



**Envisioning Excellence for
Mission Driven Success**



Privacy First: Anticipating future legislation and the impact on your operations

Thursday September 28, 2023

Amy Daultrey Krishnaswamy

Software Services Consultant

amy@amydaultrey.com

Disclaimer

This presentation does not constitute legal advice. Please seek legal guidance specific to your organization on the topics discussed.

Privacy?

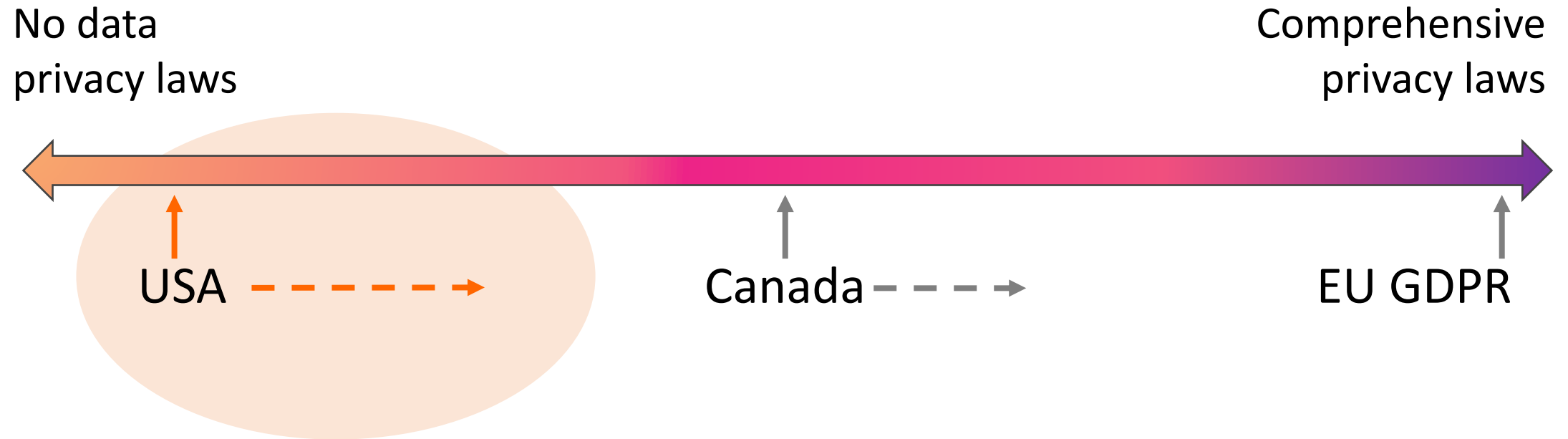
- “Information privacy is the right to have some control over how your personal information is collected and used” (IAPP)
- As custodians of donor data we should always take a **privacy first** approach to data acquisition and use.
- It's not about cyber security and data breaches but it crosses over with these.
- Inevitable that your organization will be affected by privacy law at some point (if it hasn't already).

Key terms

- **Personal data** = any information that can be connected to a person.
- **Processing** = any kind of handling of personal data (acquiring it, storing it, using it etc.)
- **Consumer data = donor data**

How do you feel your organization is handling donor privacy? Data sets need cleaning? Preferences are a bit messy? Unsure what to do about retention? Maybe your opt-out process needs work? What if you could use privacy law as a framework to get these things **done**?

