SQUIRE PATTON BOGGS

For Your Eyes Only: Dealing with Security Risks, New Privacy Laws, and Vendor Management

Presented by Squire Patton Boggs (US) LLP

For Your Eyes Only: Dealing with Security Risks, New Privacy Laws, and Vendor Management

SQUIRE PATTON BOGGS

Cecelia Dempsey
Del Monte Fresh Produce Company
Vice President, Global Legal - Corporate Services & Chief Global Privacy Officer
cdempsey@freshdelmonte.com

Daniel McVay
Intuit
Corporate Counsel
daniel_mcvay@intuit.com

Shea Leitch
Squire Patton Boggs, LLP
Of Counsel, Washington DC
shea.leitch@squirepb.com

Kyle Dull
Squire Patton Boggs, LLP
Senior Associate, New York/Miami
kyle.dull@squirepb.com

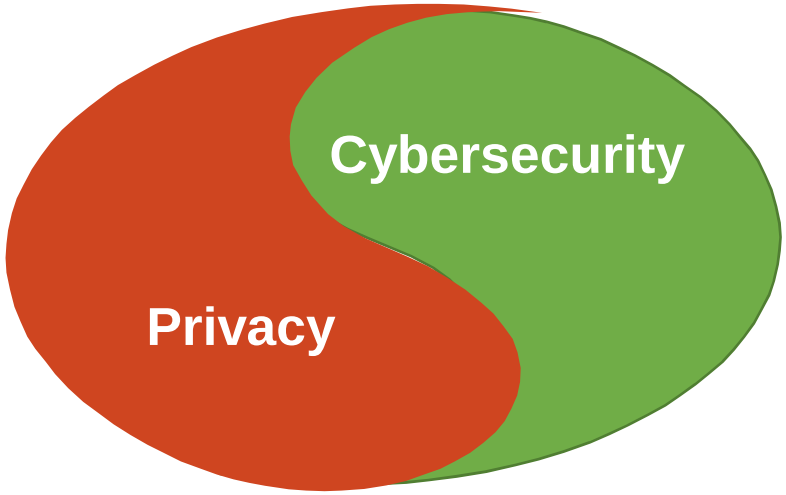
For Your Eyes Only: Dealing with Security Risks, New Privacy Laws, and Vendor Management

SQUIRE PATTON BOGGS

- Cybersecurity Risks
- New State Privacy Laws Requirements for Business
- Vendor Data Management
- What steps companies are taking to meet the changing risk environment, and the evolving legal and regulatory landscape

Privacy Basics

Privacy laws are about protecting *personal* information



Cybersecurity laws are about protecting information and systems from unauthorized access and use

- Definition of personal information *varies by law* –
  - U.S. trend is to broader definition, e.g., information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be
  - U.S. cybersecurity laws often have narrower definition

