RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PRV-R03**

New Way of Tackling Privacy Assessments

Dr. Lisa McKee, Ph.D.

Director of Governance, Risk, Compliance and Privacy
Hudl

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Today's Speaker – Dr. Lisa McKee, Ph.D.

VP & Certification Director Omaha Chapter
APMG Certification Trainer

Privacy Workforce Working Group
Risk Assessment Lead

Mentor

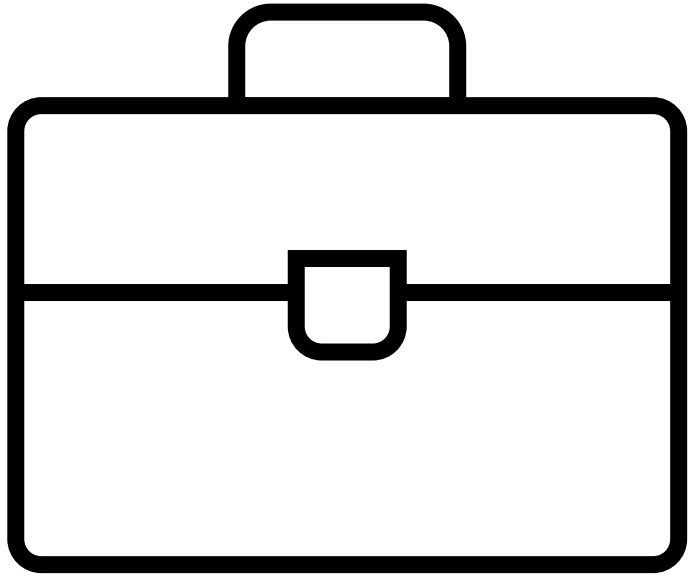
SheLeadsTech Ambassador

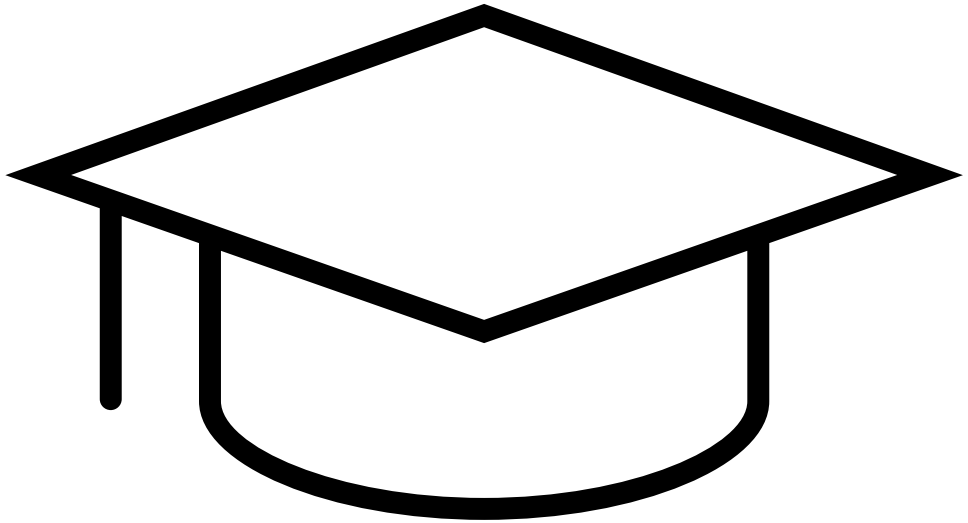
SD Affiliate Director Programs & Events
WiCyS National Mentor

Member & Tech Editor

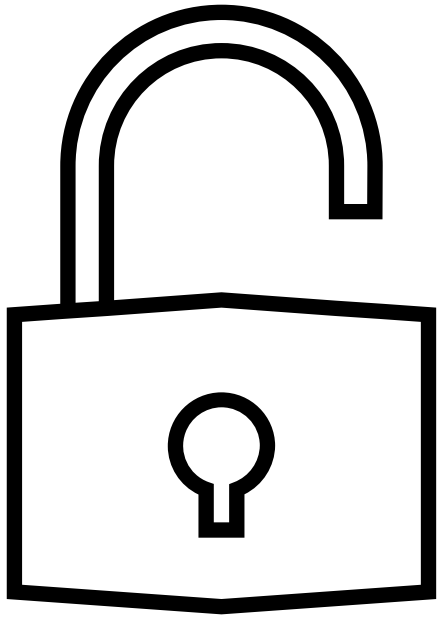
Adjunct Instructor &
PriLab Research Lead

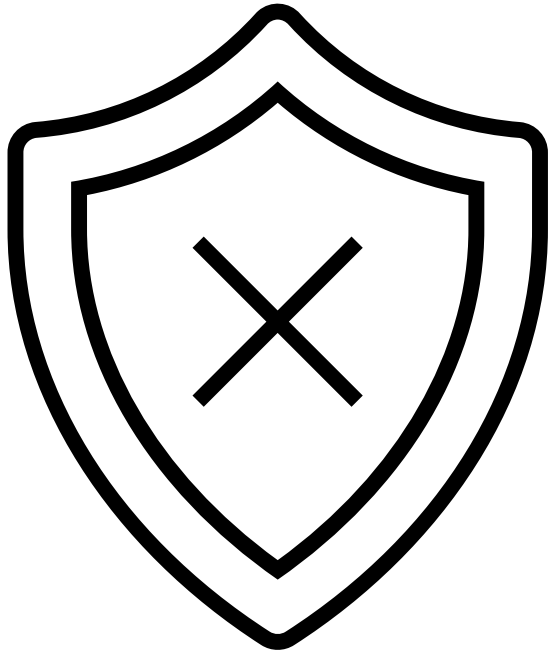
Professional or Student?

