



Sector	Sum of Fines
Media, Telecoms and Broadcasting	**€ 2,965,947,866** (at 272 fines)
Industry and Commerce	**€ 864,005,141** (at 404 fines)
Transportation and Energy	**€ 66,700,570** (at 90 fines)
Employment	**€ 48,763,177** (at 119 fines)
Finance, Insurance and Consulting	**€ 39,894,658** (at 185 fines)
Public Sector and Education	**€ 24,741,263** (at 195 fines)
Accomodation and Hospitalty	**€ 22,462,148** (at 58 fines)
Health Care	**€ 16,176,109** (at 174 fines)
Real Estate	**€ 2,597,731** (at 56 fines)
Individuals and Private Associations	**€ 1,964,446** (at 225 fines)
Not assigned	**€ 1,421,808** (at 105 fines)

Source: GDPR enforcement tracker (August 2023)
https://www.enforcementtracker.com/?insights

GDPR Today: Increasing Scrutiny Over International Data Transfers

All the Buzz

- **Schrems II decision of the Court of justice of the European Union (July 2020):** Invalidated EU-US Privacy Shield. Upheld Standard Contractual Clauses (SCCs) but made data transfers significantly harder.
- **New EU SCCs for data transfers (June 2021):** Required pre-existing arrangements to be repapered.
- **EDPB recommendations issued (June 2021):** Requires **transfer impact assessments** and **supplementary measures** to be adopted:
  - Pseudonymization or encryption, with the key held in Europe under control of the data exporter → Can be difficult to implement in practice
- **Google Analytics, Mailchimp, Cloudflare decisions: DPAs ordered the transfer of data to the US to stop, but no fines were issued**

Impact of the New EU/US Trans-Atlantic Data Privacy Framework

GDPR - Data Transfer Mechanisms

All the Buzz

- **Adequacy decisions** (Art. 45 GDPR): transfers to countries that have been recognized as providing an adequate level of protection do not need specific authorization
  - European Commission and the UK Government have each given an adequacy decision to one another
  - 15 countries have been granted adequacy under the EU GDPR
  - 11 countries have been granted adequacy under UK GDPR
- In the absence of an adequacy decision, **safeguards** (Art. 46 GDPR) are needed, such as:
  - **Standard Contractual Clauses** + Transfer impact assessment (post-Schrems II)
  - Binding Corporate Rules
    - Supplementary measures required post-Schrems II (Pseudonymization or encryption, with the key held in Europe under control of the data exporter)
- If additional safeguards cannot be implemented in a specific case, **derogations** (Art. 49 GDPR) may apply (e.g., consent).

What is the EU-US Data Privacy Framework?

- **10 July 2023:** European Commission adopted an adequacy decision for the EU-US Privacy Framework ("DPF")
  - Free flows of EEA personal data to US entities certified under the EU-US Privacy Framework
  - At present, only US entities subject to enforcement powers of FTC or US Department of Transportation can certify under the framework
  - US entities need to self-certify to the US Department of Commerce's International Trade Administration that they will comply with the DPF's principles
  - All organisations that maintained their certifications under the EU-US Privacy Shield remain certified under the DPF

What is the EU-US Data Privacy Framework? (cont.)