SQUIRE PATTON BOGGS

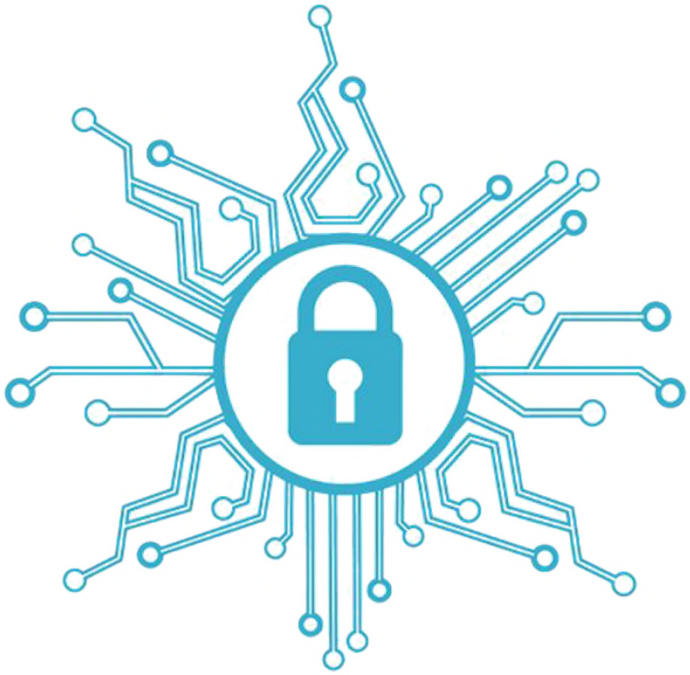
Security Risks

SEC Guidance and Proposed Regulations

- 2011 Staff Guidance:
  - No law or regulation explicitly requires disclosure of cybersecurity risks.
  - Guidance advises companies to disclose material cybersecurity risks and incidents.
  - Disclosures should be tailored to registrant's circumstances and avoid boilerplate.
  - Risks, events, and their surrounding circumstances should be disclosed if "material".
- 2018 Commission Statement and Guidance on Cybersecurity Disclosures:
  - Reiterates 2011 guidance to consider disclosing material cybersecurity risks and incidents in registration statements, periodic reports, and other filings.
  - "Materiality" – substantial likelihood that a reasonable investor would consider the information important in making an investment decision.
- 2022 Proposed Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
  - Reporting on 8-K of incidents within **4 days** of determining materiality.
  - Reporting on periodic reports of information regarding registrant's policies and procedures to identify and manage cyber risks, management's role in implementing cyber policies and procedures, and board of directors' cybersecurity expertise and oversight of cybersecurity risk.
  - Updates in periodic reports regarding previously disclosed cybersecurity incidents.

NYDFS Regulations

- Cybersecurity standards for organizations regulated by the NYDFS:
  - Cybersecurity Program must include:
    - Cybersecurity policies
    - CISO
    - Penetration testing and vulnerability assessments
    - Audit trails
    - Access privileges
    - Application security
    - Risk assessments
    - Third party management
    - MFA
    - Employee training and monitoring
    - Incident response plan



- Proposed amendments:
  - Large entities classified as “Class A” entities with heightened obligations, including:
    - Third party auditing of cybersecurity program
    - Third party risk assessments
    - Required EDR and centralized logging
    - Heightened access control requirements

Other State Law Requirements

SQUIRE PATTON BOGGS

- Massachusetts Cybersecurity Requirements:
  - Applicable to any “persons that own or license personal information about a resident of the Commonwealth”
  - Requires WISP and employee data handling requirements that include disciplinary consequences for failure to abide by data protection rules.
- CCPA “reasonable” security requirement
- Colorado, Virginia, Connecticut, and Utah require implementation of “reasonable” or “appropriate” security controls
- State data breach notification laws
  - Florida, for example: “Each covered entity, governmental entity, or third-party agent shall take **reasonable measures** to protect and secure data in electronic form containing personal information.”

Implementing Appropriate Cybersecurity

SQUIRE PATTON BOGGS

	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
What safeguards are available?	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

SQUIRE PATTON BOGGS

State Privacy Law

Overview and Trends: Historic State of Play

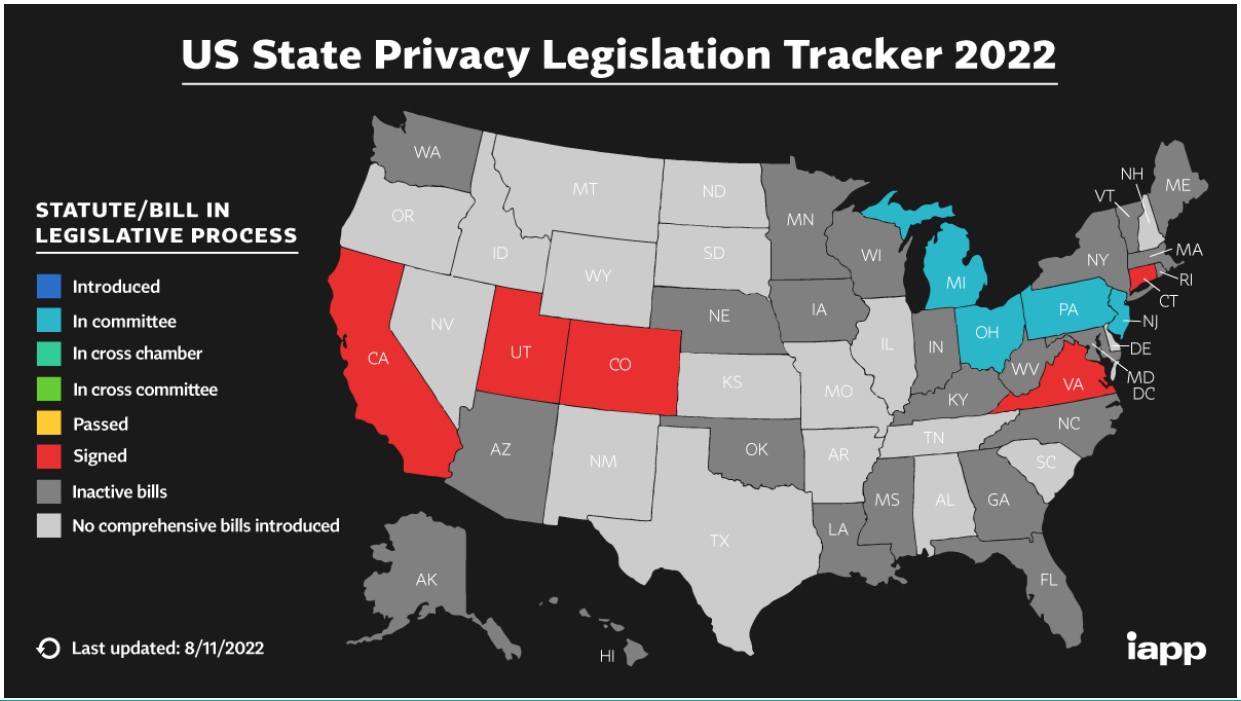
US data privacy laws have traditionally focused on specific sectors.

