2025 Mo-Kan

Annual Labor & Employment Law Seminar

Fisher Phillips

Breach Point: Protecting Employee & Company Data in a Risky World

October 30, 2025

Laura Brown
lkbrown@fisherphillips.com
(816) 460-0208


TIESTO
MGM
GRAND
GRAND
CIRQUE DU SOLEIL
CBS
EVENING
NEWS
WITH NORAH O'DONNELL


NEWS FLASH

It’s Happening Everyday…

Class Action Lawsuits

$5M EyeMed data breach class action settlement

EyeMed Vision Care LLC agreed to a $5 million class action lawsuit settlement to resolve claims it failed to prevent a 2020 data breach that...

24 hours ago

Canadian Tire says customer info caught in data breach on e-commerce platform

Breach includes names, addresses, emails, birth years, incomplete credit card info

The Canadian Press · Posted: Oct 14, 2025 10:39 AM CDT | Last Updated: 2 hours ago

The Harvard Crimson

Harvard Investigating Security Breach After Cybercrime Group Threatens To Release Stolen Data

Harvard is investigating a data breach after a Russian-speaking cybercrime organization claimed it was preparing to release information...

16 hours ago

Five million Qantas customers have had personal information leaked on the dark web. Here’s what you need to know

One expert warns frequent flyer details could be used to create fake flight rescheduling emails or fraudulent redemption offers.

FOX4KC.com

https://fox4kc.com › press-releases › accesswire › lessin...

Lessing's Hospitality Group Data Breach Under ...

1 day ago — On October 3, 2025, Lessing's Hospitality Group began notifying impacted individuals, and on October 6, 2025, it filed notice of the **breach** with ...

The HIPAA Journal

https://www.hipaajournal.com › cyberattack-on-sunflo...

Cyberattack on Sunflower Medical Group Affects ...

Mar 11, 2025 — Cyberattacks and **data breaches** have been announced by Sunflower Medical Group, The Center for Digestive Health, NVW Newco, Endless Mountains ...

BleepingComputer

SimonMed says 1.2 million patients impacted in January data breach

U.S. medical imaging provider SimonMed Imaging is notifying more than 1.2 million individuals of a data breach that exposed their sensitive...

1 day ago

The Verge

Discord blamed a vendor for its data breach — now the vendor says it was ‘not hacked’

5CA, a customer service support company that Discord said was breached as part of a "security incident" where 70000 government ID photos may...

