Auditing Data Privacy in a Post-GDPR World
Agenda

- Which Privacy Law Applies to Me?
- Regulatory Overview
- Security and Privacy Considerations
- Internal Audit Considerations
- Q&A
Which Privacy Law Applies to Me?
Regulatory Drivers for Privacy

Historical Drivers

- Gramm-Leach-Bliley Act - Financial Information.
- Family Educational Rights and Privacy Act (FERPA) - Student Records.
- Health Insurance Portability & Accountability Act (HIPAA) - Health Information.
- Payment Card Industry Data Security Standard (PCI DSS).
- Individual State Laws.

Emerging Drivers

- California Consumer Privacy Act (CCPA) “GDPR”-like requirement for California businesses and residents.
- Brazilian General Data Protection Law (LGPD) “GDPR”-like requirement for Brazilian businesses and residents.
Does GDPR Apply to Me?

- Applies to:
  - Organizations with establishments or operations in the EU.
  - Organizations not located in the EU, if they offer free or paid goods or services to EU residents or monitor the behavior of EU residents.
- Applies to both EU customers and EU employees for all businesses subject to the law.
- A breach of the GDPR can result in a fine of up to 4% of annual global turnover or €20 million (whichever is greater).
Does CCPA Apply to Me?

Applies to Any for-profit entity doing business in California, that meets one of the following:

- Firms that have global gross revenue over $25 million annually
- Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices.
- Derives 50% or more of its revenues from selling personal data.

An establishment in California is not required to be subject to this law.

Will be Implemented on January 1, 2020 and enforcement will begin as soon as July 1, 2020

Will be the most stringent US privacy law to date and carries fines of $2,500 - $7,500 per data subject.
Does LGPD Apply to Me?

- Applies to all companies that have an establishment in Brazil, or offer services to the Brazilian market must comply by August 1, 2020.
- Rights extend to Brazilian customers, employees and/or contractors of all businesses subject to the law.
- A breach of the LGPD can result in a fine of up to 2% of annual global turnover or R$50 million (whichever is greater).
- Data subject rights and regulatory requirements closely follow those of the GDPR.
Looking Ahead…

Potential for a U.S. Federal Data Privacy Law

- Many industry giants, such as Facebook, Apple, Google and Microsoft, have declared support for a stringent U.S. federal data privacy law. Such legislation is currently being considered by Congress.

- Apple CEO, Tim Cook, recently praised Europe's "successful implementation" of the GDPR, and said that "It is time for the rest of the world … to follow your lead. We at Apple are in full support of a comprehensive federal privacy law in the United States."

- Many believe such a law must contain a preeminence clause, effectively voiding state laws, such as the CCPA.

- Until such a time, businesses must be aware of potential privacy legislation in states which they conduct business.
Academic Institution Hypothetical

- Academic Institution located in the US
- International Students from the EU
  - Accepts Applications from EU Residents
  - Direct mailing and marketing to EU addresses
- Relationships with EU universities
  - Coordinated study abroad programs
- Offers distance learning programs to all English speakers, regardless of where they live
Oil and Gas Hypothetical

- Oil and Gas company located in the US
- No EU customers or employees
- Has salespeople in each US state.
- No direct operations in the EU
- Contracts with vendors who operate in the EU, South America, and shares employee data with your company.
**Financial Institution Hypothetical**

- US based bank with no branches in the EU
- Targets a global audience through online ads
- Serves customers in each US state
- Allows non-residents to apply for credit or open an account using an ITIN instead of a SSN.
Healthcare Hypothetical

- US based hospital specifically targets Residents Across the EU and US to promote medical travel
- Hospital conducts medical research and accepts patients from the EU in the program.
- Hospital maintains a partnership with an EU-based medical facility and exchanges employee or provider personal information
- Hospital or provider offers tele-health services to EU residents.
What about Professional Services Firms?

- Law Firms?
- Consultants?
- Auditors?
- Marketing Agencies?

How to define the lawful basis and the legitimate interests of clients?
Regulatory Overview
Key Elements of the GDPR

- Expansion of Territorial Scope (Article 3)
- Lawfulness of Processing (Article 6)
- Consent (Article 7)
- Data Rights (Articles 12-23)
- Third Party Management and Processing Agreements (Articles 27-30)
- Secure Processing (Article 32)
- Breach Response and Notification (Articles 33-34)
- Data Protection Impact Assessment (Article 35)
- Data Protection Officer (Article 37)
- Cross-Border Data Transfers (Articles 44-49)
Cross-Border Data Transfers

Cross-border transfers of EU originated data to the United States is prohibited under the GDPR, unless one of three requirements are met:

- Standard Contractual Clauses
- Binding Corporate Rules for data transfer
- Certification Under the Privacy Shield Framework

Privacy Shield is a program sponsored by the FTC and DOC which companies can self-certify under showing they are committed to following the privacy principles of the GDPR.
Privacy Shield: Steps to Certification

1. Map out your data footprint and security controls
2. Determine how HR data will be handled. Contractual Clauses or Privacy Shield?
3. Create and post a GDPR compliant Privacy Policy online
4. Establish a process to handle customer requests for access, correction, retention and erasure.
5. Assess data sharing practices with vendors and attach a Data Processing Addendum (DPA) to each contract
6. Establish a means for verifying compliance annually
7. Select an Independent Recourse Mechanism for customers
8. Nominate a Privacy Shield Contact Person
9. Self-Certify on Privacy Shield’s website and wait to receive your certificate
GDPR Penalties

• The most serious infringements:
  • Not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. - the greater of 4% of global revenue or €20 million
  • A company could be fined the greater of 2% of global revenue or €10 million for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment.
  • Retroactive penalties? EU Justice Commissioner Vera Jourová said the new GDPR rules "cannot be applied in this [Facebook Cambridge Analytica scandal], because there's no retroactivity possible."
  • If the Facebook Cambridge Analytica breach had been reported after May 25, 2018, Facebook could have faced fines of up to €1.3 billion.
Google fined $57 Million Under GDPR

• Google’s U.S. entity was fined $57 million in January 2019 for failure to comply with GDPR consent requirements.