	Laws
Health Care	HIPAA (including HITECH and GINA)
	42 CFR Part 2
	State laws governing health privacy
Financial	Gramm-Leach-Bliley Act (GLBA)
	Fair Credit Reporting Act (FCRA)/Fair and Accurate Credit Transactions Act (FCTA)
	State laws (e.g., NY DFS rules)
Educational	Family Educational Rights and Privacy Act (FERPA)
Other	State laws governing "personal information" generally – Every state has "breach" laws – Roughly half of states have "security laws" (with CA, MA and NV generally more stringent than others outside financial/health) – States have varying "privacy laws" that are generally applicable (e.g., state unfair/deceptive trade practices, online privacy, etc.)
	COPPA/Children, Video Privacy Protection Act (VPPA), Electronic Communications Privacy Act, Cable TV Act
By Activity	TCPA, CANSPAM
Standards	Payment Card Industry Data Security Standard (PCI-DSS)

New State Privacy Laws

State law trend toward comprehensive privacy laws

- California Consumer Privacy Act (CCPA) – Effective since January 2020
- California Privacy Rights Act (CPRA) – Most provisions effective January 1, 2023
- Virginia Consumer Data Protection Act (VCDPA) – Effective January 1, 2023
- Colorado Privacy Act (CPA) – Effective July 1, 2023
- Utah Consumer Privacy Act (UCPA) – Effective December 31, 2023
- Connecticut Data Privacy Act (CTPA) – Effective July 1, 2023



Graphic from International Association of Privacy Professionals (IAPP)

Who and What is Regulated

SQUIRE PATTON BOGGS

- Business/controller
- Personal information/personal data broadly defined
  - Not only obvious data like name and SSN, but also pseudonymous identifiers like cookie IDs, IP addresses and mobile ad IDs
- Consumer Privacy Rights businesses must offer and honor
  - Access, correct, delete, opt-out of sale, non-discrimination, etc.
- Significant obligations on businesses
  - Notification, vendor management, training, record keeping, etc.
- Stiff penalties under the laws
  - US$2,500 per violation (California)
  - US$7,500 per intentional violation (California)
- Limited private rights of action

Key Terms

- Business / Controller
  - Most states are focused on for-profit entities that meet certain thresholds
  - Thresholds in each state – most are based on the number of data subjects processed, but not in California
- Personal Information / Personal Data (different terms—essential similar meanings)
  - information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
  - Does not include publicly available information (definition differs by state) or de-identified or aggregate information.
- Exemptions/Exclusions
  - GLBA/Financial Institution; FCRA/Credit Reporting; HIPPA/Health; COPPA/Children; FERPA/Educational; DPPA/Drivers Information; Vehicles; Air Carriers; etc...
  - But note the California AG's recent enforcement examples…

Consumer Rights Across States

SQUIRE PATTON BOGGS

The following chart demonstrates the similarities and differences of the current US consumer privacy laws of general application, and compares them to the GDPR:

