How To Build Bridges Between Privacy and Security in a Digital Trust World

GRC – BeConnected - March 28, 2024

Ulrika Dellrud

Chief Privacy and Data Ethics Officer, Smarter Contracts

Privacy and Security, while different, are **dependent on one another** and cannot live without each other. The presentation will show why it is key that both functions **work together and collaborate**, why and how they can **learn from one another**, what the **key overlapping areas** are and what that means from a practical point of view. I will highlight the benefits of a joint and cooperative approach to both topics as cooperation in both fields returns beneficial outcomes for both when aligned, especially in a **digital trust world.**

Digital trust is a broad topic that goes beyond compliance. It involves **treating siloed areas of an organization as part of a cohesive whole.**

Digital trust brings together many of the disciplines already critical to an organization, including compliance, **security, privacy**, communications, information technology, marketing and operations. Alignment should exist between these areas because all have a significant, direct impact on how others perceive the organization—especially its brand and reputation—and are integral to adding value to the organization itself and its future digital transformation initiatives.

This is where digital trust guidance will have a significant impact. Only 20 percent currently use a framework for their digital trust practices, even though 56 percent believe that it is extremely/ very important for an organization to have this framework. Among those that do use a framework, COBIT® (27 percent) is the most popular, followed by the SAFE Identity Trust Framework (10 percent).

ISACA **is developing a new digital trust ecosystem framework to help organizations ensure that their digital trust initiatives are in line with their unique mission, vision, values, goals and objectives.**

*from ISACA State of Digital Trust report 2023*

2024 – YEAR OF COMPLIANCE

- **DATA ACT (Jan 2024 + 20 mos)** regulation on harmonised rules on fair access to and use of data,

- **DIGITAL MARKETS ACT (March 6, 2024)** aims to address the dominance of big tech platforms, foster innovation and competition, and further protect user privacy

- **DIGITAL SERVICES ACT (February 17, 2024)** regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.

- **DATA GOVERNANCE ACT (applies September 2023)** cross-sectoral instrument that aims to regulate the re-use of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes

- **ARTIFICIAL INTELLIGENCE ACT (May 2024 + 24 mos)** classify and regulate AI applications based on their risk to cause harm ntroduces specific transparency obligations to ensure that humans are informed when necessary, fostering trust.

I N T E R A C T I O N

- **NIST2 DIRECTIVE (applies Jan 2025):** level up their cybersecurity governance, risk management measures and prepare for the new reporting obligations.

- **DORA (applies Jan 2025)** Digital Operational Resilience Act, comprehensive ICT risk management framework for the financial sector

- **EUROPEAN CYBER RESILIENCE ACT (early 2024 + 2 yrs)**

- **EUROPEAN CYBER SECURITY ACT** – certification of cybersecurity products

- **PSD3/Payment Services Regulation (2026)** the rules set out to ensure PSPs complete comprehensive due diligence to mitigate the risk of financial fraud

- **Open Finance Framework (FIDA)**

COMMON DENOMINATOR: RISK AND COMPLIANCE GOVERNANCE WITH **PRIVACY AND SECURITY AS THE CORNERSTONES**
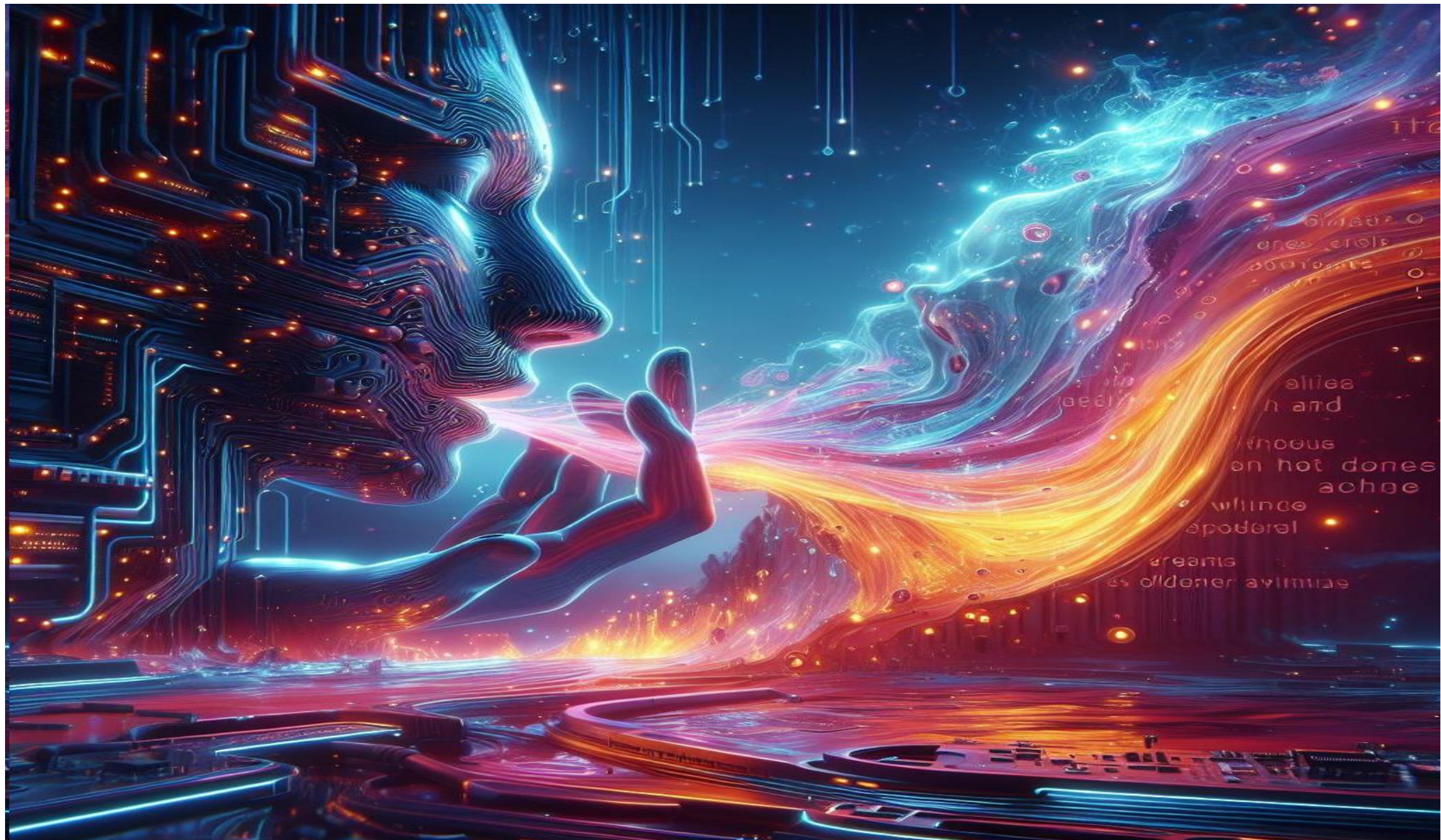
Privacy Matters.

