PROGRAM MATERIALS
Program #36154
May 26, 2026

GDPR in Practice: Data Privacy Compliance, Risk Management & Operational Readiness

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

GDPR in Practice: Data Privacy Compliance, Risk Management & Operational Readiness

Speaker: Justin Muscolino,
JTM Compliance Training

JTM Compliance TRAINING

Agenda

- GDPR Background and Overview
- Key Definitions
- Principles and Legal Basis
- Individual Rights Under GDPR
- Rights under GDPR
- Data and Security Breaches
- Future of GDPR

JTM Compliance
TRAINING

GDPR Overview

- The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).
- It applies to organizations worldwide if they handle the data of EU residents. GDPR strengthens privacy rights by giving individuals control over their personal data and imposing strict obligations on organizations.
- It came into effect on May 25, 2018, replacing the 1995 Data Protection Directive. This regulation enforces transparency, security, and accountability in data handling. Non-compliance can lead to heavy fines, reputational damage, and legal action.
- Understanding GDPR is essential for ensuring data protection and regulatory adherence.

Background of GDPR

- GDPR is the EU's flagship data protection law designed to strengthen individuals' privacy rights and ensure organizations process personal data responsibly.
- GDPR applies to all businesses handling data of EU citizens, regardless of their location. It was introduced to unify data protection laws across the EU, replacing the fragmented national regulations under the 1995 Data Protection Directive.
- GDPR aims to increase transparency, accountability, and security in data processing activities. Organizations must obtain clear and informed consent before processing personal data, ensure data accuracy, and implement appropriate security measures. Individuals have enhanced rights, including the right to access, rectify, and erase their data. The regulation mandates that businesses appoint Data Protection Officers (DPOs) if they process large volumes of sensitive data.
- Non-compliance can result in significant penalties, with fines reaching up to €20 million or 4% of global annual turnover.
- GDPR also establishes strict breach notification requirements, requiring organizations to report data breaches within 72 hours.

Key Definitions

- To fully understand GDPR, it is important to define key terms used within the regulation. Personal Data refers to any information related to an identified or identifiable natural person.
- This includes names, email addresses, location data, and even IP addresses. Processing refers to any operation performed on personal data, such as collection, recording, storage, retrieval, or deletion.
- A Data Controller determines the purpose and means of processing personal data, while a Data Processor handles data on behalf of the controller. Consent under GDPR must be freely given, specific, informed, and unambiguous, with a clear affirmative action indicating agreement.
- The Right to be Forgotten allows individuals to request the deletion of their data under certain circumstances. Profiling involves the automated processing of personal data to evaluate aspects like behavior or economic status.
- A Data Breach occurs when personal data is accessed, disclosed, or lost in an unauthorized manner.
- Pseudonymization is a data protection measure that replaces identifying data with artificial identifiers.
- Organizations must classify data appropriately, implement necessary security controls, and ensure they process data lawfully.

Principles of GDPR

- GDPR is built on seven core principles that guide how personal data should be handled. These principles ensure that organizations process data responsibly and transparently.
- The Lawfulness, Fairness, and Transparency principle requires that personal data be processed legally and with clear communication to the data subject.
- The Purpose Limitation principle states that data should be collected for specified, explicit, and legitimate purposes.
- Under Data Minimization, organizations should only collect and process the data that is necessary for their stated purposes. Accuracy ensures that personal data is kept up to date and corrected without delay. The Storage Limitation principle requires that personal data is kept only as long as necessary. Integrity and Confidentiality demand that data be processed securely to protect against unauthorized access, loss, or damage.
- Accountability principle places the burden on organizations to demonstrate compliance with GDPR. These principles form the foundation of data protection under GDPR, ensuring that personal data is processed in a way that respects privacy rights. Businesses must integrate these principles into their data handling practices to meet compliance requirements.

Legal Bases for Data Processing

- Under GDPR, organizations must have a valid legal basis for processing personal data. There are six lawful bases outlined in the regulation.
- Consent is the most well-known basis, requiring a clear and affirmative action from the data subject before processing their data.
- Contractual Necessity applies when processing is required to fulfill a contract with the data subject.
- Legal Obligation allows data processing when required by law, such as tax or employment regulations. Vital Interests can justify processing if it is necessary to protect someone's life.
- Public Task applies to processing carried out in the public interest or in the exercise of official authority.Legitimate Interests allows processing if an organization’s legitimate interests outweigh the data subject’s rights and freedoms.
- Organizations must determine the appropriate legal basis before processing any personal data and document their decision-making process. It is also important to note that individuals can challenge the basis for processing their data, especially in cases where consent is the legal basis.

