IMPLEMENTING PRIVACY PROGRAMS IN A RAPIDLY EVOLVING COMPLIANCE CLIMATE

April 2021
JAMES AMSLER
FIP, CIPM, CIPT, CIPP/E, CIPP/US
Director, Governance, Risk & Compliance
BDO Digital

615-493-5681
jamsler@bdo.com
Key Topics

1. Introduction to Data Protection
2. Key Regulations
3. Data Protection Obligations
4. What’s Next?
Introduction to Data Protection
Tell me about you!

What is your role in your Organization’s (or Clients’) Data Protection Program?

A. I own it entirely.
B. Supporting the Program is a key part of my responsibilities.
C. I deal with this from time to time.
D. What Data Protection Program?
E. I have no idea what this is.
Privacy and Data Protection Law

Comparing And Contrasting Key Terms

**PRIVACY**
Respect for...
- Private life
- Family life
- Home
- Communications

**DATA PROTECTION**
Protection of personal data
- Fair processing
- Specified purposes
- Consent or lawful grounds
- Access and rectification
The “Targeted Buying Experience”
Is This You?

“I’m a frequent coffee drinker, I’m part of the club. I have a card.

Do you have a card?”

- Will Ferrell, Kicking and Screaming (2005)
According to Boston Retail Partners, 37 percent of retailers use more personalized service as an incentive to have consumers identify themselves.
Attitudes on Data Protection Among U.S. Consumers

Says a company’s ability to keep their data privacy is extremely important

78%

Say businesses focus on profits over protecting consumers’ privacy rights

73%

How many household brands can you name have publicly announced breaches of personal data in the last 2 years?

Source: Harris Poll for IBM, online survey of 2,039 U.S. Adults March 27-29
Consumers’ Level of Trust

Source: PWC online and video survey of 12,000 U.S. adults, Aug-Sept 2017
What Do I Really Need To Know About Data Protection?

All regulations and frameworks address:

1. Right to Access
2. Right to be Forgotten
3. Breach Notification
What Is My Right To Access?

Upon request, a company must provide a copy of an individual’s personal data, including:

- Copy of the data (free of charge)
- Purpose of processing
- Data types being processed (name, address, etc.)
- Retention periods
What Is My Right To Be Forgotten?

• AKA, Right of Erasure
• Primary paint point
• Data may reside on multiple systems, platforms, and storage mechanisms
• Many organizations don’t know where the data is
• GDPR and CCPA don’t care how difficult this is to enforce
• Solution: Actively purge data that is no longer needed
• This right is not absolute and may be refused
What Is Breach Notification?

- May or may not be mandatory
- Is the breach likely to “result in a risk for the rights and freedoms of individuals”
- Many organizations already have mature breach notification regimes in place
- State-level Breach Notification Laws (50! Finally!)
- GDPR: 72-hour notification requirement
Summing It Up

Privacy is Contextual

2 Themes (so far)
- Privacy exists in Tension with other rights and concepts
- Paradox between how people value protection of their data, and yet share it freely

Organizations must support individuals’ rights to:
- Know what information companies collect about them
- Request actions on their data, including deletion
- Be notified if their information has been breached or mishandled in some way
Key Regulations
It’s Not Just About Laws and Compliance

- Compliance
- Safeguard Data
- Reduce Risk of Lawsuits
- Increase Revenues

- Meet External Expectations
- Enhance Reputation and Brand
- Value of Information Assets
Data Protection Around the World

- Canada
- U.S.
- Europe
- Asia-Pacific
- China
- Africa
- Australia
- Latin America
- New Zealand
- Japan
- New Zealand
History of European Data Protection

1948 - Universal Declaration of Human Rights (UN)

1950 - European Convention on Human Rights (Council of Europe)


1981 - Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (‘Convention 108’)

1995 - Data Protection Directive

2000 - eCommerce Directive
GDPR Overview

BE AWARE OF ...
What consumers can do, organizations must do, regulators may do
GDPR Enforcement Isn’t Only About the Fines

CCPA Overview

BE AWARE OF ...
What consumers can do, organizations must do, regulators may do
GDPR and CCPA Summaries

- Restrictions on how and why businesses can process personal data
- Additional protections for sensitive personal data
- Privacy by design and privacy by default
- Opt-in consent when consent is required

- Personal data includes data about devices and households
- Right to object/opt out only covers the sale of personal information
- Access rights to personal information limited to PI collected in the past 12 months
California Privacy Rights Act (CPRA)
SUPPLEMENTS THE CCPA

Privacy Regulatory Agency
Whereas CCPA is managed by the California Office of the Attorney General, the CPRA creates the Consumer Privacy Protection Agency to oversee and enforce the law, the first such privacy regulatory agency in the U.S.

Data Sharing Definitions
CPRA extends data SALE rights from CCPA to include data SHARING practices. The law also creates new definitions for CONTRACTOR and SERVICE PROVIDER, along with new contract requirements.

