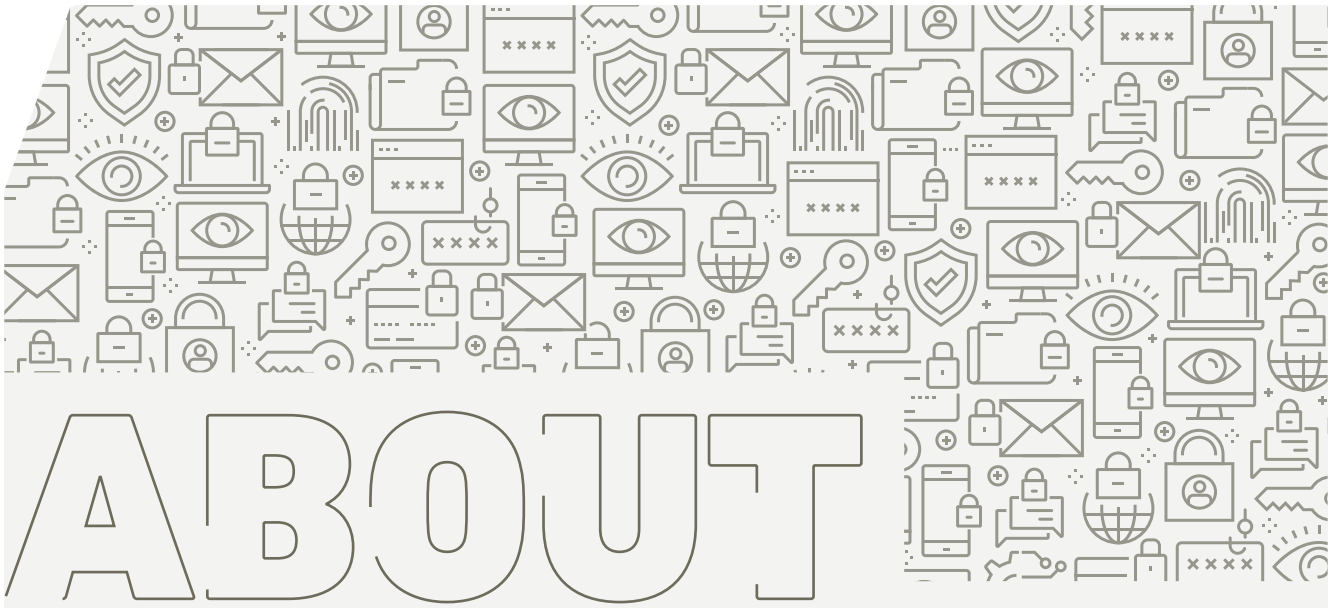
TACKLING DATA PRIVACY ISO 27701

BUREAU VERITAS



ABOUT

this white paper

Data privacy is a major issue today.

The quantity of data collected by businesses, combined with concerns over how it is used, have made governments aware of the need to protect consumers, resulting in stringent regulations such as the European General Data Protection Regulation (GDPR).

But regulation can only go so far in driving change.

The International Standards Organization has developed a new standard to help businesses keen to address data privacy and protect their customers: ISO 27701. The purpose of this white paper is to explain how implementing and certifying this management system can support you in addressing data privacy throughout your organization.

CONTENTS

DATA PROTECTION
has moved up the business agenda

In today's digitalized and globalized society, we have no choice but to share our personal information. Everything happens online: from banking, shopping and ordering pizza, to booking cinema tickets, dating and sharing photos. As more and more data is collected and processed, consumers, regulatory bodies and governments are increasingly concerned about how it is used - and protected from misuse.

We are right to be concerned. In recent years, there has been no shortage of high-profile scandals involving companies collecting customer data without permission or using information inappropriately or even illegally. In addition to how they use it, how organizations protect our personal information is of paramount importance. Improperly handled data can result in the disclosure of confidential and potentially sensitive information leading to everything from a client's bank account being drained to national security breaches.

The business impact on companies hit by a cyber-attack or involved in a data misuse scandal can be significant. From compensating customers to investigating the incident, the costs can be huge. In the longer term, a company's reputation can be severely harmed – as can its share price.

To win consumer trust and gain competitive advantage, companies must make data privacy and security a top priority. Compliance with new and increasingly stringent regulation is a license to operate. Certification to a recognized data privacy standard is a powerful demonstration of a commitment to protecting the privacy of all stakeholders.

