GDPR ESSENTIALS
END-USER COMPLIANCE TRAINING
POTENTIAL MAXIMUM GDPR PENALTY

1 Walmart

Revenue: $482B

Profits: $15B

GDPR Fine: -$19B
WHAT IS DATA PRIVACY?
MOST NOTABLE US/CA PRIVACY LAWS

- Federal Trade Commission Act, Section 5
- California Online Privacy Protection Act (CalOPPA)
- State data breach notification laws
- Health Insurance Portability and Accountability Act (HIPAA)
- CAN-SPAM and COPPA
How is GDPR relevant for US companies? What happens in cases of non-compliance?

- GDPR not only applies to organizations located within the EU, but it also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects.

- Applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of company’s location.

- Organizations can be fined up to 4% of annual global turnover, or 20,000,000 Euros, for non-compliance. The owners, shareholders, or members of a corporation can be held personally liable for corporate debts (Art. 82).
• World’s largest professional association dedicated to privacy
• 40,000+ Members Worldwide in 110 countries
• 15,000+ Certified Individuals
• IAPP’s mission: To define, promote and improve the privacy profession globally
WHAT’S REQUIRED?
WHAT DATA PRIVACY SKILLS ARE NEEDED?
Article 39: The data protection officer shall have at least the following tasks:
(1b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits

Article 47:
(2h)...the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling
(2n)...the appropriate data protection training to personnel having permanent or regular access to personal data

Article 70: The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:
(1v) promote common training programmes...
GDPR ESSENTIALS

- IAPP compliance eLearning offering: GDPR Essentials
- Two modules
  - Data Privacy Essentials
  - General Data Protection Regulation (GDPR)
- Estimated training time is 45-60 minutes
- Requires employee to pass inline assessments to receive passing score
- No tailoring/customization to eLearning content (can add additional documents/links to CHOICE platform)
- Available in the following languages:
  - British English
  - French
  - German
  - Italian
  - Universal Spanish
1. OTP must sign new OTP agreement which includes option to resell GDPR Essentials

2. OTP can sell to any client with up to 50k employees globally; >50k employees option to refer to IAPP and receive 30% referral fee
   - Ex: Facebook ~25k employees = Direct; Google ~85k employees = Referral

3. OTP to provide LO Customer Service with following for each client:
   a. Signed GDPR Essentials client agreement (1 per client)
   b. Client global employee count
   c. Client website

4. Customer Service will process order providing a multi-use key with the maximum number of uses within the tier. For example, if 3,000 global employees multi-use key with maximum of 5,000 redemptions is provided
   - Note: GDPR Essentials is available through LO CHOICE only – not available to be delivered through any 3rd party LMS systems; would need to refer to IAPP

5. LO to provide CHOICE compliance reporting to OTP (4 reports included, additional provided at additional fee)
**Investment**

<table>
<thead>
<tr>
<th>Min Employees</th>
<th>Max Employees</th>
<th>OTP Price</th>
<th>Client SRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>$3,900</td>
<td>$5,070</td>
</tr>
<tr>
<td>101</td>
<td>500</td>
<td>$5,265</td>
<td>$6,845</td>
</tr>
<tr>
<td>501</td>
<td>1,000</td>
<td>$7,020</td>
<td>$9,126</td>
</tr>
<tr>
<td>1,001</td>
<td>2,000</td>
<td>$9,126</td>
<td>$11,864</td>
</tr>
<tr>
<td>2,001</td>
<td>5,000</td>
<td>$12,285</td>
<td>$15,971</td>
</tr>
<tr>
<td>5,001</td>
<td>10,000</td>
<td>$17,550</td>
<td>$22,815</td>
</tr>
<tr>
<td>10,001</td>
<td>20,000</td>
<td>$25,272</td>
<td>$32,854</td>
</tr>
<tr>
<td>20,001</td>
<td>30,000</td>
<td>$31,590</td>
<td>$41,067</td>
</tr>
<tr>
<td>30,001</td>
<td>50,000</td>
<td>$35,100</td>
<td>$45,630</td>
</tr>
</tbody>
</table>

*Note: Pricing is based on the number of global employees*
Questions?
• Certified Information Privacy Professional (CIPP)
  • Privacy laws, regulations and frameworks: the “What” of data protection

• Certified Information Privacy Manager (CIPM)
  • Implementing privacy in an organization: the “How” of privacy from a management perspective

• Certified Information Privacy Technologist (CIPT)
  • Implementing privacy in applications and systems: the “How” of privacy from a technology perspective

NOTE: CIPP, CIPM and CIPT are all accredited under ISO standards
A 4-day program covering both the what and the how of information privacy, providing both knowledge of privacy laws and practices.”
BENEFITS OF IAPP CERTIFICATION AND MEMBERSHIP

• IAPP certifications are ANSI-accredited to rigorous ISO standards
• Membership provides support throughout a career, extending beyond the few days of training
• Access to a network of 40,000+ data protection professionals around the world
• Largest privacy and educational events in the world (Washington, DC, Brussels, Toronto, Singapore and more)
• Daily e-news digest (The Daily Dashboard) for top privacy stories from
• Extensive online Resource Center and ongoing research
• Local KnowledgeNet (chapter) networking/educational meetings
Article 33: Notification of a personal data breach to the supervisory authority:
(1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it...

Article 34: Communication of a personal data breach to the data subject
(1) When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay
## INCIDENT RESPONSE PREPAREDNESS

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Threats and Attacks</td>
<td>24%</td>
</tr>
<tr>
<td>2.0 Data Collection and Analysis</td>
<td>23%</td>
</tr>
<tr>
<td>3.0 Incident Response Methods, Tools, and Techniques</td>
<td>22%</td>
</tr>
<tr>
<td>4.0 The Incident Response Process</td>
<td>18%</td>
</tr>
<tr>
<td>5.0 Vulnerability Assessment</td>
<td>13%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
CYBER & DATA PRIVACY COMBINED LEARNING PATH

SECURITY and PRIVACY PROFESSIONALS

End User
- All Staff
- CyberSAFE
- Privacy Core

IT PROFESSIONAL
- Foundational
  - A+
  - Network+
  - CloTP
  - Security+
  - CIPP
- Intermediate
  - CFR
  - CySA+
  - CIPT
  - CSC
- Specialist
  - Manager/Other
    - CIPM
    - CASP
    - CISPP
    - ISO 27001
    - RESILIA

Logical Operations: CyberSAFE, CloTP, CFR, CSC
CompTIA: A+, Network+, Security+, CySA+, CASP
ISC2: CISSP
IAPP: Privacy Core, CIPP, CIPM, CIPT
OTHER: ISO 27001, RESILIA
CYBERSECURITY VS DATA PRIVACY – OR IS IT?

**CYBERSECURITY**
- Keeping Data Safe
- Protecting
- Maintaining
- Controlling

**DATA PRIVACY**
- Security
- Collection
- Use
- Handling
- Sharing