All the Buzz

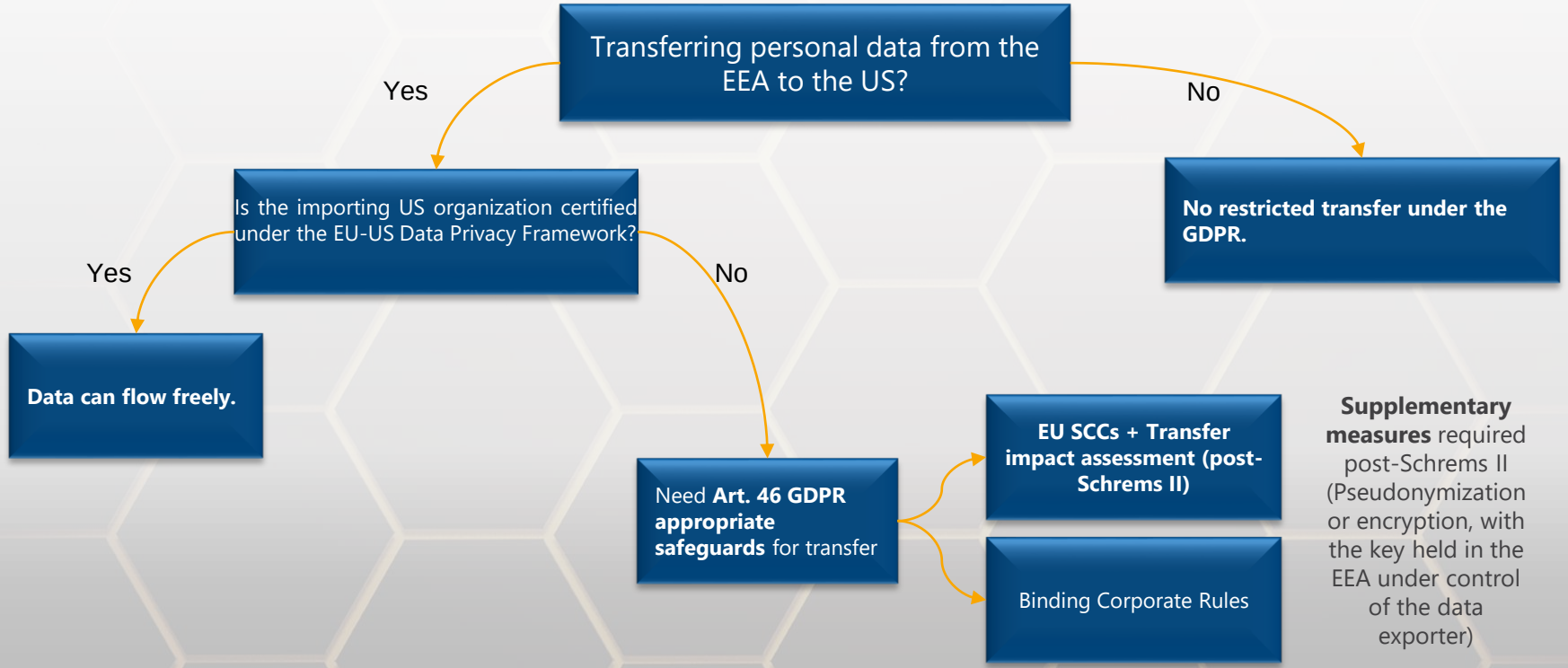
- **DPF Principles:** US entities who self-certify must declare compliance (and comply!) with DPF principles under US law:
  - Principles similar to Privacy Shield
  - Transparency obligations through privacy policies and individuals data access rights
  - US entities accountable for onward transfers
  - Similar security requirements to GDPR
  - Similar data minimisation requirements as GDPR
  - Recourse and enforcement, includes arbitration requirement

Data Privacy Framework 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

- **No certification = no change** except that DPF can be taken into account when conducting Transfer Impact Assessments