How it all started

1890 - Two United States lawyers, Samuel D. Warren and Louis Brandeis, write The Right to Privacy, an article that argues the "right to be left alone", using the phrase as a definition of privacy.

1948 - The Universal Declaration of Human Rights is adopted, including the 12th fundamental right, i.e. the Right to Privacy.

1950 - The EU Convention on Human Rights sequence of fundamental rights is amended, with articles now appearing in a different order.

1980 - OECD issues guidelines on data protection, reflecting the increasing use of computers to process business transactions.

1981 - The Council of Europe adopts the Data Protection Convention (Treaty 108), rendering the right to privacy a legal imperative.

1983 - The Federal Constitutional Court of Germany reaches a fundamental decision regarding the census judgment. The verdict is considered a milestone of data protection.

1993 - PC Brown is charged with the UK Data Protection Act 1984 offence of using personal data or a purpose other than that described in the Data Protection Register - ruling is overturned.

1995 - The European Data Protection Directive is created, reflecting technological advances and introducing new terms including processing, sensitive personal data and consent, among others.

2014 - A ruling by the Court of Justice of the EU finds that European law gives people the right to ask search engines like Google to remove results for queries that include their name. The concept becomes known as "the right to be forgotten".

2016 - The General Data Protection Regulation (GDPR) is approved by the EU parliament after 4 years of discussions.

2018 - GDPR is being enforced, replacing the Data Protection Act.

2018+ - Responsible management of personal data through mature IT governance, transparent processes and modern applications.
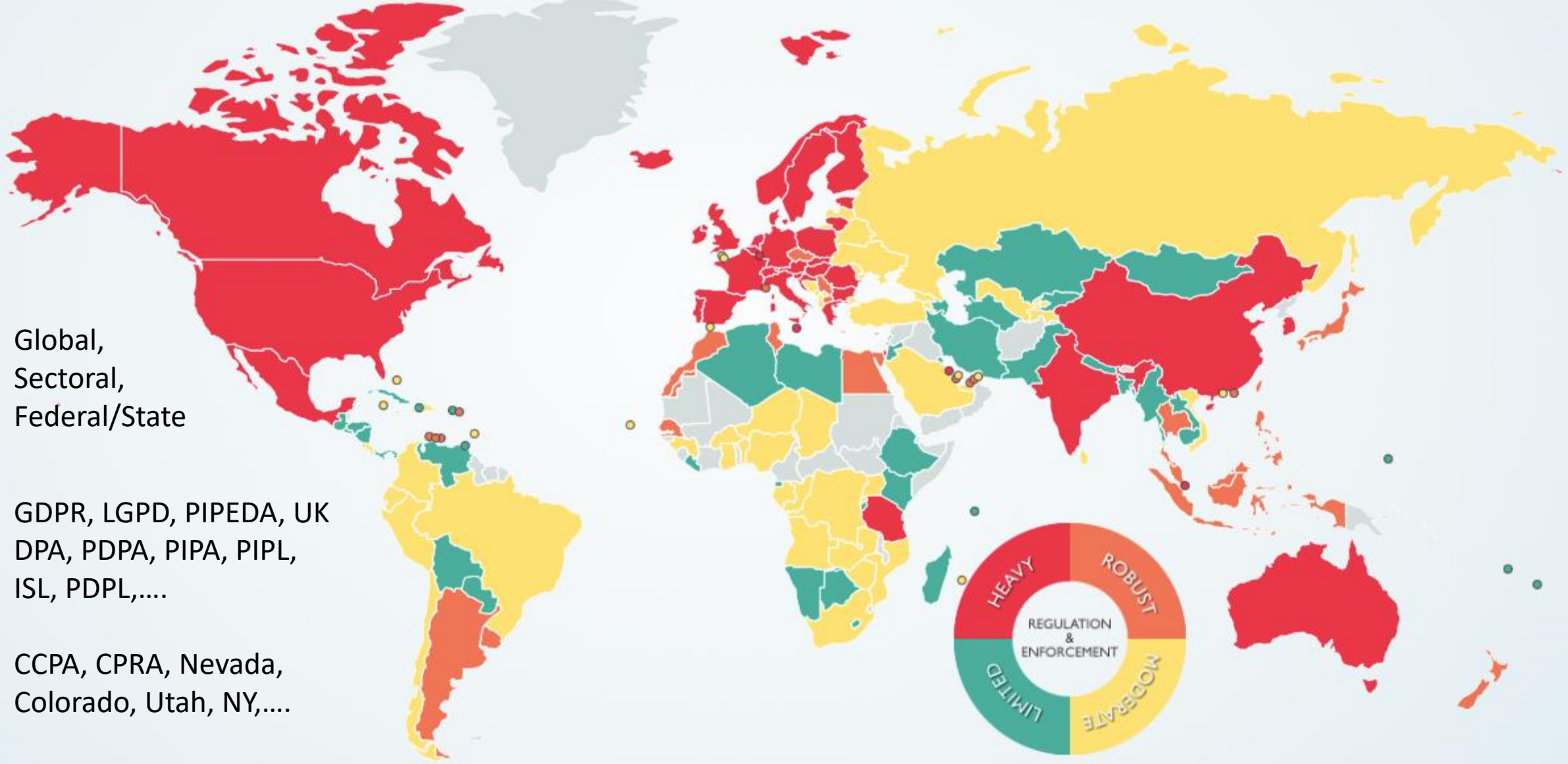
OECD Privacy Principles
(Fair Information Practices)
1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