• Google allegedly built advertising profiles on EU residents from Android phone use without plainly explaining what they were doing with user data or obtaining consent in a manner consistent with the GDPR.

• The French Supervisory Authority maintained that Google lacked transparency with users, provided inadequate processing details and did not request valid consent regarding ad personalization.

• The Supervisory Authority noted that having such details multiple clicks away from the Privacy Policy was not adequate.
GDPR Readiness

1. Have you appointed a DPO?
2. Do you know your EU data footprint?
3. Have you conducted a compliance assessment?
4. Have you inventoried all systems processing GDPR data?
5. Are you aware of all usages of your customer and employee data?
6. Have you updated your governance structure to ensure ongoing compliance?
7. Have you implemented processes to achieve reporting requirements with Supervisory Authorities?
8. Have you implemented processes to address customer requests for personal data access, correction, retention and erasure?
9. Have you determined what legal means you will use for cross-border data transfers?
10. Have you implemented privacy by design?
Security and Privacy Considerations

“You can have security without privacy, but you can’t have privacy without security.”
Security and Privacy Relationship

Security
• Confidentiality
• Integrity
• Availability

Privacy
• Data usage, lawful processing, individual consent
• Rights of the Individual
• Retention and preservation
• Breach notification
Control Examples

Security Controls
• User Access Controls

Privacy Implication
• Minimum necessary
• Need to know
Control Examples

Security Controls
- Encryption and Hashing

Privacy Implication
- Privacy law safe harbor
- Pseudonymization
Internal Audit Considerations
**Internal Audit’s Role**

• Data privacy requires a shift in focus from the business. A focus on security, although potentially beneficial for privacy, does not ensure the business is protecting data via policies and procedures, robust processes, and governance.

• Internal audit can play a much needed role in:
  1. Assessing the status of compliance with privacy regulations and
  2. Identify risks and safeguards related to data privacy.

Taking on these roles will guide the business towards responsible data stewardship.

**Importance of Strong IT Governance and Data Governance**
Data Privacy Objectives

- Secure Processing
  - Encryption of data at rest and data in motion.
  - Access control to ensure the minimum necessary.
  - Data loss prevention (DLP) controls.
  - Integrity controls.

- Data Rights of the Individual
  - Right to: access, erasure, rectification, portability.

- Breach Notification
  - Breach risk assessment.
  - Notification timelines (72 hours - GDPR, 60 days - HIPAA, etc.).

- Third Party Risk Management
  - Vendor due diligence activities.

- Data Retention and Disposition
Scoping a Data Privacy Assessment

Scoping Example: Higher Ed Data Processing

*Enterprise Level Data Processing*
- Accounting and Finance
- Human Resources and Payroll

*Institution Level Data Processing*
- Student Records
- Marketing

*Department Level Data Processing*
- Research and Grants
- Clinical / Health Services
## eCommerce Privacy Assessment Example

<table>
<thead>
<tr>
<th>Processing Level</th>
<th>Data Processing</th>
<th>Sensitive Data Overview</th>
<th>Privacy Compliance Requirement</th>
<th>Data Privacy Objective</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Payments</td>
<td>Online payment processing for customers through eCommerce site.</td>
<td>PII, CHD, GDPR Data</td>
<td>• PCI • GDPR</td>
<td>Policies and procedures are in place to fulfill erasure requests from customers.</td>
<td>▪ Retention requirements for data have been defined. ▪ Lawful basis for continued data process has been defined. ▪ Customers have an electronic means for making erasure requests. ▪ Data on archive media is appropriately purged as needed.</td>
</tr>
</tbody>
</table>
### Higher Ed Data Privacy Assessment Example

<table>
<thead>
<tr>
<th>Processing Level</th>
<th>Data Processing</th>
<th>Sensitive Data Overview</th>
<th>Privacy Compliance Requirement</th>
<th>Data Privacy Objective</th>
<th>Privacy Controls</th>
</tr>
</thead>
</table>
| Department – Grants | Grant to perform a study of high school graduation rates in the State of California. | PII of K-12 student population. | • FERPA  
• CCPA | Ensure appropriate Data Retention requirements are implemented for research grant data. | All PII is anonymized prior to archiving. |

<table>
<thead>
<tr>
<th>Processing Level</th>
<th>Data Processing</th>
<th>Sensitive Data Overview</th>
<th>Privacy Compliance Requirement</th>
<th>Data Privacy Objective</th>
<th>Privacy Controls</th>
</tr>
</thead>
</table>
| Enterprise – Marketing | Alumni Donations | University Student PII | • FERPA  
• GLBA | Graduating students consent to alumni marketing related activities. | Students are provided data privacy consent forms prior to graduation describing data usage by the University after graduation. |
Q&A