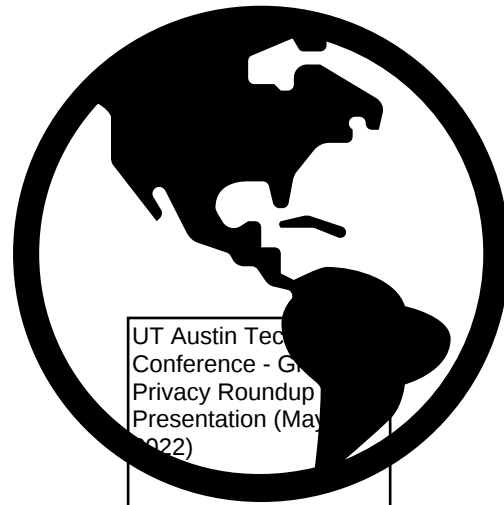
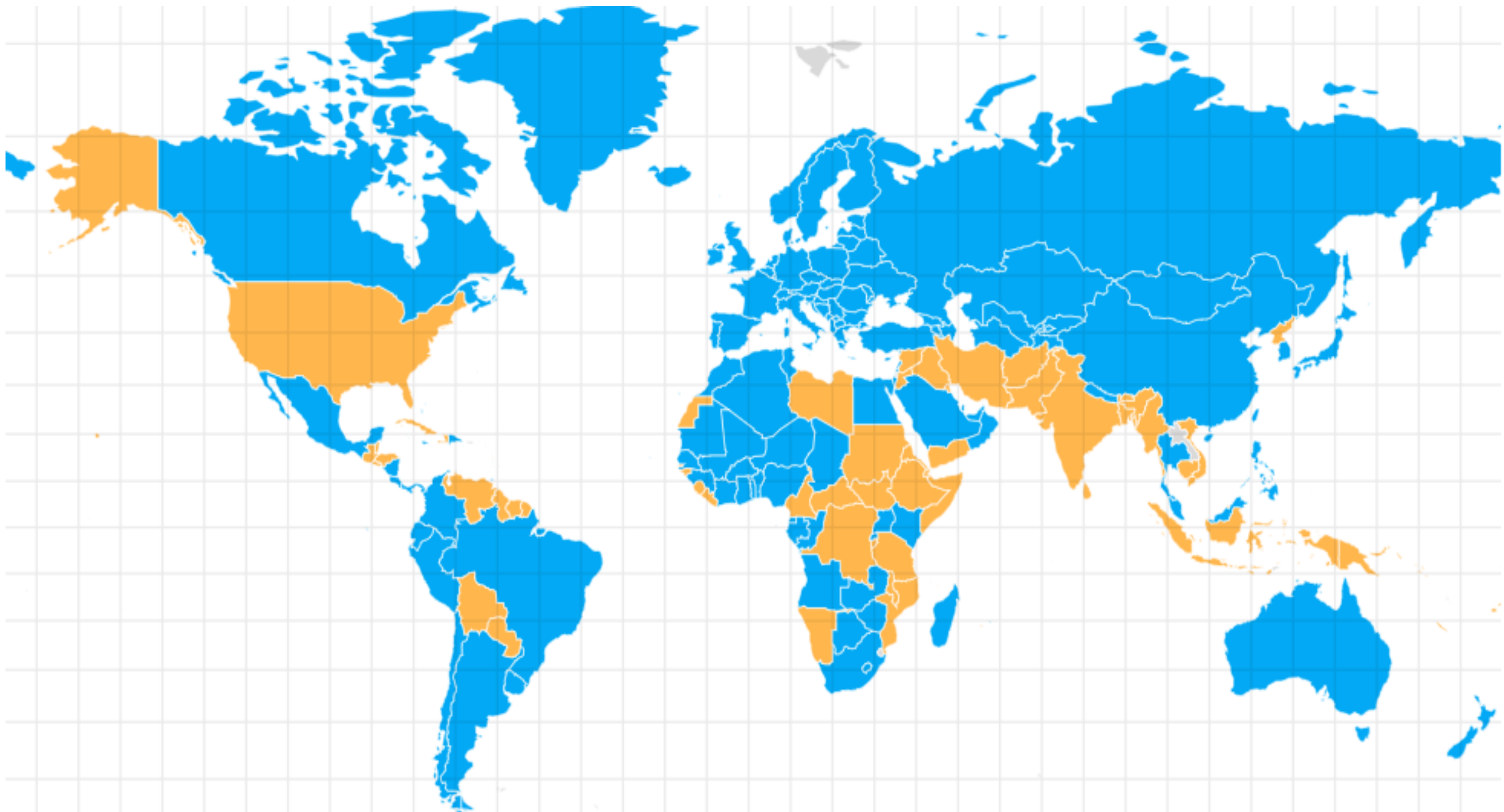