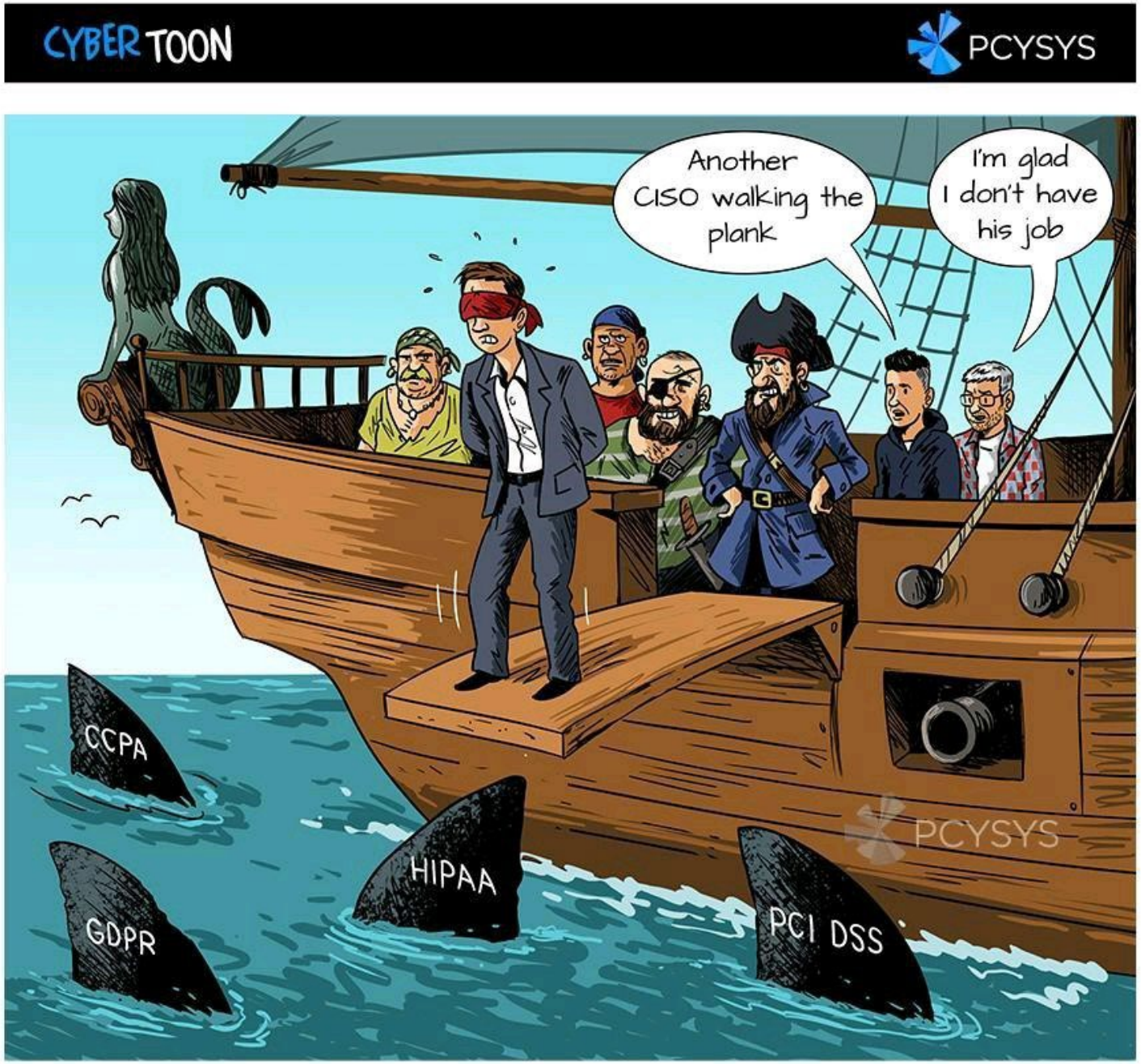




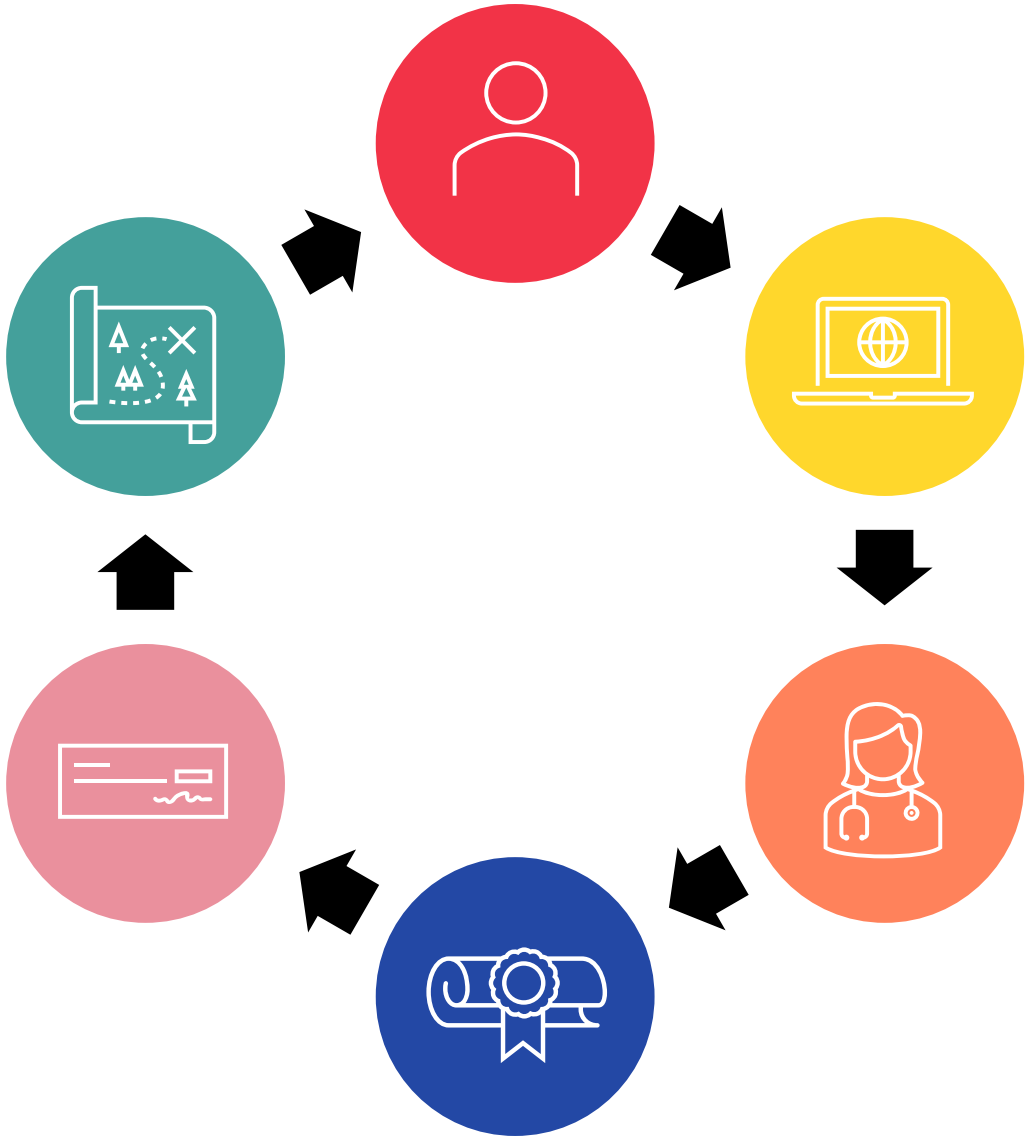
Security vs. Privacy






CYBER TOON
PCYSYS
Another CISO walking the plank
I'm glad I don't have his job
CCPA
GDPR
HIPAA
PCI DSS
PCYSYS

Categories of Personal Data



Core Privacy Rights

Access

- Free access to personal information that is collected on the consumer.
- Includes providing who else has access to the information.
- Must be prompt
  - US 45 days
  - EU 30 days
  - **Brazil 15 Days!**

Disclosure

- Provide privacy and data collection policies at or before time of collection.
- Disclose purpose of the information collection.
- Inform consumers of their rights under GDPR / CCPA.

Consent

- Consent must be obtained to market to the consumer (GDPR).
- Consumer can object to automated processing of data (GDPR).
- Consumer can opt out of having their information sold or transferred to other businesses or third parties (CCPA).

