Octal0g1k
ANSWERING YOUR CYBER CHALLENGES

ISO 27701

Addressing the concerns of 'Personally Identifiable Information' (PII)

It was estimated that in 2018, the world over organizations lost an estimated $600 billion in the global economy due to cybercrimes. This number is estimated to cross $1 trillion in total losses in year 2020. This is not startling, as it is baffling that half of the organizations had not implemented an end-to end cyber prevention and incident response mechanism. This is more puzzling when cybercrimes pertain to the personal information.

The buzzword around breach of 'personally identifiable information' (PII) has been real and dangerous. In year 2020 alone, there had been more than ten big data breaches such as offering of over 267 million Facebook profiles for sale on dark web sites and hacker forums, the dump was offered for £500 ($623) and did not include passwords. In October 2020, a huge data breach at US VoiP provider Broadvoice had exposed more than 350 million customer records, including names, phone numbers and even call transcripts. A research report by cybersecurity company Kaspersky Stalkerware is a kind of malware that records data being entered into a device and sends it to a third party that's supplied to the program on installation. These two examples showcase the importance to protect the PII in the current and evolving cyber threat environment.

Defining the Personally Identifiable Information (PII):

Every organization would have a set of datasets that could be marked and mapped as sensitive and labeled as 'personal data'. From a European Union perspective, "information which can identify a person via an ID number, or factors specific to physical, physiological, mental, economic, cultural or social identity". According to the National Institute for Standards and Technology (NIST), the following items definitely qualify as PII, because they can unequivocally identify a human being: full name (if not common), face, home address, email, ID number, passport number, vehicle plate number, driver's license, fingerprints or handwriting, credit card number, digital identity, date of birth, birthplace, genetic information, phone number, login name or screen name. That being said, every country does have a differentiated definition for PII, and that ultimately is at risk factor.

Information Security Management System and the ISO 27701:

An information security management system (ISMS) is a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. An ISMS embeds a number of information controls without which information would remain disorganized and disjointed. An ISMS is a system of processes, documents, technology and people that helps organizations manage, monitor and improve their information security in one place. ISO 27001 is the first global privacy standard that describes best practice for an ISMS and demonstrates

the importance of and demand for improved privacy protection. The ISO 27701, thus assists in demonstrating compliance with privacy regulations around the world.

ISO 27701:2019

The ISO 27701:2019 is a certifiable extension to ISO/IEC 27001 certifications and provides a compliance framework and enable organizations to assess, treat, and reduce risks associate with the collection, maintenance and processing of personal information. As ISO 27701 makes organizations responsible and accountable for Personally Identifiable Information (PII) by providing requirements on managing, processing, and implementing safeguarding policies, thus, keeping personal data safe and secure.

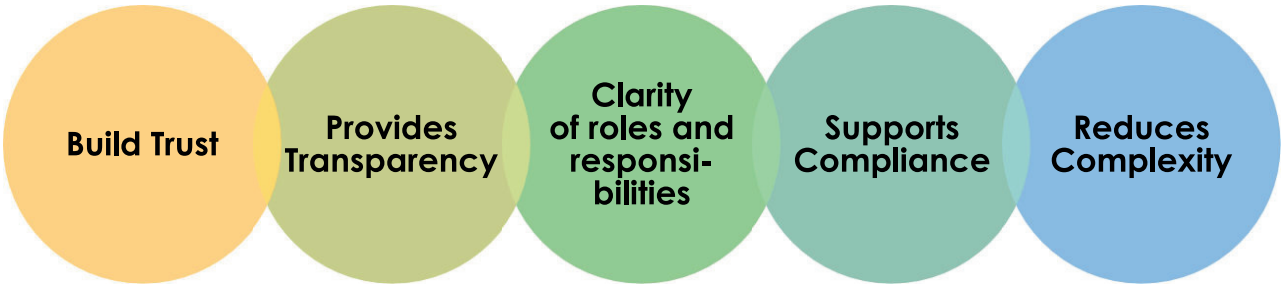
Why implement ISO 27701:

ISO 27701 is considered as a set of gold standard for compliance with the General Data Protection Regulation (GDPR). Thus, any organization implementing ISO 27701 naturally demonstrates their ethical, GDPR-ready data protection standards to customers, prospect, employees and more.

