Parker Poe
Attorneys & Counselors at Law

Data Privacy & Artificial Intelligence in the States, Europe & USG

Steve Britt, CIPP/Europe, CIPM
Counsel, Cyber, Data Privacy & Technology
Parker Poe Adams & Bernstein LLP
stevebritt@parkerpoe.com

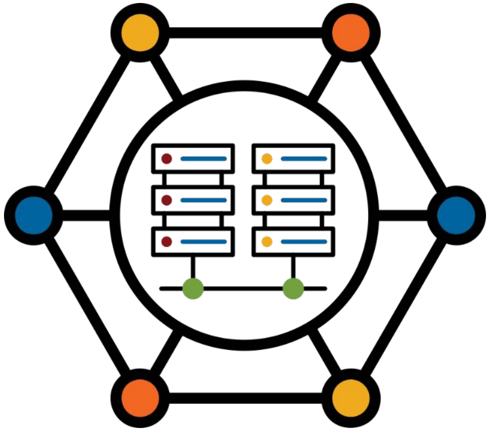
© 2023 Parker Poe Adams & Bernstein LLP | **parkerpoe.com**

Today's Agenda

- ❑ GDPR + 15 other State data privacy laws
- ❑ What do these laws have in common? How do they differ?
- ❑ E.U. Artificial Intelligence Act
- ❑ White House Bill of Rights for A.I.
- ❑ NIST A.I. Risk Management Framework
- ❑ President's Executive Order on Artificial Intelligence
- ❑ Congressional Proposed Frameworks
- ❑ 2 new Cyber FARs (all DoD & civilian contractors)

The Two Pillars of “Data Protection”

DATA SECURITY



Protecting data & the computers it lives on

DATA PRIVACY

Protecting the rights of data subjects

You can have Data Security w/o Data Privacy – You can’t have Data Privacy w/o Data Security

GDPR (*where it all began*)

Applies to **for-profit & non-profit** entities (online & offline data) that are:

- “Established” in EU (27 member states), or
- **Market goods or services** to EU residents (even online), or
- **Profile** EU residents for marketing

Governs collection/use of EU resident data

Broad data rights (Right to Know/Correct/Delete/Opt-Out/Portability)

Employee training & detailed recordkeeping

Data Protection Impact Assessments (DPIAs) – different than US DPAs

Restricts cross-border transfers of EU Data (includes remote access from US)

Fines up to 4% of global revenue + class actions

© 2022 Parker Poe Adams & Bernstein LLP | **parkerpoe.com**

California Consumer Privacy Act (CCPA)

- Enacted 06-28-2018, effective 01-01-2020

- For-profit entity doing business in California with (i) $25mm in annual gross revenue worldwide; **OR** (ii) annually processing data of 100,000 Californians; **OR** (iii) 50% revenue comes from selling data

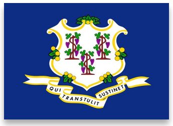
- Grants "consumers" the right to know, correct and/or delete their personal information and control its use or sharing with third parties

- Homepage website button (***Do Not Sell My Personal Information***) for sale of personal data, which includes transfer to website analytics provider if not under restrictive contract)

- AG fines of $2500-$7500 per violation

- Private cause of action for data breach due to inadequate security

5 new state laws take effect in 2023

• California Privacy Rights Act:	01/01/2023	
• VA Consumer Data Protection Act:	01/01/2023	
• Colorado Privacy Act:	07/01/2023	
• Connecticut Data Privacy Act:	07/01/2023	
• Utah Consumer Privacy Act:	12/31/2023	

10 new laws passed in 2023

Washington My Health My Data Act:	03/31/2024
Nevada Consumer Health Data Privacy:	03/31/2024
Florida Digital Bill of Rights Act:	07/01/2024
Texas Data Privacy & Security Act:	07/01/2024
Oregon Consumer Privacy Act:	07/01/2024
Montana Consumer Data Privacy Act:	10/01/2024
Iowa Consumer Data Protection Act:	01/01/2025
Delaware Personal Data Privacy Act	01/01/2025
Tennessee Information Protection Act:	07/01/2025
Indiana Consumer Data Protection Act:	01/01/2026

What Do These Laws Have in Common?

- For-profits collecting 100,000 residents' data (TN 175K, MT 50K, DE 35K)
- Define "**personal information**" & "**sensitive data**" (race, ethnic, religious, immigration, mental health)
- Grant broad data rights (Right to Know/Access/Correct/Delete/Opt-Out)
- Restrict sale of data, use of sensitive data, targeted advertising & profiling
- All but 2 require ***Data Protection Assessments***
- All require new data privacy notices ***before collection of personal data***
- Data transfers to 3rd parties require restrictive contracts
- A.G. fines (no private C/A except WMHMDA)
- A.I. & automated processing rules (algorithms, training data, etc.)