Revised July, 2013

THE UNIVERSAL DECLARATION OF HUMAN RIGHTS

Convention 108 on data protection

GDPR

Data Protection Laws Around The World 2024
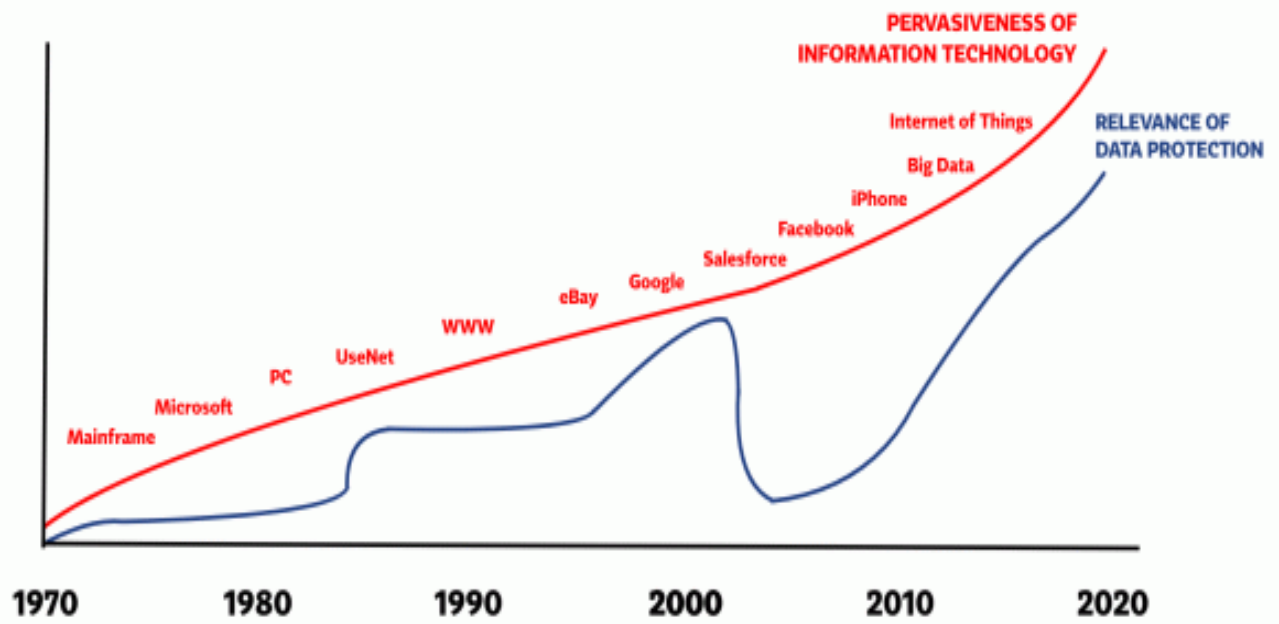

Global,
Sectoral,
Federal/State

GDPR, LGPD, PIPEDA, UK
DPA, PDPA, PIPA, PIPL,
ISL, PDPL,….

CCPA, CPRA, Nevada,
Colorado, Utah, NY,….

HIPAA, GLBA, COPPA,
FCRA, E-Privacy,…..

REGULATION & ENFORCEMENT
HEAVY
ROBUST
LIMITED
MODERATE

Key terms and acronyms

KEY TERMS	KEY ACRONYMS	KEY TERMS
• Controller	• GDPR	• Penetration tests
• Processor	• DSR	• Vulnerability tests
• Data Subjects	• RTBF	• Ransomware attacks
• Third Parties and DPAs	• ROPA, DPIA	• Firewalls
• Accountability – Responsibility	• LIA	• Operating systems
• Privacy By Design and Default	• TIA	• Malware
• Transfers – US, Cloud	• SAFEHARBOR/PRIVACY SHIELD/DATA PROTECTION FRAMEWORK	• Anti-virus
• Personal Data Breach	• SCCs	• Network security
• Legitimate Interest	• BCRS	• DDos Attack
• Consent	• DPA	• Hacking
• Case law judgements - ECJ	• DPO	• Security incident
		• Patching
		• Confidentiality
		• Integrity
		• Availability

Personal Information or Personal Data

Personal data refers to any information **that relates to an identifiable individual, either directly or indirectly.** It can include a wide range of information, such as names, addresses, email addresses, phone numbers, identification numbers (e.g., social security numbers), biometric data (e.g., fingerprints, facial recognition data), IP addresses, online identifiers (e.g., usernames, cookies), insights derived from analysis

Personal data can also encompass more **sensitive** information, such as racial or ethnic origin, political opinions, religious beliefs, health information, sexual orientation, and genetic data.

