



# **PRIVACY LAW ABROAD AND AT HOME:**

## **How Does the EU/UK GDPR Compare to Privacy Laws in the United States?**

**Doug Curwin, Sarah Leathwood, James Castro-Edwards, Nancy L. Perkins, Jami Vibbert**

May 18, 2022

# Agenda

---

## Data Protection Fundamentals

- The EU/UK privacy framework
- US privacy law and legislation



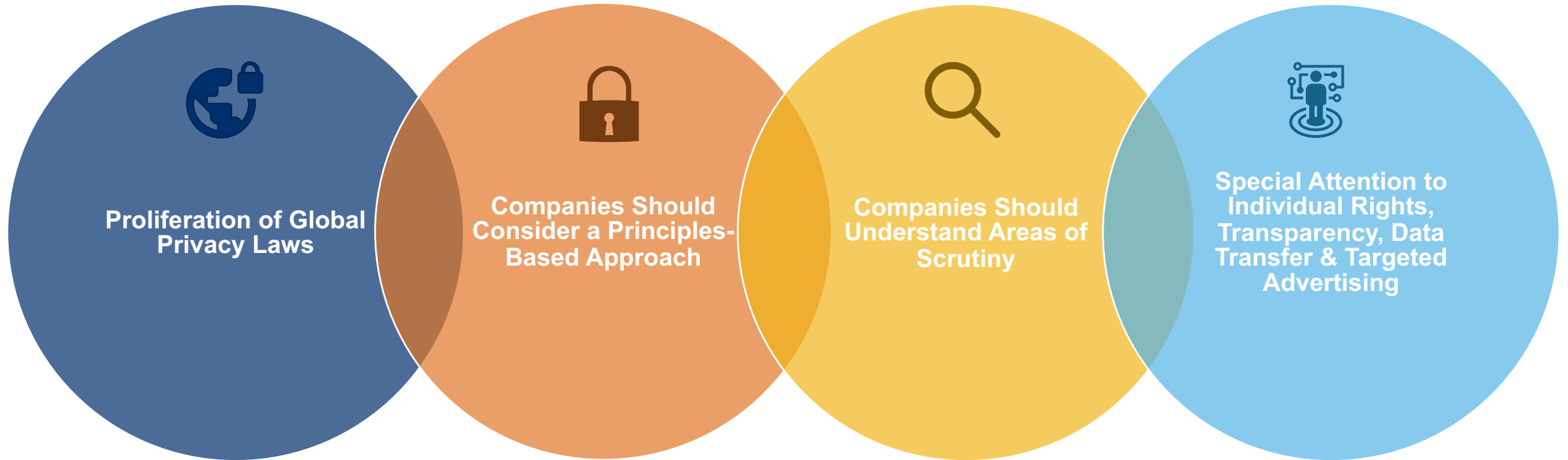
## Practice Points

- What data is covered? How is it different and does it matter?
- Handling individual rights globally
- Notices and transparency
- Cross-border data transfers
- Cookies and targeted ads

