Risk Scenarios for GDPR Consideration

Examples of risks/events in GDPR that Controllers and Processors need to prepare/plan for

Symantec.

Practical Scenario 1: How could I protect against personal data loss?

- **Data In Motion:**
  - Collection on a website: Is the traffic encrypted?
  - Transfer via email: Is the email encrypted?
  - Transfer via a platform: Is the platform secure?
- **Data At Rest:**
  - Storage on servers: Is the data center secured?
  - Storage at end-points: Are the devices protected?
- **Data In Use:**
  - In house: Is access control in place?
  - Outsourced: Are cloud and shadow IT addressed?
  - In management: Is data loss prevention in place?

Practical Scenario 2: How do I mitigate the risk to data subjects?

- **General Risk Assessment**
  - Do I track threats affecting my line of business?
  - Do I track the risk to the kind of data I handle?
  - Do I track the risk posture of the vendors I use?
- **Risk Of Breach Of Sensitive Data, Of Professional Secrecy:**
  - Do I classify information based on sensitiveness?
  - Do I apply specific policies to specific categories?
- **Risk Of Identity Theft Or Fraud:**
  - Do I segregate directly identifiable information?
  - Do I restrict access to re-identification keys?
  - Is my certificate and key management robust?

Practical Scenario 3: Minimising Risk In Case Of A Breach

- **Pseudonymisation (article 32 paragraph 1(a)):**
  - Have I pseudonymised the data?
  - Can I prevent reversal of pseudonymisation?
- **Encryption (article 33 paragraph 3(a)):**
  - Can I prove that the breached data is encrypted?
  - Can I prove that the encryption is strong enough?
- **Ongoing Testing and Evaluation (Article 32 1(d))**
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Recommendations

- **Use this year wisely,** implementation may take longer than you think
- **Engage with your Board,** report on progress in addressing data privacy through your security program
- **Understand,** and **tackle** your big data privacy and security **risks**
- **Document** what **personal data** you hold and ensure lawful use
- Identify where **technology** can help you achieve **compliance:**
  - Prepare: Understand IT (and data) environment and risks
  - Protect: Secure Personal Data Everywhere
  - Detect: Breach monitoring and detection
  - Respond: Incident Response planning