7 hours ago

The Legal Landscape

Data Privacy Laws and Regulations and the Intersection of Employment Law

Federal Data Privacy Laws

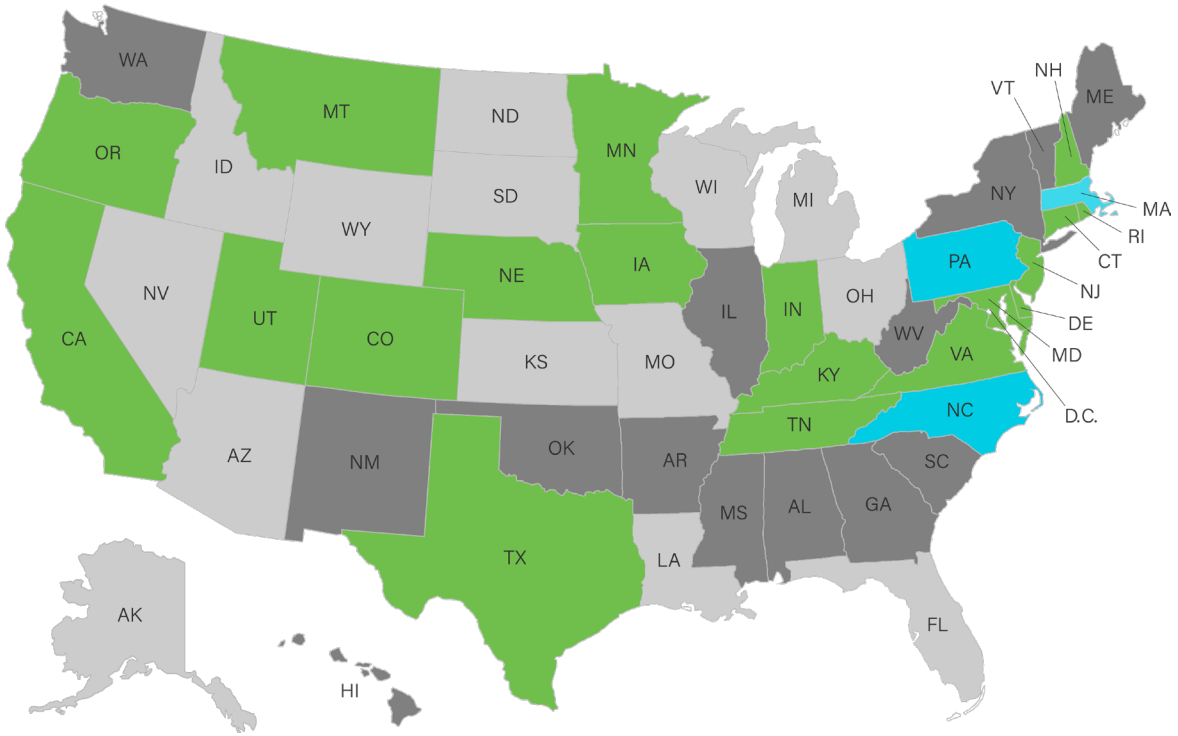
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Trade Commission Act (FTC Act)
- Fair Credit Reporting Act (FCRA)
- Telephone Consumer Protection Act (TCPA)
- Computer Fraud and Abuse Act (CFAA)
- Stored Communications Act (SCA)
- Government contractor privacy/training compliance
- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)

State Data Privacy Laws

- Consumer privacy laws (CCPA and 19 others)
- Biometric privacy laws (IL BIPA, TX, WA)
- Consumer health data laws (WA, NV, CT)
- New York Shield Act
- Data security and breach notification laws (all 50 states)
- Employee monitoring laws
- AI/ADMT legislation
- Off-duty conduct laws
- Social media monitoring laws
- GPS/geolocation tracking laws
- Wiretapping laws

State Consumer Privacy Laws

US State Privacy Legislation Tracker 2025



Eight in Effect Pre-2025:

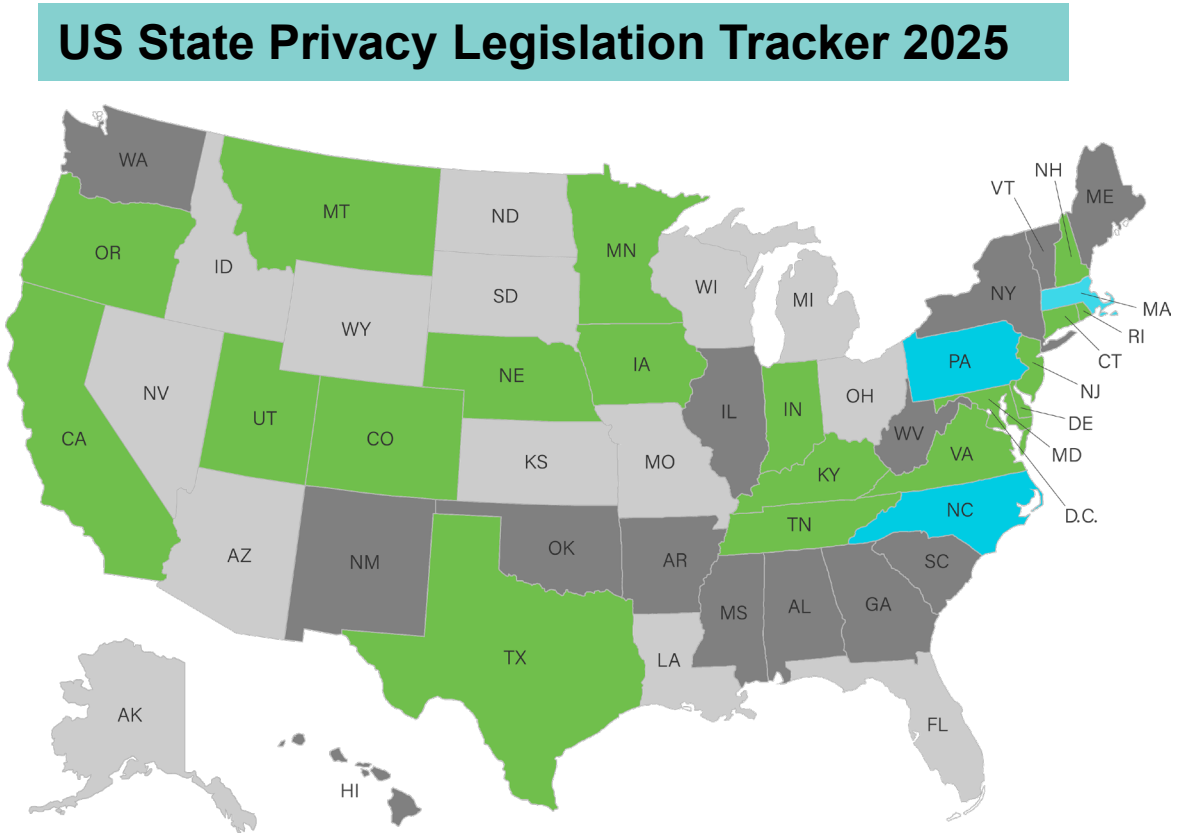
- California
- Colorado
- Connecticut
- Montana
- Oregon
- Texas
- Utah
- Virginia

