Accountability and Demonstrating Compliance

the GDPR requires a data controller to demonstrate that data processing activities comply with the GDPR's requirements.

This requires more than just establishing data protection policies and procedures. Accountability requires a data controller to be able to demonstrate compliance with the GDPR by showing the supervisory authority and individuals how the data controller complies, on an ongoing basis, through evidence of:

- Internal policies and processes that comply with the GDPR's requirements.
- The implementation of the policies and processes into the organization's activities.
- Effective internal compliance measures.
- External controls.

Complying with the accountability principle requires the data controller to:

1. Establish a data protection compliance program and privacy governance structure
2. Implement and maintain privacy controls on an ongoing basis
3. Embed ongoing privacy measures into corporate policies and day-to-day activities, throughout the organization and within each business unit that processes personal data
4. Leverage technology to require or ensure compliance
5. Maintain documentation of the privacy measures implemented and records of compliance
6. Train employees on privacy and data protection matters
7. Regularly test the privacy measures implemented
8. Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts

Failure to comply with the accountability principle may result in fines of up to EUR20 million or 4% of the organization's total worldwide annual revenue for the preceding financial year, whichever is higher (Article 83(5), GDPR).

Demonstrating compliance will help reduce the data controller's or data processor's risk of liability including administrative fines.