32% of UK business

identified cyber security breaches in 2019 (1)

57% of consumers

describe the ability to opt-out of having their data shared with third parties as very important. (2)

88% of consumers' willingness

to share personal data depends on their trust in the given company. (3)

(1) ***UK Government,*** *Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2019*

(2) ***IBM,*** *Consumer attitudes towards data privacy survey 2019*

(3) ***PwC,*** *Consumer Intelligence Series Protect.me, 2017*

GOVERNMENT AND BUSINESS
response to date

Europe's response to the regulatory needs of our digital world was the introduction of the General Data Protection Regulation (GDPR) which entered into force in 2018. The GDPR aims to protect individuals' data, prevent security breaches and control data processing. It also harmonizes laws across the EU to simplify compliance. The GDPR's extra-territorial reach has given it impact beyond EU borders, prompting governments the world over to create or reinforce their own laws.

Many countries have introduced stringent legislation. Brazil's 2020 General Data Protection Law, for example, models its extra-territorial reach on the GDPR. Australia recently updated its data privacy regulations, and South Korea reinforced the penalties associated with its already stringent Network Act. In the United States, the state of California enacted the California Consumer Privacy Act, which gives consumers more control over how businesses collect and use their data. Meanwhile, Bahrain became the first Middle Eastern country to adopt a comprehensive privacy law.

For multinational companies, ensuring compliance with the various laws in all the countries where they do business is likely to become costly and time-consuming. The risk of non-compliance is even more problematic, with the possibility of hefty fines, damage to reputation, and loss of business. The most effective solution to ensure compliance is a structured and monitored management system consistently implemented across all at-risk operations.

1800+

data privacy laws

in place or under development worldwide

(4) ***PwC,*** *Risk Atlas 2019*

Implementing a

MANAGEMENT SYSTEMS APPROACH

Many data protection regulations such as GDPR require organizations to adopt data privacy policies and designate a specific role, charging that person with ensuring good data privacy practices are observed across the organization.

But this approach does not ensure compliance in itself. The weak link in many organizations is people. To ensure that good practices are observed requires a comprehensive system encompassing the controls to be put in place, who is responsible for ensuring they are followed, and how compliance and progress are to be monitored and assessed. In short – a management system. Putting in place a comprehensive Privacy Information Management System (PIMS) is a way to ensure that the organization addresses its own, specific risks and opportunities. It is a way to achieve not only compliance, but continual improvement.

WHAT IS ISO 27701?

The new international data privacy standard is an extension to ISO's existing standard for information security (ISO 27001). ISO 27701 enables companies who have already implemented an ISO 27001-compliant Information Security Management System (ISMS) to go further by putting in place steps to protect the data privacy of their customers and other stakeholders. It provides guidance on collecting and processing personal information for use by organizations of all types and sizes.

WHY IMPLEMENT ISO 27701?

Safeguard your reputation
by protecting consumers' personal information

Target compliance
with data protection regulations

Identify and mitigate risk
by implementing rigorous privacy controls

Inspire stakeholder trust
by putting data protection at the heart of your business

Ensure employees understand their roles
and responsibilities with regard to data privacy

Improve skills and business processes
to avoid non-compliance

ISO 27001 ISMS

the starting point for a data protection management system

WHAT ARE ISO 27001 AND ISO 27002?

The ISO 27001 standard covers requirements for implementing, maintaining and improving ISMS. An ISMS is a framework of policies and procedures that includes technical and physical controls involved in an organization's information security risk management processes. By following the best practices laid out in ISO 27001, companies can tackle security risks, protect sensitive data, and manage their security programs. ISO 27002 is a complementary standard that offers additional guidance on the process of selecting, implementing, developing and managing information security controls.

WHAT DOES ISO 27001 COVER?

The main aim of ISO 27001 is to provide requirements to establish, implement, maintain and improve a management system to assess and manage information security risks in relation to the context of the organization. It addresses asset management, operational security, access control, incident management, human resource security and physical security. As one of the most widely-accepted security standards, conformity to ISO 27001 can be used to help demonstrate compliance with stringent data privacy regulations.

WHAT ARE THEIR LIMITS?

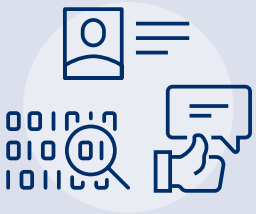
While implementing ISO 27001 is a valuable step and can support the process of GDPR compliance, by itself it is not sufficient to ensure organizations achieve regulatory compliance.

ISO 27002 provides practical guidance on information security controls but does not list individual controls in relation to specific personal data protection practices. These include consent for the processing of personal data; data portability; the right to be forgotten; the right to restriction of processing and objection; and international transfers of personal data.