# GLOBAL PRIVACY ROUNDUP

MAY 27, 2022



# PANELISTS



**Jim Sturm**  
Sr. Counsel &  
Director - Privacy &  
Data Security,  
Inspire Brands



**Lisa Zolidis**  
Head of Global  
Privacy,  
National  
Instruments



**Justin Koplow**  
Executive Director –  
Senior Legal Counsel  
for Privacy and Data  
Protection,  
AT&T



**Amanda Witt**  
Partner,  
Cybersecurity,  
Privacy and Data  
Governance Team  
Leader,  
Kilpatrick Townsend

# **AGENDA: STAYING AFLOAT AMID GLOBAL TRENDS**

- New Privacy Laws Aplenty & Implementation Challenges
- Data Minimization – Now More (or Less) Than Ever
- International Data Transfers – Still a Thing!
- Consent Standards Solidify (& Cookies Need Them Too)
- Data Subject Rights Bingo

# NEW PRIVACY LAW IMPLEMENTATION

## STEP ONE - DETERMINE IF THE LAW IS APPLICABLE

Privacy laws vary  
in scope of  
application:

- **China's Personal Information Protection Law (PIPL):** Applies to organizations operating in China and to organizations/businesses outside of China that process personal data to offer goods and services or analyze the behavior of Chinese natural persons, and to any (unspecified) "circumstances stipulated by laws and administrative regulations"
- **U.S. State Laws:**
  - **California (CCPA/CPRA):** Applies to companies with annual gross revenue >\$25,000,000, **or** buys,/sells/shares personal information of >100,000 California consumers/households per year, **or** 50% or more annual revenues from selling or sharing personal information
  - **Virginia (CDPA), Colorado, Connecticut & Utah:** Apply to companies that per year (a) control/process personal data of >100,000 state's residents, **or** (b) derive revenue or receives a discount on sale of goods by selling personal data and processes personal data of >25,000 state's residents (50% for VA, CO & UT, 25% for CT)(UT: \$25M+ revenue)
- **GDPR:** Applies to Companies Established in the EU **and** to processing of personal data by a controller or processor not established in the EU, where processing relates to offering goods and services to or monitoring behavior of EU residents

# NEW PRIVACY LAW IMPLEMENTATION

## STEP 2 – USE YOUR DATA MAPPING

### What is data mapping?

- Generally, map and document processing activities and assets that use or store personal data.
  - Source, volume, and type of personal data (or sensitive personal data)
  - Processing role (e.g., controller or processor)
  - Description of processing
  - Purposes of processing
  - Legal basis for processing (if required)
  - Recipients of personal data (i.e. vendors, distributors)
  - International data transfers and how they're protected
  - Security procedures

### Why map your personal data?

- Determine which privacy laws apply
- Ensure your organization is processing personal data according to purpose limitations
- Identify and document risks + mitigation measures
- Need a record of processing activities under the GDPR and to meet California CPRA requirements
- Need categorization of processing purposes for the CCPA/CPRA and China's Data Security Law and upcoming (draft) Regulations on Network Data Security Management

# NEW PRIVACY LAW IMPLEMENTATION

## STEP 3 - HARMONIZE COMPLIANCE ACROSS KEY FOCUS AREAS

- Periodic testing of controls
- Independent assessments
- Security considerations

### Monitoring & Auditing

### Training & Awareness

- Ongoing training & awareness activities
- Monitoring of training completion

- Notice, choice & consent
- Data minimization, use specification
- Retention & disposal
- Policies and procedures
- Privacy by Design culture
- Service/product development