Sensitive Personal Information (SPI)
CPRA creates the SPI data category with additional privacy requirements and rights. SPI includes data elements such as Social Security Number, financial account details, geolocation, biometric and genetic data, health information, and more.

Expanded Consumer Rights
CPRA expands on the rights afforded to data subjects under CCPA, to include a right to rectification, and processing/disclosure restrictions for Sensitive Personal Information.
Virginia Consumer Data Protection Act

CDPA

SUMMARY

The Virginia Consumer Data Protection Act (CDPA) will go into effect on January 1st, 2023 and will regulate consumer privacy and data protection in the State of Virginia.

The CDPA defines a “Consumer” as a natural person who is a resident of the Commonwealth acting only in an individual or household context. This definition specifically excludes individuals acting in a commercial or employment context. Therefore, the Act does not apply to the processing of employee data or personal data processed in the context of Business-to-Business activities.

Defines a new Consumer Right of Repeal: The controller shall establish a process for a consumer to appeal the controller’s refusal to take-action on a request within a reasonable time after the consumer’s receipt of the decision.

WHO MUST COMPLY?

According to the CDPA, companies that must comply if they conduct business in the Commonwealth of Virginia or produce products or services that are targeted to Virginia residents, and in a calendar year either:

- Control or process personal data of at least 100,000 consumers;
- Control or process personal data of at least 25,000 consumers; and derive over 50% gross revenue from the sale of personal data.

ENFORCEMENT

The CDPA:

- Does not define a private right of action.
- Allocates exclusive authority to the Attorney General.
- Defines a 30-day period, once the controller/processor is notified by the attorney general of a violation, by which time the controller/processor must cure the violation and provide the attorney general with an “express written statement that the alleged violation has been cured and that no further violations shall occur”.
- Specifies a $7,500 fine for each uncured violation.
- Allows the attorney general to recover reasonable expenses and attorney fees incurred in investigating or preparing the case.
# Comparison of Key Privacy Regulations

## KEY ELEMENTS

<table>
<thead>
<tr>
<th>KEY CONCEPTS</th>
<th>CCPA &amp; CPRA (California)</th>
<th>GDPR (EU)</th>
<th>CDPA (Virginia)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who is required to comply?</td>
<td>▶ Revenues &gt;$25 million+ OR ▶ Data on (CCPA: 50,000+, CPRA: 100,000+) CA residents, households, devices (CCPA only) OR ▶ 50% of revenues are from selling PI</td>
<td>▶ Offering goods or services to EU residents OR ▶ Monitoring behavior of EU data subjects OR ▶ Established in the EU</td>
<td>▶ Entities that conduct business in the Commonwealth of Virginia or produce products or services that are targeted to residents ▶ Processes or controls personal data on at least 100,000 consumers per year ▶ Processes or controls personal data on at least 25,000 consumers and derive at least 50% of its gross revenue from sale of personal data</td>
</tr>
<tr>
<td>Requires Legal Basis of Processing</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Requires fair, lawful, and transparent processing, purpose limitation, data minimization, storage limitation, accuracy, integrity, confidentiality, accountability</td>
<td>CCPA: No - only transparent processing is mandated CPRA: No - only data minimization, purpose limitation, and storage limitation are mandated</td>
<td>Yes</td>
<td>Yes-requires transparent processing, purpose limitation and data minimization</td>
</tr>
<tr>
<td>Requires international cross-border transfer safeguards</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Regulator</td>
<td>CCPA: California Attorney General CPRA: California Privacy Protection Agency</td>
<td>Data protection/supervisory authorities in member states</td>
<td>Virginia Attorney General</td>
</tr>
<tr>
<td>Potential Fines</td>
<td>▶ General Violation: Action up to $2,500 ▶ Intentional Violation: Action up to $7,500 ▶ Minor’s Data Violations: Action of $7,500 or actual damages</td>
<td>▶ Up to 2% of global annual turnover for lesser infringements ▶ 4% of global turnover or 20M Euros (whichever is higher)</td>
<td>▶ If the controller fails to cure violation within the 30-day period, the attorney general may fine up to $7,500 per violation</td>
</tr>
</tbody>
</table>
## Comparison of Key Privacy Regulations