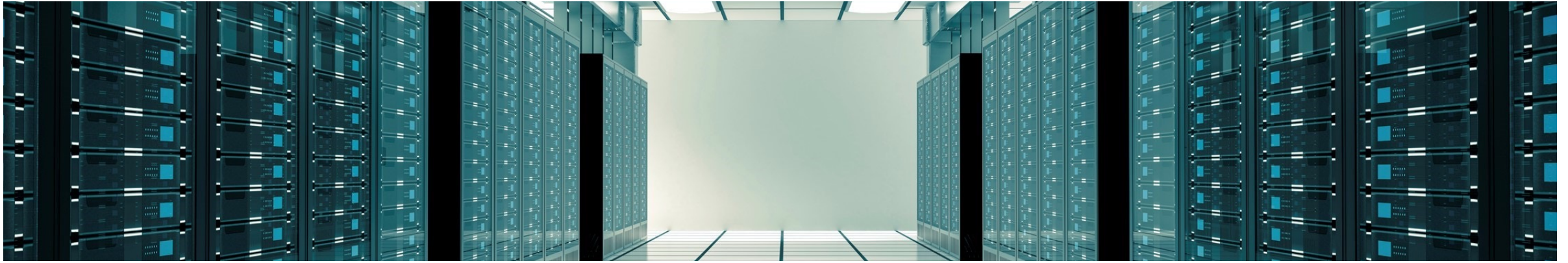
## The Global Privacy Landscape

# Key Points

---



# Data Protection Fundamentals

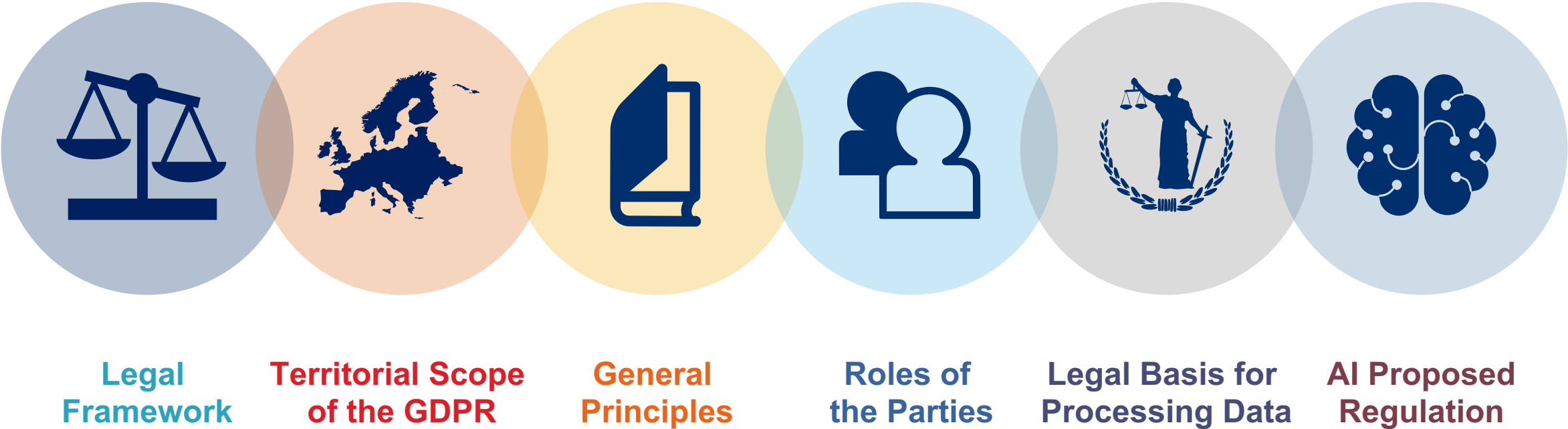




# The EU/UK Privacy Framework



# EU/UK GDPR Overview



# Legal Framework of the EU and UK Data Protection

---

## Regulation (EU) 2016/679 – GDPR

- Took effect on 25 May 2018
- Applies in all EU Member States with some additional national rules, such as health and genetic data (e.g., CNIL rules)
- Extensive guidance by the European Data Protection Board (“EDPB”)
- Landmark rulings by the Court of Justice of the European Union

## UK Data Protection Act 2018

- Supplements the UK GDPR
- Additional guidance by the UK data protection authority

## UK GDPR

- In force after Brexit, from 1 January 2021
- Incorporates the EU GDPR  
*[this presentation refers to GDPR for both the EU and the UK versions]*
- Applies together with the UK Data Protection Act 2018 and the EU GDPR, where applicable

# Territorial Scope of the GDPR

---

## GDPR Extra-Territorial Applicability Where:

- Controller/processor processing personal data in the context of activities on “**establishment**” in the EEA/UK (even if the processing takes place outside of the EEA/UK)
  - Does not matter where data subjects are located
- Controller/processor established outside EEA/UK but **offering goods/services** to data subjects in the EEA/UK, or monitoring their behaviour
  - Needs to be element of “targeting”
  - Activities need to relate to data subjects located in EEA/UK
  - “Targeting” factors could be: EU member states referred to by name, contact details for EU country stated, use of language/currency of EU country, offers of delivery in EU country (EU guidance; analogous to UK)
  - “Monitoring”: broad range – tracking, e.g., cookies/through wearable or smart devices, CCTV, geo-localization activities, personalised health analytics services online.



# Territorial Scope of the GDPR, cont'd

---

## Why Is This Important?

- 
- **The GDPR may apply to companies outside the European Union (EU)**
    - Either data controllers or data processors established outside the EU:
      - When their data processing relates to goods or services offered to data subjects in the EU, or
      - When their data processing relates to monitoring of the behaviour of data subjects within the EU
    - Example: Cloud services providers storing and transferring EU data subjects' personal data using servers outside the EU
  - **Failure to Comply with the GDPR May Lead to Enforcement Actions, Including Significant Fines**



# GDPR General Principles

## Controllers must ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with these purposes;
- Adequate, relevant and limited to what is necessary in relation to the processing purposes;
- Accurate and, where necessary, kept up to date;
- Kept not longer than what is strictly necessary for the processing purposes;
- Kept confidential, secure and protected from unauthorised or unlawful processing, accidental loss, destruction or damage.

## Another important GDPR principle is **data protection by design and by default**:

- Ensuring compliance with the GDPR principles from the beginning and throughout the data processing activities;
- Implementation of technical and organizational measures;
- Using state of the art technologies.



# GDPR General Principles

## Both the UK and EU GDPR . . .

1. Broad Definition of Personal Data

---

2. Requirements Apply Throughout Data Lifecycle

---

6. Enforcement

---

3. Individual Rights  
(Access, Deletion, Portability,  
Objection to Processing)

---

5. Oversight of Third Party  
Requirements

---

4. Oversight/Governance  
Requirements  
(Data Protection Officers)

---



# Roles of the Parties Under the GDPR

Role	Description	GDPR Compliance	Contractual Implications
<b>Processor</b>	Processes personal data on <b>behalf of, and in accordance with the instructions of,</b> controller.  Controller retains exclusive control over the purpose for which the data is processed and the content of the data.	Needs to comply with the obligations on processors under the GDPR.	Controller <b>must</b> enter a contract with any processor containing list of <b>GDPR-prescribed obligations (Article 28)</b> .  Standard Contractual Clauses published by the European Commission on 4/6/2021.
<b>Joint Controller</b>	<b>Jointly</b> decides the purposes and means of personal data processing with another controller/controllers.	Each controller remains responsible for complying with all the obligations of controllers under the GDPR.	Parties must have transparent “ <b>arrangement</b> ”. Main points of arrangement must be made available to individuals, e.g., in privacy notice.
<b>Separate Controller</b>	Both parties decide purposes and means of personal data processing, but <b>this is not done jointly</b> .	Each controller remains responsible for complying with all the obligations of controllers under the GDPR.	The GDPR does not prescribe any contract/arrangement. Parties will <b>likely want language in contract anyway</b> .