Mappings of the ISO 27701 can be done to other privacy laws as well, such as the California Consumer Privacy Act of 2018 (CCPA), Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA). Thus, ISO 27701 is likely to help organizations by providing a common standard for demonstrating compliance with many regulatory regimes.

Organizations seeking to increase collaboration between their privacy and security teams do benefit to implementing ISO 27701. Fundamentally, implementing the ISO 27701 across an organization builds trust, provides transparency to employees and stakeholders, presents a clear guideline of roles and responsibilities and thus inherently supports compliance and reduces complexity of operations.

Figure 1: Portrayal of benefits linked to implementing the ISO 27701



Who should use ISO 27701?

ISO/IEC 27701 is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations. It provides guidance for organizations who are responsible for PII processing within an information security management system (ISMS), specifically:

1. PII controllers (including those who are joint PII controllers)
2. PII processors

All organizations undertaking protection of PII must have a Data Privacy Framework in place that defines sensitive data, analyses the risks affecting the data and ensures controls at securing it.

Benefits of implementing an ISO 27701:

Privacy and data protection are high on the agenda of all stakeholders. ISO 27701 certification awarded by a reputable third-party certification body is an independent and impartial stamp of approval that demonstrates compliance and provides a competitive advantage to an organization and its customers of adequate processes and controls at safeguarding personal information. The use of ISO 27701 by a certified organization it is echoed that there is much focus and importance given at covering privacy management. It shows the stakeholders that measures have been taken to achieve compliance with applicable laws and regulations.

The GDPR mandates to have data protection inbuilt by design is a legal requirement to all organizations handling sensitive personal data. ISO 27701 is an evidence-based framework that provides guidance and compliance with GDPR requirements on data protection. In addition, continual improvement sits at the heart of ISO 27701. The systems implemented under ISO 27701 can provide evidence that the processing activities of an organization are compliant with the GDPR. ISO 27701 also adds value in its ability to give an organization insight into how well they're addressing and managing privacy.

The road ahead for ISO 27701:

Data protection is at the heart of ISO 27701, and thus essentially it mandates keeping the data secure at all stages of its collection, processing, dissemination, use, storage and disposition

safe and secure. Thus ISO 27701 must be implemented at all stages of a data life cycle within an organization and tying the ISO 27701 requirements to each level of the data life cycle shall help organizations better manage risks and implement better privacy controls in accordance to the framework.

Organizations would be able to start from the onset at better designing an application or toolkit that enables privacy protection and corresponds say to the GDPR guidelines once they have the mandate to implement the ISO 27701 framework. The ISO 27701 help organizations to hand-hold in determining the essential elements that a designer or a programmer must take into account while utilizing either the data or working with applications that request any form of PII data. Implementation of the ISO 27701 would help organizations demonstrate to individuals and the external service providers such as cloud providers the requirement to implement standards in compliance with the ISO 27701.

The ISO 27701 framework provides a standard language that is easy to communicate and showcases the minimum PII privacy requirements to all its stakeholders and those utilizing its dataset as part of any data processing eco-system and thus help an organization in easy data audits, data security, data risk management and assessment exercises. Thus, all functions and domains within an organization would be required to be in compliance and adhere to the formal contract of protecting and upholding the 'Personal Identifiable Information' – the PII.

As organizations strive hard to protect and secure PII data and work aggressively towards data protection, ISO 27701 provides a structured framework and helps in reducing risks and complexities. The ISO 27701 presents a good governance and management framework for PII's and helps in verification at every step of any audit. As the environment and context of the global cyber space evolves, organizations must identify and categorize PII data and thus allowing risk assessments to be optimized, corrections made, and threats mitigated due to any cyber incident.