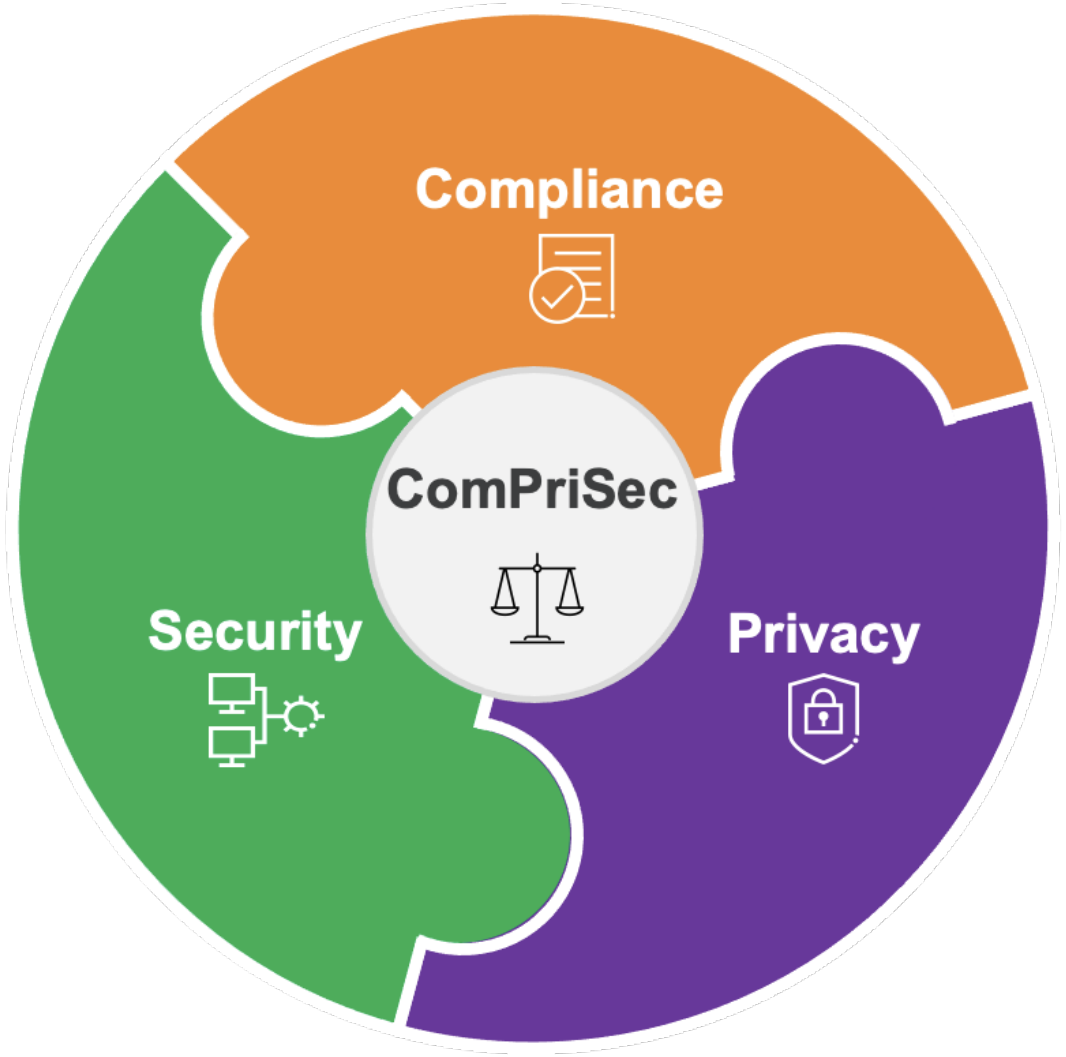
Deletion

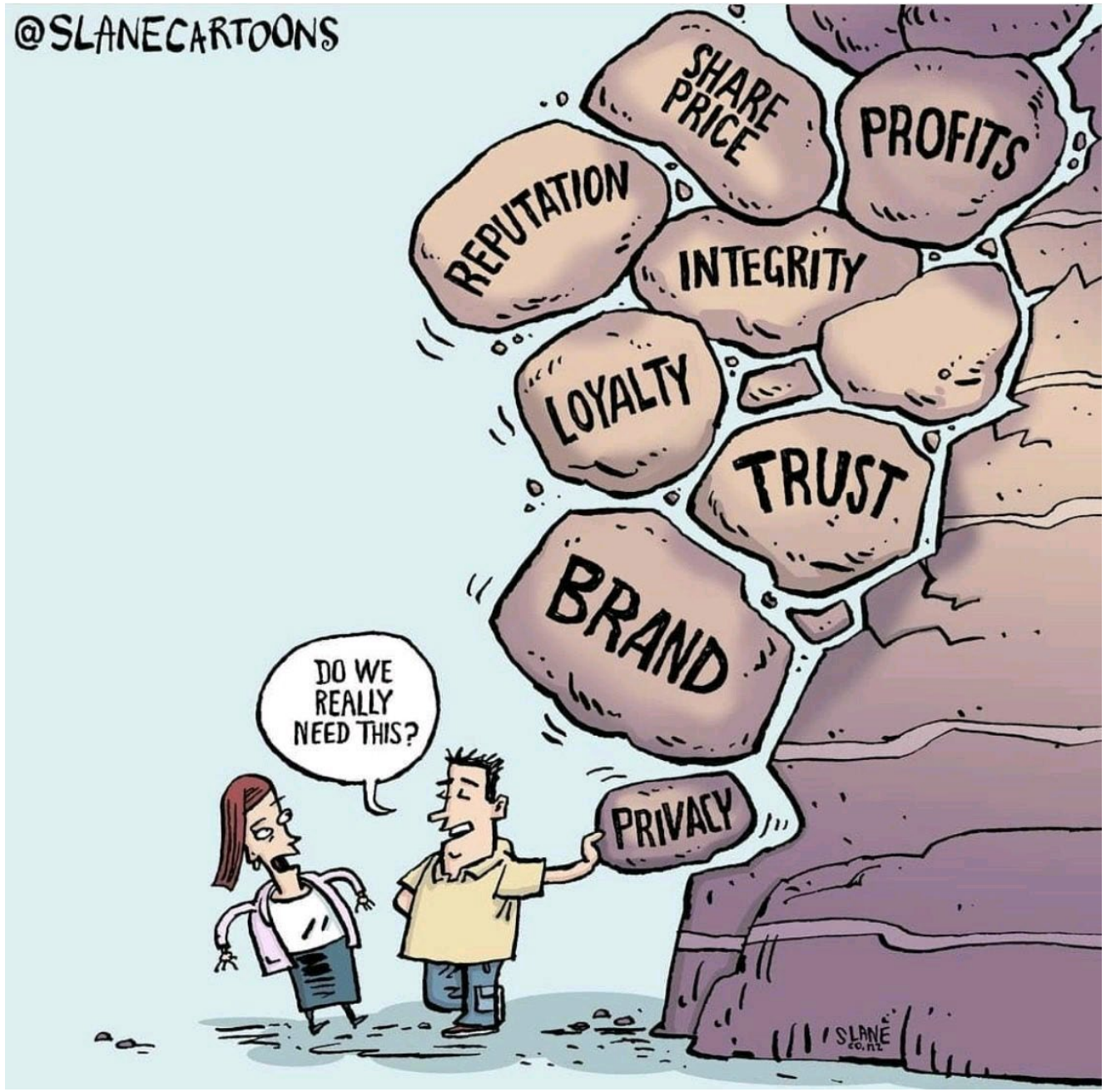
- With certain exceptions, consumers have the right to have information about them deleted.
  - All data concerning the subject (GDPR).
  - All data collected from the consumer (CCPA).

Privacy Across the Organization

- Information Technology
- Legal & Compliance
- Third Party Suppliers
- Marketing
- Finance & Accounting
- Human Resources
- Internal Audit
- Software Development

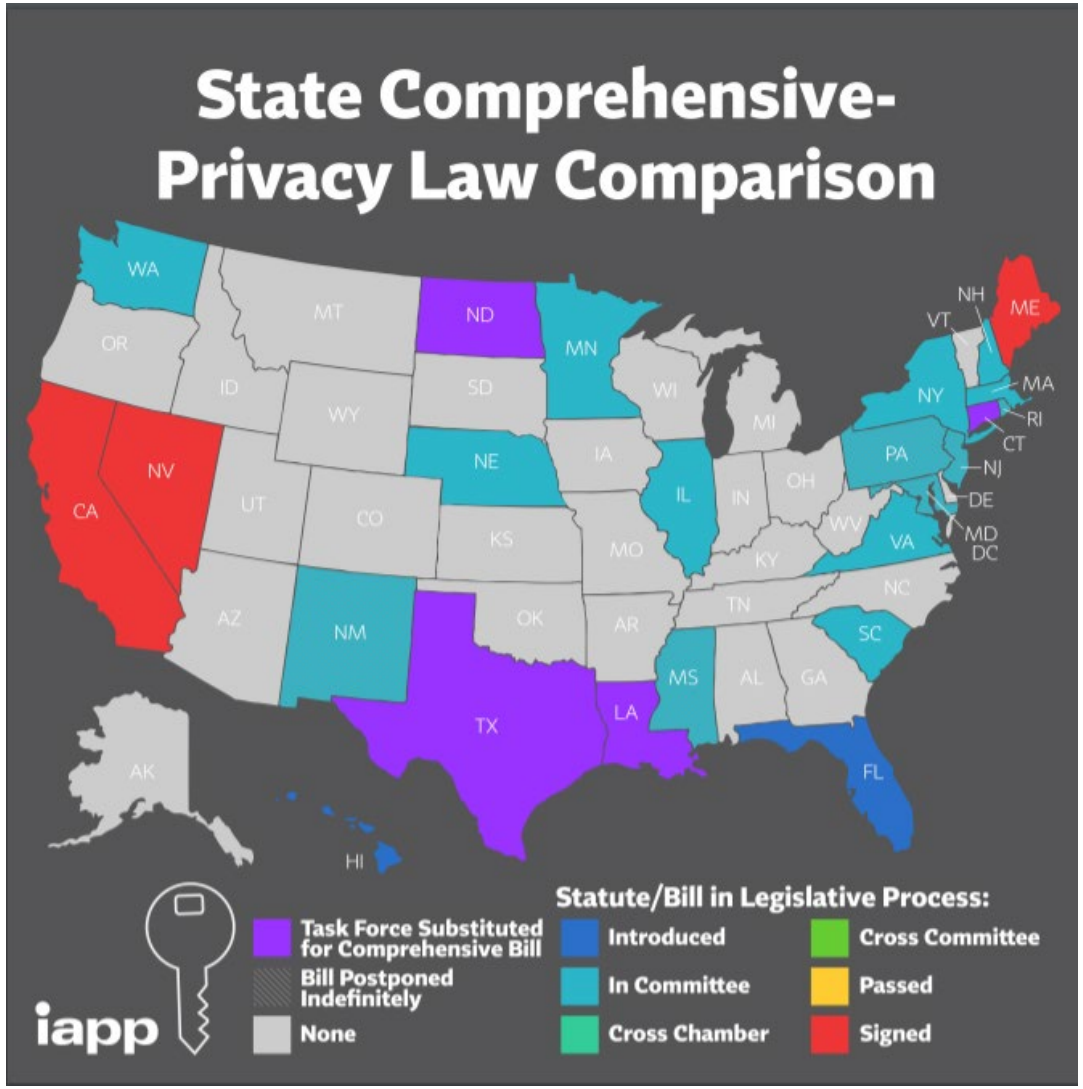
Compliance, Privacy, Security - ComPriSec