The key characteristic of personal data is that it can **be used to identify or distinguish an individual, either on its own or when combined with other information.**

Personal data is subject to privacy and data protection laws and regulations in many jurisdictions, which impose **obligations on organizations** that collect, process, or handle personal data to protect **individuals' privacy rights** and ensure the **lawful and fair treatment** of their personal information.
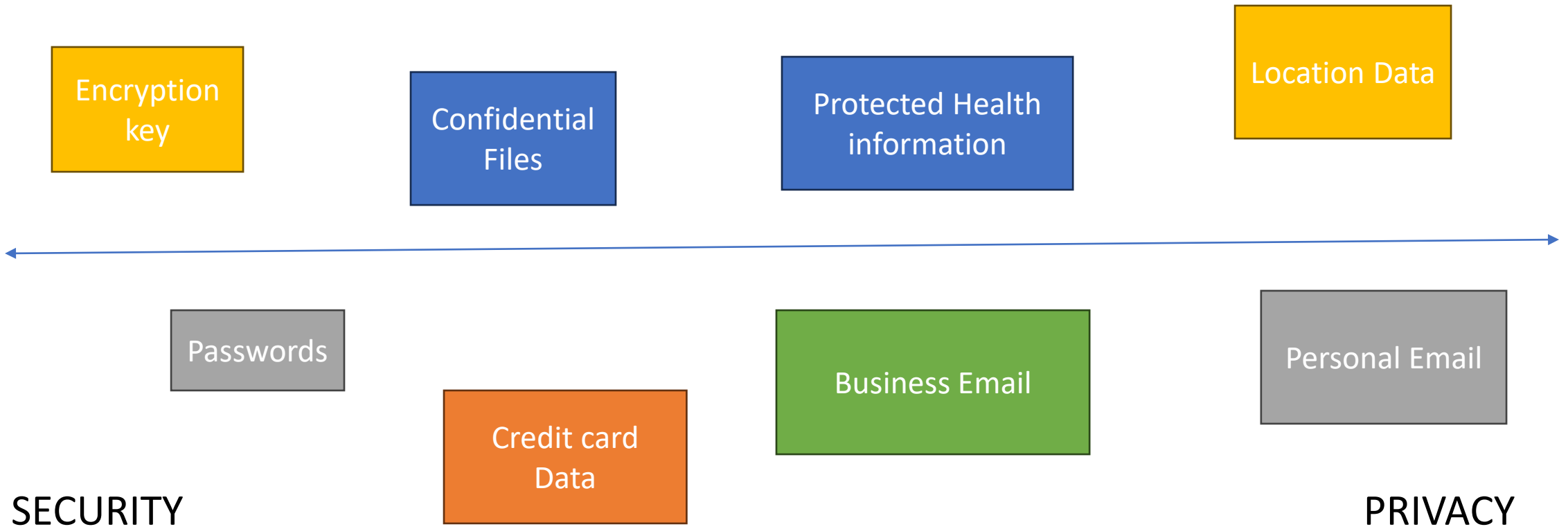
Any form: hard copy media, audio, visual,

What is the difference between a breach and a data breach?

- A security breach involves access to systems or devices, while a data breach is specifically about data. The two will commonly (but not always) occur in the same incident. You should address both in your overall security policy.

- Security breach vs Security vulnerability

TYPES OF DATA

Encryption key

Confidential Files

Protected Health information

Location Data

Passwords

Credit card Data

Business Email

Personal Email

SECURITY

PRIVACY

PRIVACY PRINCIPLES

- We are transparent about our data processing practices
- We are committed to empowering individuals to make choices about their personal information
- We only collect as much personal information as we need (purpose).
- We are fair and ethical in the processing of your personal information
- We ensure that personal information is accurate and up to date
- We protect personal information when it is shared with ==third parties==
- We ensure ==appropriate security== of personal information
- We embrace ==privacy by design and by default into the data lifecycle==
- We ensure ==confidentiality==
- We ==retain== personal information only for as long as we need it (and deleted when no longer needed)

Orgs to state why they are collecting information

Orgs to state the choices and controls an individual has over his/her data

Identify and keep track of privacy laws and regulations

Demonstrate compliance with all local and international laws

PRIVACY vs SECURITY

PRIVACY = PREVENTNG OTHERS FROM LOOKING IN

PRIVACY ENSURES THAT PERSONAL DATA/INFORMATION ARE

COLLECTED

PROCESSED

PROTECTED

DESTROYED

LEGALLY AND FAIRLY (CONTEXTUAL)

SECURITY = PREVENTING OTHERS FROM BREAKING IN

SECURITY PROVIDES PROTECTION FOR ALL TYPES OF INFORMATION SO THAT THE INFORMATION'S

CONFIDENTIALITY

AVAILABILITY

INTEGRITY

ARE MAINTAINED

PRIVACY IS THE HUMAN ASPECT OF CYBERSECURITY

View from PRIVACY perspective

- Concerned with **operational compliance** to legislation (GDPR, CCPA, LGPD, PDPA, UK GDPR)
- **Governs the relationship between the owner of the data and the organization collecting the personal data**
- Addresses what **types of personal data** is being collected, in what way and how it can be used (Marketing, HR, sensitive data, etc.)
- **Incorporates Ethics** (legal vs ethical, moral issues, societal issues, bias/discrimination)
- **Places emphasis on whom it can be shared with** (person and country (Schrems)) and **who can access it**
- **Emphasizes the need to embed privacy at the outset**
- Breach response times (48 hours)
- Provides individuals with the means to delete and/or limit what the organization can do with their data (**Data subject rights)**

View from SECURITY perspective

- Concerned with **technical compliance** (NIST, ISO (also privacy part), CSA) and **whether something is implementable**
- **Governs how confidential data is stored, accessed, and used** (access control, change controls, logging, encryption, monitoring controls, etc.)
- **Privileged Access Users, Third Parties**
- Concerns with **how data flows through the information system**, and **how security is embedded** through the SDLC
- **Protects data from breaches, leakage and threat actors**
- Security Obligations (Network security, etc.)