Statute/bill in legislative process:

State Consumer Privacy Laws

2025 Effective Dates:

- Jan. 1, 2025: Delaware, Iowa, Nebraska, New Hampshire
- Jan. 15, 2025: New Jersey
- July 1, 2025: Minnesota
- Oct 1, 2025: Maryland



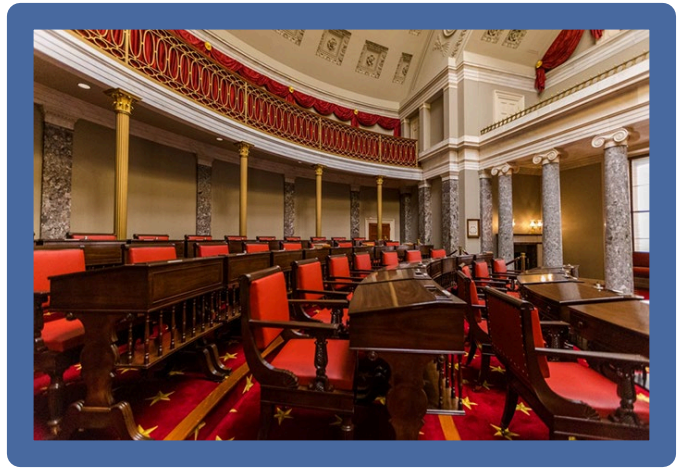
Coming 2026

Status of Federal Privacy Legislation

U.S. Senate:

Committee on the Judiciary Subcommittee on Privacy, Technology and the Law held a hearing on July 30, 2025, dedicated to federal privacy law consideration

- Part of a series on “Protecting the Virtual You”
- First hearing focused on “Safeguarding Americans’ Online Data”
- Discussed general consensus that patchwork of state laws is unworkable.
- Observed heightened urgency for federal law due to the value of data to AI development: “AI is both the gasoline and the engine for AI models”



Prior to the hearing, the Senate had not considered any comprehensive consumer privacy legislation in 2025; focus had been on children’s privacy issues.