ISO 27701 has been created to address the gap between information security practices and arrangements specific to personal data protection. For organizations looking to achieve and demonstrate their commitment to data privacy, going a step further with certification to ISO 27701 is recommended.

KEY CONCEPTS

DATA PRIVACY MANAGEMENT



PERSONALLY IDENTIFIABLE INFORMATION

Is any data that can be used to identify or trace an individual (i.e. name, social security number, credit card) and any other information linked to an individual (i.e. financial or medical records).

KNOWN AS
PERSONAL DATA
UNDER GDPR

PII PRINCIPAL

This refers to the person to whom personally identifiable information relates.

KNOWN AS
DATA SUBJECTS
UNDER GDPR

PII CONTROLLERS

Collect personal data and determine the purposes for which it is processed. More than one organization can act as PII controller ("co-controllers") making data sharing agreements necessary.

KNOWN AS
DATA CONTROLLERS
UNDER GDPR

PII PROCESSORS

Processes data on behalf of a PII controller. This category includes suppliers to PII controllers.

KNOWN AS
DATA PROCESSORS
UNDER GDPR

UNDERSTANDING ISO 27701

Taking privacy further

ISO 27701 is a privacy extension to ISO 27001 ISMS, which works by bolting privacy requirements on to an existing Information Security Management System.

At a basic level, this means reading ISO 27001 in a new way: any reference to "information security" in ISO 27001 should now be read as "information security and privacy". It also means adding privacy requirements and controls beyond those set out in ISO 27001. These are set out in clause 5 and Annexes A and B of the standard. Finally, ISO 27701 offers guidance beyond that set out in ISO 27002 depending on whether the organization is a PII controller or a PII processor.

The following pages explain some of the important points covered by ISO 27701. This is by no means exhaustive, but is intended to provide an overview of the types of requirements and guidance offered by the standard.

WHAT ARE THE MAIN REQUIREMENTS OF ISO 27701?

The new standard for data privacy requires that organizations develop a Privacy Information Management System (PIMS) specific to their business. You must first establish whether you are a PII controller or a PII processor – or both. You must also identify any applicable privacy legislation and other external or internal factors that could shape the design of its PIMS. These typically include regulations such as GDPR, but might also include, for example, contractual demands from clients.

AS AN ORGANIZATION *you need to make sure you have* ***the right processes in place to identify risks*** *relating to data processing – and then* ***ensure these processes are followed.***

Once the context and scope have been agreed, you can establish, implement and maintain a PIMS, preparing the ground for continual improvement. Many of the clauses included in ISO 27001 and other recent ISO standards relating to implementation and maintenance of the management system also apply to ISO 27701. These include the need for leadership and commitment by top management on the issue and a clear organizational structure, with roles and responsibilities for personal data management identified, assigned and thoroughly understood across the organization.

Risk identification and management is also a major requirement in ISO 27701. The information security risk assessment that forms part of ISO 27001 ISMS is extended. The new, wider risk assessment includes PII risks associated with loss of data confidentiality, integrity and availability.

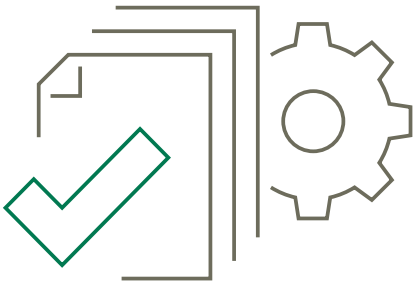
PRIVACY-SPECIFIC CONTROLS
required by ISO 27701

An important part of ISO 27701 is explaining your data privacy approach to external and internal stakeholders. You should develop a data privacy policy or enhance your existing information security policy to demonstrate your commitment to compliance with applicable regulations and any standards demanded by clients or other partners.

You should also designate a role for someone that customers can contact regarding personal data – known as a "Data Protection Officer" under GDPR. This responsible person works with the technical stakeholders in the business to develop, implement, maintain and monitor an organization-wide governance and privacy program that targets compliance with data privacy regulations. The role encompasses the development of a Statement of Applicability detailing the controls implemented, and a policy addressing the requirements for backup, recovery and restoration of PII, to identify just two examples.