Re-Cap Flowchart – EU-US Data Transfers



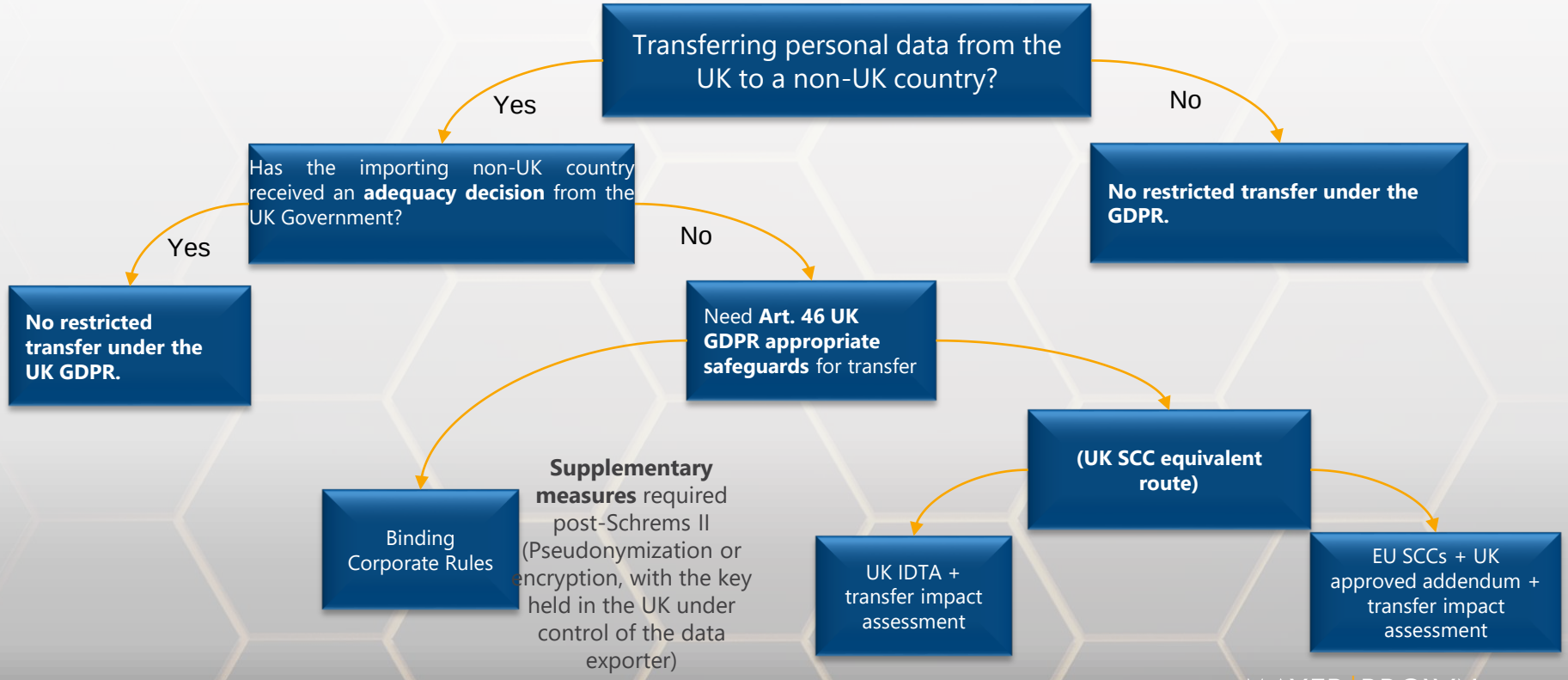
What about the UK?

All the Buzz

The EU-US DPF does not cover transfers of UK-based personal data to the US!

- **June 9 2023:** UK and the US commit in-principle to a UK-US data bridge – known as the UK Extension to the EU-US DPF
- Matter of time before the UK Government grants adequacy to the US through the UK Extension to the EU-US DPF.
- For the time being, the position remains uncharged: UK IDTA or UK Addendum to EU SCCs is required

Re-Cap Flowchart – UK International Data Transfers



Other EU and UK Privacy-related Laws Relevant to Utah Tech Companies

All the Buzz

EU Digital Markets and Data Developments

	Digital Services Act (DSA) Regulation (EU) 2022/2065	**Digital Markets Act (DMA)** Regulation (EU) 2022/1925	**Data Governance Act (DGA)** Regulation (EU) 2022/868	**Draft Data Act (DA)**
Goal	Create a safer digital space, protecting fundamental rights of users	Fairer competition in the digital markets	Aims to create a harmonized framework for public sector data to be reused	Ensure fairness in the digital environment and stimulate a competitive data market
Applies to	Intermediary services (web hosting, cloud providers, online marketplaces, social media, search engines)	Gatekeepers (large providers of core platform services, app stores, messenger services)	Data intermediation service providers (created by the DGA) and public sector	Various parties, from manufacturers of connected devices to data holders and public bodies
Impact	Several reporting obligations on content moderation activities; certain providers have obligations on algorithmic transparency and to provide options of recommender systems not based on profiling	Wide range of obligations for gatekeepers relating to data, advertising, e-commerce, interoperability and the commercial relationship between the service providers, customers and end users. Might require changes to the business models of some digital platforms	Stimulates data sharing by public bodies and data altruism; Establishes the European Data Innovation Board	May impose data sharing obligations on companies; New rules on who can use and access data generated in the EU across all economic sectors
Status	Applies to very large online platforms and search engines as of **August 2023**; will apply to other providers as of **February 2024**	Obligations to designated gatekeepers will apply as of **March 2024**	Applies from **September 2023**	EU institutions negotiating final text; Adoption expected by the end of 2023