@SLANECARTOONS
SHARE PRICE
PROFITS
REPUTATION
INTEGRITY
LOYALTY
TRUST
BRAND
PRIVACY
DO WE REALLY NEED THIS?
SLANE

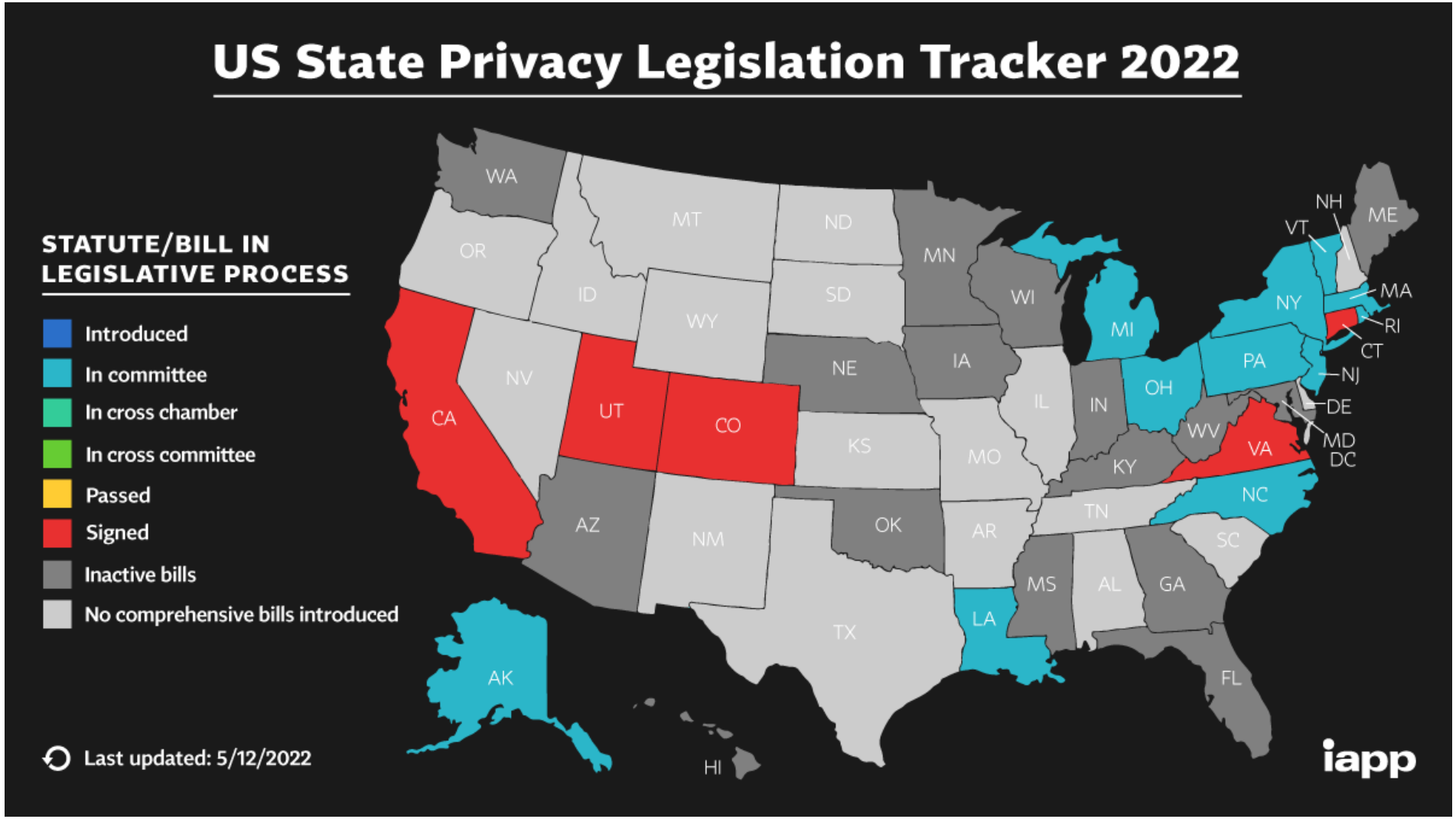
Privacy Standards

- OECD Privacy Principles 1980
- X9.99 PIA Standard 2004/2009/2020
- ISO 22307 PIA Standard 2008
- ISO 27701 Privacy Updates 2019
- NIST Privacy Standard January 2020



https://iapp.org/resources/article/state-comparison-table/#

Privacy Law Explosion



https://iapp.org/resources/article/state-comparison-table/#

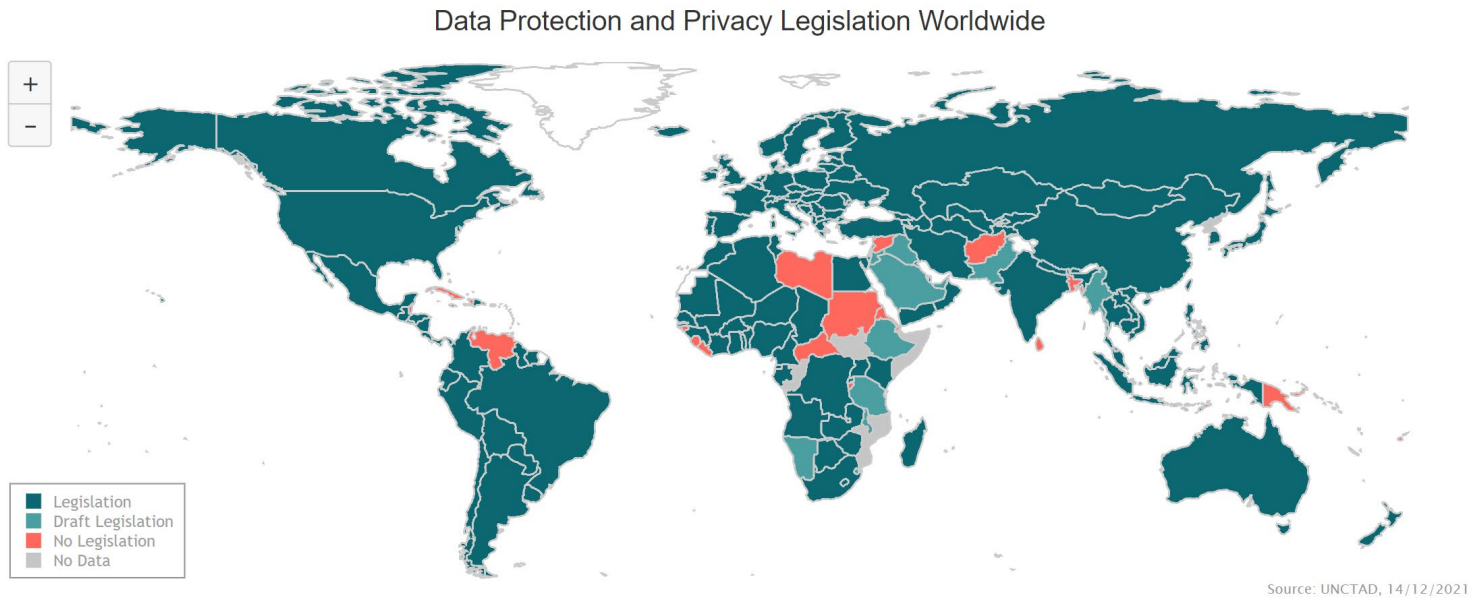
Global Privacy Laws

71%	9%	15%	5%
COUNTRIES WITH **LEGISLATION**	COUNTRIES WITH **DRAFT LEGISLATION**	COUNTRIES WITH **NO LEGISLATION**	COUNTRIES WITH **NO DATA**

