tsaaro

PIMS

Privacy Information Management System

Your Guide To Compliance

INTRODUCTION

Privacy concerns are as old as humanity. From the protection of one's body and property in ancient times, it has become a strict connection with when, how, and to what extent data and information about a person are communicated to others. Privacy is subjected to three key elements: Independent of Body, Property, or Information.

While people have a desire to protect their privacy, they invariably choose to sacrifice it in exchange for perceived benefits like money, prestige, or convenience, disregarding the potential dangers and losses. Governments' / Organizations' will to legislate over privacy is not always according to an individuals' best interests; it is sometimes in the name of a "greater good". As a key point in dealing with privacy, technology is increasingly providing the means for persons, organizations, and governments to gather, aggregate, and analyze greater information in a faster way, making privacy breaches, accidental or intentional,, increasingly severe and comprehensive.

On the other hand, this same technological environment, or cyberspace, can provide solutions to help properly protect the privacy of individuals, organizations' business, and governments' affairs, while at the same time allow them to fully enjoy modern life securely. These solutions, together with other non-technological measures, are known as cybersecurity.

This white paper provides an overview of the way in which data protection principles should be taken into account in cyberspace operations and how currently established standards and frameworks may assist to completely control, implement, operate and enhance cyber safety.

THE ISO 27001:2013 STANDARD

The ISO 27001:2013 is an Information Security Management Standard that speaks about best practices of security management and comprehensive security controls that are followed by guidance on the controls, present in the ISO/IEC 27002.

What does the ISMS bring to the table?

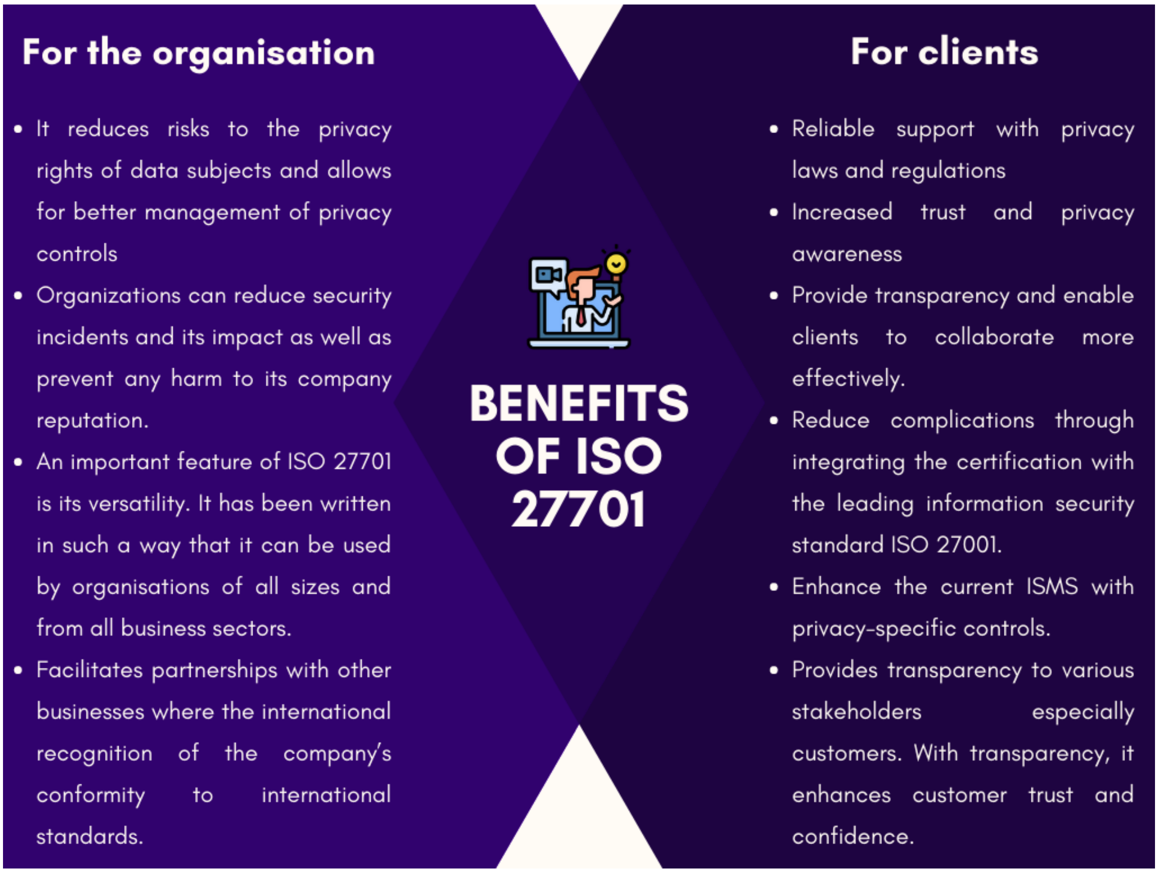
- Takes into account the impact of the company threats and vulnerabilities followed by systematically evaluating information security risks.
- Develop, Design, and Implement a comprehensive suite of information security controls and other forms of Risk Management to address Company and architecture security risks.
- Encourages continual improvement by identifying and correcting the non-conformities in the information security controls.
- Adopts overarching management process to ensure compliance with information security controls and needs on an ongoing basis.