Status of Federal Privacy Legislation

U.S House:

Republican Working Group Considering Comprehensive Framework

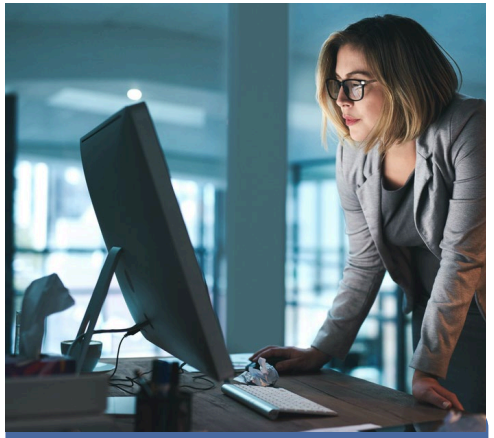
- **Dec. 2024:** Congressman Brett Guthrie (KY), Chairman of House Committee on Energy & Commerce, said that his Committee would "prefer to do a comprehensive privacy bill" while at least planning to focus on finalizing children's online safety if a comprehensive bill didn't materialize.
- **Feb. 12, 2025:** Guthrie launched 9-member Republican working group to explore options for a comprehensive framework.
- The group issued an RFI regarding a federal privacy law.
- Accepted input until April 7, 2025.

Status of Federal Privacy Legislation

House Committee on Energy and Commerce RFI Questions Included:

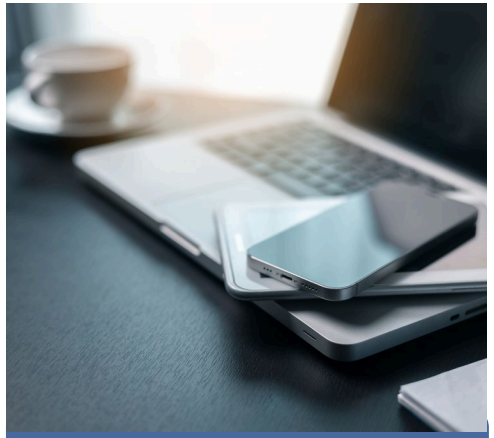
- Role of players in the data protection space (controllers, processors, third parties)
- Should there be different treatment for companies of different sizes?
- Scope of privacy laws – including definition of PI and SPI
- Scope/content of privacy disclosures
- Which consumer protections should be included?
- What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?
- Any insights learned from existing comprehensive data privacy and security laws
- Degree to which US privacy protections are fragmented at the state-level and the costs associated with fragmentation
- What is the appropriate degree of preemption that a federal comprehensive data privacy and security law should adopt?
- Efficacy of existing data privacy and security laws, including "impacts on both data-driven innovation and small businesses"
- How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?
- Who should enforce the law?
- If the FTC enforces, what resources and authorities should be made available to it?

Intersection of Employment Law



Employee Monitoring

Searches of desks, smartphones, lockers, vehicles, equipment, etc.



Monitoring employee communications, calls, emails, and internet use

Monitoring use of company vehicles

Protecting Employee Data

Employee Monitoring

Employers can generally conduct surveillance of their employees in the workplace as long as the Employer has a legitimate business purpose in doing so.

Monitoring via surveillance cameras in the workplace, common areas and entry areas is **generally lawful** provided that employees and non-employees (ex. customers, vendors) are provided **with proper advance notice** that video surveillance is or will take place.
Employers should include a statement of its intent to conduct video surveillance in Employee Handbooks (and make new hires aware during orientation) while posting signs and/or notices in various locations, including entry ways and in areas where cameras are located.

Some states include employee lounge areas among the places where video surveillance cannot take place.

Video surveillance should not occur in areas where employees have a *reasonable expectation of privacy* such as locker rooms, showers and restrooms.

Some states include employee lounge areas among the places where video surveillance cannot take place.

Searches of Property

Employers may, as a general rule, conduct a search of company-owned property, including equipment, vehicles, desks, lockers, etc., for **legitimate business reasons** as employees ordinarily should not have an expectation of privacy in these areas.

Unlike private sector employers, **public sector employers are subject to** the **Fourth Amendment** and must show that the workplace search was reasonable under the circumstances. See O'Connor v. Ortega, 480 U.S. 709 (1987).