© 2023 Parker Poe Adams & Bernstein LLP

How Do These Laws Differ?

- CO, Washington, Oregon, NV & DE apply to **non-profits**
- **3 States regulate Consumer Health Data**
- CCPA applies to $25mm global revenue regardless amt. of data collected
- Utah / TN don't apply *UNLESS* the company has $25mm annual revenue
- CA *first-in-the-nation* state data privacy regulator **(CPPA)**
- CA grants data rights to employees & B2B contacts (others exclude)
- Some states must **opt-in** to collection of sensitive data – Others **opt-out**.
- 5 states require recognition of Universal Opt-Out Mechanisms
- 4 states passed social media platform bills (parental controls)
- California and CO regulate automated data processing

© 2022 Parker Poe Adams & Bernstein LLP | **parkerpoe.com**

US A.I. Regulation Coming

- **White House Blueprint for an AI Bill of Rights (Oct 2022)**
- 5 principles to guide the design, use & deployment of automated systems:

A. Safe & Effective Systems (prior testing / risk mitigation)

B. Algorithmic Discrimination Protections (algorithmic impact assessments)

C. Data Privacy (privacy by design)

D. Notice & Explanation (notice when A.I. in use & how it functions)

E. Human Intervention (right to opt-out of automated system)

© 2022 Parker Poe Adams & Bernstein LLP

Europe's A.I. Act is Already Here

- World's first artificial intelligence law
- Covers any AI System released into the EU from anywhere
- European Commission proposed in April 2021
- Council of the EU version in December 2022
- European Parliament version released in June 2023
- Final version late 2023 / early 2024 (2-year transition)
- Risk-based standards: Unacceptable, High Risk & Low Risk

E.U. Unacceptable A.I. Uses Prohibited

- Systems w/ unacceptable risks to health & safety or fundamental privacy rights are prohibited.
- Examples:
  - Subliminal behavioral manipulation of vulnerable people
  - AI-based social scoring by public authorities
  - Biometric categorization from use of sensitive profiling data
  - Real-time biometric I.D. in public space for law enforcement
  - Predictive policing systems based on profiling
  - Emotion recognition systems

E.U. High Risk A.I. Activities

1. Real time / post remote biometric identification of natural persons
2. Operation of critical infrastructure (road, utilities, hospitals, etc.)
3. Access to education or vocational training
4. Employment, worker management or access to self-employment
5. Access to essential public or private services & benefits
6. Use by law enforcement for investigations & enforcement
7. Immigration, asylum & border control management
8. AI Systems for administration of justice & democratic processes

© 2022 Parker Poe Adams & Bernstein LLP

EU High Risk Compliance Rules

- Undergo compliance assessment before release (self v 3rd party)
- Risk management throughout System lifecycle
- Training, validation and testing w/ high quality data
- Detailed technical documentation & user instructions
- Automated logging for full traceability of operations
- Transparency enabling interpretation of performance
- Human oversight & ability to intervene
- Accurate & robust with effective cybersecurity protections
- Register stand-alone AI System in EU-wide database

E.U. Low Risk Transparency

- Since generative AI can create deep-fake texts & images, transparency for natural persons required:
  - User informed they are interacting with AI
  - User informed of use of emotion or biometric detection
  - User informed AI is source of generated / manipulated content
- AI regulatory sandboxes to develop, test & validate AI
- Innovation of AI can use sensitive data for training if controlled
- Codes of Conduct for voluntary use of high-risk rules

© 2022 Parker Poe Adams & Bernstein LLP

A.I. Permeates new CA Risk Assessment

- New “A.I” & “Automated Decisionmaking Technology” definitions.
- Risk Assessment to process sensitive data, monitor employees, track users in public, train A.I. tools, profiling, automated decisions.
- If using A.I. or automated decisionmaking technology, explain:
  - Why using A.I., how was it trained & what outputs result
  - How will quality, accuracy & reliability of data be retained
  - Logic of the technology & why it is fair & non-discriminatory
  - Metrics used to measure data quality & human involvement
  - If technology provided to others, explain appropriate uses
  - Provide 3rd party info. necessary for its own risk assessments

NIST A.I. Risk Management Framework

- Released January 23, 2023
- Voluntary framework
- *A resource for organizations designing, developing, deploying or using AI Systems*
- Goals:

  ✔ Management of A.I. risks

  ✔ Promotion of trustworthy & responsible development &

  ✔ Use of A.I. Systems
- DHS creates A.I. Task Force to enhance integrity of supply chain (screen cargo & secure critical infrastructure)