Consumer Right	GDPR	CCPA	CPRA	VCDPA	CPA	UCPA	CTPA	PICICA (NV)
Right to access	✓	✓	✓	✓	✓	✓	✓	x
Right to confirm personal data is being processed	✓	Implied	Implied	✓	✓	✓	✓	x
Right to data portability	✓	✓	✓	✓	✓	✓	✓	x
Right to delete[1]	✓	✓	✓	✓	✓	✓	✓	x
Right to correct inaccuracies/right of rectification	✓	x	✓	✓	✓	x	✓	x
Right to opt-out of sale	✓[2]	✓[3]	✓[3]	✓[4]	✓[3]	✓[4]	✓[3]	✓[5]
Right to opt-out of targeted advertising (CO, VA, UT, CT)/cross-context behavioral advertising sharing (CA)	✓	x[6]	✓	✓	✓	✓	✓	x
Right to object to or opt-out of automated decision-making	✓	x	✓[7]	x	x	x	x	x
Right to object to or opt-out of profiling[8]	✓	x	✓	✓	✓	x	✓	x
Choice required for processing of "sensitive" personal data?	Opt-In	x	Opt-Out[9]	Opt-In	Opt-In	Notice + Opp. to Opt-Out	Opt-In	x
Right to object to/restrict processing generally	✓	x	x	x	x	x	x	x
Right to non-discrimination[10]	Implied	✓	✓	✓	✓	✓	✓	x
Notice at collection requirement	✓	✓	✓	x	x	x	x	x
Specific privacy policy content requirements	✓	✓	✓	✓	✓	✓	✓	✓
Purpose/use/retention limitations	✓	Implied	✓	✓	✓	x	✓	x
Privacy and security impact assessments sometimes required	✓	x	✓	✓	✓	x	✓	x
Obligation to maintain reasonable security	✓	Implied	✓	✓	✓	✓	✓	✓

[1] In California and Utah, deletion obligations are limited to PI collected from the consumer, but in Virginia, Colorado and Connecticut, any PI collected about the consumer is in scope of the deletion right.

[2] Selling personal data under the GDPR generally would require the consent of the data subject for collection and would be subject to the right to object to processing.

[3] Any consideration sufficient, but required.

[4] Cash consideration required.

[5] In NV, website and online service operators are required to offer an "opt-out," but only for limited disclosures of certain information and only if the disclosure is made in exchange for monetary consideration.

[6] However, certain data disclosures inherent in this type of advertising are arguably a "sale," subject to opt-out rights.

[7] Subject to substantial expansion under CPRA regulations. Based on preliminary rulemaking activities, it appears that the CPPA is contemplating a GDPR-like approach for automated decision-making and profiling.

[8] CPRA's concept of profiling subject to change under the regulations. The profiling concepts in the other 2023 state privacy laws require legal or substantially similar effects.

[9] Under the CPRA, the Sensitive PI opt-out right applies to certain processing activities beyond business purposes that are to be defined in CPRA regulations.

[10] The CCPA (and likely the CPRA) take a more onerous approach to non-discrimination with respect to financial incentives and price/service differences, requiring businesses to prove that they are reasonably related to the value of the consumer's data to the business.

CPRA Changes

- Data Retention Schedules in the Privacy Policy
- HR Data and B-to-B Data – carve out sunsets on January 1, 2023
  - This data will be fully subject to all of the requirements of the CCPA/CPRA
  - As result, a business's CCPA/CPRA program will need to cover HR and B-to-B Data
- This is a significant change for businesses that do not touch traditional consumer data
- Pre-collection notices to applicants, employees and contractors are still required.
- Covered Businesses should:
  - Perform a gap analysis
  - Provide a full privacy policy to HR data subjects (content requirements in the Regulations)
  - Implement mechanism to accept HR data subject and B-to-B data subjects
  - Provide CCPA/CPRA rights to Shore up agreements with Service Providers

CCPA Enforcement Example

- First public settlement (naming the business) announced on August 24
  - Third Party Cookies and the Sale of PI
  - Failure to honor GPC
  - Alleged a violation of California's UCL (UDAP) but settlement was based only on alleged violations of CCPA
- $1.2m in civil penalties. AG's interpretation that each "sale" of PI or each failure to honor a GPC is an individual violation of the CCPA and thus the penalty amount can compound signification.
- AG also posted addition enforcement examples targeted:
  - Business that provides platform for virtual healthcare services (Non-Compliant Privacy Policy; Non-Compliant Notice of Collection)
  - FinTech (Non-Compliant Privacy Policy; Non-Compliant Opt-Out Process; Missing Notice)