SELECT A COUNTRY

SELECT A REGION

DOWNLOAD FULL DATA



https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Privacy Assessment Requirements

#	Regulation	Date
27	GDPR – Applies to all European Union Member States	April 2016
1	Japan – Protection of Personal Information Act	May 2017
1	Australia – Privacy Act	February 2018
1	Israel – Protection of Privacy Law (PPA) Amendment	February 2018
1	Nigeria – Data Protection Regulation (NDPR)	January 2019
1	Thailand – Personal Data Protection Act (PDPA)	February 2019
1	India – Personal Data Protection Bill (PDPB)	December 2019
1	Egypt – Law No. 151 to Protect Personal Data	February 2020
1	Chile – Constitutional Amendment for Data Privacy as a Human Right	March 2020
1	South Africa – Protection of Personal Information Act (POPIA)	July 2020
1	Brazil – Brazilian General Data Protection Act (LGPD)	September 2020
1	Switzerland – Data Protection Act (DSG)	September 2020
1	China – Personal Data Protection Laws (PDPL)	October 2020
1	Canada – Digital Charter Implementation Act (Amends PIPEDA)	November 2020
1	New Zealand – Privacy Act Amendments	December 2020

https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws

Evolution of Data Breaches

2022 and Beyond
- Additional US Privacy Laws (UT/VT)
- Transition CCPA → CPRA

2016-2021
- NIST PF
- CCPA
- ISO 27701
- EU: GDPR

2010s
- Maine
- Nevada: SB 220
- Bahrain
- India: IT Rules, PDPB
- Singapore, Thailand
- Brazil

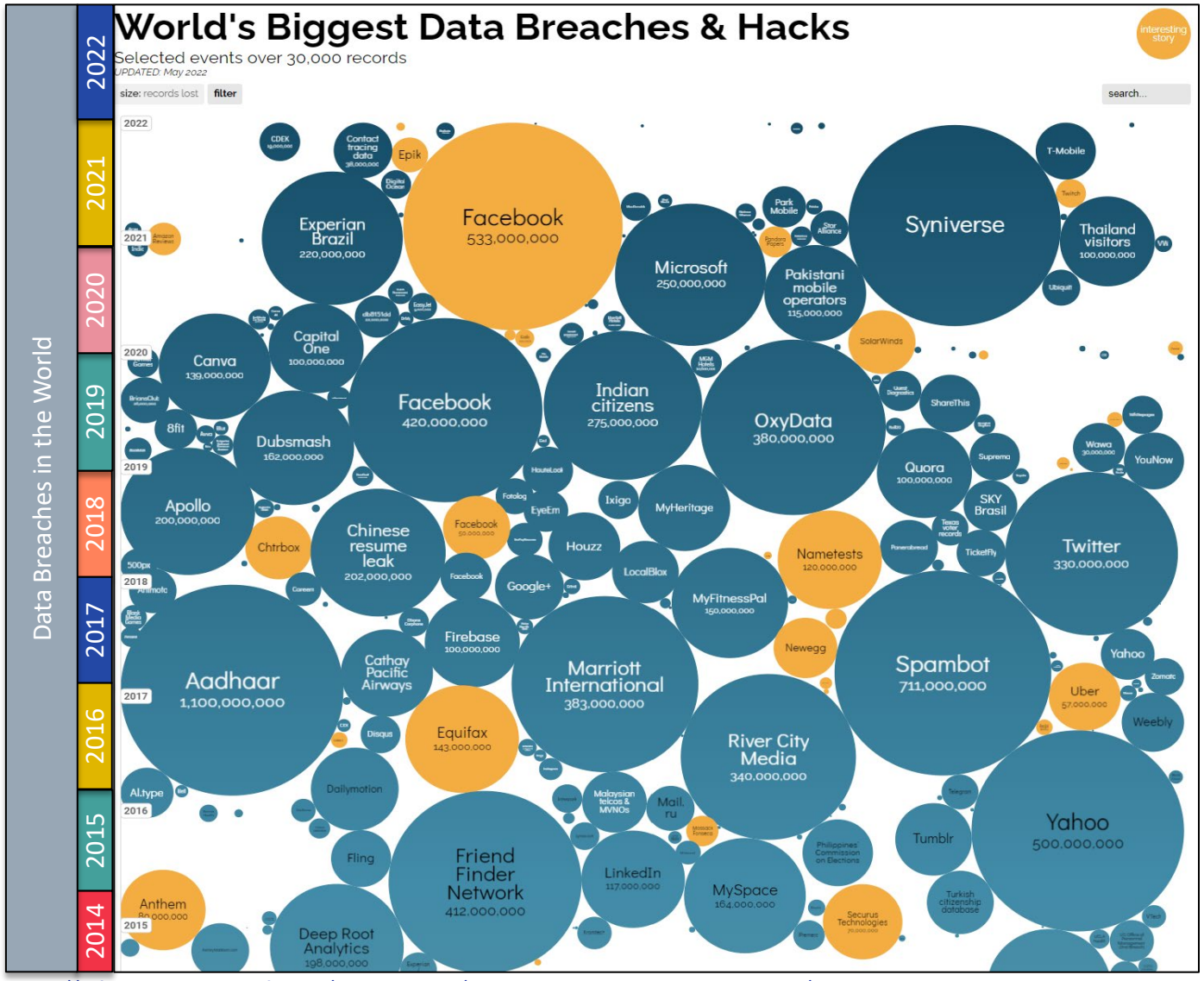
2000s
- Alberta: Personal Information Protection
- British Columbia: PIPA
- California Civil Code

1990s
- Directive 95/46/EC
- HIPAA
- GLBA

1980s
- OECD Privacy Guidelines
- Convention 108

1970s
- Privacy Act 1974
- FCRA

Velocity of Data Privacy Regulations and Industry Standards



https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Privacy Dumpster Fire

Assessments ≠ Data Processing

EU Information Commissioner's Office

ico.
Information Commissioner's Office

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

DPIA template
20180209
v0.3

1

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

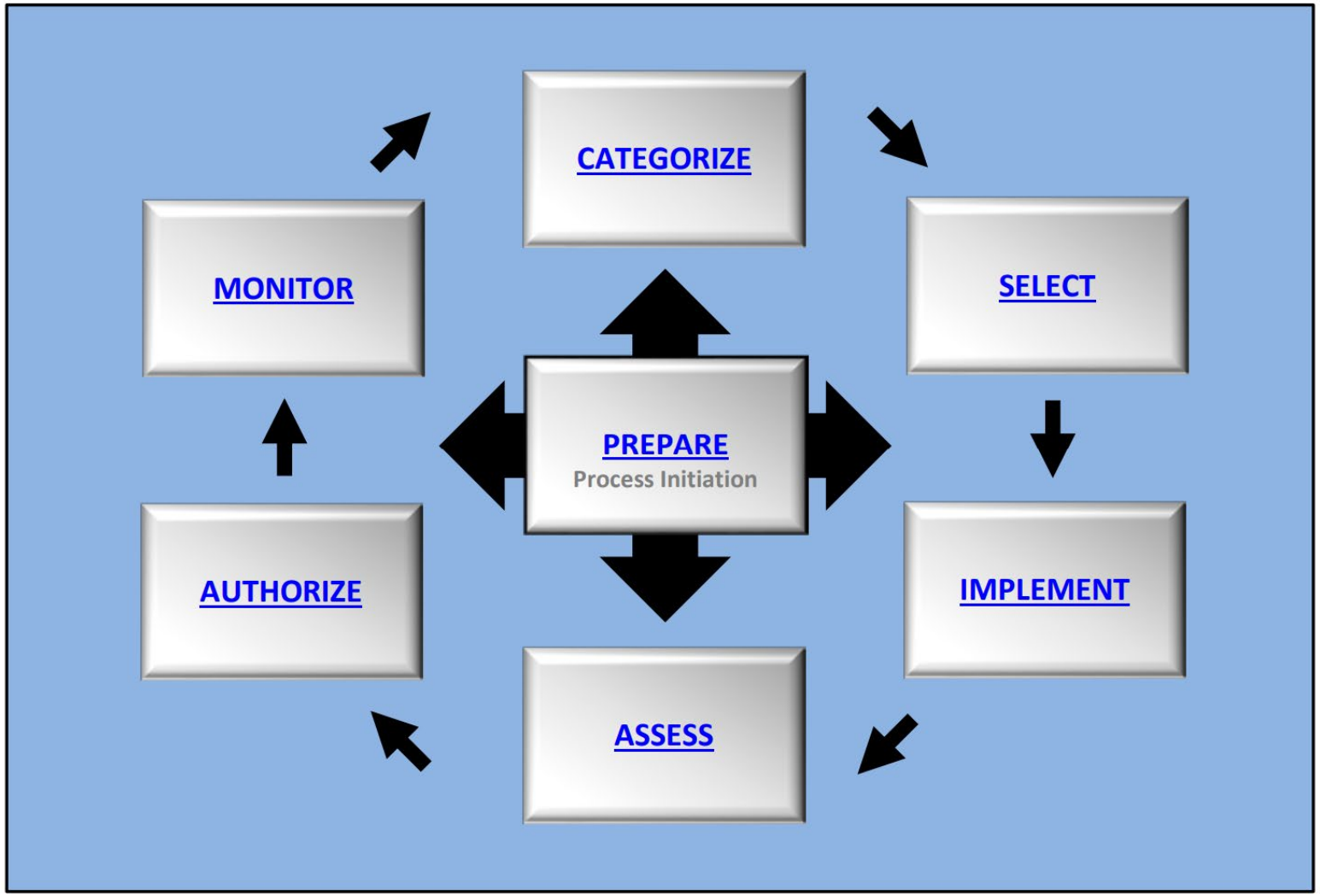
https://gdpr.eu/wp-content/uploads/2019/03/dpia-template-v1.pdf

