How does ISO27001 help in achieving GDPR Compliance?

VISTA INFOSEC®
TRUSTED ADVISORS ASSURED COMPLIANCE

Data protection and Privacy are today the top-most priority for organizations dealing with sensitive and confidential data. There are many regulatory frameworks established around it to ensure organizations adopt industry best practices to secure their environment. GDPR Regulation is one such framework established in the EU to ensure Data Protection and Privacy. However, due to the stringent regulation and security requirements, most organizations struggle to achieve Compliance. For those organizations looking to achieve GDPR Compliance, implementation of the ISO27001 framework will make your compliance journey a lot easier. In today's article, we have discussed how implementing ISO27001 Standard will help in achieving GDPR Compliance.

ISO27001 Standard and GDPR Compliance

ISO 27001 Certification is a recognized international standard for information security management. Although the standard is not exclusive to Personal Data Protection, yet many requirements are in common with the GDPR Regulation. Implementing the ISO27001 Standard makes it a lot easier for achieving Compliance. But, ISO 27001 and GDPR can by no means be used interchangeably. ISO 27001 simply provides a framework to ensure certain measures are implemented that also facilitates the GDPR compliance regime. Let us take a closer look at the standard and the regulatory requirement to understand what all does ISO27001 cover in the GDPR Compliance.

What is in common between ISO27001 Standard and GDPR Compliance?

ISO 27001 Standards can be used for achieving compliance. Given below are some standard framework that overlaps with GDPR Compliance requirements -

Risk Assessment – Risk Assessment which forms an integral part of ISO27001 Standard, is also an essential part of GDPR Compliance. Similar to the ISO 27001 standard which includes identifying risk and applying control measures to reduce the risks to an acceptable level, GDPR too requires organizations to conduct a Data Protection Impact Assessment (DPIA) to implement measures to reduce the level of risk exposure. So, implementing ISO27001 Standard as an integrated part of your Risk Management program will also help you meet the GDPR risk assessment requirement.

Breach Notification – Articles 33–34 of the GDPR Regulation requires organizations to notify authorities within 72 hours of a breach of personal data. With similar requirements in ISO27001, which addresses information security incident management controls require organizations to report security incidents promptly and communicate the events in a way that facilitates timely and corrective actions to be taken.

Data Protection by Design- As under Article 25 of the GDPR Regulation organizations are required to implement technical and organizational measures that ensure data protection and privacy by design. It also requires organizations to protect data privacy by default and ensure only essential information required for a specific purpose must be processed and used. So, Privacy by Design which is a mandatory GDPR requirement can be achieved with ISO 27001 standard which also outlines similar requirement which ensures information security is an integral part of information systems across the entire lifecycle.

Retention of records - As under the GDPR Regulation Article 30 requires organizations to maintain records of processing activities, including categorizing of data, the purpose of processing, and general description of the relevant technical and organizational security measures in place. GDPR also calls for personal information to be not stored for longer than needed. Similarly, ISO 27001 requires organizations to document their security processes, and details of their security risk assessments and risk treatment as per Clause 8. Further, it requires information assets to be classified, inventories, and have in place procedures to ensure the use of data use is defined.

Asset Management- The Annex A of ISO 27001 Standard which focuses on Asset Classification and Management will also include Personal Information as Information Security Assets. This will automatically lead organizations to classify the type of Personal Data involved, where for long is it stored, its origin, and who can access it, which are all the requirements of the GDPR. This would basically be in context to handling, controlling, and/or processing Personal Information.

Can ISO27001 Certification alone be enough for achieving GDPR Compliance?

ISO 27001 Standard is an industry best practice for Information Security and an excellent framework for GDPR Compliance. Organizations that implemented the standard will most likely find it easy to achieve GDPR Compliance. Implementing the standard will ensure the protection of Personal data and ensure the minimization of the risk. With many standard requirements overlapping, implementing the internationally recognized ISO 27001 standard will definitely ease the process of compliance. Although achieving compliance to GDPR Regulation will also require the implementation of other additional security and privacy measures as stated in the GDPR Regulatory framework.

Conclusion

Organizations that have implemented or in the process of implementing the ISO 27001 standard are definitely in a much better position to achieve compliance with the GDPR requirements. Implementation of ISO 27001 Standards will help organizations meet quite a few overlapping requirements. But as experts we also recommend organizations to perform a gap analysis to assess their current position and accordingly implement relevant controls for risk containment associated with confidentiality, integrity, and availability of personal data. Even though ISO Standards may not guarantee GDPR Compliance, it yet comes handy for it provides a practical framework for developing strategies, and building comprehensive policies to minimize security risks that lead to breaches. Organizations, in general, must consider pursuing ISO 27001 certification and GDPR for building security strong and effective measures to protect sensitive data. **Original Source:-** isoupdate **Written by:-** VISTA InfoSec

Do write to us your feedback, comments and queries or, if you have any requirements: info@vistainfosec.com

You can reach us on:

USA	INDIA	SINGAPORE	UK
+1-415-513 5261	+91 73045 57744	+65-3129-0397	+447405816761

© VISTA InfoSec ®