A (rudimentary) spectrum

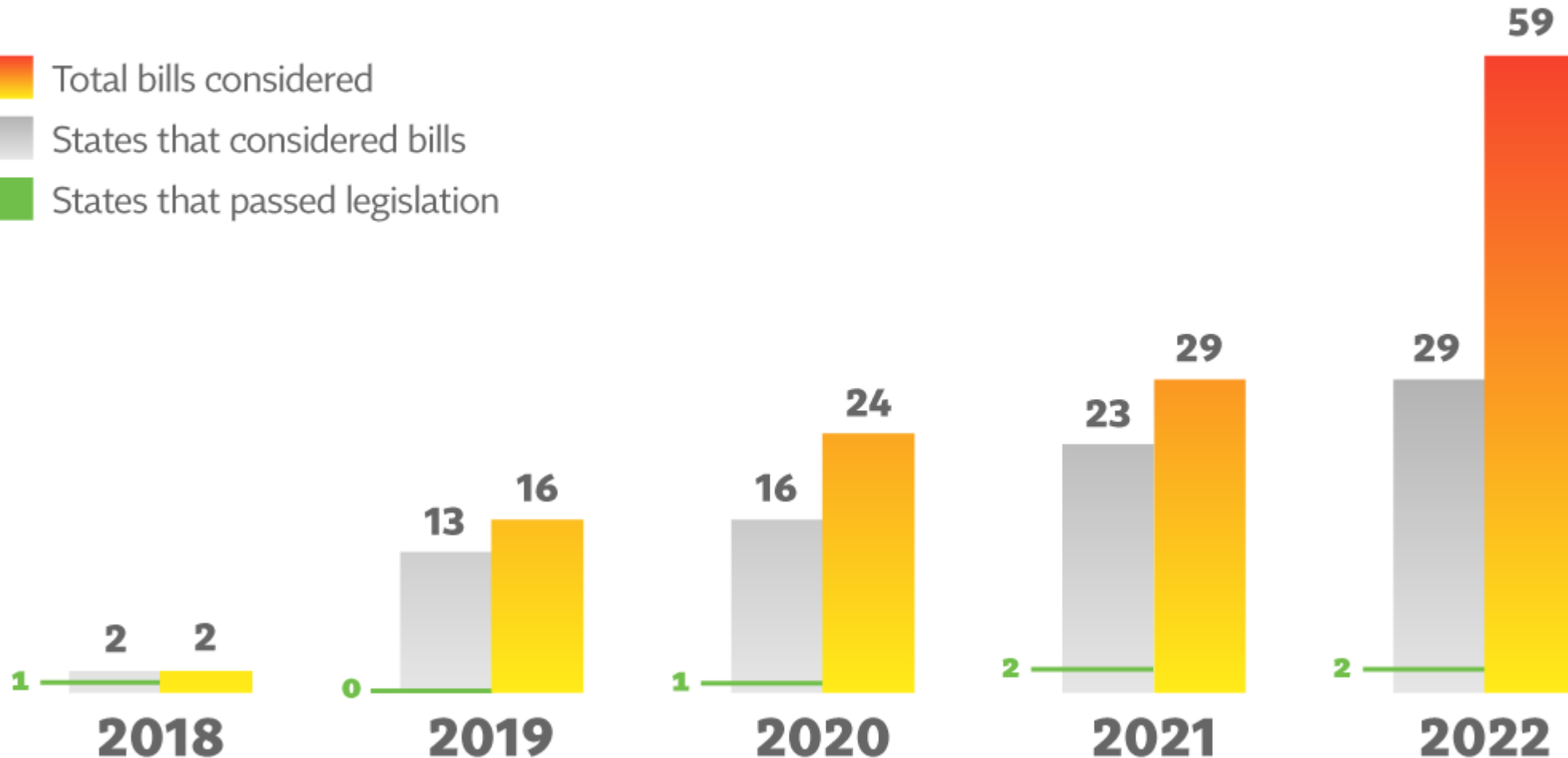


The Growth of State Privacy Legislation

iapp.org

Comprehensive consumer privacy bills considered from 2018-2022

- Total bills considered
- States that considered bills
- States that passed legislation