Employers should **communicate their right to conduct searches** in the Employee Handbook and state that employees should not have a reasonable expectation of privacy when using property owned by the Employer.
The Employer should include examples of the circumstances under which it might chose to conduct a search of its property, **including the investigation of suspected employee misconduct**. Further, Employers should have written policies that cover employee use of Employer owned equipment/property.

Employers, who permit employee to use their personal devices for work, should have a written **BYOD Policy that sets forth device protocols** such as the requirement for anti-virus and mobile device management software before the device is used for work.

Monitoring Employee Conversations

There are three federal statutes that come into play when considering Employer monitoring of employee communications in the workplace, the Wiretap Act, the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA).

To avoid liability under the ECPA and SCA, employers who maintain their own email systems and provide internet access, should have a written policy that provides that the employer, for legitimate business reasons, may monitor and review emails sent or received on its email system on a device provided by the employer or a personal device used for work purposes as well as internet activity.

The employer's policy should state that the employee's use of its email system provides consent to the employer to access and review any email messages sent or received over the system for a valid business purpose or review the employee's internet usage. Having employees sign **an acknowledgement of receipt of the employer's electronic communications policy** at the commencement of employment is recommended.

Monitoring Company Vehicles

Many Employers monitor employee use of company vehicles with GPS devices. The data garnered from these devices can often aid in the defense of wage and hour lawsuits and in other cases where the employee's use of the vehicle deviated from company policy.

Employers who elect to use GPS monitoring devices should always notify the employee that a GPS device has been placed on the company-owned vehicle and obtain a signed consent to the monitoring.

Unless prohibited by state law, monitoring an employee's personal vehicle when used in the course and scope of employment may be permitted only where a signed consent is obtained. Monitoring the employee's personal use of a personal vehicle should not occur.

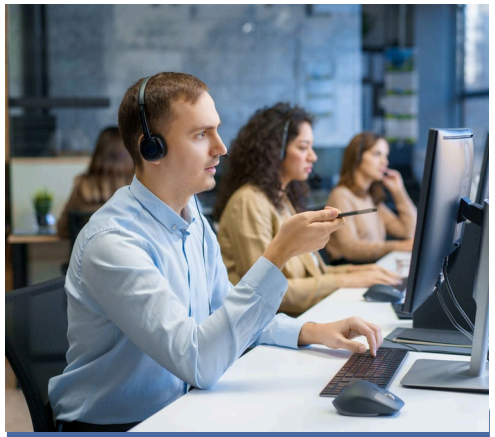
Data Privacy Risks

What's At Stake in the Workplace?

What's At Stake in the Workplace?

Employee Data

Company Data



Customer Information

Data on Personal Devices and Remote Work Sites

Types of Risks

Phishing Attacks: Phishing attacks are a significant risk, where deceptive emails or other communications trick users into revealing sensitive information.

Unsecured Networks: Transmitting data over an unsecured network can make it easy for attackers to intercept and steal data.

Malware: This software can infiltrate a computer system to steal, damage, or disrupt data.

Data Breaches: Unauthorized access to data repositories can lead to significant data loss and exposure to sensitive information.

Lack of Encryption: Sensitive data that isn't encrypted is at risk, particularly during transmission or in case of data breaches.

Poor Access Management: If user access controls are not strictly managed, individuals might gain access to sensitive data.

Types of Risks (cont.)

Data Sold to Third Parties: Without strict control over third-party data sharing, companies risk the privacy of their customers.

Poorly Configured Cloud Services: Products hosted on public clouds might expose data if not properly configured and secured.

Non-compliance with Data Privacy Regulations: Companies that fail to comply with data privacy laws risk fines, sanctions, and damage to their reputation.

Outdated Security Systems: Organizations are at risk if they do not consistently update and patch their software systems, as outdated systems often have known vulnerabilities that can be exploited.

Data in Transit: Data being transferred from one location to another is vulnerable to interception and attacks.

BYOD Culture: The "Bring Your Own Device" culture can pose a threat as personal devices may lack the same level of data security as company-owned devices.

Social Engineering: Manipulative tactics that trick individuals into disclosing confidential information.