### Processes & Controls

### Governance & Accountability

### Risk & Compliance

- Applicable laws and regulations
- Cross-border data transfers
- Data flow mapping & inventory
- Risk assessments
- Data classification

- Risk valuation of third-party relationships
- Contract negotiation
- Third-party assessment questionnaire/audit
- Reporting and ongoing evaluation

### Third Party & Vendor Management

### Incident Response

- Defined response and breach notification plan
- Vendor/third-party incident response
- Customer correspondence

# NEW PRIVACY LAW IMPLEMENTATION

## STEP 4 - PROJECT PLANNING CHECKLIST

- **Functional Areas**: e.g., data mapping, contracts, consumer rights, notices, universal opt-out
- **Personnel**: how much can be accomplished by legal versus cross-functional teams?
- **Timing**: internal completion timelines, public launch dates, and effective dates
- **Budget**: what is feasible? What does 'good' look like?



# QUIZ BREAK - TEST YOUR PRIVACY SENSITIVITY

**Do you provide your birthdate when a company asks for it?**

1. Never.
2. Not my *real* birthdate.
3. Only if it's a company that actually needs it, like my life insurance company or the CPA who's preparing my tax return.
4. Always. Isn't it nice that they care? They might even send me a birthday email!



# DATA MINIMIZATION

## OVERVIEW

Data Minimization is a fundamental privacy principle that focuses on:

- Smart and limited collection of personal data, and
- Limited retention of personal data.

### Collect

Only the minimum personal data needed for your defined purpose.

### Share

Only the minimum necessary.

Only with the fewest number of people who must have access.

### Keep

Only as long as you need the personal data.

Only as long as the data is actually being used.

# DATA MINIMIZATION

## *A FUNDAMENTAL PRINCIPLE EXPLICITLY REQUIRED BY LAW*

### Selected Global Examples

China's PIPL - The collection of personal information shall be limited to the **minimum scope required by the purpose** of processing, and personal information may not be collected excessively.

EU GDPR - Personal data shall be **adequate, relevant and limited to what is necessary** in relation to the **purposes** for which they are processed ('data minimisation').

Brazil - LGPD: Principle of necessity: "limitation of the processing to the **minimum necessary** to achieve its **purposes**, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing".

United States – Some U.S. state laws, including the California Privacy Rights Act, mandate retention requirements based on the **data minimization** and **purpose limitation**.

# DATA MINIMIZATION

## CHECKLIST

- ☐ Provide data collection guidance that requires analyzing what data is absolutely necessary and eliminates the extraneous
- ☐ Document purposes for collection – accountability for “why”
- ☐ Implement accurate public-facing privacy notices, including point-of-collection purpose notices
- ☐ Define clear personal data retention schedules based on business need and conforming to legal requirements
- ☐ Establish functional data disposal mechanisms (both technological and manual) that map to the data retention schedules
- ☐ Ensure internal privacy and record retention policies match requirements

# INTERNATIONAL DATA TRANSFERS

## OVERVIEW

Global focus remains on protecting personal data that transfers across borders.

- European Union & the United Kingdom:
  - Strong distrust of the ability for companies in the United States to truly protect personal data from government surveillance continues to drive doubt.
  - Even the new EU Standard Contractual Clauses aren't enough in some regulators' view.
  - New UK IDTA
- China: Similar caution underlies increased data transfer protection obligations in the newly-implemented PIPL (eff. November 2021).
- South America:
  - Brazil's LGPD contains similar cross-border transfer requirements to the GDPR
  - Argentina has its own set of Standard Contractual Clauses and models its approach on GDPR.