NIST Privacy Framework

Category	Subcategory
Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
	ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.
	ID.RA-P3: Potential problematic data actions and associated problems are identified.
	ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
	ID.RA-P5: Risk responses are identified, prioritized, and implemented.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

NIST Risk Management Framework (RMF)



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Department of Homeland Security

Privacy Compliance Process

https://www.dhs.gov/compliance

Fines and Penalties

complianceweek.com/data-privacy/handm-germany-fined-413m-in-one-of-largest-gdpr-penalties/29556.article

TOPICS | WEBCASTS & TRAINING | EVENTS | RESOURCE LIBRARY | SPECIAL REPORTS

DATA PRIVACY

H&M Germany fined $41.3M in one of largest GDPR penalties

By Jaclyn Jaeger | Thu, Oct 1, 2020 11:56 AM

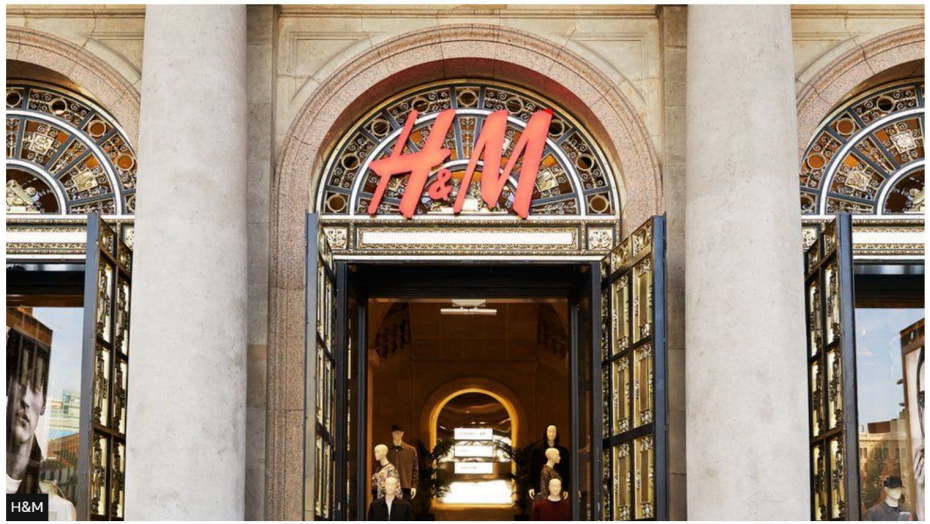
The Data Protection Authority of Hamburg (HmbBfDI) announced Thursday it fined H&M Germany €35.2 million (U.S. $41.3 million) for violations of the EU's General Data Protection Regulation (GDPR) for the excessive monitoring of several hundred employees by one of the clothing retailer's German subsidiaries.

https://www.enforcementtracker.com/
https://ccpa-info.com/litigation-tracker/

bbc.com/news/technology-54418936

H&M fined for breaking GDPR over employee surveillance

5 October 2020



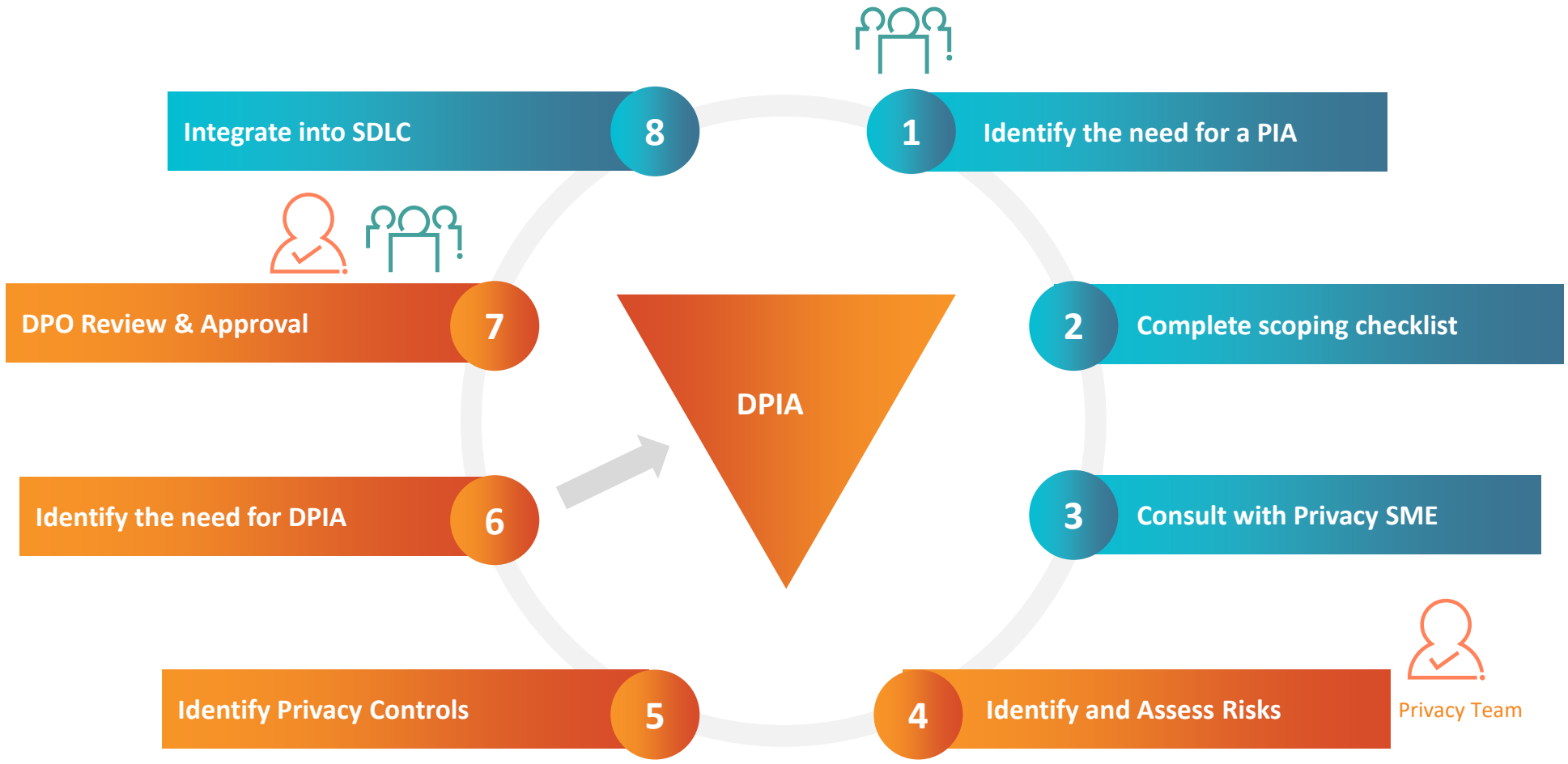
H&M has been fined €35.3m (£32.1m) for the illegal surveillance of several hundred employees.