Highlights From Federal Legislation

SQUIRE PATTON BOGGS

- High-sensitivity categories of information--SSN, biometric information, genetic information, non-consensual intimate images, “precise” geolocation, and physical activity from a wearable device. There would also be sensitive information, more broadly speaking, and only the sensitive information would be subject to sharing restrictions. (This would include browsing history.)
- Access, correction, deletion, and portability rights.
- An explicit requirement that for material changes in a privacy policy, you have to notify customers who had received the prior policy, and give them a chance to withdraw consents they had given.
- A broad-spectrum prohibition on discrimination in products or services, and large companies would have to do self-assessments of their algorithms for potential discrimination.
- Cybersecurity safeguards mirroring the federal requirements for financial institutions.
- A private right of action, starting 4 years after the effective date; coupled with an opportunity to get FTC approval for your compliance program, and following your FTC-approved program as a safe harbor.
- General preemption of state privacy laws.
- On September 1, Speaker Pelosi issued a statement on the ADPPA echoing California’s concerns on the ADPPA’s preemption provisions, and she has reportedly stated that she would not hold a vote on the ADPPA in its current form.

SQUIRE PATTON BOGGS

Vendor Management

Key DPA Concepts to Consider

SQUIRE PATTON BOGGS

- Controller (aka business) vs processor (aka contractor or service provider)
- What personal information/data is involved?
- What is the scope of processing?
- Is the transfer of data a “sale” subject to a consumer’s right to opt-out?
  - Service provider or contractor?
  - Sharing at the consumer’s direction vs. third parties that control the collection of personal information/data

Vendor Management Obligations

SQUIRE PATTON BOGGS

- What do these laws require controllers/businesses to do? Requirements include:
  - Restrict processors' use of personal information/data
  - Audit processors
  - Pass through consumer requests
  - Ensure processors are subject to duty of confidentiality
- What do these laws require processors/service providers to do? Requirements include:
  - Securely process personal information/data
  - Limit data use to providing services (with limited exceptions)
  - Assist with honoring consumer requests
  - Notify controller of breaches

DPA Requirements

SQUIRE PATTON BOGGS

- Limits vendor's use of PI to providing the contracted for services
- Restrict vendor from:
  - Selling or sharing PI
  - Processing PI outside of direct business relationship between the parties
  - Combining PI received from/on behalf of business with PI from other sources
- Require vendor to:
  - Comply with laws and notify business if can no longer meet obligations
  - Ensure PI security
  - Assist with consumer requests
  - Notify business of breach of security of PI and assist with response
  - Provide information for business to conduct data protection assessments
  - Delete PI at end of processing
  - Cooperate with audits
  - Provide business an opportunity to object to engagement of subcontractors

Other considerations

- Insurance?
  - What types and do you know what it covers?
- Limitations on Liability?
- Indemnification?

SQUIRE PATTON BOGGS

How are businesses meeting these requirements?

SQUIRE PATTON BOGGS

Data Privacy Objectives/Goals

- Protect Data Privacy by Design
- Protect Data Privacy by Default
- Support Regions in protecting personal data and lead Incident Response Teams
- Lead Center of Excellence