President’s Executive Order

- Safety & Testing of foundation models w/ national security/public health risk
  - Developers must share safety test results of foundation models
  - NIST sets standards – DHS & DOE apply stds to industry
- Content Authentication and Privacy
  - DOC stds for detecting/authenticating/watermarking content
- National Security – Cyber/NS memo
  - HHS rules re health care, DOT rules re transportation
- Responsible AI Use by US Government
  - OMB guidance, Agency Chief AI Officers, priority A.I. acquisition
  - Rules to disclose foreign IaaS subscribers re malicious training of A.I.
- Equity and Civil Rights
  - DOL rules; protect disabled, regulate use of biometric data
  - OSTP report on use of A.I. in criminal justice system
- Promote AI Innovation & Competition (US & Abroad)
  - Pilot program for A.I. R&D; multi-stakeholder collaboration, etc.

Blumenthal (D-CT) / Hawley (R-MO) Framework for A.I.

- Chair / Ranking Senate Judiciary S/C on Privacy & Tech.
- Licensing regime with new independent oversight body
- Harms A.I. triggers fines & ***private cause of action***
- Restrictions on export of A.I. tech to China, Russia, etc.
- Transparency disclosure of training, accuracy & safety of A.I.
- Strict limits on use of generative A.I. by kids (prior notice, right to human review, etc.

© 2022 Parker Poe Adams & Bernstein LLP

Senate Commerce Committee Weighs In

- Thune (R-SD), Klobuchar (D-MN), Wicker (R-MS), Hickenlooper (D-CO), Capito (R-WV) & Lujan (D-NM)
- Artificial Intelligence Research, Innovation & Accountability (**AIRIA**)
- Title I (Innovation): DOC certification stds High & Critical Impact
  - Detect / authenticate content created by machines
  - GAO to survey barriers to use of A.I. in Federal agencies
- Title II (Accountability): NIST oversight of non-Federal and Federal Use
  - Critical impact (non-DoD) biometric I.D., infrastructure or space
  - High Impact (non-DoD) housing, employment, credit, ed, health
  - Transparency reports and risk management assessments
  - Self-certifications w/ $300,000 fines & civil actions
- E.O. actions in 12 months – Critical Impact Plan over 3 years
- Compliance testing, evaluation, validation & verification (TEVV)

© 2022 Parker Poe Adams & Bernstein LLP

FAR re Cyber Incident Reporting & Info Sharing

- Compliance “**material to eligibility & payment of”** Gov’t contracts
- Contractors of information & communications tech (ICT) - 75% of all
- “Security incident” = discovery malware/data transfer unauth system
- Broad range of IOCs - data must be retained for 12 months
- Mandatory reporting (CISA portal) w/in 8 hours + every 72 hours
- Subcontractors must report to prime or next higher tier
- Upon CISA request, “full access” to physical / electronic systems
- SBOM: Required for all software used in contract (no incident req’d)
- Compliance required even if operating in foreign country

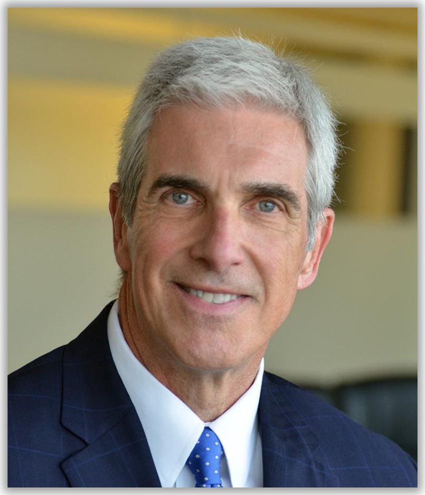
© 2022 Parker Poe Adams & Bernstein LLP | **parkerpoe.com**

Cyber Requirements for Unclassified FIS

- **Both rules apply to both DoD & civilian contractors**
- No exceptions re simplified acquisition/commercial items/COTS
- Contractors developing, operating or maintaining a Fed'l info system
- Compliance "**material to eligibility & payment**" of Govt contracts
- Cloud-based services require FedRAMP safeguards
- Engage in continuous monitoring and data disposal
- On-prem services require annual impact analysis under FIPS #199
- **Contractors must indemnify USG for liability from loss of gov't data, introduction of malware or unauthorized disclosures**
- *NIST Secure Software Development Form (**SSDF**) 06-12-23 critical + 09-14-23 other

© 2022 Parker Poe Adams & Bernstein LLP

Questions & Follow-up



Steve Britt, CIPP/Europe, CIPM
Counsel, Cyber, Data Privacy & Technology
Parker Poe Adams & Bernstein LLP
stevebritt@parkerpoe.com
m: (703) 989-7525