Legal Risk and Exposure

Internal Risks

Data breaches

- Liability
- Notification Obligations
- Fines

Insider threats

- Disgruntled employees
- Negligent handling of data

Third Party Risks

HR Vendors

- Payroll services
- Benefits
- Employment and Salary Verification

Supply Chains

Litigation Risks

Class Action

Regulatory Enforcement

Practical Consequences

Data Breach Can Lead to Direct Financial Loss:

- **Ransoms** in the case of ransomware attacks
- **Compensating** affected parties
- Reduced in business **valuation**
- harm to **reputation**
- Loss of customer **trust**
- Potential **lawsuits**

Coinbase Hack 2025

Coinbase (May 2025)

- Coinbase confirmed in May 2025 that the personal data of **less than 1% of its users** was exposed after scammers bribed external customer support agents.
- The insiders provided sensitive customer details, including names, account information, and partial SSNs.
- An attempt was made to ransom the data for $20m, but **Coinbase refused**.
- According to Reuters, the **breach may cost Coinbase up to $400 million.**

AT&T (2024-2025)

- Massive breach exposing data of 73 million current and former customers — including Social Security numbers and account credentials — after records surfaced for sale on the dark web (2024).
- Regulators and class-action plaintiffs allege **AT&T failed to safeguard consumer information and delayed disclosure**; lawsuits seek damages for identity theft risk and privacy violations.

Meta (2022)

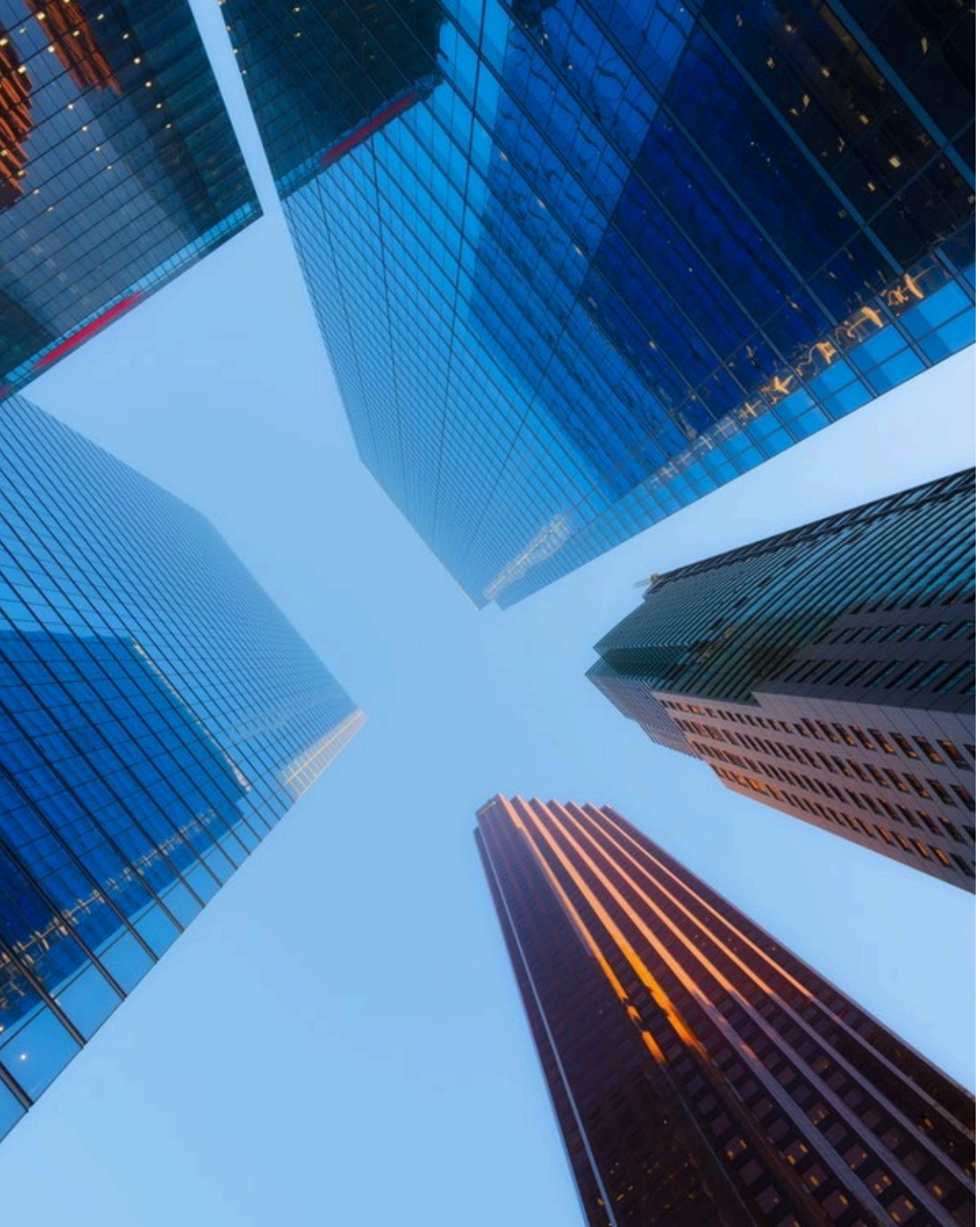
- Meta Platforms Inc. was **fined 17 million euros ($19 million) for violating the European Union's privacy rules by failing to prevent a series of data breaches on its Facebook platform in 2018.**
- The Irish Data Protection Commission, the lead EU privacy watchdog for Meta, said it found that Facebook "failed to have in place appropriate technical and organizational measures."
- Facebook in 2018 became **the first big test case for the EU's General Data Protection Regulation** when the Irish watchdog announced an investigation into a breach that affected as many as 50 million accounts. Tuesday's probe was started in December that year, looking into 12 breach notifications by Facebook, including ones caused by a software bug that gave outside developers access to the photos of millions of users.