# Legal Basis for Processing Under the GDPR

## To Process Any Kind of Personal Data Fairly: Need Lawful Basis Under Article 6 GDPR

- Consent (informed, not bundled up in a document, clear, affirmative action, retractable)
- Contractual obligations (e.g., HR data to benefits provider)
- Legal obligations (e.g., compliance with safety obligations)
- Vital interests of the data subject
- Task in the public interest
- Legitimate interests → catch-all legal basis but requires balancing test

## To Process Special Categories of Data: Need Also Legal Ground Under Article 9 GDPR

- Consent
- Public interest in the field of public health
- Archiving and scientific research purposes

## National Laws May Impose Additional Restrictions on the Lawful Bases for Processing of “Regular” and “Special Categories” of Personal Data

- E.g., UK Data Protection Act 2018

# EU Proposed Regulation on Artificial Intelligence

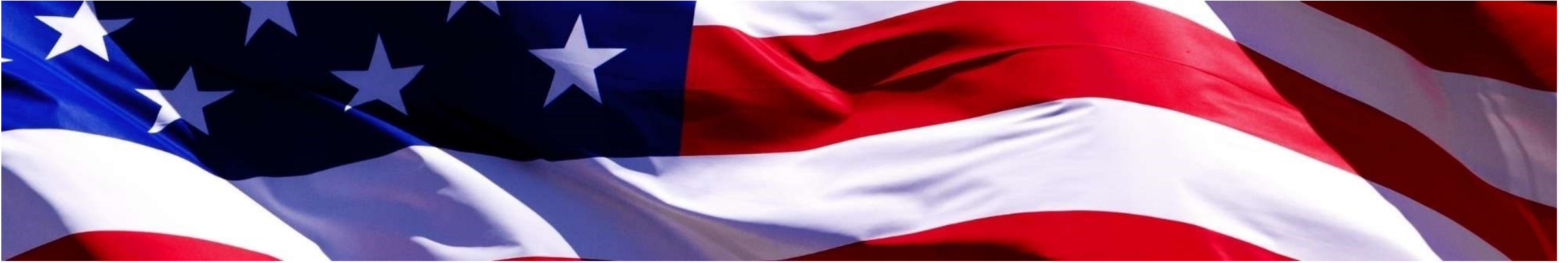
---

- On April 21, the European Commission proposed legislation for the regulation of artificial intelligence systems in the European Union, including externally located systems with output used inside the EU.
- The proposal adopts a risk-based approach:
  - It prohibits a few uses of AI, such as use of AI for social scoring;
  - It imposes numerous requirements on high-risk AI systems (classified as such based on their intended use), such as obligations on the systems design or obligations of documentation, explainability and disclosure;
  - Low-risk AI systems would remain mostly unregulated under the proposed regulation, apart from certain transparency requirement.
- The proposed regulation is now subject to standard legislative procedures in the Parliament and the Council of the EU.

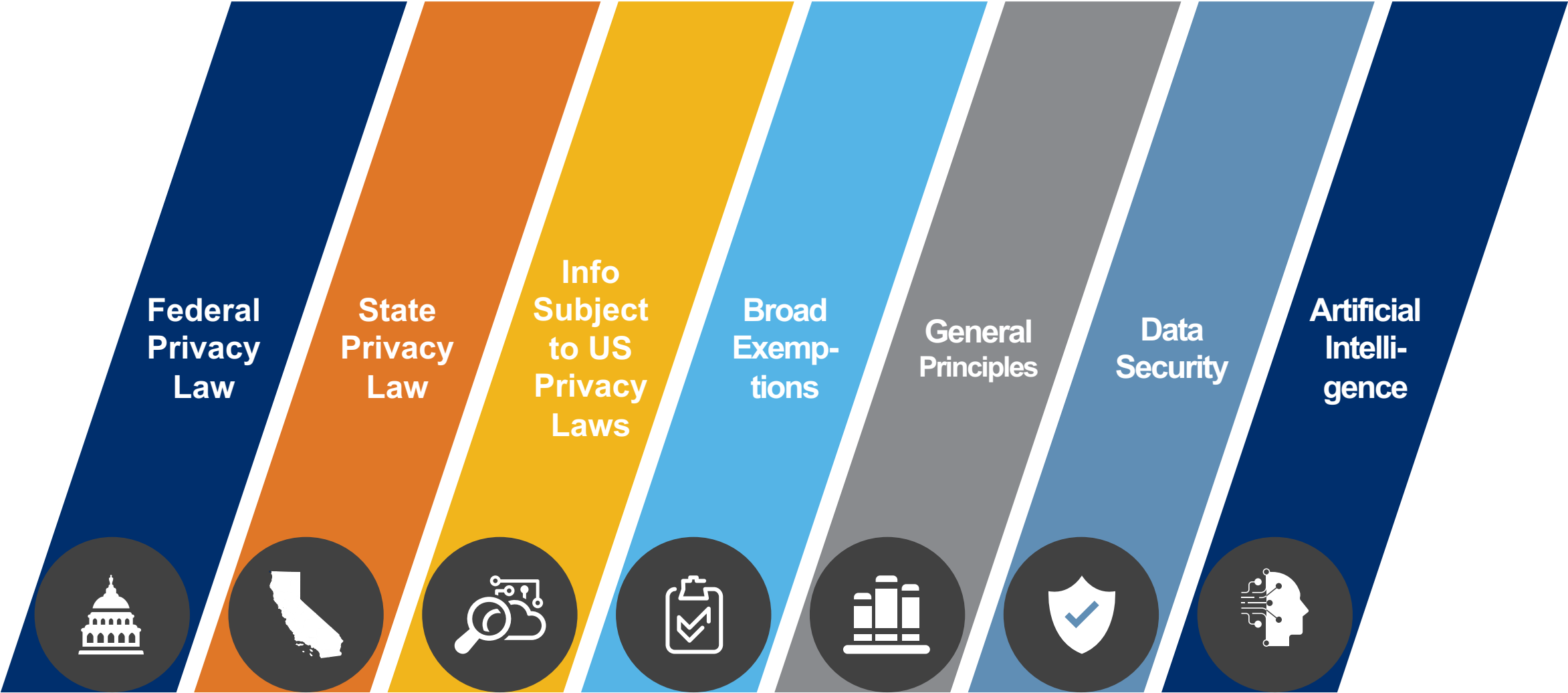




# **U.S. Privacy Law and Legislation**



# US Privacy Law Overview



# Federal Privacy Law

---



- Unlike the EU, the United States has no overarching law for privacy and data protection.
- Federal privacy laws focus on specific industries or types of personal data, such as:
  - Medical information
  - Financial information
  - Social Security Numbers
  - Information used to make employment, credit, or insurance decisions
  - Personal information collected by or for the government
  - Driver's license information
- The different laws and regulations have various definitions of what information is protected ("nonpublic personal information," "personally identifiable information," "protected health information," etc.).