Individual Rights Under GDPR

- GDPR grants individuals a range of rights designed to give them greater control over their personal data. These rights ensure transparency and allow individuals to act if they believe their data is being mishandled.
  - The Right to Access allows individuals to request copies of their personal data from organizations.
  - The Right to Rectification enables them to correct inaccurate or incomplete data. The Right to Erasure, also known as the "Right to be Forgotten," permits individuals to request the deletion of their data under certain conditions, such as when the data is no longer necessary.
  - The Right to Restrict Processing allows individuals to limit the use of their data while disputes are being resolved.
  - The Right to Data Portability lets individuals obtain their data in a structured, commonly used format and transfer it to another organization.
  - The Right to Object allows individuals to challenge the processing of their data, especially for direct marketing purposes.
- Individuals have rights related to Automated Decision-Making, ensuring they are not subjected to decisions made solely by automated processes without human intervention. Organizations must establish procedures to handle these requests efficiently and within GDPR's required timelines.

Right to Access and Rectification

- The Right to Access allows individuals to request access to their personal data held by organizations. This right ensures that individuals are aware of what personal data is being processed and why.
- Upon request, organizations must provide a copy of this data, typically within one month.
- The Right to Rectification grants individuals the ability to correct inaccuracies in their personal data. If incorrect or incomplete information is identified, organizations must take action to rectify it promptly.
- Both rights are crucial for transparency, empowering individuals to control their personal data and ensure its accuracy. Companies must have mechanisms in place to respond efficiently to access and rectification requests.

Right to Erasure (Right to Be Forgotten)

- The Right to Erasure, commonly known as the "Right to Be Forgotten," allows individuals to request the deletion of their personal data under certain conditions.
- This includes when data is no longer necessary for its original purpose, when the individual withdraws consent, or when the data has been unlawfully processed. Organizations must assess each request carefully, considering any legal obligations for data retention.
- This right is essential for promoting privacy and allowing individuals to manage their digital footprint. However, it does not apply universally, especially in cases where data processing is required for legal or contractual reasons.

Right to Data Portability

- The Right to Data Portability enables individuals to obtain and reuse their personal data across different services.
- This right allows individuals to request their data in a structured, commonly used, and machine-readable format. They can then transfer this data to another organization, improving control over how their personal information is used.
- This provision is especially important in industries where consumers switch services frequently.
- For organizations, this right emphasizes the need to maintain data in interoperable formats. Companies must ensure their data systems are compatible with the requirements for portability, balancing flexibility with privacy concerns.

Right to Object and Restriction of Processing

- The Right to Object allows individuals to object to the processing of their personal data in specific circumstances. This includes processing for direct marketing, scientific research, or public interest tasks.
- If individuals object, the organization must cease processing unless there are compelling legitimate grounds to continue, such as legal obligations or overriding public interests.
- The Right to Restriction of Processing permits individuals to request that their data is temporarily not processed. This right can be exercised when an individual contests the accuracy of their data or objects to processing.
- Organizations must ensure they can implement these rights effectively, maintaining transparency in their processing activities.

Security Obligations Under GDPR

- GDPR mandates that organizations implement appropriate technical and organizational measures to ensure the security of personal data. This includes preventing unauthorized access, accidental loss, or damage to the data.
- Security measures should be tailored to the specific risks posed by the data processing activities. Regular risk assessments are essential to identify vulnerabilities and adjust security protocols as needed.
- GDPR requires that data controllers and processors use encryption, secure storage, and other safeguards to protect personal data. It is vital for organizations to have a robust security framework that complies with GDPR's stringent requirements to protect individuals' privacy rights.

Data Breach Notification Requirements

- Under GDPR, organizations must notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach that could result in harm to individuals.
- The notification must include details of the breach, the affected data, and any steps taken to mitigate potential risks. If the breach is likely to result in high risks to individuals' rights and freedoms, those individuals must also be informed without undue delay.
- Effective data breach management processes, including clear reporting protocols, are crucial for compliance. Organizations should prepare for breaches by having response plans in place to act swiftly and minimize damage.