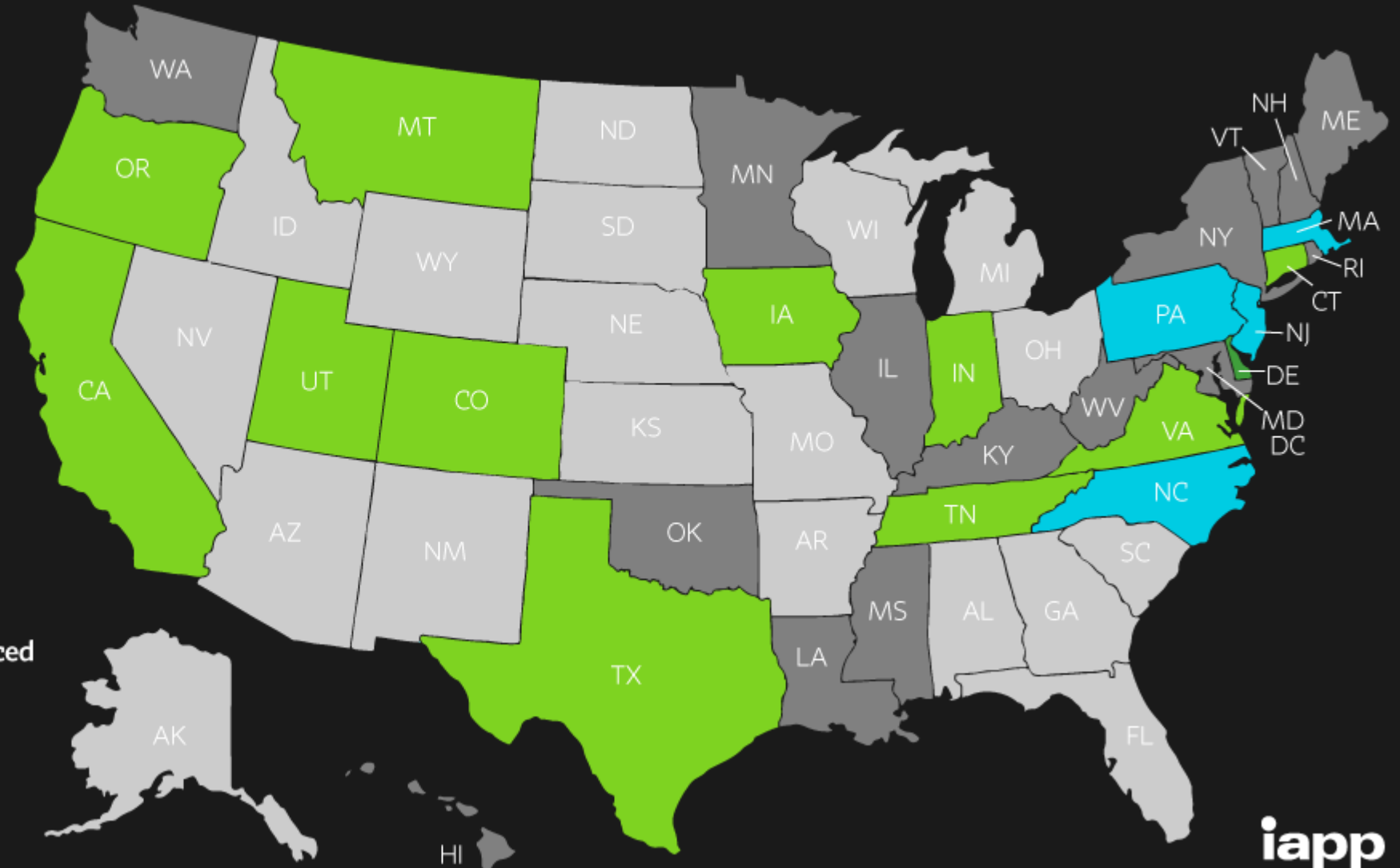
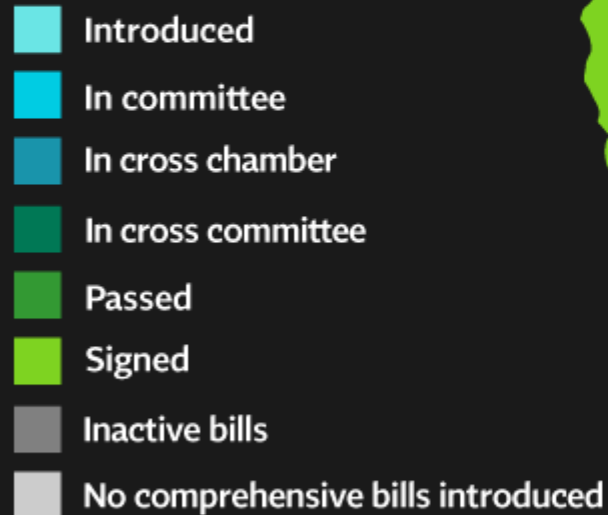
Recap: State bills considered