THERE IS NO PRIVACY WITHOUT SECURITY
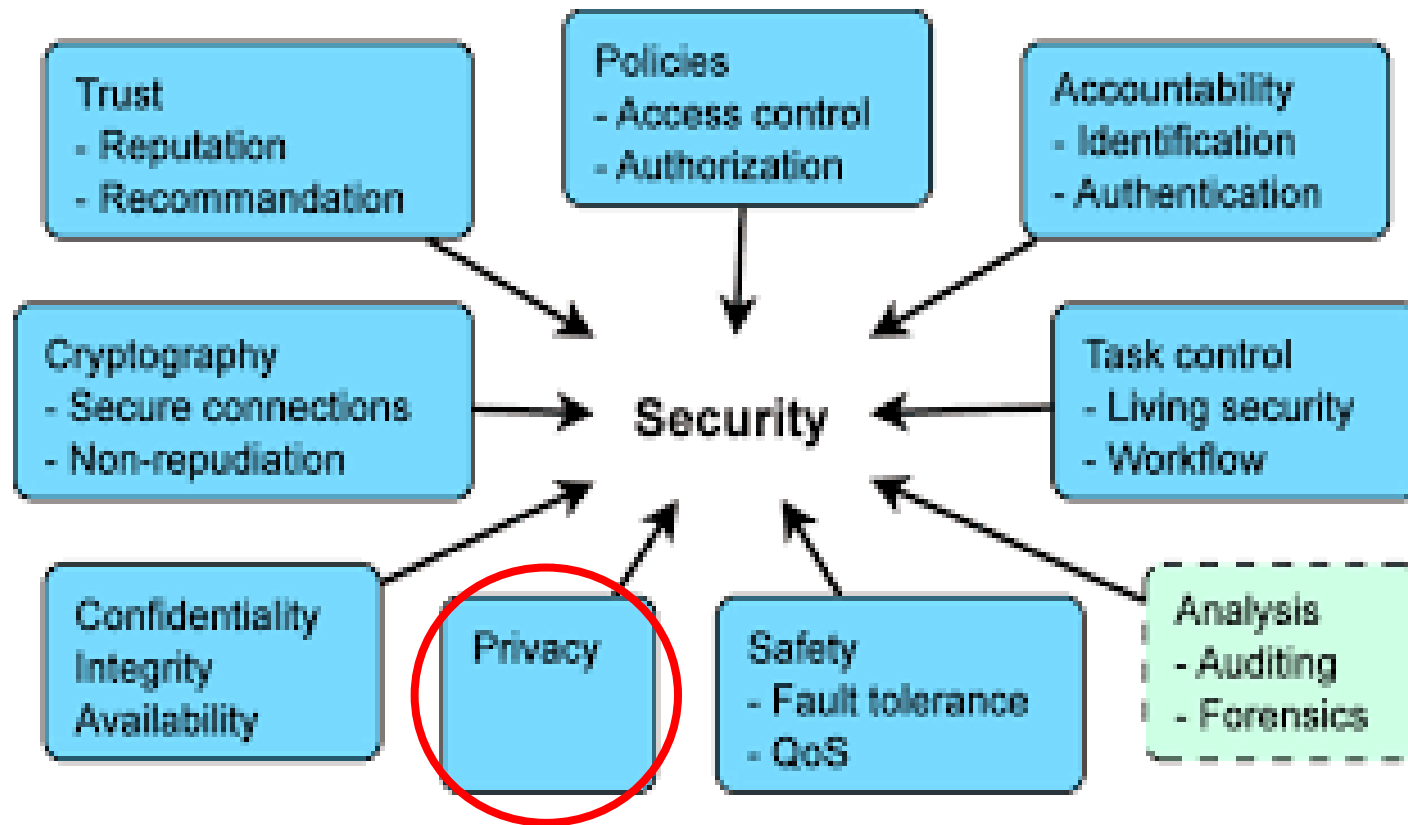
MOST COMMON AREAS FOR COLLABORATION

- Define common policies and procedures for classifying, storing and accessing data (access controls, passwords, etc.)

- Collaborate on data discovery

- Data inventories and records of processing

- Data Protection and Privacy impact assessments (DPIAs/PIAs)

- Establish and enforce encryption requirements for data types according to policies

- Create controls to protect, using, sharing, retaining the personal data

- Ensure individuals can access their data
    - need to access systems in order to respond promptly and within timeline
    - not just front end – also very much the backend – very operational, IT will need to know where data is

- Align vendor management and product approval assessments and collaborate on assessment/due diligence (eg NIST2 says you need to monitor your 1/3 parties, GDPR the same)

- Vendor exit strategies

- Privacy **and security** by design

- Align breach handling/incident management - Data/Security incidents vs personal data /privacy breaches

- Third party contracts and agreements

- Common training/awareness

- DORA, NIS2 – GDPR applies, but DORA (fin services and ICT third parties) and NIS 2 (essential services) complement and sometimes have additional requirements (security, documentation, risk assessments, breach reporting…)

Privacy Programs

- Privacy Frameworks (NIST and OASIS)

- Privacy Standards (ISO 27001/27701/31700, IEEE)

- Privacy Risk Frameworks and Registers (risk to individual, PIAs, DPIAs, TIAs, etc.)