# INTERNATIONAL DATA TRANSFERS

## *EEA: NEW SCCS – PRACTICAL STEPS FOR IMPLEMENTATION*

### ■ Timeline

- September 27, 2021 – the deadline to start using new SCCs for new data transfers
- December 27, 2022 – replace the old SCCs for old data transfers

### ■ Steps to Take Immediately

- Identify all contracts that rely on the SCCs
- Determine which modular approach is appropriate for each contract
- Develop a plan for replacing the old SCCs
- Verify insurance coverage
- Implement internal data protection safeguards



# INTERNATIONAL DATA TRANSFERS

## *UK DATA TRANSFERS*

- On March 21, 2022, the UK's new International Data Transfer Agreement ("IDTA") and the international data transfer addendum to the EU's Standard Contractual Clauses ("Addendum") came into effect.
- Data exporters will be able to use the IDTA or the Addendum to comply with Article 46 of the UK GDPR when making restricted transfers and will replace the current SCCs for international transfers.
- The IDTA and the Addendum take into account the Schrems II decision.
- Implementation:
  - Use the IDTA or the Addendum for all new contracts for transfers of personal data from the UK to a third country, by no later than **September 21, 2022**; and
  - Replace all old EU SCCs with the IDTA or Addendum for ongoing transfers from the UK to a third country, by no later than **March 21, 2024**.



# INTERNATIONAL DATA TRANSFERS

## *NEW TRANS-ATLANTIC FRAMEWORK (PRIVACY SHIELD 2.0) & CBPR*

- On March 25, 2022, the United States and the European Commission committed to a new **Trans-Atlantic Data Privacy Framework** to replace the invalidated EU-U.S. Privacy Shield Framework
  - The new Framework will ensure that:
    - Signals intelligence collection may be undertaken only where necessary to advance legitimate national security objectives
    - EU individuals may seek redress from a new multi-layer redress mechanism that includes an independent Data Protection Review Court
    - U.S. intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards
  - Companies will need to self-certify adherence to the Principles through the U.S. Department of Commerce
- On April 21, 2022, the United States, Canada, Japan, the Republic of Korea, the Philippines, Singapore and Chinese Taipei (Taiwan) announced the creation of the **Global Cross-Border Privacy Rules (CBPR) Forum**.
  - The CBPR Forum:
    - Builds on the 21-nation Asia-Pacific Economic Cooperation CBPR System created in 2005 & updated 2015
    - Will expand the existing CBPR System to establish an independently administered broader international certification system open to more countries
    - Will give certification to companies that meet high privacy and data security standards to act as a transfer mechanism recognized as a valid legal basis for transfer
    - Focuses on interoperability designed to bridge national varying privacy regimes

# INTERNATIONAL DATA TRANSFERS

## CHINA

China's Personal Information Protection Law (PIPL) (effective November 2021)

### ■ Data localization

- The Cybersecurity Law (CSL) of 2017 contains data localization requirements for personal information held by Critical Information Infrastructure (CII) Operators (Art. 37). There are numerous other data localization requirements pertaining to specific sectors and types of data (e.g., banking, healthcare, internet mapping).
- PIPL requires CII operators or entities processing a large amount of information to store the data locally, and if transfer is necessary, pass a security assessment (PIPL Art. 40).

### ■ International transfer restrictions

- Under PIPL, in general, organizations are required to provide individuals with certain information about the transfer, obtain specific consent, adopt measures to make sure the third country provides the same level of protection, and carry out a data protection impact assessment (PIPL Arts. 39, 38, 55). They must also meet one of the conditions for transfers, such as passing a security assessment (mandatory for certain organizations) or concluding a standardized contract (PIPL Art. 38)
- Foreign entities can be added to a sanctions list whereby they may be restricted or prohibited from receiving personal information.
- There is no similar process to the GDPR for authorities to designate countries as having adequate safeguards.

# INTERNATIONAL DATA TRANSFERS

## LATAM (BRAZIL & ARGENTINA)

- Brazil's LGPD (2020) mirrors GDPR cross-border transfer requirements, e.g., transfer mechanisms or adequacy; prior specific consent. (General restriction on international transfers, with exceptions.)
- Brazil's regulator (ANPD) has yet to release a list of countries with adequacy decisions. The ANPD is expected to release guidance on cross-border transfers in 2022.
- The ANPD will regulate the use of model DTAs, SCCs, etc. The ANPD's director indicated that she prefers a simpler approach to SCCs rather than the EU approach complicated by *Schrems II*.
- Hosting data in foreign countries is considered a form of international data transfer.

### Data localization

- The LGPD does not specifically regulate data localization, but other laws may apply, including for the financial and public sectors.