2018: 2

2022: 59

US State Privacy Legislation Tracker 2023

STATUTE/BILL IN LEGISLATIVE PROCESS



🔄 Last updated: 8/4/2023

iapp

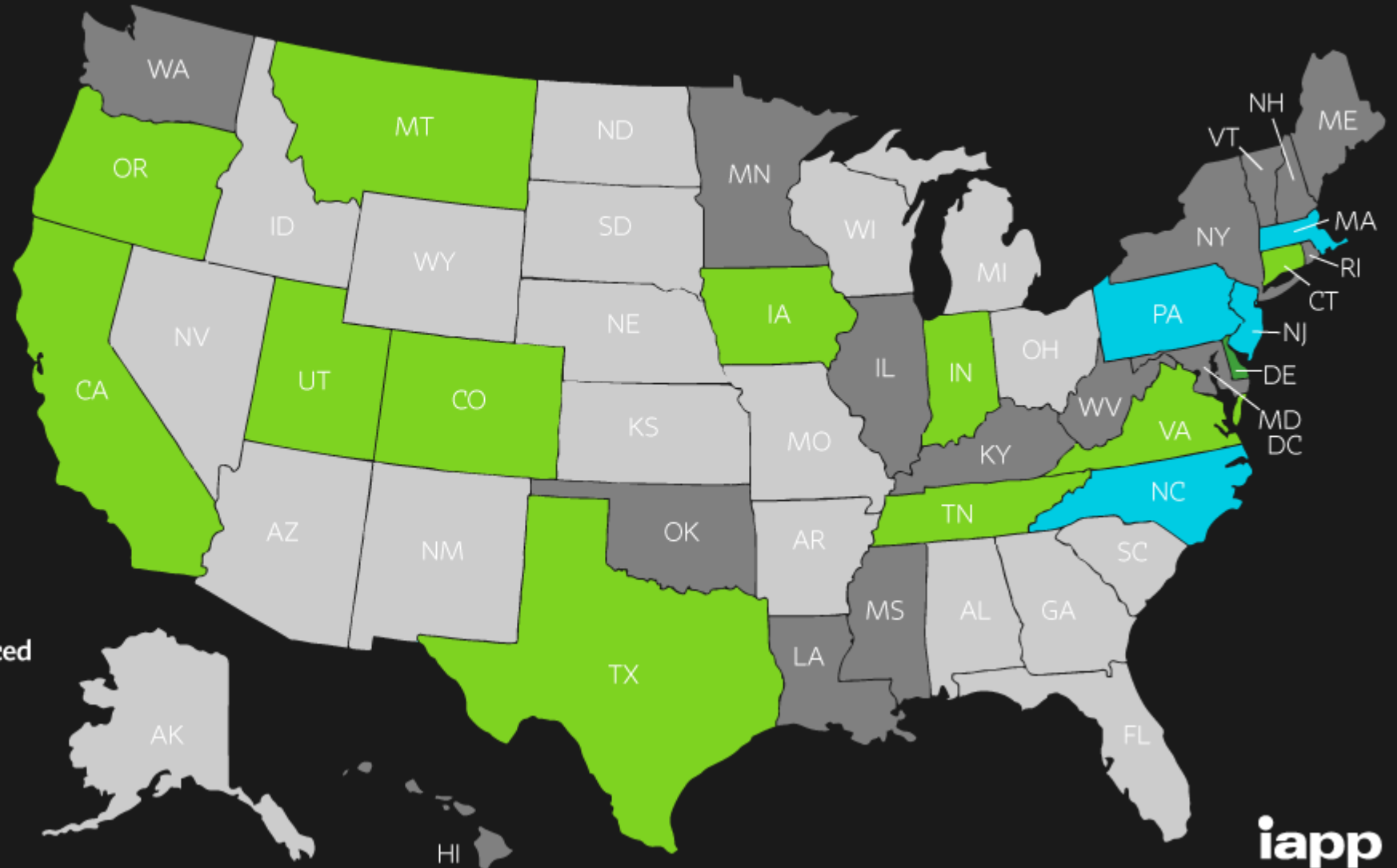
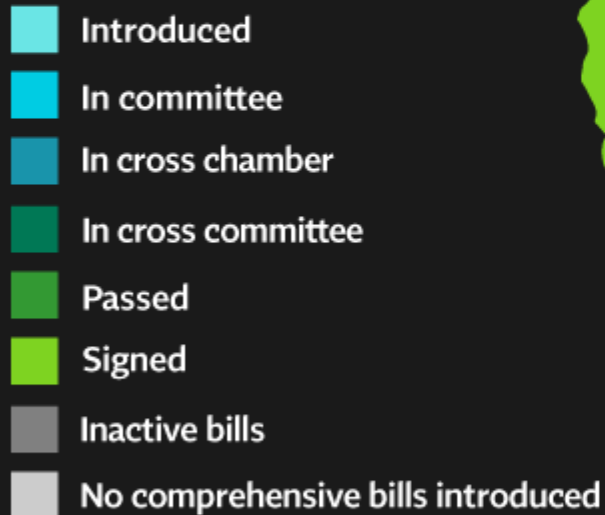
Federal...when, not if

~~American Data Privacy and Protection Act~~
2023-24 Congress: 19 privacy bills

State precedents

- Colorado (July 2023) first to not exempt nonprofits
- Oregon (July 2024) is the second
- **That's 2 out of 11 enacted bills so far that do not exempt nonprofits**
- Thresholds for compliance (ie. processing 50k or 100k residents' data/year)
- Texas precedent: no threshold but small businesses exempt.
- Per-violation fines. Typically \$7,500-\$20,000.