Summary: *Digital regulation interplays with GDPR; EU is progressively expanding regulation beyond the realm of personal data. These developments will likely be relevant for businesses in the mid- to long-term.*

Draft EU AI Act

All the Buzz

- Proposed regulation aimed at harmonizing requirements for AI systems used, put into service or placed in the market in the EU, with a **risk-based approach** to AI.
- AI systems to be categorized in different levels, with different obligations:
  - Systems deemed to involve unacceptable risk will be **prohibited** (e.g., social scoring);
  - High-risk systems will need to comply with **strict conformity and documentation requirements**;
  - Limited risk systems will need to comply with **transparency** obligations.

Fines of up to **€40,000,000** or **7% of total worldwide annual turnover** (whichever is higher)

Apr. 2021
- Proposal by the EU Commission

Dec. 2022
- Council adopts its position on the text

14 June 2023
- EU Parliament adopted its position

Council, Commission and Parliament engaged in **trilogue negotiations** to agree on a **common version** of the text

Draft EU AI Act: High-Risk AI Systems

All the Buzz

AI systems covered by EU Directives or Regulations for certain categories of products, such as:

- Machinery
- Safety of toys
- Civil aviation
- Medical devices
- Type-approval requirements for motor vehicles
- Lifts and their safety components

AI systems intended for use in certain areas and use cases, such as:

- Biometric identification and categorization of natural persons
- Safety components in the operation of critical infrastructure
- Education and vocational training
- Employment and workers' management
- Access to essential private or public services and benefits
- Law enforcement
- Migration, asylum and border control management
- Administration of justice and democratic processes

Draft EU AI Act: Key Obligations for High-Risk AI

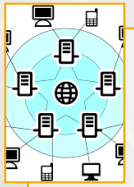
All the Buzz

Data governance: training, validation and testing data must be **relevant**, **representative**, **free of errors** and **complete**

Testing: testing methods must be **suitable** to evaluate the **effectiveness** of the AI system throughout its **lifecycle**

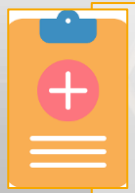
Transparency and oversight: system must enable users to **interpret and appropriately use** its output, and be subject to **effective human oversight**

Accuracy, robustness, cybersecurity: system must be accurate and **resilient** against **errors, faults, or attempts by unauthorized third parties** to alter its use or performance



Record keeping: when operating, system must generate logs that allow some **traceability** of its functioning

Risk management system: the risks associated with the use of the AI system must be **properly and continuously assessed**, and subject to suitable **mitigation measures**



Quality management system: providers must have **written policies, procedures and instructions** that document its approach to:

- **Design, development, quality control, examination, test and validation of the system**
- Processes in place for **data management**, **risk management**, **post-market monitoring**, **reporting** of serious incidents or malfunctioning
- The **accountability framework** in place setting out the **responsibilities of management and staff**

UK AI White Paper

All the Buzz

- On 29 March 2023, UK Government published its AI White Paper
- Pro-innovation framework to "make responsible innovation easier"
- 5 principles:
    1. Safety, security, robustness
    2. Appropriate transparency and explainability
    3. Fairness
    4. Accountability and governance
    5. Contestability and redress
- No new "heavy-handed" legislation but empowering existing regulators to ensure tailored, context-specific, risk-based, proportionate and adaptable regulation of AI in the UK
- Creation of a new central function to support existing regulators

UK to Host First Global AI Regulation Summit

All the Buzz

FINANCIAL TIMES

UK COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

UK politics & policy + Add to myFT

Britain to host first global AI regulation summit in autumn

UK can exert leadership in setting 'guardrails' for new technology, Sunak to tell Biden in Washington meeting

Rishi Sunak, UK prime minister, will on Thursday hold talks in US with President Joe Biden about enhancing 'economic security' © Niall Carson/PA Wire

George Parker in Washington JUNE 7 2023 103

Rishi Sunak, UK prime minister, will on Thursday announce that Britain will this autumn host the first global summit on the regulation of artificial intelligence, after a meeting in Washington with President Joe Biden.