### KEY ELEMENTS

<table>
<thead>
<tr>
<th>KEY CONCEPTS</th>
<th>CCPA &amp; CPRA (California)</th>
<th>GDPR (EU)</th>
<th>CDPA (Virginia)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statutory Damages/ Private Right of Action</td>
<td><strong>CCPA</strong>: Action available if unredacted or unencrypted personal information has been breached. <strong>CPRA</strong>: Action also available if email address, password, or security question and answer are breached</td>
<td>EU citizens can pursue compensation claims against controllers or processors for damages</td>
<td>No private right of action</td>
</tr>
<tr>
<td>Resolution Timeframe (Cure Period)</td>
<td>Within 30 days of being notified</td>
<td>Not applicable</td>
<td>Within 30 days of being notified</td>
</tr>
<tr>
<td>Breach Notification Timeframe</td>
<td>Prescribed in CA’s Breach Notification Law, California Civil Code. Division 3, Part 4, Title 1.81, Section 1798.82: Without undue delay, as quickly as possible</td>
<td>Without undue delay and, where feasible, not later than 72 hours after becoming aware of a breach</td>
<td>Without undue delay</td>
</tr>
<tr>
<td>Consumer Access Request Response Timeline</td>
<td>45 days</td>
<td>30 days</td>
<td>30 days</td>
</tr>
<tr>
<td>Do Not Sell My Personal Information Posted on Website</td>
<td>Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>Ability to Offer Incentives in Exchange for Data</td>
<td>Permissible</td>
<td>Permissible, but adopt with caution</td>
<td>Not Permissible</td>
</tr>
<tr>
<td>Opt-in-Consent for Minors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right of Portability, Access and Deletion</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to Rectification</td>
<td><strong>CCPA</strong>: No, <strong>CPRA</strong>: Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Right to object to processing and automated decisions</td>
<td><strong>CCPA</strong>: No, <strong>CPRA</strong>: Additional Guidance Expected</td>
<td>Yes</td>
<td>No however, if the controller sells personal data to third parties, or engages in targeted advertising, the controller must provide consumers means to opt out. Yes</td>
</tr>
<tr>
<td>Requires Data Protection Officers</td>
<td>No</td>
<td>Yes, in certain cases</td>
<td>No</td>
</tr>
</tbody>
</table>
Privacy Laws by Industry

- Energy
- Human Resources
- Marketing
- Government
- Healthcare
- Financial
- Telecom
- Online

Sector-based and contextual laws
Cross Border Transfers

- Adequacy decisions
- Appropriate safeguards
- Derogations

Adjust the privacy program to the most stringent legal requirements to which the processing is subject.
Balancing Compliance and Corporate Strategy
Data Protection Obligations
The Role of Internal Audit

“Nothing exists.”
Compliance Obligations are Constantly Evolving

New laws and regulations are constantly emerging.

Laws such as the CCPA and proposed NYPA define overlapping requirements, but also include key differences.

How can organizations adapt to constantly changing, sometimes complimentary, and sometimes contradictory compliance requirements?
Privacy Compliance Journey

<table>
<thead>
<tr>
<th>1</th>
<th>Assess</th>
<th>Personal data sources &amp; flows</th>
<th>Governance &amp; operating model</th>
<th>Collection, aggregation, use, storage, sharing/selling, disposition notices and policies</th>
<th>Service provider &amp; third-party contracts</th>
<th>Risk-prioritized roadmap &amp; action plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Design</td>
<td>Personal data sources &amp; flows classifications</td>
<td>Governance &amp; operating model</td>
<td>Notices, policies &amp; procedures</td>
<td>Service provider &amp; third-party contract T&amp;Cs</td>
<td>Consumer requests response workflows</td>
</tr>
<tr>
<td>3</td>
<td>Implement</td>
<td>Technical, organizational, administrative controls</td>
<td>Governance &amp; operating model</td>
<td>Notices, policies &amp; procedures updates</td>
<td>Renegotiated service provider/ third-party contracts</td>
<td>Consumer requests center</td>
</tr>
<tr>
<td>4</td>
<td>Monitor &amp; Govern</td>
<td>Consumer requests center &amp; breaches</td>
<td>Maintain required documentation</td>
<td>Iterate &amp; improve</td>
<td></td>
<td>Turnkey privacy compliance program</td>
</tr>
</tbody>
</table>
FTC Guidance on Data Protection Obligations

The FTC has made “reasonable data security and protection” a legal requirement. The FTC’s documented obligations for companies include:

1. **Take Stock** - Inventory your PI and know where it is located
2. **Scale Down** - Minimize the data that you store to is business purpose
3. **Lock It** - Physical, Electronic, Processes, Education
4. **Pitch It** - A good case for a solid *Electronic Records Management* implementation
5. **Plan Ahead** for the eventual data breach in the organization
What’s next?
Theme: Technology Leads, Regulations Lag
Technology-Driven Privacy Threats

- Machine Learning
- Geo-Tagging
- Facial Recognition
- Drones
- Tracking / Surveillance
- Internet Monitoring
- Audio / Visual Surveillance
- Vehicular Automation
- Wearable Devices
- Location Tracking
- Social Media Bots
- Context Aware Computing
- Web Tracking
- Anthropomorphism
Drones

Any type of audio or video surveillance can be privacy invasive and the objectives for performing it should outweigh the privacy drawbacks and risks.
Anthropomorphism

SPEECH RECOGNITION

- Smart phones
- Remote controls
- Home smart speakers
Questions?
BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 700 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 88,000 people working out of nearly 1,800 offices across over 160 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

www.bdo.com