US State Privacy Legislation Tracker 2023



🔄 Last updated: 8/4/2023

iapp

Commonalities: consumer rights

- Right to access, correct and delete (including data from third parties)
- Right to opt out of targeted advertising, selling data & profiling
- Right to opt out of data being processed
- Right against automated decision making
- Right to obtain list of third parties data shared with

Commonalities: business/org obligations

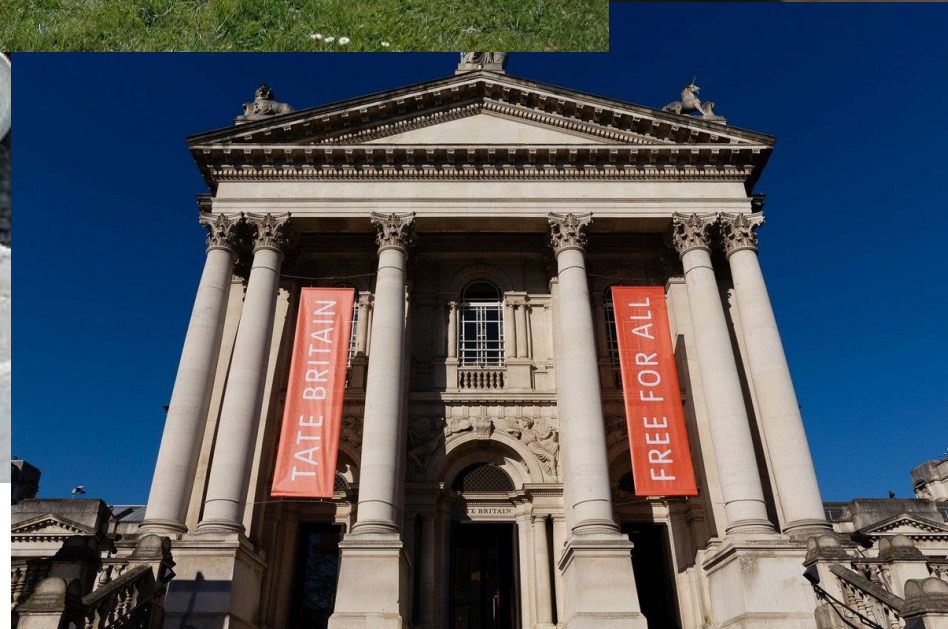
- Privacy notices that are clear and easy to find
- Limit data collection to what is **adequate, relevant and necessary** to serve purposes contained in privacy notice
- Take all steps to secure personal data
- Don't collect sensitive data without consent (includes transgender/nonbinary status)
- Provide a means for consumers to opt out
- Be ready to recognize UOOMs at a future date (Oregon: 1/1/26)
- Conduct risk assessments of projects, procedures