Exclusive news, data

REUTERS World Business Markets Sustainability Legal More

Disrupted

UK PM Sunak pitches Britain as future home for AI regulation

Reuters

June 12, 2023 12:00 PM GMT+1 · Updated 2 days ago

[2/6] British Prime Minister Rishi Sunak attends the London Tech Week at the Queen Elizabeth II Centre in London, Britain June 12, 2023. Ian Vogler/Pool via REUTERS

Ana Hadnes Bruder
Partner, Frankfurt
+49 69 7941 1778
abruder@mayerbrown.com

Ana Hadnes Bruder is a partner in Mayer Brown's Frankfurt office and the global Cybersecurity & Data Privacy practice. Ana advises clients on **Data Privacy and Cybersecurity** matters, including preparing for and reacting to cyber-attacks, assessing and making required data breach notifications, analyzing data protection implications of new products and tools, developing strategic compliance roadmaps and implementing them.

Another focus of Ana's practice is **Artificial Intelligence (AI)**. Her practice covers both the intersection between AI, privacy and cyber and the proposed regulatory requirements around AI. Ana assists clients with data and corporate governance best practices, AI impact assessments and more broadly with AI risk management frameworks.

Ana further advises on **Technology Transactions** including cloud services, data and software licensing agreements, SaaS agreements, software development projects, e-commerce, and related Cybersecurity & Data Privacy questions.

Ana is a registered lawyer in Germany and Brazil and has twelve years of international experience as legal counsel in Brazil, France and Germany. She speaks English, German, French, Portuguese, Italian and Spanish.

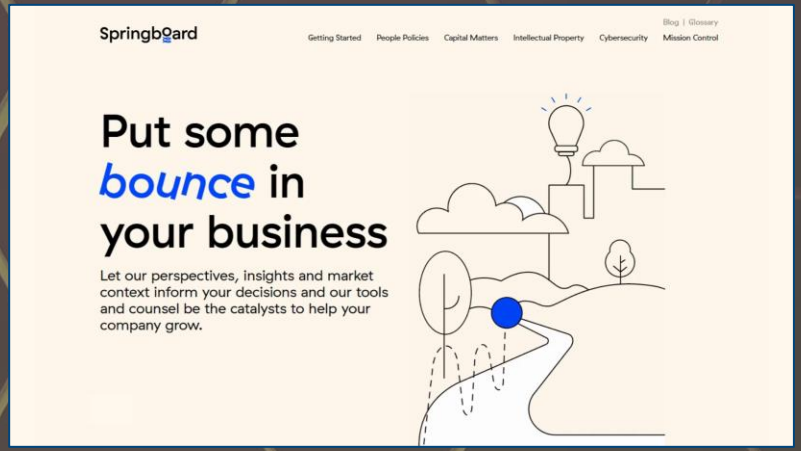
Before joining Mayer Brown, Ana gained experience representing foreign clients in judicial proceedings in Brazil and also worked as in-house counsel for a leading French company in Paris.

Reece Randall
Associate, London
+44 20 3130 3064
rrandall@mayerbrown.com

Reece Randall is an associate in the Intellectual Property & IT Group, as well as the Technology & IP Transactions and Cybersecurity & Data Privacy practices of the London office. He joined Mayer Brown as a trainee in 2018 and spent six months on secondment with the M&A underwriting team of a leading Lloyd's insurer.

Reece advises clients on a broad range of **Intellectual Property, Technology, Cybersecurity and Data Privacy** matters. His experience includes advising on intellectual property exploitation and licensing, GDPR compliance projects, data breach and cybersecurity incident response and negotiating data protection and intellectual property provisions in commercial agreements. Reece also regularly advises on intellectual property, data protection and technology aspects of corporate transactions.

Additional Resources



Thank You

Americas | Asia | Europe | Middle East

mayerbrown.com

MAYER | BROWN

Legal Framework – GDPR