THE ISO/IEC 27701:2019 STANDARD

ISO 27701 focuses on the development, implementation, maintenance and continual improvement of a privacy information management system (PIMS). It is an extension of the already established ISO/IEC 27001 information security management system (ISMS) and ISO/IEC 27002 information security controls code of practice requirements. The standard sets different controls for organizations depending on their role as data controller, data processor, or both, making it the premium international standard for managing privacy risks and meeting regulatory requirements for protecting personal data.

IMPORTANCE OF ISO/IEC 27701

Almost every organization process personally identifiable information (PII), including private, client, and employee data. As organizations grow, expand, and adopt new technologies, the volume, and variety of processed PII increases. Data privacy laws and regulations in force around the world must also adapt to the demands and risks of the changing online environment.



For the organisation

- It reduces risks to the privacy rights of data subjects and allows for better management of privacy controls
- Organizations can reduce security incidents and its impact as well as prevent any harm to its company reputation.
- An important feature of ISO 27701 is its versatility. It has been written in such a way that it can be used by organisations of all sizes and from all business sectors.
- Facilitates partnerships with other businesses where the international recognition of the company's conformity to international standards.

BENEFITS OF ISO 27701

For clients

- Reliable support with privacy laws and regulations
- Increased trust and privacy awareness
- Provide transparency and enable clients to collaborate more effectively.
- Reduce complications through integrating the certification with the leading information security standard ISO 27001.
- Enhance the current ISMS with privacy-specific controls.
- Provides transparency to various stakeholders especially customers. With transparency, it enhances customer trust and confidence.

Released in the summer of 2019, ISO/IEC 27701 is the latest standard extension to the well-known ISO 27001 norm for information security management system (ISMS) requirements. ISO/IEC 27701 provides guidelines to extend an already existing ISMS by adding components to support a privacy information management system (PIMS). ISO/IEC 27701 certification is solely awarded as a supplement to ISMS certification according to ISO/IEC 27001.

ISO/IEC 27701: Follow industry leading controls aligned to GDPR, ISO 27001, and ISO 27002!

In legal terms, however, the most interesting feature of ISO/IEC 27701 is that it offers guidance to conform to GDPR: if an organization is applying ISO/IEC 27701, then they can be confident that they have in place certain obligations of their business under the European GDPR.

Therefore, if an organization is thinking about ISO/IEC 27001 implementation, and is worried that they are not confident that it conforms to GDPR standards, and what best practices are required to know how to carry out controls, ISO/IEC 27701 is an excellent tool do so.

The European Union General Data Protection Regulation (GDPR) (2016/679), was enforced on May the 25th, 2018. The new Data Privacy legislation proposed a new set of obligations to both Data Controllers and Processors. The ISMS lists out details on multiple areas such as:

Supplier and Service chain relationships

The GDPR applies also to suppliers processing personal data on behalf of others; it requires controls and restrictions to be included informal agreements. The ISO 27001 standard requires the protection of the organization's assets that are accessible by suppliers and for organizations to monitor the service delivery of suppliers against information security requirements. To ensure a robust supplier and service chain, a set of controls should be demanded from the suppliers to use in the services they provide to the organization.

Risk assessment

The high fines that will be enforced by the new regulations (up to €20 million or up to 4% of the annual worldwide turnover of the parent company) could have a major financial impact on any organization. The ISO 27001 Standard requires an organization to conduct a risk assessment on their information assets, which should consider the increased risk to personal information and potential financial implications. The risk assessment is done periodically and helps in minimizing the risk and their impacts on operations.