Oof this is a lot



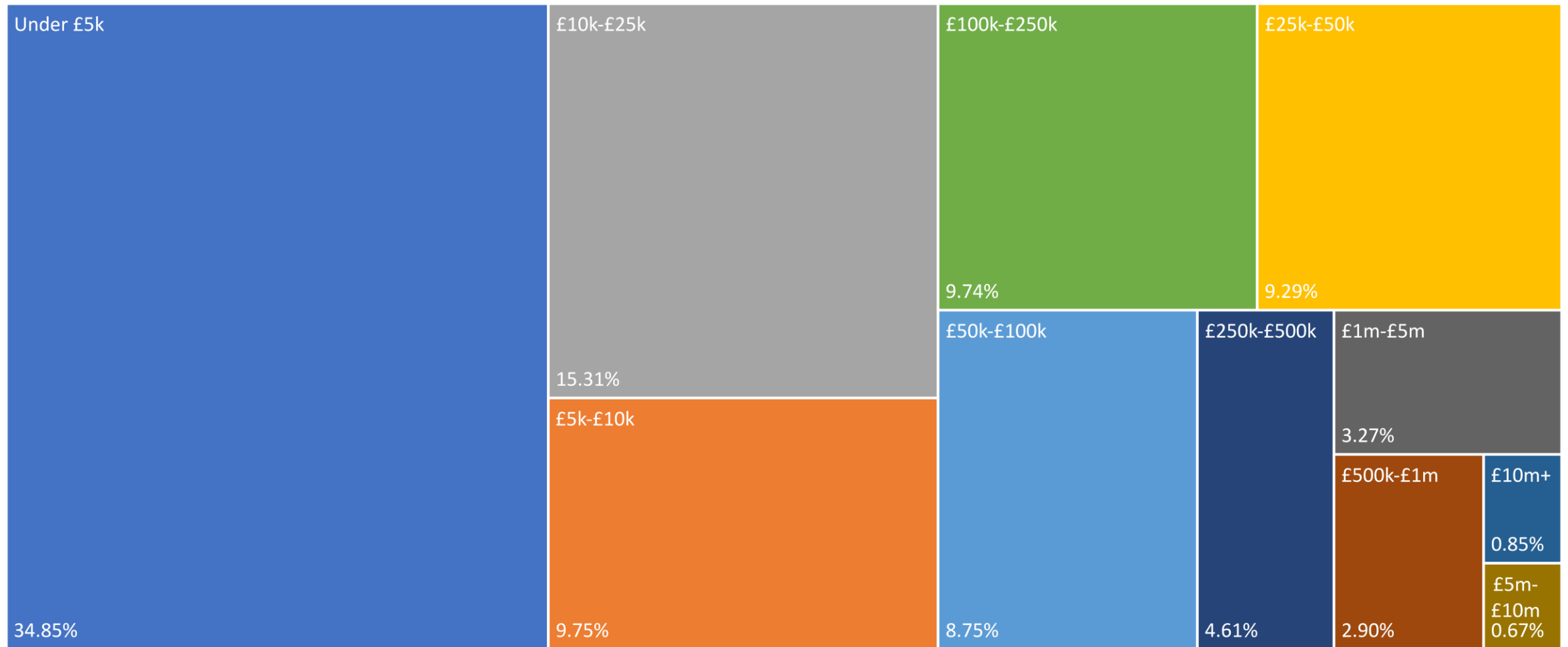
You have nothing to lose in aiming for compliance even if you are not legally required to.

(More on the potential positives later!)



aasp
2023
SUMMIT
SEPT. 27-29
Chicago, IL

UK charity sector

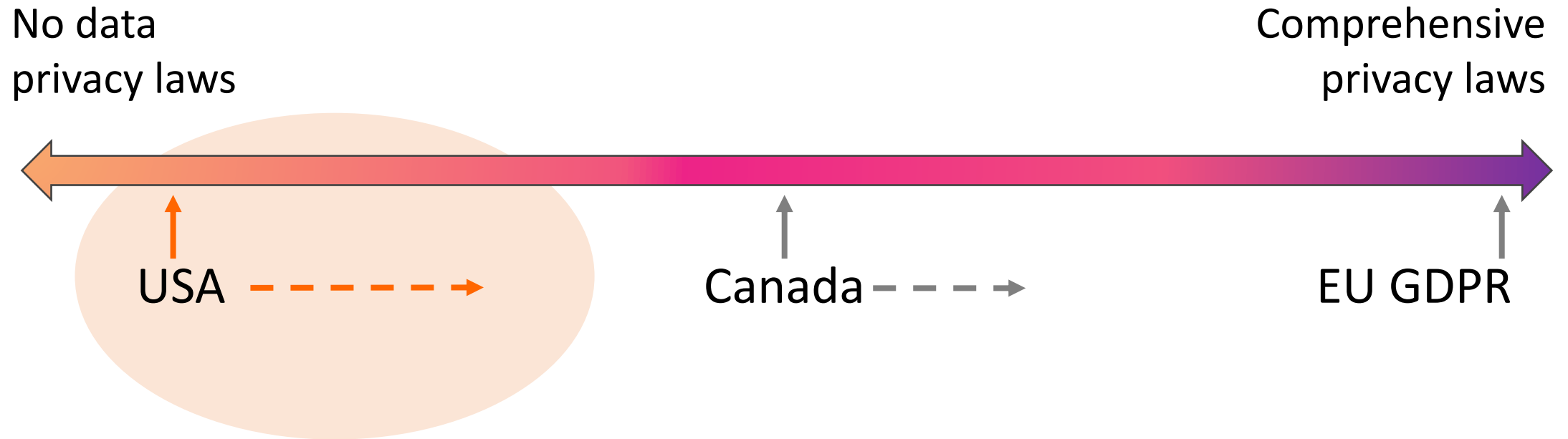


169,070 charities in 2023 <https://register-of-charities.charitycommission.gov.uk/sector-data/charities-by-income-band>