# Who Regulates at the Federal Level?



## BANKING REGULATORS

Financial Institutions and Their Service Providers

- Gramm-Leach-Bliley Act (GLBA)



## DEPARTMENT OF HEALTH & HUMAN SERVICES

Health Care Providers, Health Insurance Plans, and Their “Business Associate” Service Providers

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act



## FEDERAL COMMUNICATIONS COMMISSION

Entities that Use Personal Information for Telemarketing Purposes (Including Text Messaging)

- Telephone Consumer Protection Act (TCPA)



## FEDERAL TRADE COMMISSION

Almost All Entities (Limited Exceptions for Banks, Insurers, Common Carriers) that Engage in Interstate Commerce

- Actions based on alleged “deception” or “unfairness”
- Children’s Online Privacy Protection Act (COPPA)
- Fair Credit Reporting Act

# What Remains Federally Unregulated?



## FINANCIAL INFORMATION NOT PROCESSED BY FINANCIAL INSTITUTIONS

Banking regulators do not regulate most merchants, some fintech companies



## HEALTH INFORMATION NOT SUBJECT TO HIPAA

HIPAA does not regulate many entities that handle personal health information (e.g., WebMD, employers, pharmaceutical companies)



## LOCATION INFORMATION

Subject to Federal Trade Commission actions only in selected circumstances



## INFORMATION USED FOR TARGETED INTERNET ADVERTISING

Subject to Federal Trade Commission actions only in limited circumstances



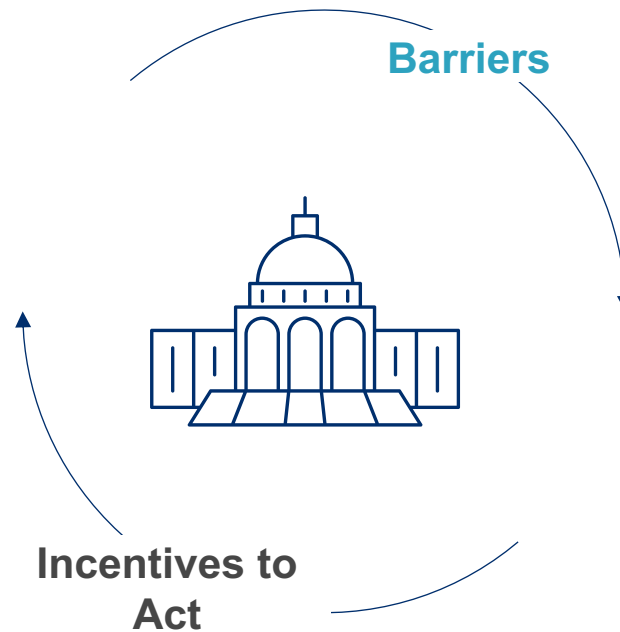
# Will Congress Do More?

---

## Incentives to Act

---

- Industry wants uniformity
- Bipartisan agreement on need for basic privacy protections








## Barriers

---

- Industry demands federal preemption of growing body of state laws
- State governments oppose preemption
- Private right of action

# States Filling the Privacy Void

 <div>California</div> <div>California Consumer Privacy Act (CCPA) [2021] California Privacy Rights Act (CPRA)* [January 2023]</div>	 <div>Colorado</div> <div>Colorado Privacy Act (CPA) [July 2023]</div>	 <div>Connecticut</div> <div>Personal Data Privacy &amp; Online Monitoring Act (CPDPA) [July 2023]</div>	 <div>Utah</div> <div>Utah Consumer Privacy Act (UCPA) [January 2023]</div>	 <div>Virginia</div> <div>Virginia Consumer Data Protection Act (VCDPA) [January 2023]</div>
---	---	---	--	---

# What Information is Typically Subject to US State Privacy Requirements?

---

- **“Personal Information” (broad definition)**
  - “Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”
  - Inferences drawn from any such identifiable information ... to create a profile about a consumer
- **Examples (*not* exclusive):**
  - Identifiers: names, addresses, email addresses, IP addresses, geolocation data, characteristics of protected classes (race, religion, etc.), Internet or other electronic network activity, such as browsing history

# Typical Exemptions for Federally Regulated Personal Information



- “Protected Health Information” (PHI) collected by a HIPAA-covered entity or business associate



- Information collected as part of a clinical trial subject to the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the FDA



- Non-public personal information subject to the federal Gramm-Leach-Bliley Act governing financial institutions



- “Consumer Report” information protected under the federal Fair Credit Reporting Act

# Exemptions for Employment-Related Information

---

- **Employment-related information:** personal information:
  - About a consumer and collected and used solely in the context of a consumer acting (currently or formerly) as the business' job applicant, employee, owner, director, officer, or contractor;
  - Provided to a business as emergency contact information of, or needed to administer benefits for, a person related to a job applicant, employee, owner, director, officer, medical staff member, or contractor of the business.
- **BUT:** Under CA law, basic notices to employees and job applicants about what elements of their personal information is being collected, how it is used, and with whom it is shared are required.