- Privacy (Data) Governance

- Privacy Controls

- Privacy Audits

- Privacy Maturity

→ Demonstration of Documentation and Accountability (collaboration is essential)
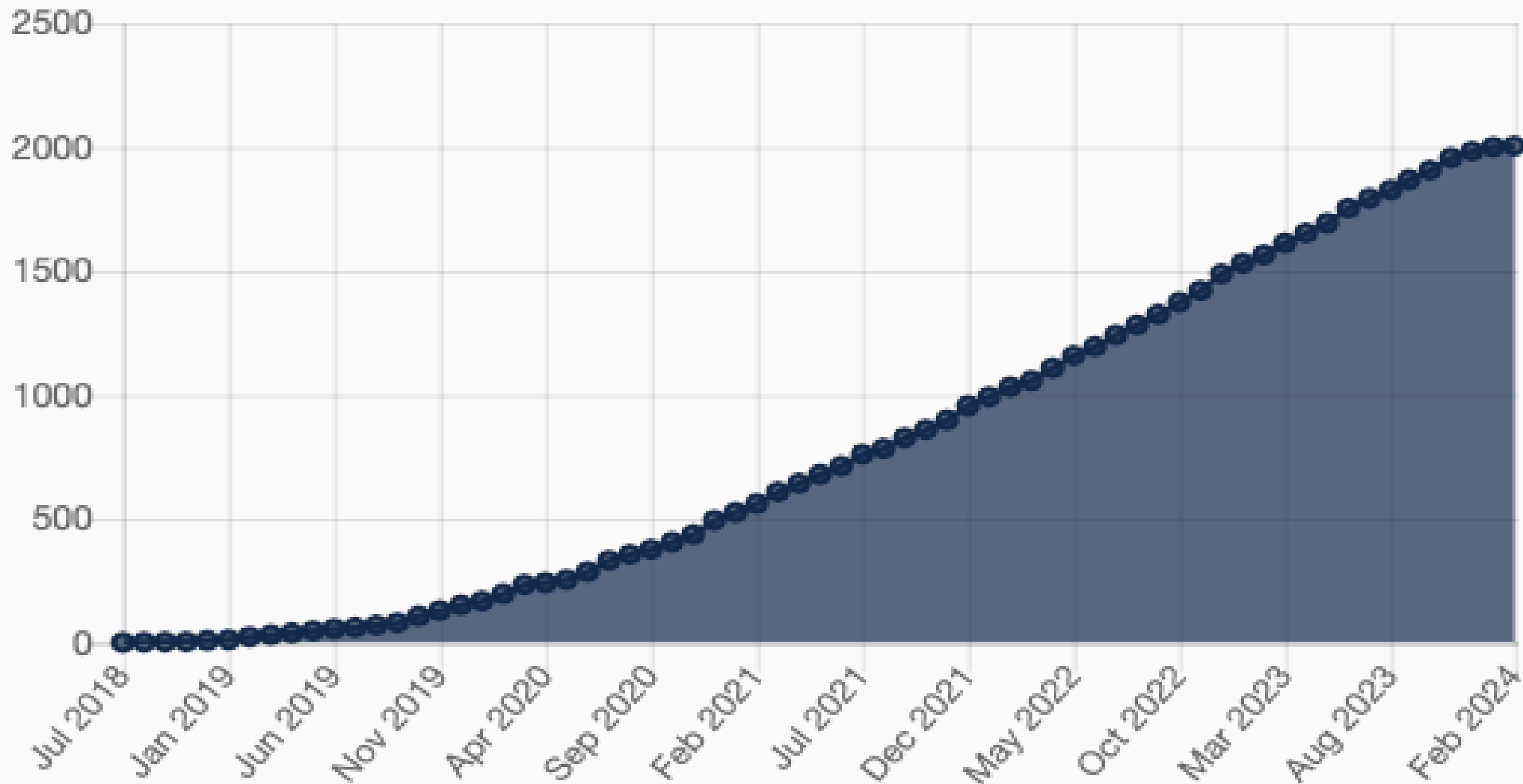
Statistics: Highest individual fines (Top 10)

The following statistics shows the highest individual fines imposed to date per data controller (only top 10 fines).

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	1200000000	Insufficient legal basis for data processing	2023-05-12
2	Amazon Europe Core S.à.r.l.	Industry and Commerce	LUXEMBOURG	746000000	Non-compliance with general data processing principles	2021-07-16
3	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405000000	Non-compliance with general data processing principles	2022-09-05
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390000000	Non-compliance with general data processing principles	2023-01-04
5	TikTok Limited	Media, Telecoms and Broadcasting	IRELAND	345000000	Non-compliance with general data processing principles	2023-09-01
6	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265000000	Insufficient technical and organisational measures to ensure information security	2022-11-25
7	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225000000	Insufficient fulfilment of information obligations	2021-09-02
8	Google LLC	Media, Telecoms and Broadcasting	FRANCE	90000000	Insufficient legal basis for data processing	2021-12-31
9	Facebook Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000	Insufficient legal basis for data processing	2021-12-31
10	Google Ireland Ltd.	Media, Telecoms and Broadcasting	FRANCE	60000000	Insufficient legal basis for data processing	2021-12-31

Statistics: Fines by type of violation

The following statistics show how many fines and what sum of fines have been imposed per type of GDPR violation to date.

Note: Only fines with valid information on the amount of the fine and on the type of violation are taken into account.