GDPR is everything you imagine it to be

- 28 countries (EU+UK), 24 languages, 500+ million people
- Unified separate laws
- It's complicated
- But everyone is aware of it
- Impacted everyone. No thresholds. A blunt instrument.
- Hefty fines (4% of annual global turnover)
- Privacy-first is the standard, not a fringe topic

US will not get GDPR verbatim but...




The challenges will be similar

- Guidance will be late and lack specificity to sector
- Some organizations will be unnecessarily cautious to reduce liability
- Scammers will try to monetize the uncertainty
- Small orgs with no legal resources will struggle (collaboration will help)
- Late action will cost time and money

The rewards will be sweet

- A chance to dedicate resources to cleaning, reducing, refreshing data
- A chance to obtain long reaching consent
- Increased engagement
- Better metrics on engagement, interests, preferences
- A chance to demonstrate to your donors that they can trust you with their information

A photograph of a child standing on a wide set of stone steps in front of a stone wall. The child is wearing a cap and overalls, looking down at the steps. The steps are made of large, light-colored stone blocks and lead up to a wall of similar stone blocks. The lighting is warm, suggesting late afternoon or early morning. The text "Yes but this. And I don't believe we'll be affected." is overlaid in white on the right side of the image.

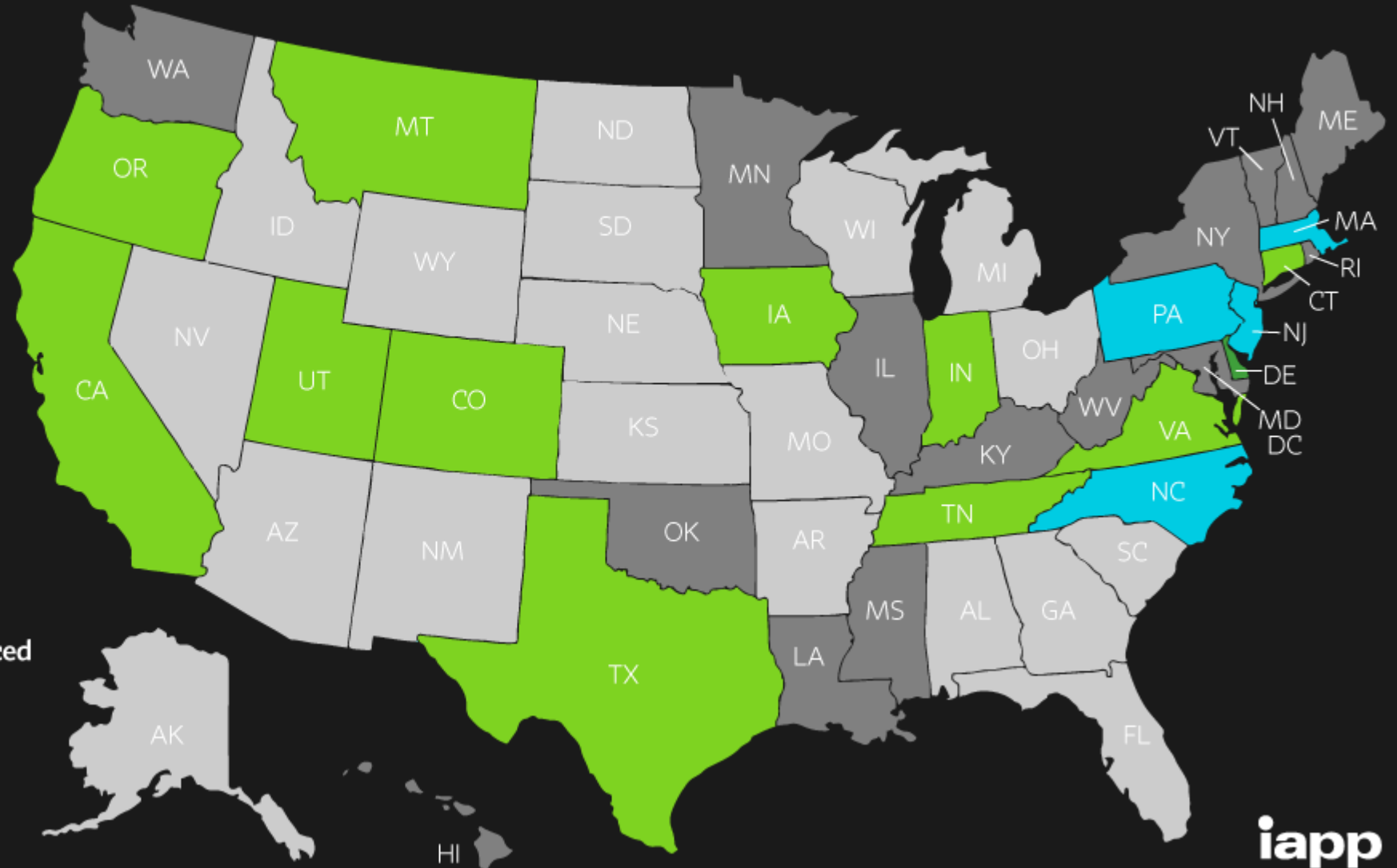
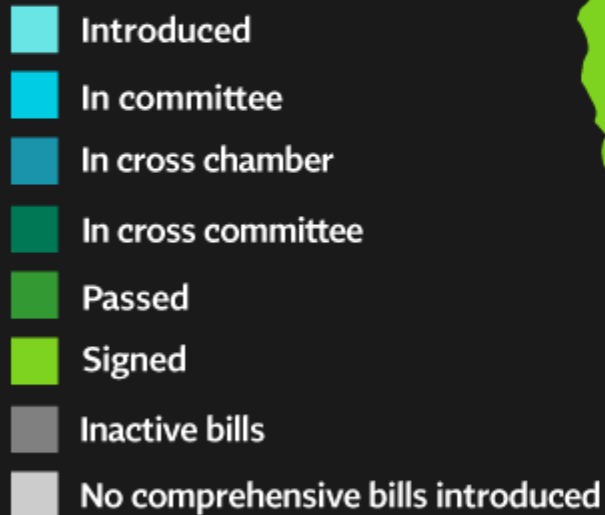
Yes but this.
And I don't
believe we'll
be affected.