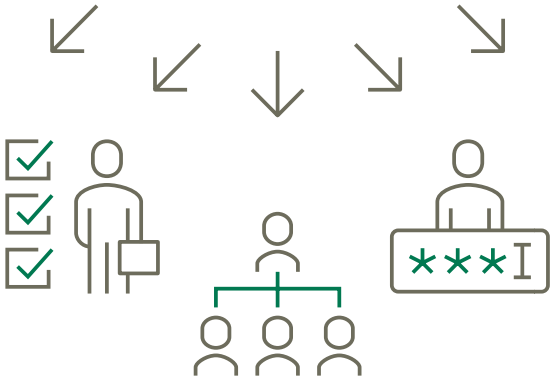
THE IMPORTANCE OF ACCESS RIGHTS

One important topic covered by ISO 27701 is access rights. The standard sets out procedures for registering and de-registering users for systems and services that process PII. Each user should have a personal access ID, and the record of user profiles should be kept up-to-date. This is essential to another key aspect of the PIMS – event logging. These logs record access to PII (who, when, to whom, any changes) with reviews of event logs used to identify any irregularities.



YOUR MANAGEMENT SYSTEM

should detail roles, responsibilities and access rights



The standard also includes practical guidance relating to control of personal information in specific situations. For example, you should ensure that the use of mobile devices does not lead to a data breach; similarly, it recommends that you only allow the use of removable storage devices that allow encryption. Organizations are encouraged to minimize printing of personal data files, and take technical measures to ensure that when storage space is reassigned, intentionally deleted PII is no longer accessible.

ADDITIONAL GUIDANCE
for PII controllers and processors

WHAT ADDITIONAL GUIDANCE APPLIES TO PII CONTROLLERS?

Clause 7 together with Annex A set out specific guidance for PII controllers. The guidance goes into extensive detail on how PII should be managed, covering aspects such as:

- The need to identify the specific purpose for which data is collected
- Ensuring individuals understand why, and how their data is being processed
- Obtaining consent for data processing
- Ascertaining compliance with relevant regulations
- Considerations relating to PII sharing, transfer and disclosure
- Privacy by design and privacy by default
- etc.

...AND TO PII PROCESSORS?

Clause 8 together with Annex B cover specific PIMS guidance for PII processors. Much of this relates to how a PII processor should conduct its business in order to support its PII controller customers to ensure compliance. Specific sub clauses cover contracts, for example, and the need to provide the customer with records relating to data processing to demonstrate – and help the customer demonstrate - compliance. Topics such as PII sharing, transfer and disclosure are also covered, setting out the specific role of the PII processor.

SECURE SYSTEMS

A KEY FEATURE OF ISO 27701

While much of ISO 27701 relates to organizational procedures and behavior – creating a culture of data privacy – some clauses relate specifically to design of systems themselves. Systems and components related to PII processing should be designed following the principles of privacy by design and privacy by default (see below). They should also make it easy for the organization to implement controls. In particular, data collected should be limited to what is strictly necessary for the identified purposes.

PRIVACY
by DEFAULT

requires organizations to have an information system that guarantees a high level of PII protection at all stages. The result is a high level of reassurance for customers that their data is secure, as well as compliance with regulatory requirements.

PRIVACY
by DESIGN

requires organizations to take into account respect for PII protection in the design of products and services using personal data.

ISO 27701

COMPLIANT IN 3 STEPS

Ready to get started?
Bureau Veritas Certification can support you to achieve data privacy best practice

1 ASSESS YOUR NEEDS

Have you already implemented an ISO 27001 Information Security Management System? If so, you're already on the road to data privacy compliance. Carry out a gap assessment of your current ISMS against the requirements of ISO 27701. If you don't yet have an ISMS, don't worry: you can implement both standards at the same time.

› ***Watch a Bureau Veritas webinar on how to get started***

2 DESIGN YOUR PIMS

Modify and build upon your ISMS to take into account data privacy requirements. Remember that the success of your management system will depend on people: managers need to understand the system and their responsibilities within it.

› ***Bureau Veritas can support you with training for implementers, managers and internal auditors***

3 GET CERTIFIED

Certification to ISO 27701 provides independent assurance that you have implemented the standard across your organization and that any non-conformities are addressed. In doing so, it supports you to achieve regulatory compliance, and demonstrate to customers that you take data privacy seriously. If you don't yet have an ISMS, don't worry: you can implement both standards at the same time.

› ***Bureau Veritas provides accredited certification to both ISO 27001 and ISO 27701***

SHAPING A WORLD OF TRUST

Bureau Veritas is a Business to Business to Society company, contributing to transforming the world we live in. A world leader in testing, inspection, certification and technical services, we help clients across all industries address challenges in quality, health & safety, environmental protection and social responsibility.

For more information, contact Bureau Veritas:

Le Triangle de l'Arche
8 cours du Triangle
CS 90096
92937 Paris La Défense Cedex
FRANCE

certification.contact@bureauveritas.com

www.bureauveritas.com

BUREAU VERITAS

Editorial & Design: hollisbean.com / +33 1 83 62 20 41 / Image credits: iStock