The company kept "excessive" records on the families, religions and illnesses of its workforce at its Nuremberg service centre, the German data protection watchdog found.

New Unified Privacy Assessment Methodology

Privacy Assessment Methodology – Inventory

Privacy Assessment Methodology – Need



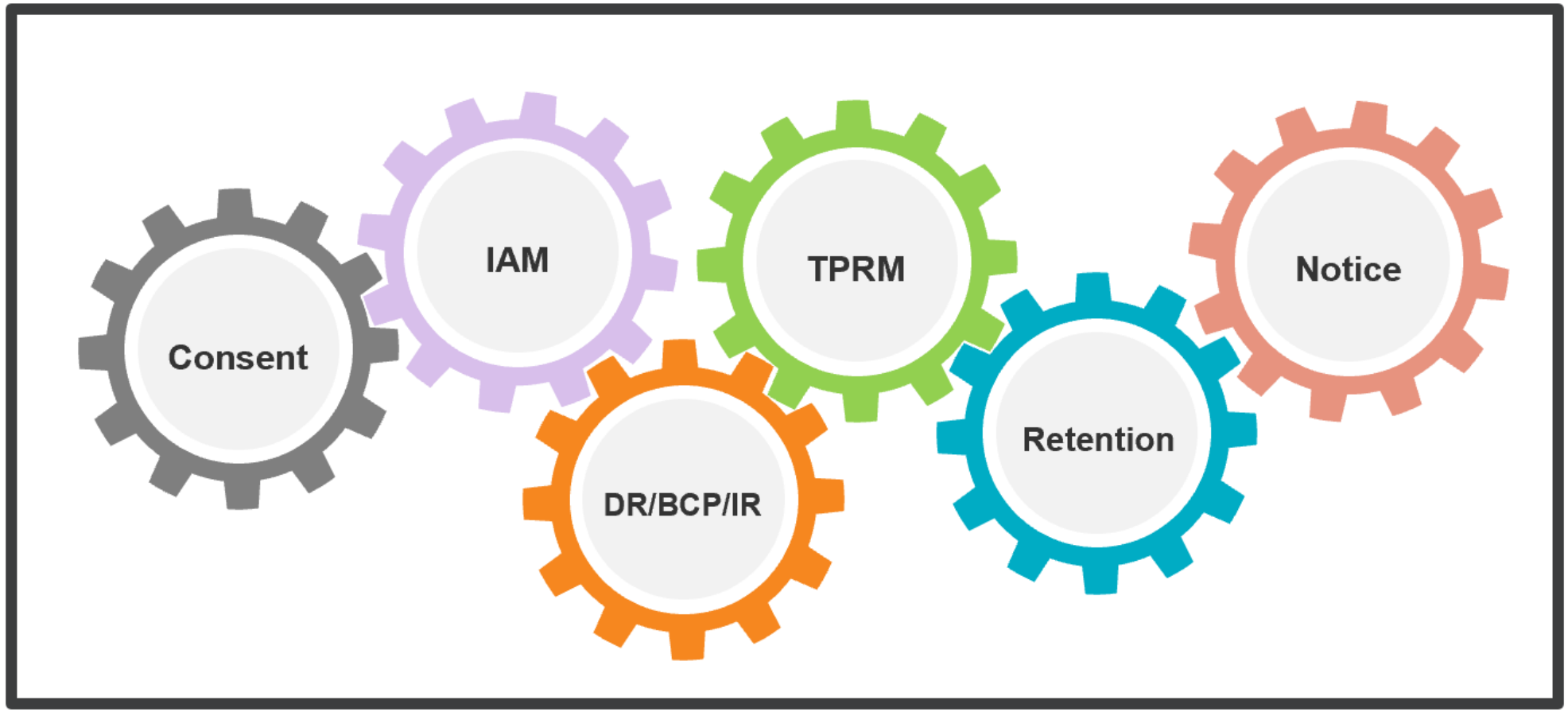
Activities completed by Project Teams (this could be as part of the SDLC, or Change Management Process)

Privacy Assessment Methodology – Assess

- Overcollection of Data
- Inappropriate Data Usage
- High Risk Data Processing
- AI/ML Bias in Decisioning
- Ineffective Security/Privacy Controls
- Lack of Policies & Procedures
- No DPO/CPO
- Missing Regulations

Privacy Assessment Methodology – Develop

SDLC – Adopting Privacy by Design



Privacy Assessment Methodology – Develop

HOW TO GET STARTED IN PRIVACY ENGINEERING

1 Pursue a cross-disciplinary education.

- If you are still in college or exploring higher-ed options, seek a degree in privacy engineering, computer science, software/computer engineering, networking, information systems, data science or analytics, cybersecurity, or other technical field, and take courses that focus on privacy.
- Look for opportunities to take data protection-related courses across schools or pursue continuing education online, in areas such as cybersecurity, user testing, risk management, law, and UX or UI design.
- Practice privacy skills through an internship or externship with a local company, government privacy office, think tank or civil rights advocacy organization. Learn how to work with technical, legal and business professionals.

2 Search for career opportunities beyond Big Tech.

- Don't limit yourself as to where you might work or what your title might be. Nearly all companies and industries today require technology and data skills. Consider positions where privacy engineering is a component of the role that could grow, whether in more traditional companies that are expanding their digital presence, newer startups or as part of larger teams within more recognizable tech companies.
- Consider post-graduate fellowships in organizations with a privacy focus, such as the IAPP, Future of Privacy Forum and academic research centers, such as Berkman Klein Center for Internet & Society at Harvard University.
- Explore privacy careers listed on the IAPP's Career Central page.

4 Network, network, network: Engage with privacy professionals.

- Become a member of the IAPP and join the Privacy Engineering Section.
- Attend virtual and, when possible, in-person privacy conferences, IAPP privacy engineering forums, PEPR, PETS, SOUPS and others, KnowledgeNet Chapter meetings, and after hours events. Some conferences provide scholarships for students. Or pitch a session for a speaker pass.
- Reach out to privacy professionals in your community, and arrange to meet for coffee.
- Seek out opensource initiatives that focus on solving data and privacy problems to learn tech practices.
- Subscribe to a privacy email list, such as the IAPP Privacy List.

5 Become an expert in your own privacy.

- Learn to follow your data. Understand where it goes and who controls it.
- Manage your own privacy with mobile device settings, encryption, location tracking, etcetera.

6 Earn privacy credentials.

- Become a Certified Information Privacy Technologist.
- Earn privacy-related continuing education credits through conferences, trainings, etcetera.

https://iapp.org/resources/article/infographic-how-to-get-started-in-privacy-engineering
https://iapp.org/connect/join-privacy-engineering-section-advisory-board//

3 Write about privacy issues.

- Pick a niche that interests you, get smart about it, and start writing — blogs, papers, op-eds and even tweetstorms will all help you stand out in the field.
- Self-publish. Platforms like LinkedIn and Medium make it easy.
- Submit your work for consideration to the IAPP's publications, which are increasing coverage of more-technical privacy developments.

7 Stay informed about privacy issues.

- Subscribe to mailing lists: IAPP Daily Dashboard, Morning Consult Tech, New York Times Bits, ReCode, TechCrunch, opensource.com.
- Follow interesting people and those they follow on Twitter, LinkedIn and other social media.

8 Find a niche.

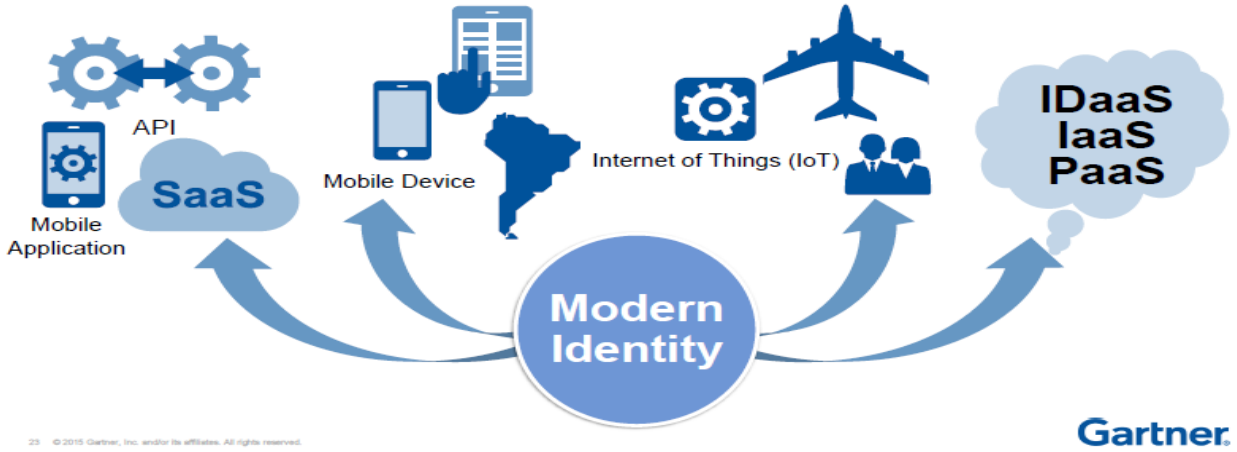
- Dive deeper into a particular technology, standard, privacy framework or privacy-enhancing technique. Make it your specialty. You have to start somewhere, and having a home base makes it easier to wrap your head around the intersection of privacy, data and tech. A particular interest also demonstrates to employers that you are dedicated to the field.