- Argentina's Personal Data Protection Act (PDPA) was enacted in 2000.
- Main Regulations enacted in December 2001
- 2002 - recognized as adequate in Opinion 4 of 2002 by EU Commission
- Article 12 of the PDPA prevents the transfer of personal data to a country that does not provide an adequate level of protection.
- International transfers: Argentine SCCs approved 2016
- Transfers to non-adequate countries only permitted if:
  - Data subject expressly consents
  - Data is transferred pursuant to an agreement with SCCs
  - Intragroup transfers if Binding Corporate Rules have been put in place

# INTERNATIONAL DATA TRANSFERS

## *CHECKLIST*

- ☐ Assess and document where international data transfers are happening (internal and external)
- ☐ Determine whether data localization requirements apply
- ☐ Prioritize transfer types, third parties, and countries for selecting appropriate transfer mechanisms that work for your client.
- ☐ Execute data protection agreements, including SCCs (where needed), to establish appropriate transfer-related obligations.
- ☐ Conduct and document transfer impact assessments.

# QUIZ BREAK - TEST YOUR PRIVACY SENSITIVITY

**Do you allow apps on your phone to track your location?**

1. No. I turn them all off.
2. Sometimes. I usually keep location “off,” but sometimes turn it “on” for maps apps when I actively need directions.
3. Yes, all of them. It is vitally important that Old Navy know where I am at every moment of every day.
4. They can track my location??



# CONSENT

## OVERVIEW

### Selected Global Examples

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

**Brazil LGPD:** Consent means a **free, informed and unambiguous** manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose.

**China PIPL:** Where the handling of personal information is based on individuals' consent, that consent shall be given **voluntarily and explicitly** by individuals who are **fully informed**. Where laws and administrative regulations provide that independent or written consent shall be obtained for the handling of personal information, follow those provisions.

**United States:** Notice and Consent must be reasonably and fully informed under Federal Trade Commission Act Section 5 fairness requirements. Emerging U.S. state laws make additional explicit requirements (see next slide).

# CONSENT

## COMPARING U.S. STATE LAWS & EU GDPR

**CCPA/CPRA:** “Consent” means any **freely given, specific, informed, and unambiguous** indication of the consumer’s wishes, including by a statement or by a clear affirmative action, that signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.

### Not consent:

- Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information
- Hovering over, muting, pausing, or closing a given piece of content
- Agreement obtained through use of dark patterns

**Opt-in consent required for financial incentive programs & for consumers under 16**

|                                                           | Colorado CPA | Virginia & CT | California CCPA, as amended by CPRA | Utah CPA | EU GDPR |
|-----------------------------------------------------------|--------------|---------------|-------------------------------------|----------|---------|
| Right to opt-out of sale                                  | ✓            | ✓             | ✓                                   | ✓        | ✗       |
| Opt-in or opt-out for processing of sensitive information | Opt-in       | Opt-in        | Opt-out                             | Opt-out  | Opt-in  |

# QUIZ BREAK - TEST YOUR PRIVACY SENSITIVITY

**How often do you clear cookies on your Internet browser?**

- A. Weekly. I prefer to set my own path online.
- B. 1-2 times a year, usually when I hear a news story about a privacy breach.
- C. Never. It's nice to know I have company following me around the web.
- D. The only kind of cookies I know come with chocolate chips.



# COOKIES

## EXAMPLE BANNERS



### Your privacy



California residents have certain rights with regard to the sale of personal information to third parties. Guardian News and Media and our partners use information collected through cookies or in other forms to improve experience on our site and pages, analyze how it is used and show personalized advertising.

At any point, you can opt out of the sale of all of your personal information by pressing

[Do not sell my personal information](#)

You can find out more in our [privacy policy](#) and [cookie policy](#), and manage your choices by going to 'California resident – Do Not Sell' at the bottom of any page.

### Managing your preferences about cookies

Some features of this website rely on services offered by third-party sites (twitter feed, videos). If you give your consent, these third-party sites will drop cookies that will allow you to visualize on our site content hosted by these third-parties, and share our contents. They will collect your browsing data and use the data collected via their cookies for purposes they have determined in accordance with their privacy policy (link below). You can give or withdraw your consent on this page. You can express your choice globally or purpose by purpose.