Snapchat Insider Data Leak

- Snapchat experienced a data breach that exposed the payroll information of around 700 current and former employees. A high-ranking payroll employee was tricked by an email impersonating CEO Evan Spiegel and unknowingly sent over sensitive data.
- Social engineering (CEO impersonation/phishing).
- Names, Social Security numbers, wage information, and other personal details were leaked. While the financial impact wasn't publicly disclosed, the incident caused embarrassment for a technology company that promotes privacy and security as core features of its platform.

...But We Aren't as Big as AT&T or Facebook!!! We Must be Fine!? Right!?

DATA BREACHES AFFECT BUSINESSES OF ALL SIZES



Best Practices for Data Protection

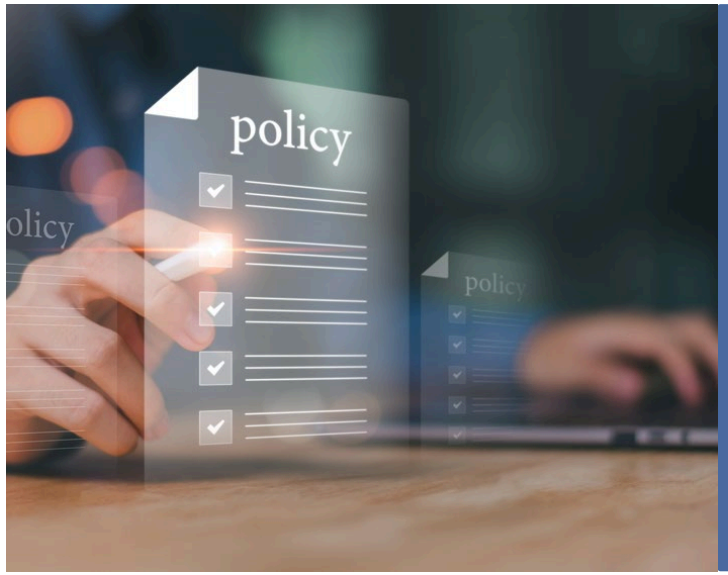
Action Plan for Human Resources and Company Leaders

Understand Your Data

Data Audit:

- What do we collect, why, and how long do we keep it?
- Understand the data your organization processes.
- Identify what types of personal data you have.
- Consider creating data mapping and a clear inventory.