# Exemption for B2B or “Commercial” Personal Information

---

- Under CA law, most requirements do not apply to personal information:
  - about a consumer acting as an entity representative (employee, owner, director, officer, contractor)
  - “reflecting” a communication or transaction between the business and the consumer” that:
    - “occurs solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from the entity the consumer represents”
- Under VA, CO and UT law:
  - “Consumer” personal informational excludes personal information regarding a natural person acting in a commercial context

# State Law General Principles

## All Five States' Consumer Privacy Laws Have Some Form Of:



# What About Data Security Requirements?

---



- California and several other states require “reasonable security” procedures and practices
  - There is no statutory or regulatory definition of “reasonable security”



- Security measures must be designed to prevent unauthorized access and exfiltration, theft, or disclosure of non-encrypted and non-redacted personal information



- Failure to do so may trigger class action lawsuits

# Data Security Breach Notification

---

Most U.S. states require notification to affected individuals, certain state agencies, and in some cases the media, of a breach in the security of information that contains:

- An individual's first name or first initial *and* last name *in combination with* any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - Social Security number
  - Driver's license number or state identification card number
  - Account number, credit or debit card number, *in combination with* any required security code, access code, or password that would permit access to an individual's financial account
  - Medical information
  - Biometric information
  - Health insurance information

# US Privacy Law Provisions on Artificial Intelligence

---

- California and several other states require:
  - Disclosure of the practice of using personal information for AI purposes
  - Providing individuals the right to opt out of the use of their personal information for AI purposes
- California's law currently lacks exceptions to these requirements
- Regulations are forthcoming that will flesh out the statutory mandates



# Practice Points



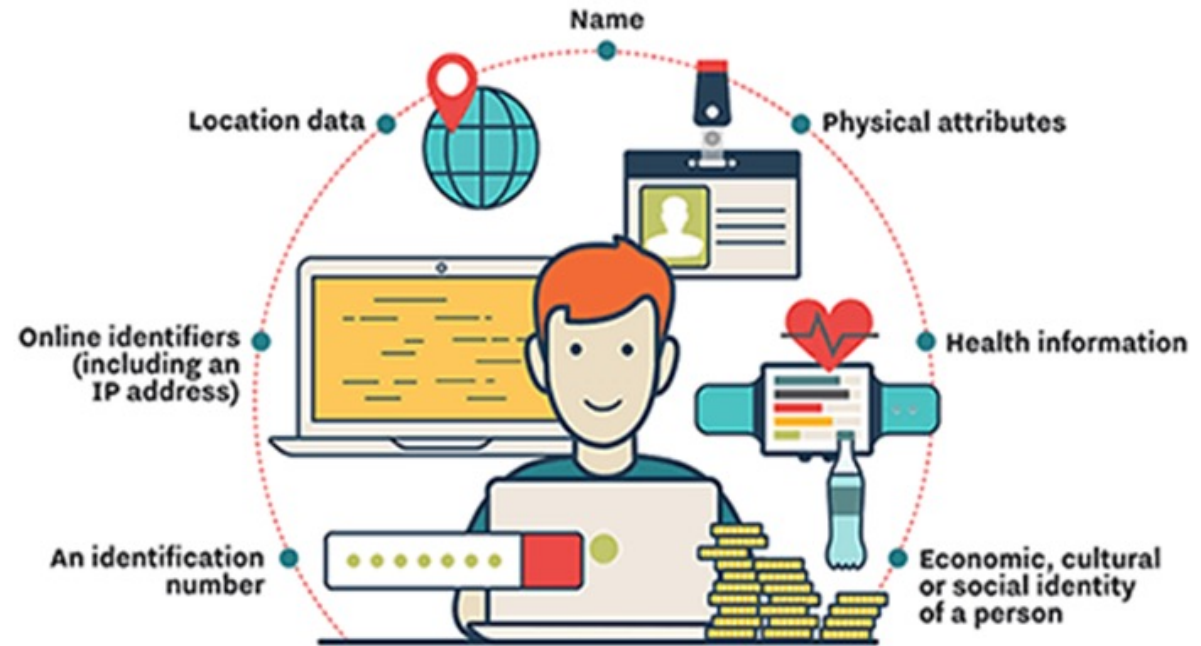






# What Is Personal Data?

- Very broad definition of personal data:
  - any information relating to an identified or identifiable natural person (direct or indirect identification);
  - Pseudonymized data in Europe: anonymous to the person accessing it but still personal data, as it can be linked back to an individual.
- Two categories of personal data:
  - “regular” personal data; and
  - “special categories of personal data” (aka sensitive personal data), including data relating to health, genetic, racial or ethnic origin and political opinions -> the bar of the protection is set higher



# Anonymization of Personal Data Under the GDPR

---

Under the GDPR, anonymous information is information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that **the data subject is not or no longer identifiable**.

⇒ GDPR does not concern the processing of **truly** anonymous information, including for statistical or research purposes.

! In order to be truly anonymised under the GDPR, companies must strip personal data of sufficient elements that mean the individual can no longer be identified. However, if companies could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised.

! The process of anonymisation constitutes processing of personal data!