1. By total sum of fines:
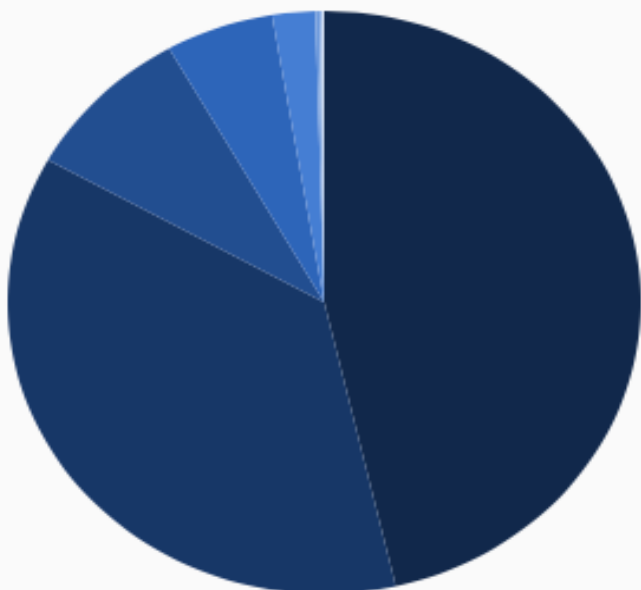
	Violation	Sum of Fines
	Non-compliance with general data processing principles	€ 2,081,000,659 (at 562 fines)
	Insufficient legal basis for data processing	€ 1,649,428,512 (at 624 fines)
	Insufficient technical and organisational measures to ensure information security	€ 391,263,875 (at 362 fines)
	Insufficient fulfilment of information obligations	€ 247,481,060 (at 187 fines)
	Insufficient fulfilment of data subjects rights	€ 98,366,170 (at 194 fines)
	Unknown	€ 9,250,000 (at 9 fines)
	Insufficient cooperation with supervisory authority	€ 6,205,529 (at 108 fines)
	Insufficient fulfilment of data breach notification obligations	€ 2,613,282 (at 36 fines)
	Insufficient data processing agreement	€ 1,057,110 (at 11 fines)
	Insufficient involvement of data protection officer	€ 955,300 (at 20 fines)

COLLABORATION IS KEY

- Same language *(e.g., CDPSE)*
- Common definitions
- Embed Privacy and Security in the organization – Privacy/Security champions/SPOCs/Align resources
- Regular calls/interaction/sharing of ideas and goals
- Position within the organization – seat at the table – tone from the top – convince C-suite
- Find your biggest ally – CTO?
- Data Governance
- Common/easy reporting w a central reporting point (regulatory technology)
- Budgets decrease – join forces
- Quantification of ROI (data-driven approaches) – making cybersecurity/digital trust part of business growth strategy
- Upskill, Go outside of your comfort zone

HOW TO BUILD BRIDGES BETWEEN PRIVACY AND SECURITY IN A DIGITAL TRUST WORLD

"To achieve a balanced approach, organizations should establish comprehensive legal frameworks and regulations, such as GDPR in Europe and CCPA in the US, outlining clear guidelines for personal data collection, storage, and usage.

Incorporating privacy into system design from the outset, practicing data minimization, and employing encryption techniques are vital steps to minimize breaches and protect privacy.

Robust access controls, transparency, and accountability measures ensure data is handled securely and ethically.

Respect for user consent and control, along with privacy impact assessments, facilitates proactive risk mitigation.

Collaboration between privacy and security teams, coupled with continuous monitoring and compliance mechanisms, solidifies trust among users and safeguards against unauthorized access and misuse of sensitive information."

Benefits of Data Protection (Privacy and Security)

Privacy and Security cannot simply protect data with technical controls

- Establishes customer/partner/merchant trust
- Ensures company is protected against security and privacy threats
- Safer & more secure products
- Creates the right organizational culture
- Crucial in demonstrating accountability and to respond coherently to RFIs, pass audits, etc.
- Shifts in conversation where cybersecurity and privacy are perceived as a defense mechanism rather than as an opportunity for business growth
- Increases in company's ROI by tying privacy and security to concrete business goals (risk, CX, compliance, revenue expansion, governance, operational resilience)

What happens if there is no data protection?

- Data Breaches
- Fines or sanctions
- Loss of customer trust
- Poor incident response
- Business disruption (lost $$$)
- …

From ISACA state of Digital Trust report 2023 page 12

Respondents report that high levels of digital trust can lead to the following benefits.
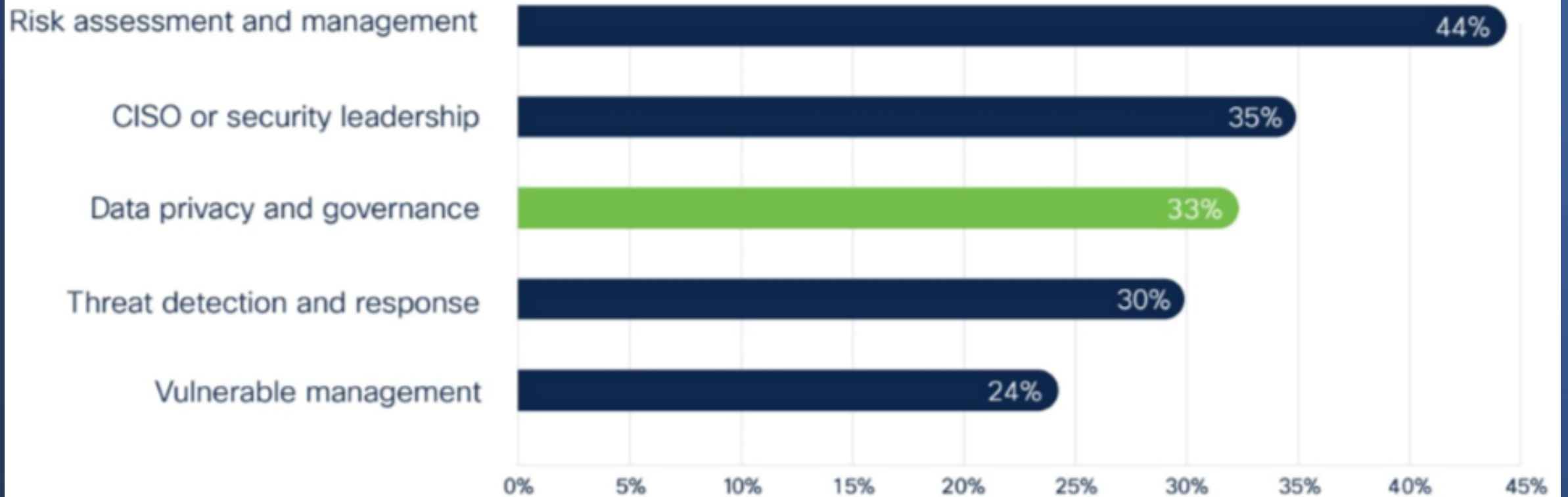Digital trust related benefits
1. Positive reputation (67%)
2. More reliable data for decision making (57%)
3. Fewer privacy breaches (56%)
4. Fewer cybersecurity incidents (56%)
5. Stronger customer loyalty (55%)
6. Faster innovation due to confidence in their technology and systems (42%)
7. Higher revenue (27%)