Cooperation with authorities

Under the GDPR, organizations must cooperate with the authorities e.g. privacy or data protection regulators. The ISO 27001 requires that "Appropriate contacts with relevant authorities shall be maintained". Within the ISO 27001 certification process, this was included in the Information Security Roles and responsibilities within our organization.

Reporting breach notification

Under the GDPR, companies need to notify Data Authorities within 72 hours after a personal data breach has been identified. The ISO 27001 required an incident management process to be put into place so that information security events get reported through appropriate management channels as quickly as possible.

Data classification

Personal data must be processed in a manner to ensure appropriate security. The ISO 27001 always suggests that information shall get an appropriate level of protection indispensably in accordance with its importance to the organization.

Asset management

The GDPR requires companies to understand what personal data they collect, how it is obtained, where it is stored, how long it is kept for and who has access. The ISO 27001 mandates organizations to identify their assets and define appropriate protection responsibilities.

Documentation

Under EU GDPR, controllers must maintain documentation concerning privacy e.g. for the purposes for which personal information is gathered and processed, "categories" of data subjects and personal data. The ISO 27001 requires documentation to be kept based on the complexity of processes and their interactions.

Privacy by Design

The adoption of Privacy by Design is another GDPR requirement. The ISO 27001 ensures that information security is designed and implemented as an integral part of the entire development and lifecycle of information systems. Within the certification process, a set of guidelines of Secure Software Development is crucial for Products' Development Processes.

HOW TO IMPLEMENT ISO 27701

Key modifications must be made to the overall ISMS structure, existing controls described in Annex A, and the implementation of the control objectives relevant to PII processors and controllers. Transition to ISO/IEC 27701 may be simpler for organizations with a structure and process supporting GDPR requirements. ISO/IEC 27701 also supports efforts towards compliance with data protection laws in both cases, however, the appropriate and effective implementation of processes into the scope of the ISMS must be ensured.

The successful incorporation of ISO/IEC 27701 into an existing information security management system (ISMS) depends on:

- A gap assessment of the existing ISMS according to ISO/IEC 27701 requirements
- Identification of gaps and an action plan providing a gap solution strategy
- Adjusting the scope
- Adaptation of controls from ISO/IEC 27001 to the new Requirements
- Clarifying whether you are a PII controller, processor, or most likely, both
- List of processing activities
- Expansion of the asset management
- Incorporation of new requirements into the ISMS design
- Evaluate the expanded ISMS with risk assessment, and monitoring, internal auditing, management review, and other relevant appraisal tools.

COMPANY PROFILE

Tsaaro provides privacy and cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include Privacy compliance, DPO-as-a-service, Vulnerability Assessment & Penetration Testing, Cyber Strategy, DPIA to name a few, delivered by our expert privacy professionals recognized by IAPP.

We take a pragmatic, risk-based approach to provide our clients with real-world, workable advice, and support, that helps them deal with a wide range of security and privacy challenges.

CONTACT US

Assess risks associated with modern cybersecurity risks and strengthen your data protection roadmap through our wide catalog of services.

Addresses:

Tsaaro India Office
Manyata Embassy Business Park,
Ground Floor, E1 Block,
Beech Building, Outer Ring Road,
Bangalore- 560045
India
P: +91-0522–3581306

tsaaro

OUR TEAM

- **Akarsh Singh**

(CEO & Co-Founder Tsaaro)
Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

- **Krishna Srivastava**

(Co-Founder & Head of Cyber Security Tsaaro)
Krishna is an ex-KPMG data security consultant. His expertise lies in Information Security and Data Privacy Compliance.

REVIEWER

- **Anselmo Diaz Valiente**

(Principal Consultant at 2|SEC)
Anselmo is a Experienced consultant involved in a variety of projects, requiring the application of expert knowledge in Information Security and Data Protection. Ample of experience in auditing and providing consultancy to organisations across diverse sectors.

- **Sumeet Das**

(Client Account Executive- OneTrust)
Sumeet is a Sales Enthusiast with 9+ Years of rich experience in aspects of Account Management and New Business Development. He uses deep Industry analysis, insight, and team approach to support business diversification and drive organizational improvement.

Tsaaro Netherlands Office
Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31 686053719

Email us:

info@tsaaro.com