Data Protection Impact Assessments (DPIAs)

- A Data Protection Impact Assessment (DPIA) is a process designed to identify and mitigate risks associated with data processing activities.
- DPIAs are mandatory when introducing new technologies or processing methods that could impact the privacy of individuals. The assessment evaluates the necessity, proportionality, and potential risks of the data processing and recommends measures to address them.
- Conducting DPIAs ensures that organizations address privacy risks early in the project planning stages. Regular DPIAs help maintain compliance with GDPR while fostering a culture of privacy awareness within the organization. They are also essential when processing sensitive data or engaging in large-scale data processing.

Role of Data Protection Officers (DPOs)

- A Data Protection Officer (DPO) is responsible for ensuring an organization's compliance with GDPR.
- The DPO advises on data protection matters, monitors data processing activities, and acts as a point of contact for individuals and regulatory authorities. They play a vital role in conducting DPIAs, managing data subject rights, and responding to data breaches.
- The DPO must be independent, an expert in data protection, and report directly to senior management. While not mandatory for all organizations, appointing a DPO is strongly recommended for public authorities or organizations involved in large-scale data processing. Their role is essential for fostering a privacy-conscious culture.

International Data Transfers and GDPR

- GDPR regulates the transfer of personal data outside the European Economic Area (EEA) to ensure the data remains protected.
- Organizations must ensure that data transferred to third countries is subject to adequate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).
- In cases where adequate protection is not guaranteed, alternative measures must be implemented, including additional contractual clauses or the use of certifications. Transfers to countries with lower data protection standards, such as the U.S., require heightened scrutiny.
- GDPR compliance requires organizations to carefully assess and implement mechanisms that ensure international data transfers are safe and compliant.

Enforcement and Penalties

- Non-compliance with GDPR can result in significant penalties, including fines of up to €20 million or 4% of global turnover, whichever is higher.
- Enforcement is carried out by national supervisory authorities within the EU, who have the authority to investigate organizations, issue warnings, and impose corrective measures.
- Penalties are determined based on the severity and scope of the violation, as well as whether the organization has shown due diligence in mitigating risks.
- The risk of penalties underscores the importance of maintaining GDPR compliance, as well as establishing effective data protection frameworks and employee training programs to minimize risks of violations.

Case Studies of GDPR Violations

- Several high-profile GDPR violations have highlighted the serious consequences of non-compliance.
- One example is the fine imposed on Google for failing to obtain valid consent for data processing activities.
- Another case involved British Airways, which was penalized for inadequate data protection measures that led to a significant data breach. These cases demonstrate the financial and reputational risks associated with violating GDPR.
- They emphasize the importance of comprehensive data protection strategies, including clear consent processes, data breach prevention, and proper security measures. Learning from these cases helps organizations understand the practical impact of GDPR violations.

Best Practices for GDPR Compliance

- To achieve GDPR compliance, organizations must implement several best practices. This includes ensuring data is processed lawfully, securely, and transparently.
- Regularly updating data protection policies and conducting staff training are crucial for creating a privacy-conscious culture.
- Organizations should also establish clear procedures for handling data subject requests and data breaches. Utilizing encryption, pseudonymization, and robust access controls helps protect personal data.
- Conducting regular risk assessments, including DPIAs, ensures ongoing compliance. By adopting these best practices, organizations can reduce the risk of non-compliance while demonstrating their commitment to safeguarding individuals' privacy rights.

Future of GDPR and Data Protection Trends

- The future of GDPR and data protection is shaped by evolving technologies, such as artificial intelligence, big data, and cloud computing.
- As these technologies become more integrated into businesses, data protection regulations will likely become stricter, focusing on emerging risks like algorithmic decision-making and automated profiling.
- There is growing attention on the rights of data subjects, with potential new regulations that address issues such as biometric data and privacy in the metaverse. Organizations must stay agile, keeping up with new developments to ensure continuous compliance with GDPR and to protect against evolving data privacy threats.

THANK YOU!

Contact Information:
JTM Compliance Training
Justinmuscolino@gmail.com

JTM Compliance
TRAINING