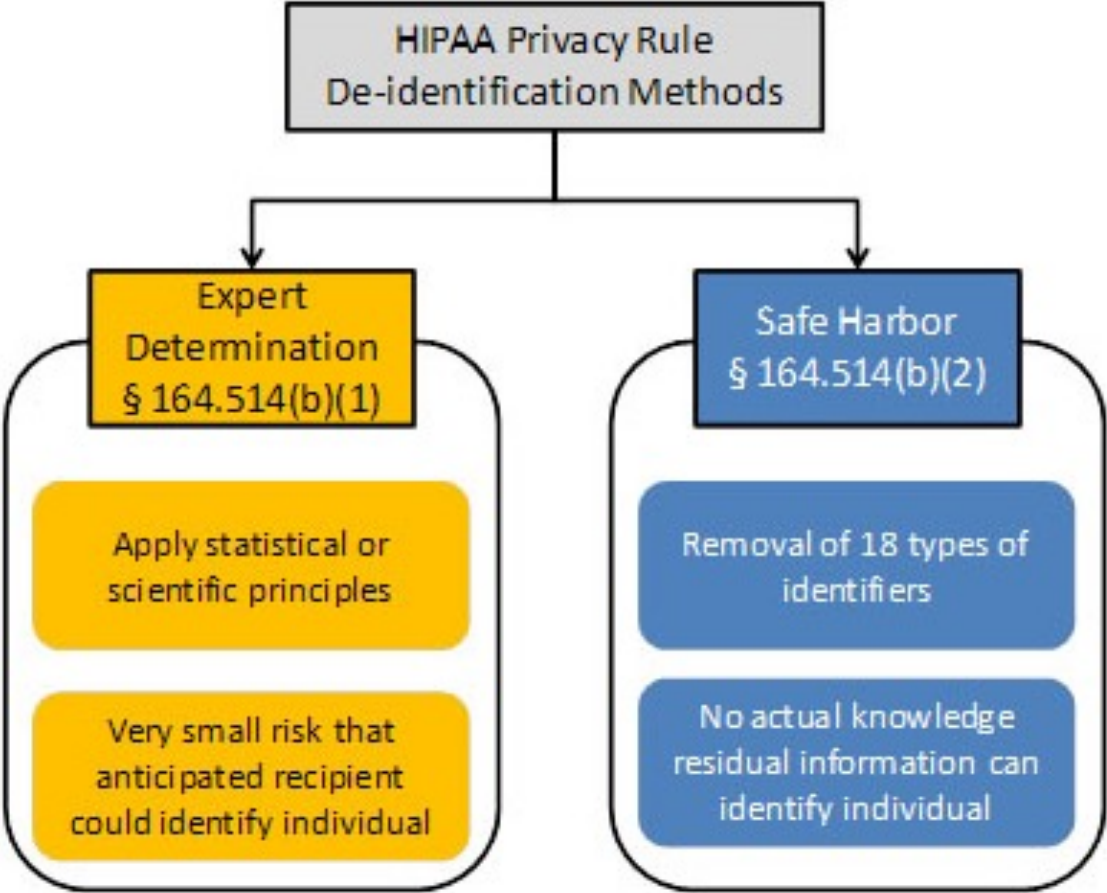
# De-identification of Personal Data Under the CCPA

---

**“Deidentified” Information:** Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, *provided that a business that uses the information:*

- Has technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
- Has business processes that specifically prohibit reidentification of the information;
- Has implemented business processes to prevent inadvertent release of deidentified information; and
- *Makes no attempt to reidentify the information*

# De-identification of Protected Health Information Under HIPAA



# “Safe Harbor” De-identification Under HIPAA

---

All of the following must be removed -- with respect to an individual as well as his or her relatives, employers, and household members:

- Name
- SSN
- Date of birth
- Date of hire
- Dates of service
- Telephone or fax numbers
- Email address
- Medical record number
- Health plan beneficiary number
- Geographic identifiers smaller than a state
- Certificate/license numbers
- Vehicle
- URLs
- IP address numbers
- Biometric identifiers
- Photographic image
- Other unique identifying numbers or codes

# Handling Individual Rights Globally



# Rights of Data Subjects Under the GDPR

## Most important: right to access the personal data

- Allows data subject to obtain access to personal data and copies of data
- Time for controller to respond reduced from 40 days to one month (possibility to extend by another 2 months if request complex)
- No fee charged unless request “manifestly unfounded or excessive”

## Right to rectify the personal data

## Right to restrict the processing of the personal data

## Right to be forgotten or to erase the personal data

## Right of data portability

## Right to object to the processing of personal data in the case of automated decisions such as profiling (right to object)



# Rights of Individuals Under Certain US Federal Laws

---

- **HIPAA**

- Notice: Right to receive a Notice of Privacy Practices
- Choice: Right to control uses and disclosures of protected health information (PHI)
- Access: Right to review medical records
- Correction: Right to request updates or corrections to PHI
- Accounting: Right to know what uses and disclosures have been for purposes other than treatment, payment, and “health care operations”

- **Gramm-Leach-Bliley Act**

- Notice: Right to receive annual Privacy Notice
- Choice: Right to opt out of certain uses and disclosures

# Rights of Individuals Under U.S. State Consumer Privacy Laws

---

- **Notice**

- Right to receive Privacy Policy or Notice before or at point of data collection
  - Must describe the business's practices and the consumer's rights with respect to personal information
  - Must state whether inferences are drawn from any personal information to create a profile about a consumer

- **Choice**

- Right to opt of sales of personal information or use of the information for targeted advertising

- **Access and Deletion**

- Right to a copy or description of personal information held by a business
- Right to request deletion of the personal information

# Notices and Transparency




# One Size Fits All or Many Notices?

---



## All Privacy Laws Have a Transparency Requirement

- You must tell people what you are doing with their data
- In many jurisdictions, this includes employees



