Dev mistri - 2424033

Answer: Add an Introduction

⟹ (Key principles of Data security Governance and their applicaetion:

Data security governance is built on accountelbility, transparency, risk management, and compliance. Assigning data ownership ensures accountelbility, while documenting data handling supports GDPR transparency. A governance committee can align security efforts with the company's European expansion.

expand more

- Start with a Data Protection Impact Assessment (DPIA) to map personal Data. Ensure lawful processing, valid consent, and tools for data subject rights. Use encryption, multifactor authenticeetion, and strong control. Have a 72-hour breach response Plan as per GDPR Article 33.

Why GDPR? ; link to the needs of the company

How to implement GDPR in this context

- Risk Assessments help identify and address threats to sensitive data. Classifying data by sensitivity (e.g. confidential, restricted) ensures proper protection through access controls and encryption, reducing regulatory and financial risks.

How? → The steps of RA plan

- Use tools like CASBs to detect unauthorized apps and enforce software usage policies. Vet all third-party vendors with risk assessments, require GDPR-compliant contracts (DPAs), and audit them regularly for compliance and security.

- Promote regular, role-based training and phishing simulations to boost awareness. Leadership should lead by example, while Security Champions in departments reinforce good practices. Encourage safe reporting to build a security-first culture.

Euro!

Conclusion

Dev Mistri

→ In today's data-driven business landscape, securing information assets is essential to maintain trust, ensure compliance, and support organizational growth. This response explores the key principles of data security governance, GDPR compliance, and the importance of risk assessment in establishing a secure and compliant data environment.

Effective data security governance is built on foundational principles such as accountability, transparency, risk management, and compliance with regulations. Accountability ensures that clear ownership of data assets is established across the organization. This can be achieved by assigning specific roles like Data stewards, who are responsible for managing and safeguarding data within their departments. Transparency is equally crucial, as it facilitates regulatory compliance particularly under frameworks like GDPR by providing clear documentation of data processing activities. Risk management involves identifying and mitigating threats to data confidentiality, integrity and availability.

Lastly, compliance ensures that the organization adheres to legal and industry standards. Creating a governance committee helps unify these efforts, enabling coordinated policies and procedures across department, which is particularly important for companies expanding into regulated markets like the European Union.

- The GDPR is vital for businesses that process personal data of EU citizens, as it ensures individual privacy rights and imposes strict obligations on data handlers. For this company, GDPR compliance is not only a legal necessity due to its European expansion but also a competitive advantage that builds customer trust. Implementation begins with a data protection Impact Assessment to understand how personal data is collected, processed, and stored. The company should establish lawful bases for data processing, such as consent or legitimate interest, and implement user-friendly tools to manage data subject rights. Strong technical controls like encryption and access restrictions must be supported by policies and

Staff training. A ~~Data~~ DPO should oversee ongoing compliance, while a clear incident response plan ensures timely breech reporting as mandated by GDPR Article 33.

- Risk Assessment is Structured process to identify, evaluate, and address Potential threats to data security. A step by step plan for this company includes:

- Asset Identification
- Threat Analysis
- Vulnerability Assessment
- Risk Evaluation
- Risk Mitigation planning
- monitoring and Review

Conclusion:

A strong data security governance strategy with GDPR compliance and ongoing risk assessment is vital for protecting sensitive information. Clear data ownership, transparency, and proactive risk management strengthen security. GDPR compliance builds trust and supports growth. while a culture of awareness ensures long-term resilience.