Policies and Procedures



- Review and implement robust confidentiality and acceptable use policies
- Data retention policies
- Privacy policies
- Strong onboarding and offboarding processes

Vendor Management

HR vendors use employee data, and employers must protect that use.

Conduct proper due diligence of the HR vendor before sharing data.

- Is your HR vendor selling your employees' data?
- Does your HR vendor use your employees' data outside the scope of the service provided?
- Even reputable and well-known HR vendors may be doing both.
- There are vendors who have technology to address these issues.

Contracts with clear security expectations

Ongoing monitoring of vendor practices

Vendor Management

Due Diligence Tips

Request the following information from the vendor:

- History of data breaches
- Data breach prevention strategies
- Current data breach security measures
- Incident response and business continuity plans
- The vendor's own employee data use and maintenance policy
- Data deletion policy

Vendor Management

Contract Tips

Contracts with clear security expectations, including:

- Scope of acceptable data use
- Data deletion requirements
- Post-termination rights and obligations
- Responding to consumer requests
- Obligations in the event of a data breach
- Compliance with privacy laws **(be specific)**
- Maintain strict security measures

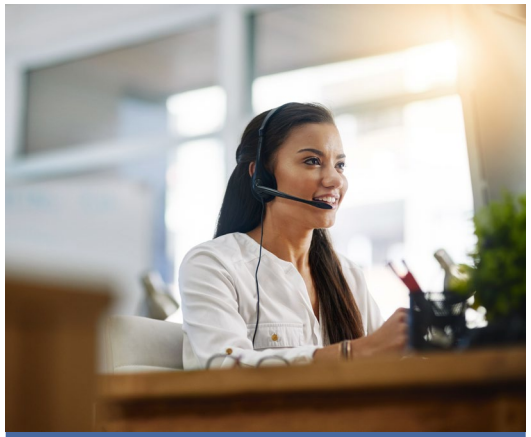
Secure Your Data

- Protect your data by implementing robust cybersecurity practices
- Develop strong access controls with multi-factor authentication
- Create layered permissions for employee access **(business need to know)**
- Data encryption for sensitive information
- Secure network infrastructure with firewalls

Training and Communication

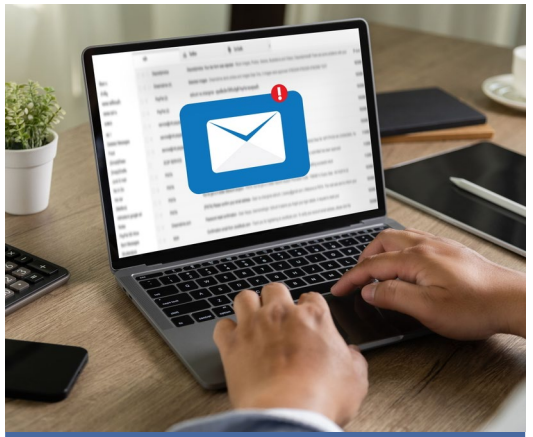
- Conduct regular training on confidentiality policies
- Conduct regular cybersecurity tests
- Conduct phishing simulations

Incident Response Plan



Who to call

What to do



Who to notify

Who to Call?

- Legal
- HR
- Accounting / Finance
- Computer Forensic Analyst
- Cyber Insurance Carrier
- Leadership and Decision Makers

Summary of Action Plan

#1 – Data Audit: Know what you have.

#2 – Training and Communication: Educate employees about data privacy requirements and the importance of protecting personal data.

#3 – Conduct Regular Audits: Continued Assessment of areas of risk and testing of the effectiveness of security measures is critical.

#4 – Partner with IT and Legal: Perform ongoing risk assessments and stay up-to-date on changing data privacy laws

#5 – Plan for Breach: Have a process in place for managing data breaches.

QUESTIONS?

THANK YOU!