
Data Privacy
integrity
Ethics & Compliance Training

integrity
Ethics & Compliance Training

Topic 1 – What Is Data Privacy?

1. **Video**: Every time you go online or fill out a form, you give away information about yourself. Keep clients' information private. Ethical and legal obligation to keep information private.
2. **Interactive Screen**: What do data privacy rules apply to? Types of data. Terminology, PII in the US, personal data in Europe. Know the types of data we hold, where data is held, what it's used for and the consequences of a breach.
3. **Interactive Screen**: What is the GDPR? Who does it apply to? Penalties. Consent.
4. **Interactive Screen**: Rights of data subjects under GDPR. Breach notification. Right of access. Right to be forgotten. Data portability.
5. **Scenario**: Unsolicited calls and mailshots from a marketing company. How did they get information?
6. **Key Learning**: Your name, address, and telephone number can all be used to uniquely identify you, as can your login and payment details for retail sites. All this data is classified as personal data/PII.
7. **Scenario**: The pieces of data that can be used to identify an individual.
8. **Key Learning**: It's important that you know what data qualifies as personally identifiable information and understand how PII can be combined to identify an individual.
9. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 2 – The Consequences of a Data Breach

1. **Interactive Screen**: Real-life examples of the consequences of a data breach.
2. **Scenario**: Clicking on a link in a suspicious email.
3. **Key Learning**: Phishing attacks attempt to gain sensitive information by pretending to be from a friendly source. Official sources will never email or text you looking for login or account details.
4. **Scenario**: Consequences of installing malware by mistake.

5. **Key Learning**: Introducing malware to our network would have huge repercussions. Malware may steal workplace login details and place our company and our clients' data at risk.
6. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 3 – Protecting Data

1. **Text & Image Screen**: We all have a responsibility to protect the data of our clients and employees. Privacy incidents are often caused by people making simple mistakes out of line with our policies.
2. **Interactive Screen**: Principles of data protection: notice and purpose, consent, security and access, disclosure and accountability.
3. **Interactive Screen**: Real-life example of how to protect data when working remotely.
4. **Scenario**: How to protect customer information.
5. **Key Learning**: Data must be stored securely and accessed only by authorized users. Policies must be in place to protect the anonymity of those about whom the data is stored.
6. **Scenario**: Ensuring security of personal information.
7. **Key Learning**: When using data outside of its normal intended environment, the data must be anonymized so as to remove any trace of personal information by which the customer can be identified.
8. **Scenario**: Consequences of a data breach.
9. **Key Learning**: Not following principles of proper protection of personal data/PII can have huge ramifications.
10. **Assessment**: Five-question quiz on the content presented in this topic.

integrity
Ethics & Compliance Training

Topic 4 – Protecting Confidential Information

1. **Interactive Screen**: Classifying information: public, internal, confidential, restricted.
2. **Interactive Screen**: Protecting information in communications: email, social media, phone, fax.
3. **Scenario**: Classifying information before sharing with a vendor.
4. **Key Learning**: Choosing a classification level to apply your data is a business decision based on how sensitive the data is. When you classify information and then follow the rules that apply, you help protect our company in the event of a security breach.
5. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 5 – Handling Sensitive Information

1. **Interactive Screen**: Sharing information. NDAs and CDAs. Working with contractors and agents. Disclosure.
2. **Interactive Screen**: Storing data. Disposing data. Disposing of confidential information.
3. **Interactive Screen**: Examples of the precautions to take when handling information.
4. **Scenario**: Emailing a report containing confidential data.
5. **Key Learning**: Don't disclose confidential information unless you have received prior approval from the appropriate department. Never transmit sensitive or confidential information by any method in an unprotected format – use the encryption software authorized by the IT department.
6. **Assessment**: Five-question quiz on the content presented in this topic.

Topic 6 – Speaking Up

1. Summary screen that wraps up the module and provides details of where to go to speak up.
2. Attestation screen where learners attest that they will always adhere to data privacy policies.