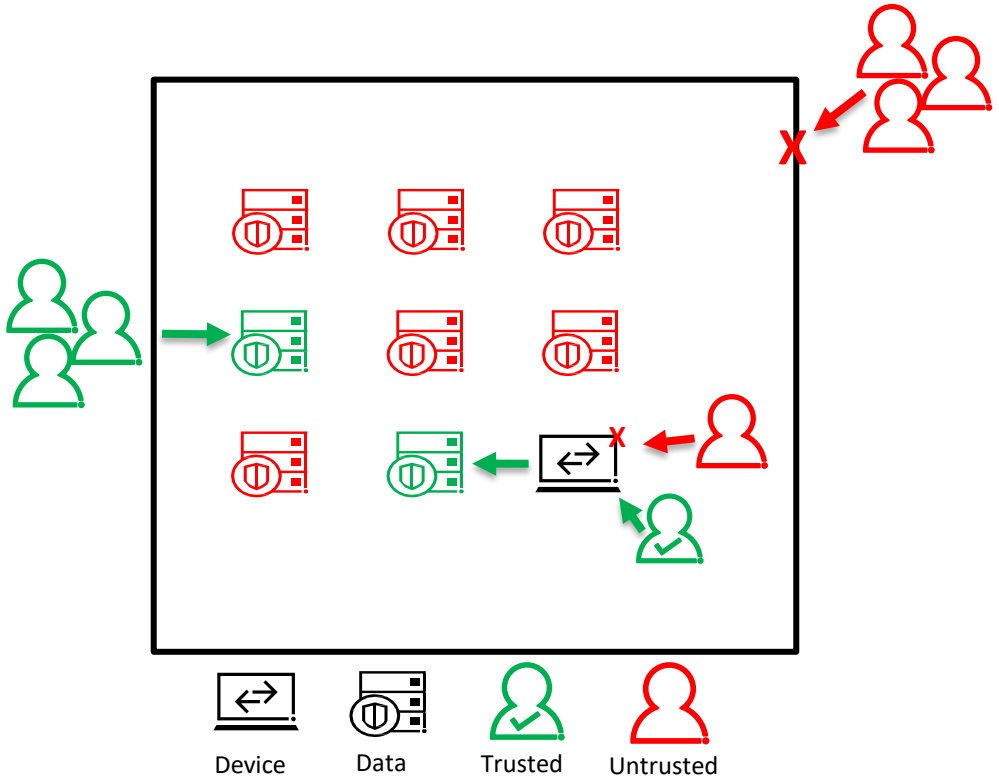
iapp

https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

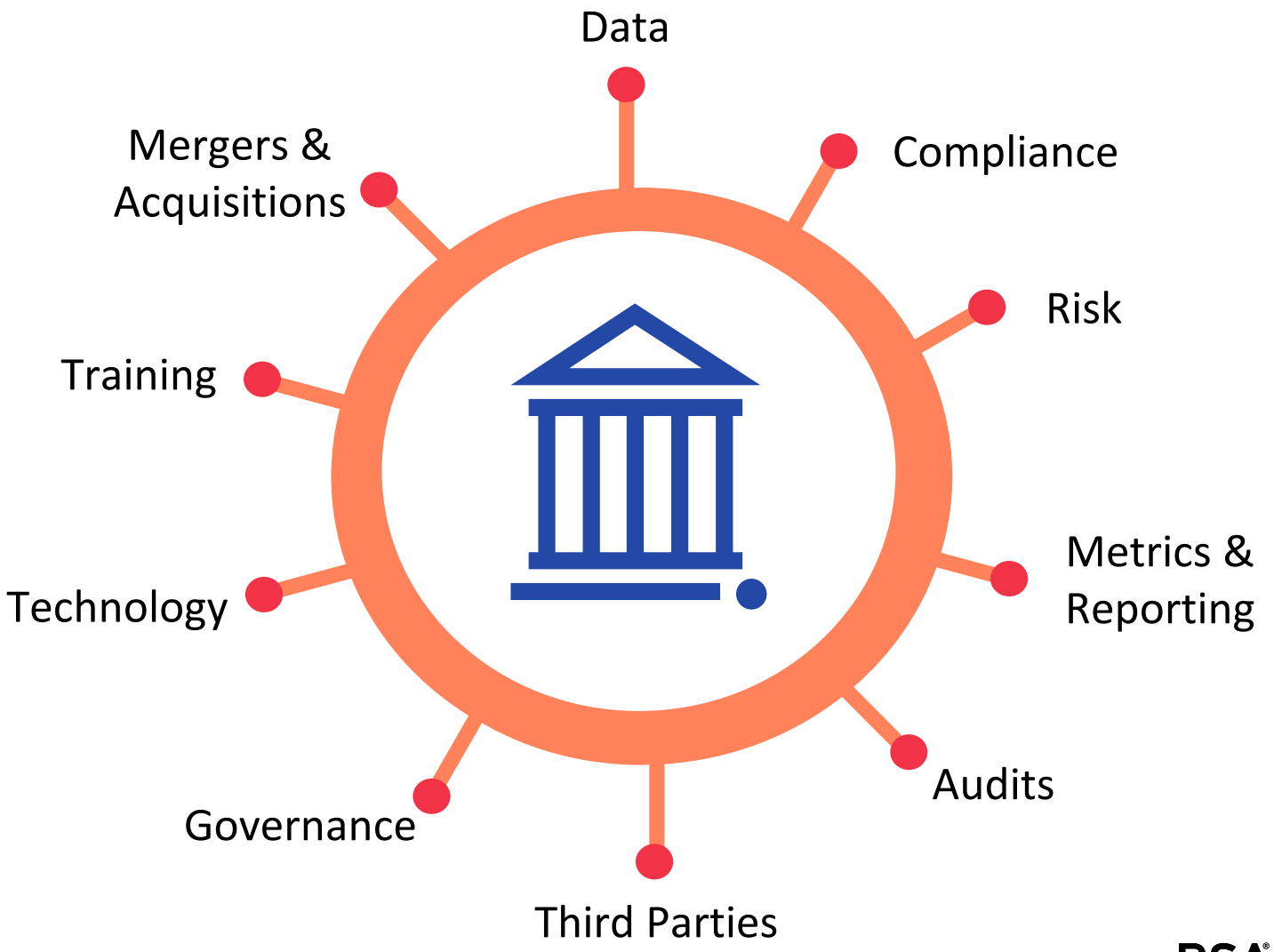
Privacy Assessment Methodology – Develop

Zero Trust Privacy





Privacy Assessment Methodology - Monitor



Privacy Tools & Resources

GRC SOLUTIONS

PRIVACY SOLUTIONS

SUBSCRIPTIONS

MEMBERSHIPS

INDUSTRY GROUPS

TRAINING

Applying the New Privacy Assessment Methodology

- 1 Week
  - Identify privacy function and current assessment methodology
- 3 Months
  - Compare new methodology to current methodology
  - Identify efficiencies gained with new methodology
- 6 Months
  - Communicate and implement new methodology
- 12 Months
  - Conduct initial assessment using new methodology
  - Identify solutions to gaps identified
  - Monitor for changes

Just Start Somewhere!

Let’s Connect!

Reach out to the speaker

Dr. Lisa McKee
Director of Governance, Risk, Compliance and Privacy
Hudl
Lisa.McKee@Hudl.com
Connect on LinkedIn

RSAConference2022

Thank You!