## Typically, the Transparency Requirement Is Met with a Notice

- Online Notice
- Employee Notice
- Notice as Part of Terms & Conditions



## What Are the Pros and Cons of a One-Size-Fits-All (or Most) Approach?

# Cross-Border Data Transfers – Help!



# Transfers of Personal Data to Jurisdictions Outside the EEA/UK

---

- **Personal data can be transferred outside the EEA or the UK only if the GDPR requirements are met**
- EEA and UK exporters may only transfer personal data to countries that provide an “adequate level of protection” for personal data;
- Complexities around transfers to the USA
- Major implications for multinational clients making transfers of data around the world:
  - Employers sending HR data to parent companies outside the EEA or the UK
  - Businesses sending customer data to group companies outside the EEA or the UK
  - Life sciences companies sending patient data overseas
- Also easy to inadvertently transfer data
  - Client/HR database – accessible from outside the EEA or the UK



# What is a “Data Transfer” Under the GDPR?

---

- EDPB Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers of Chapter V of the GDPR
- **3 cumulative criteria:**
  - *A controller or a processor is subject to the GDPR pursuant to Article 3 for the processing of personal data.*
  - *The controller or processor (data exporter) transmits or makes available the personal data to another controller, joint controller or processor (data importer).*
  - *The data importer is in a third country, regardless of whether or not this data importer is subject to the GDPR in respect of the given processing in accordance with Article 3.*
- The collection of personal data **directly** from data subjects in the EEA and **at the subjects’ own initiative** does not constitute a Transfer.
- Even if there is no transfer under the GDPR, the transmission of personal data may include risks that need to be identified and mitigated.



# Permitted International Data Transfers Under the GDPR

---

- Countries offering adequate protection of personal data, according to adequacy decisions by the European Commission (EC) or the UK Secretary of State. So far, the following countries:
  - Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Republic of Korea, the United Kingdom, Switzerland and Uruguay – NOT USA
  - UK after Brexit -> UK granted an adequacy decision – but this is subject to ongoing review in case of divergence from the EU
  - If UK not adequate – would need to adopt other mechanisms if data to flow freely from EU to UK
  - UK considers rest of Europe – adequate – permit flows from UK to EU



# What Other Mechanisms That Allow Transfer Of Data Outside EEA/UK?

---

In absence of an adequacy decision, transfers in accordance with:

- **Standard contractual clauses** (adopted by EC or the UK);
- Binding corporate rules (for intra-group transfers);
- Last resort: one of the exceptions set out in Article 49 of GDPR (e.g. consent, performance of a contract, important reasons of public health):
  - Very limited and subject to “necessity test”;
  - Some of them could be used only for “occasional” transfers.

# Recent Developments in International Data Transfers

---

## **Schrems II case** (Case C-311/18 Data Protection Commission vs. Facebook Ireland and Maximilian Schrems)

- **Invalidated EU-US Privacy Shield Framework** (Decision (EU) 2016/1250):
  - Privacy Shield incompatible with the requirements of GDPR;
  - US national security, public interest, and law enforcement over the privacy rights of data subjects;
  - Scope of U.S. intelligence law (FISA) goes beyond that which is necessary and create disproportionate invasions of privacy;
  - Lack of formal protection for individuals under USA law.
- Validity of Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR) confirmed, but due diligence and transfer impact assessment necessary (assessment of the adequacy of third country laws in light of the obligations of the parties under the transfer mechanism and adoption of extra measures if laws are insufficient)
  - Some transfers may continue under Article 49 GDPR conditions (in absence of other transfer mechanisms and under strict conditions)

# Standard Contractual Clauses

---



- On June 4, 2021, the European Commission (EC) published **a new version of the Standard Contractual Clauses (New SCCs)** for personal data transfers to third countries outside of the European Economic Area (EEA), not subject to an adequacy decision by the EC.
- The New SCCs replace the prior controller-to controller and controller-to-processor SCCs.
- Reasons of adoption:
  - ✓ Aligning with GDPR requirements;
  - ✓ Reinforcing additional requirements for the validity of SCCs as a transfer mechanism, set out by the European Court of Justice in *Schrems II* decision;
  - ✓ Adapting to the realities of the digital economy, the increased complexity of data processing operations and transfer scenarios and the potential of many parties to be involved in processing activities.

# Design, Scope and Features of the New SCCs

---

## Modular Approach

- Modular clauses for different data transfer contexts: (i) controller-to-controller; (ii) controller-to-processor; (iii) processor-to-controller; (iv) processor-to-processor transfers.

=> **More practical and realistic approach.**

## Geographical Scope

- Data exporter does not need to be established in the EEA.
- New SCCs applicable only when the processing of the personal data by the data importer is not subject to the extraterritorial scope of the GDPR -> still uncertainty on this point.

## Possibility of Multi-Party Agreements

- More than two parties are able to execute the New SCCs.
- New parties can accede to the New SCCs - “docking clause”.

=> **More flexibility.**

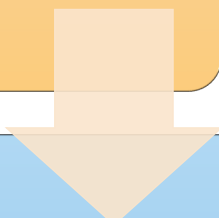
# Timeline for Implementation of the New SCCs

---

New SCCs entered into force on June 27, 2021.



Organizations could continue concluding agreements based on the prior SCCs until September 27, 2021, after which date the prior SCCs were repealed. Now, **only the New SCCs** can be executed.



Organizations can still rely on pre-existing data transfer agreements based on the prior SCCs until December 27, 2022, under certain circumstances.

# UK and Switzerland Approach Towards the New SCCs and Data Transfers

---



- For personal data transfers from the UK to “non-adequate-countries”, a UK international data transfer agreement or a UK addendum to the new EU SCCs are applicable since 21/3/2022, replacing the prior SCCs.



- The Swiss Data Protection Authority (DPA) **approved** the use of the New SCCs for personal data transfers from Switzerland to “non-adequate” countries, provided that they will be adapted and/or supplemented as necessary in order to comply with the Swiss law.