ALLOW

DENY

### Sky uses cookies to create a better experience for you

Sky's trusted [partners](#) need your permission to store and access cookies, unique identifiers, personal data, and information on your browsing behaviour on this device. This only applies to Sky.com. You can change your preferences at any time via the Privacy Options at the end of each page. You don't have to accept, but some personalised content and advertising may not work if you don't. Click the arrows below to find out more about how your data is used.

Store and/or access information on a device



Personalised ads and content, ad and content measurement, audience insights and product development



Precise geolocation data, and identification through device scanning



Click Manage Preferences below to see how and why our partners may use your data. There you can also review where they claim a legitimate interest to process your data, and object to that if you want.

[Manage Preferences](#)

Agree



### Privacy Preference Center

Hereafter, you will find a description of various cookies that we use on our website and you can set your preferences. You can change your cookie settings at any time, for example by clicking on the "Cookie Settings" link at the bottom of the website. For further information on how we process data in connection with cookies on our website, please refer to our [cookie policy](#).

Strictly Necessary

Always Active



Functional



Performance



Marketing and Analysis



Social Media



ALLOW ALL

CONFIRM MY CHOICES

By clicking "Accept All Cookies", you agree to the storing of first and third party cookies on your device to enhance site navigation, analyze site usage, enable social media features and assist in our marketing efforts. [Cookie Policy](#)

[Cookies Settings](#)

Reject All

Accept All Cookies

# COOKIES

## *EVOLUTION OF RULES*

- E-Privacy (2002-18) – Soft opt in; opt out opportunity also to be provided.
- GDPR (2018-present) – Pre-ticked boxes no longer okay. Silence or inaction is not valid consent.
- CCPA/CPRA – Do Not Sell [or Share] My Personal Information – right to opt out includes targeting cookies; valid consent must be “freely given, specific, informed and unambiguous indication of consumer’s wishes” – no presumption.
- EU Supervisory Authorities – Consent may not be obtained by soft opt in or cookie wall; continued browsing is not valid consent; only strictly necessary cookies are exempted.\*
  - Some, including the French CNIL, deem personalization and some analytical cookies to be exempt.
- European Data Protection Board (May 2020) – Confirmed soft opt-in is not valid consent; cannot deny access if individual has not consented to tracking technologies.

# COOKIE BANNERS

## *MANY CONSIDERATIONS*



- Notice and Consent must be clear and unambiguous (an enforcement priority under the CCPA)
- Expanding rights under CA, CO, VA, UT and CT comprehensive privacy laws
- User Experience – meeting both growing privacy expectations and functional ease
- Transparency is also key
- Session replay - defense against wiretap claims

# COOKIES

## ENFORCEMENT

### Increased **DPA** enforcement across **EMEA**; complaints by **NOYB**

- December 2021 - France fined Meta €60M for inadequately facilitating refusal of cookies
- December 2021 - France fined Google €61.50M for inadequately facilitating refusal of cookies
- December 2020 - France fined Amazon €35 million in relation to cookie consents
- December 2020 – France fined Google and Google Ireland €100M for cookie violations on google.fr

### Focus on ability to “reject all” in cookies banners

- April 2022 – Hamburg DPA said Google and YouTube banners were in violation; need option to “reject all” as easily as “accept all”
  - Decision based on France’s CNIL decision in December 2021 regarding Meta (Facebook) and Google
- April 2022 – Google LLC sued by the Consumer Advice Centre of North Rhine-Westphalia in Berlin Regional Court over google.de cookies banner
  - Ability to reject all is much more complicated than ability to accept all (2 levels of banner, >3 categories of cookies); use of dark patterns (encouraging comprehensive consent)

# CONSENT/COOKIES

## *CHECKLIST*

- ☐ Determine if consent is the most appropriate lawful basis of processing for the purpose and data subjects
- ☐ Document the conditions of consent and implement such into the processing program
- ☐ Establish appropriate governance and methods for cookie consent
- ☐ Choose whether a single global approach or a geo-differentiated approach based on opt-in vs. opt-out rules is best for your client
- ☐ Provide a readily available method to revoke consent
- ☐ Make clear to data processors limitations on subsequent data use