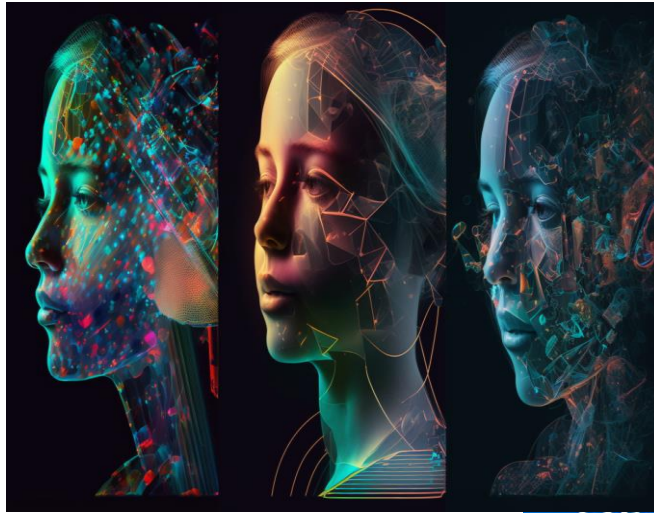**Consequences of lack of digital trust**
Respondents say organizations with a low level of digital trust often experience the following consequences
1. Reputation decline (63%)
2. More cybersecurity incidents (59%
3. More privacy breaches (58%)
4. Loss of customers (56%)
5. Less reliable data for decision making (54%)
6. Negative impact on revenue (42%)
7. Slower ability to innovate (36%)

Top job responsibilities among security professionals

| Responsibility	Percentage
Risk assessment and management	44%
CISO or security leadership	35%
Data privacy and governance	33%
Threat detection and response	30%
Vulnerable management	24%

What's Next?

ENVIRONMENTAL
GHG Emissions
Biodiversity
Waste & Water Management
Use of Natural Resources

SOCIAL
Diversity & Inclusion
Consumer Protections
Community Support

NUTRITION & HEALTH

GOVERNANCE
Business Ethics
Corruption
Accounting Transparency
Management Structure
Employee Relations

OPEN DATA DEFINITION
1. Availability & access
2. Re-use and redistribute
3. Universal participation

GDPR
AI ACT
DA
DGA
DMA
DSA
DORA
NIS2
…

Data
Zero Trust
User
Applications
Network Traffic

BLOCK CHAIN

MACHINE LEARNING
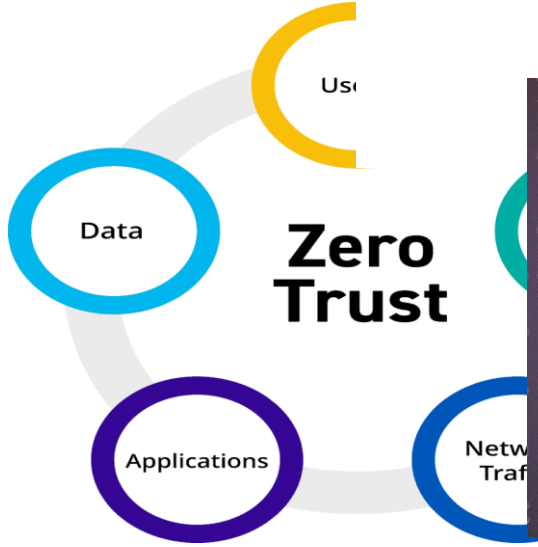
Final Thoughts – Take Aways

"2024 promises to be another robust year in the data protection industry as the pace of technological and regulatory change accelerates in the space"

- **NEW LAWS AND EVOLVING TECHNOLOGIES** (75% of world's pop will have their personal data covered by one or more privacy leg - Gartner)

- **INCREASED THREATS / BREACHES/ENFORCEMENT** (Gen AI breaches and fines and Increased fines and Consumer awareness)

- **CHILDREN'S ONLINE SAFETY**

- **EXPLOSION OF UNSTRUCTURED DATA**

- **CONTINUED AI PROFILERATION AND LEGISLATION**

- **INCREASED INTERTWINING BETWEEN COMPETITION AND DATA PROTECTION LAW**

Gartner 2024 Privacy trends

- Data localization (incl local cloud storage)

- Privacy Enhancing Computation (PEC) Techniques (ensuring that sensitive information is kept confidential when it is used by multiple parties to collaborate on tasks)

- AI Governance

- Centralized Privacy UX (self service), and

- Hybrid Everything (including accurate (intrusive) monitoring)

THANK YOU!