The link between ISO/IEC 27001 and GDPR

ISO/IEC 27001 and GDPR at their core have in common the commitment to properly process and store the sensitive and confidential data. Therefore, the implementation of ISO/IEC 27001 comprehensive framework steers compliance with the EU GDPR, as many of the EU GDPR requirements are covered by ISO/IEC 27001. However, particular controls have to be adjusted to address the protection of personal data within Information Security Management System.

If you already have an ISO/IEC 27001 framework in place, you will not face duplication of effort, cost and time to comply with GDPR requirements.

GDPR encourages the implementation of ISO/IEC 27001 as an approach to ensure easier GDPR compliance. The ISO/IEC 27001 certification supports organizations in creating better business efficiency, safeguards the valuable assets such as personal data, protects staff and organization's reputation, and simultaneously facilitates the attainment of compliance objectives. Some of the GDPR requirements are not directly covered in ISO/IEC 27001; however, ISO/IEC 27001 provides the means to push you one step closer to accomplishing conformity to the regulation.

In case that an organization is not ISO/IEC 27001 certified, then GDPR may be a good catalyst in considering implementing such scheme for higher information protection assurance. Thus, by being ISO/IEC 27001 compliant you demonstrate that the data owned and used is managed based on data protection regulations.

ISO/IEC 27001		GDPR	
Control	Notes	Article	Summary
A.18.1.4	The ISO/IEC 27001 specifically mentions compliance obligations related to Privacy and Protection of Personally Identifiable Information (PII), where it obliges organizations to protect PII in line with relevant legislation and regulation. In the context of GDPR, privacy is largely a matter of securing people's personal information, particularly sensitive data stored electronically.	1	This Regulation sets down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
6.1.2, A.8.1.1 A.8.2 A.8.3 A.9.1.1 A.9.4.1 A.10 A.13.2 A.14.1.1 A.15 A.17 A.18 (almost all)	Personal information should be adequately secured by business processes, systems, network etc. In order to satisfy the requirements on how personal data should be handled, the organizations need to have clear understanding of what type of personal data is used and owned, where such data is stored, and/or who are the privileged users that can assess the data. Even though not explicitly specified, accountability is an important concept within the 'Leadership' section of ISO/IEC 27001.	5	Personal data must be: (a) processed lawfully, fairly and transparently; (b) collected for specified, explicit and legitimate purposes only; (c) adequate, relevant and limited; (d) accurate; (e) kept no longer than needed; (f) processed securely to ensure its integrity and confidentiality. The "controller" is accountable for ensuring information security and demonstrating the fulfillment of GDPR principles.
A.12.1.1	Operating procedures must be documented and made available to all users who need them	12	Communication with data subjects must be transparent, clear and easily understood.
A.12.1.1 A.14.1 A.9 A.16 A.12.3 A.18.1.3	Involves requirements to check, edit and extend stored information, with various controls concerning identification, authentication, access, validation etc. It may also affect backup and archived copies.	16	Individuals have the right to get their personal information corrected, completed, clarified etc.
6.1.2 A.14.1.1 A.9 A.16 A.12.3 A.8.3.2	Involves system and process requirements to erase individuals' personal stored data.	17	Under GDPR, individuals have the right to be forgotten (have their personal data deleted and no longer used).

A.14	This control ensures that the entire cycle of an information system is supported by Information Security.	25	Privacy by Design requires that each product or system that employs personal data for various reasons must ensure the protection of these data during the whole life-cycle.
8.3	This requires the implementation of risk treatment plans, and retention of the documented information of the information security risk treatment results.	25	Proper personal data protection by design and by default
7.5	This control involves the need for a well-designed, structured, controlled, managed and a maintained set of ISMS documentation. Example: having a standard document information (such as title, date, author and reference), review and approval activities, version controls, suitable access rights and distribution etc.	30	Controllers must maintain documentation about privacy e.g. the purposes for which personal info is gathered and processed, also the categories of data subjects and personal data etc.
A.16 A.18.1.4	Under the ISO/IEC 27001, breaches would normally be handled within the Information Security Incidents Management, but under GDPR's breach notification requirement, the 3-day deadline must be fulfilled.	33	Privacy breaches that have exposed or harmed personal info must be notified to the authorities promptly (within 3 days of becoming aware of such breaches, unless delays are justified).
6.1.2 A.6.1.3 A.8.2.1	The ISO/IEC 27001 standard facilitates organization's implementation of data policy and personal information protection. GDPR also emphasizes that privacy risk assessment should be integrated in the risk assessment activities for new IT system developments, changes of business projects etc.	35	One of the crucial GDPR risk assessment requirements is the Data Protection Impact Assessment (DPIA), which evaluates the privacy risks.
6 A.18.1.4	Huge fines are clearly intended to be a strong deterrent; thus, indicating the consequences of failing to prevent data breaches, as well as failing to achieve GDPR compliance.	83	Depending on the infringements and circumstances, fines may reach €20 million, or up to 4% of total worldwide annual turnover.

As a result, any organization that has already implemented or is in the process of ISO/IEC 27001 implementation, is in an excellent position to show compliance with the new GDPR requirements.

Are you ready to comply with the GDPR?