# DATA SUBJECT RIGHTS

*GDPR, LGPD, PIPL*

| EU GDPR                                                                                                                                                                                                                                                                                                                                                                                                        | Brazil LGPD                                                                                                                                                                                                                                                                                                                                                                                                                | China PIPL                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Right to transparent communication and information</li><li>• Right to access</li><li>• Right to rectification</li><li>• Right to erasure</li><li>• Right to withdraw consent</li><li>• Right to restrict processing</li><li>• Right to data portability</li><li>• Right to object</li><li>• Right to not be subject to automated decision-making (profiling)</li></ul> | <ul style="list-style-type: none"><li>• Right to receive information about treatment / processing</li><li>• Right to access</li><li>• Right to rectification</li><li>• Right to delete and block unnecessary or excessive data or data processed in non-compliance with the LGPD</li><li>• Right to revoke consent</li><li>• Right to portability</li><li>• Right to not be subject to automated decision-making</li></ul> | <ul style="list-style-type: none"><li>• Right to know</li><li>• Right to consult (similar to access)</li><li>• Right to request correction or completion (similar to rectification)</li><li>• Right to request deletion</li><li>• Right to withdraw consent</li><li>• Right to data portability</li><li>• Right to restrict processing</li><li>• Right to refuse handling of personal information</li><li>• Right to not be subject to automated decision-making</li></ul> |

# DATA SUBJECT RIGHTS

## US PRIVACY LAWS

|                                         | Colorado CPA | Virginia CDPA | California CCPA, as amended by CPRA | Utah CPA | Connecticut DPA |
|-----------------------------------------|--------------|---------------|-------------------------------------|----------|-----------------|
| Right of Access                         | ✓            | ✓             | ✓                                   | ✓        | ✓               |
| Right of Rectification                  | ✓            | ✓             | ✓                                   | ✗        | ✓               |
| Right of Deletion                       | ✓            | ✓             | ✓                                   | ✓        | ✓               |
| Right of Restriction                    | ✓ (P)        | ✓ (P)         | ✗                                   | ✓ (P)    | ✓ (P)           |
| Right of Portability                    | ✓            | ✓             | ✓                                   | ✓        | ✓               |
| Right to Opt Out of Sales               | ✓            | ✓             | ✓                                   | ✓        | ✓               |
| Right Against Automated Decision Making | ✓ -          | ✓ -           | ✗                                   | ✗        | ✓               |
| Private Right of Action                 | ✗            | ✗             | ✓ (L)                               | ✗        | ✗               |

# DATA SUBJECT RIGHTS

## TIMING

| GDPR                                                                                                                                                                     | LGPD                                                                                                                                                                                                                                                    | PIPL                                                                                                                                                                                                                   | CPRA                                                                                                                                           | VA, CO, UT, CT                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Within one month of receipt of the request with a two month extension option.</p> <p><b>*Consider identity verification procedures given recent EDPB guidance</b></p> | <p>Confirmation of the existence of processing or access must be provided immediately when provided in a simplified format, or within 15 days from the date of the data subject's request when provided by means of clear and complete declaration.</p> | <p>Where individuals request to consult, copy, correct, or complete their personal information, it shall be provided in a timely manner.</p> <p>Information handlers must proactively delete personal information.</p> | <p>Within 45 days of receipt of a verifiable consumer request to access, delete, or correct, but only 15 business days to opt-out of sale.</p> | <p>Within 45 days of the receipt of a request with a 45 day extension option, which is not exercisable if the controller declines to take action.</p> |

# DATA SUBJECT RIGHTS

## *CHECKLIST*

- ☐ Identify data subject rights under applicable privacy laws and anticipated volume of requests.
- ☐ Plan strategic response times in consideration of available resources and legal timeframes.
- ☐ Harmonize data subject rights response procedures to the extent possible.
- ☐ Implement at least a manual verification process as part of response procedures.
- ☐ Explore automation based on expected volume and available resources.
- ☐ Monitor and document volume, categories and sources of requests and response times.

# QUESTIONS?