The do-nothing approach

- Relies on consumers knowing when nonprofits are exempt.
- Assumes your donors won't care about any of it.
- Relies on the trend of exemption (9 out of 11 bills so far have nonprofit exemptions). This could easily change. Plus wildcard variations (Texas).
- Short lead-in times to compliance (typically a year); is that enough time to respond and prepare? Do you have the resources to act that fast?

US State Privacy Legislation Tracker 2023

STATUTE/BILL IN LEGISLATIVE PROCESS



🔄 Last updated: 8/4/2023

iapp

You have nothing to lose in aiming for compliance even if you are not legally required to. This is a rare opportunity to direct resources to data quality, data processing and donor care.

Ok I'm in. What do I do first?

DREAM
BIG.

Where to start

- Thoughtful, early planning is best
- Use Colorado and Oregon as a guide
- Take talking points to your team
- Follow what's happening in the states in which you have constituents/operations

Talking points

What personal data do we have?

Do we have anything considered sensitive?

Do we have data we don't need?

Why do we have this data?

Where are we asking our donors their preferences and opt-in, and how are we storing this?

Where are all the places we gather data from?

What's our privacy policy?
Is it easy to understand?

What's our data retention policy?

Top tips

1. Incorporate privacy and preferences messaging into marketing and stewardship.
2. Train staff **early and often** so concepts and procedures become second nature.
3. To help implement data minimization use a traffic light data entry system (see handouts).

Top tips

4. Form task groups across departments (see case study in handouts).
5. Test your procedures for honoring preferences and opt-outs, **make sure everything works as it should** – especially from donor point of view.
6. Don't wait for your database and other systems to be improved to support privacy law requirements.
Assume you'll be working with the tools you have right now.

This is a rare opportunity to direct resources to data quality, data processing and donor care. An early start reduces the impact on your crucial operations. You'll be ready.

Resources

- See handouts in the app or ask me amy@amydaultrey.com
- Track state legislation: iapp.org/resources/article/us-state-privacy-legislation-tracker
- and federal: iapp.org/resources/article/us-federal-privacy-legislation-tracker
- Topic guides, loads of useful links, reading material at amydaultrey.com/resources



Thank you!

amy@amydaultrey.com

LinkedIn: [amydkrishnaswamy](#)