# EU-South Korea Data Transfers

---



- In **June 2021**, the EU Commission initiated the procedure for the adoption of an **adequacy decision** for the free flow of personal data to the Republic of Korea.
- EDPB issued an opinion on the draft adequacy decision => overall positive assessment of the level of protection afforded by the South Korean framework, but some concerns regarding e.g., effective remedies of EU data subjects, rights of redress and exemptions of the law for pseudonymised data, which should be further assessed and clarified by the EU Commission.
- Approval of EU member states pending before EU Commission adopts the adequacy decision.



# Cookies and Targeted Ads



# Recent EU Decisions and Findings Concerning Cookies

## Google Analytics

- Austrian and French Data Protection Authorities and the European Data Protection Supervisor
- Personal data transfers outside the EEA that occur when using Google Analytics are complex

## German Court Decision

- On December 1, 2021, a German Court held that companies may not use a cookie management provider that relies on a US-based service to collect personal data, regardless of whether data leaves the EEA, without an adequate transfer mechanism.
- The ruling here assumes that a cross-border “transfer” subject to GDPR transfer rules occurs—even if data never actually leaves the EEA—if the recipient of data may formally be subject to data production requests by non-EEA authorities.

# US State Laws Target Targeted Ads

---



- US has not targeted cookies in the way Europe has, BUT
- In both a compliance function and an individual rights function, states have targeted behavioral or targeted advertising
  - Do Not Sell and Do Not Share buttons
  - Opt-Out requirements
  - Privacy-by-design requirements



# Global Privacy Law Landscape: Selected Examples





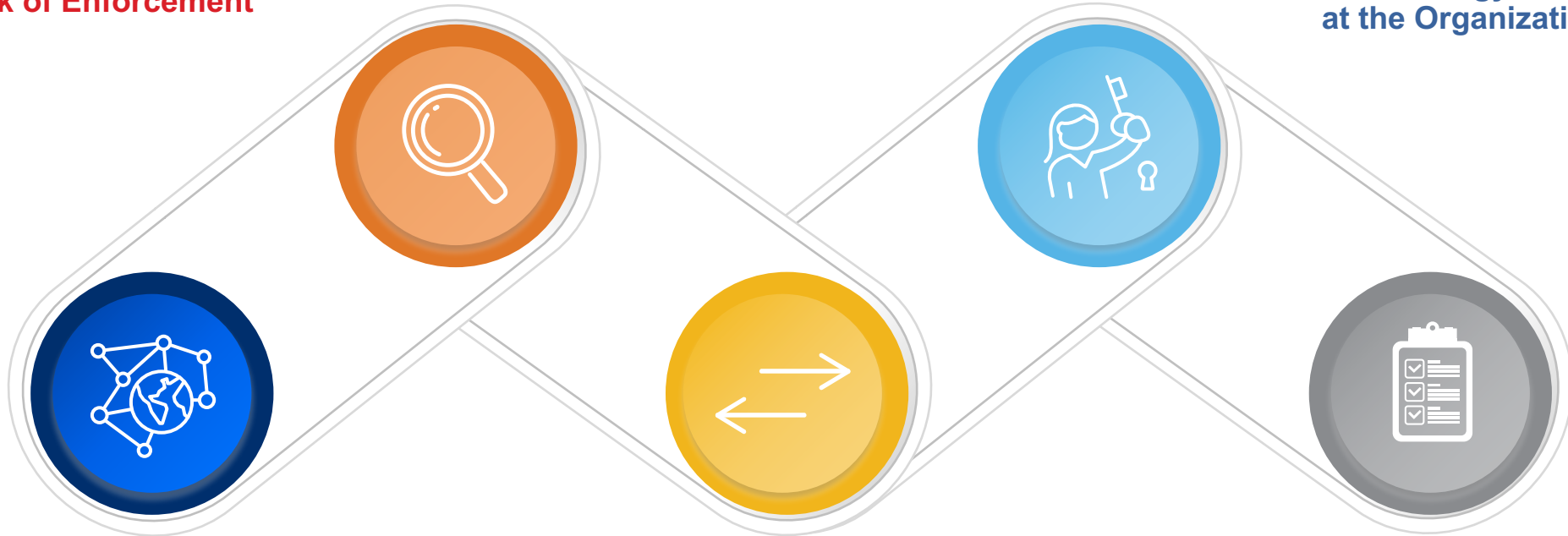
- Brazil's federal data privacy law (**LGPD**): First comprehensive data protection regulation—entered into force on **September 18, 2020**, but the penalties set out in LGPD started to be enforceable in **August 2021**
- Largely based on the GDPR



- Personal Information Protection Law (**PIPL**): First comprehensive data protection law—took effect on **November 1, 2021**. Will apply alongside existing Chinese data privacy and cyber laws
- Extraterritoriality
- Modelled in part on the GDPR, but has important differences

# Takeaways

**Areas to Focus on to Reduce  
Risk of Enforcement**



**Need for Someone to Create &  
Maintain Strategy for Privacy  
at the Organization**

**Complications with Taking a  
Jurisdiction-by-Jurisdiction  
Approach to Privacy**

**Handling Data Transfers  
Requires Process &  
Organization**

**Make Sure to Understand and  
Prioritize Risk!**



# Thank you!

---



**Doug Curwin**

**VERACYTE**  
Seattle

Doug.Curwin@veracyte.com



**Sarah Leathwood**

**DANAHER LIFE SCIENCES**  
London

Sarah.Leathwood  
@dhlifesciences.com



**James Castro-Edwards**

**ARNOLD & PORTER**  
London

James.Castro-Edwards  
@arnoldporter.com



**Nancy L. Perkins**

**ARNOLD & PORTER**  
Washington, DC

Nancy.Perkins@arnoldporter.com



**Jami Vibbert**

**ARNOLD & PORTER**  
New York

Jami.Vibbert@arnoldporter.com