Privacy Performance Indicators

SQUIRE PATTON BOGGS

A. Align with business initiatives and realities

B. Function as enabler within sound privacy parameters to assist with privacy and data security issues

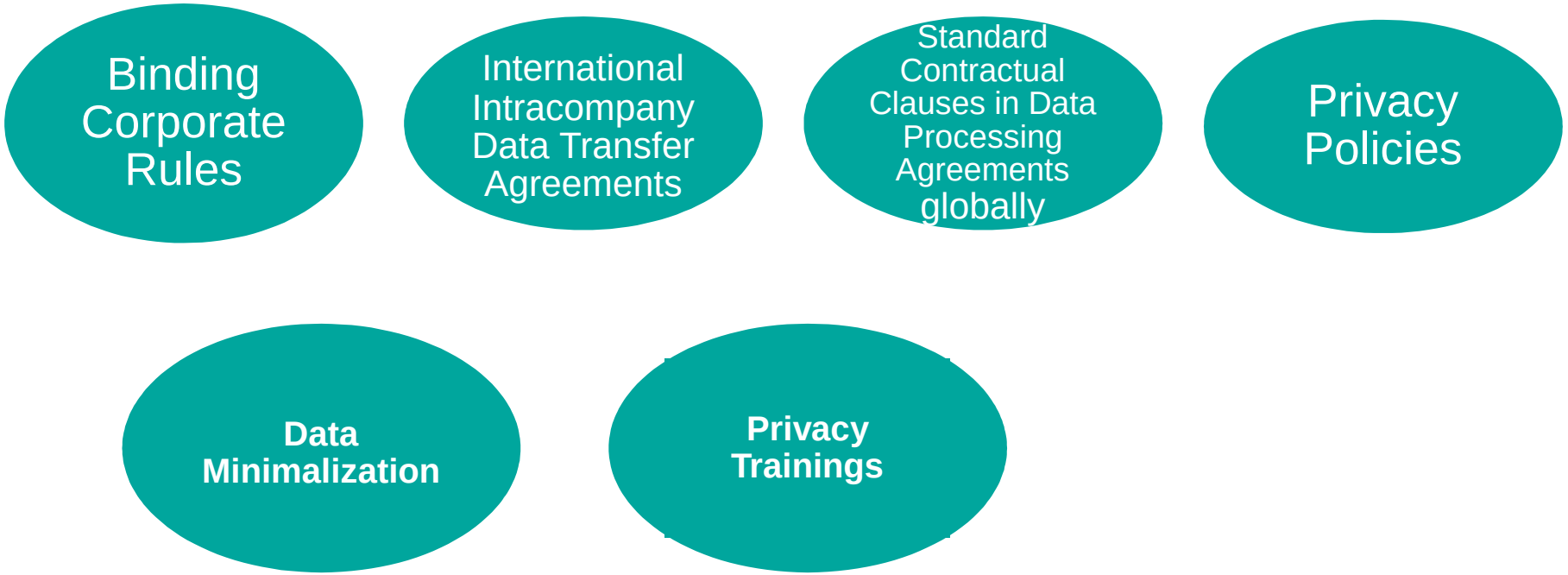
C. Visibility across relevant business units and across the global legal function as a whole

D. Implement Privacy and Data Security Policies, Procedures and Best Practices

E. Establishing and implementing Standards, Policies, Guidelines, Procedures, Best Practices, Systems, Tools and Templates

F. Conducting trainings globally

Privacy By Design Safeguards



How to Implement Privacy Safeguards

SQUIRE PATTON BOGGS

- Map personal data
- Support colleagues with privacy hotline
- Implement and update Regional General Data Protection policies in compliance with ever changing privacy landscape globally.
- Stay current on ever changing privacy regulation landscape globally.
- Create Standard Contractual Clause Templates and add to data processor agreements.
- Conduct Data Protection Impact Assessments where needed.
- Implement and monitor Individual Rights Data Subject Tools as required by local privacy laws using automated system, if possible
- Prepare, obtain and store consents where needed.
- Update Intra-Company International Data Transfer Agreements as needed.
- Data minimalization and designation of sensitive data in corporate recordkeeping (using automated system, if possible).
- Continuous privacy trainings globally.

EU Data Transfer Recommendations

SQUIRE PATTON BOGGS

Privacy and Data Security

SQUIRE PATTON BOGGS

A. Documents Retention Timeframe Updates -- LESS IS BETTER

B. Data Minimization and Designation of Sensitive Data

C. Revamp Data Storage and Retention to Create Efficiencies

D. Privacy Policy Implementation and Updates in line with new laws

E. Update DSAR Procedures and Automate in line with new laws

F. Conduct trainings

G. Tabletop exercises, audit vendors, retain forensic investigator and obtain cyber insurance

Steps to Take by Year-end

SQUIRE PATTON BOGGS

1. Assess readiness and conduct a gap analysis and develop a project plan
2. Update data inventory
3. Revise notices, policies and procedures
4. Refine consumer request program
5. Implement impact assessment program
6. Update data protection agreements and reassess the status of data disclosures and recipients
7. Complete data retention schedule and program implementation
8. Implement reporting, record-keeping and training
9. Shore-up data security and breach preparedness
10. Determine if all US consumers will get all rights (i.e., the highest level) regardless of residency, or develop and rollout a state-by-state approach

ConsumerPrivacyWorld.com

SQUIRE PATTON BOGGS

Scan the QR CODE to visit SPB's blog and subscribe to stay informed on the evolving law on data privacy, security and innovation.

Or email us at:

Shea Leitch

shea.leitch@squirepb.com

Kyle Dull

kyle.dull@squirepb.com