bsi.

...making excellence a habit.™

Privacy matters

Managing personal information with ISO/IEC 27701

A BSI whitepaper for business

Introduction

Digitalization, globalization and personalization of services, from booking a doctor's appointment to internet banking, have led to greater collection and processing of personal information than ever before. And this trend is growing as opportunities for new services arise, and new players enter the market.

There are now so many different platforms people use as part of their daily routine where personal information is collected such as the growth in mobile applications, loyalty schemes, connected devices and location-based advertising. This means we are regularly handing over our data without thinking it through, creating more data flows than ever before. And whether it's dating sites, telecoms providers or public service organizations, there is barely a day that goes by when you look at the news and don't see reference to a data breach where personal records have been compromised. This has only increased the focus on issues surrounding the misuse of personal information, meaning organizations cannot afford to be complacent.

Greater awareness of these issues has led to growing concern, among both individuals and governments, around how personal data is collected, used and protected; in response, some governments have proposed or enacted new regulations aimed at providing guidelines and requirements for treatment of personal data.

Within Europe, the introduction of the General Data Protection Regulation (GDPR) provides a harmonization of data privacy laws that reflect the realities of the digital world we now live in.

Many other countries, such as Korea, Australia and China, are also creating data protection legislation. In anticipation of the increased regulatory environment and a need for a common set of concepts to address the protection of personal data, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have taken the initiative to create standards to provide such guidance. These standards have the benefit of providing frameworks for assisting organizations to demonstrate personal data protection and privacy compliance with different laws in a changing regulatory landscape. Certification may also be a useful tool for organizations to add credibility to their commitment to privacy and related obligations.

Managing personal information

Given the dynamic environment in which we operate, the need for guidance on how organizations should manage and process data to reduce the risk to personal information is getting more important. Guidance, in the form of a new international standard, for how organizations should manage personal information and assist in demonstrating compliance with updated privacy regulations around the world is therefore very powerful. That's why ISO/IEC 27701 for privacy information management has been developed.

What is ISO/IEC 27701?

This new international standard is officially called ISO/IEC 27701 (Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines).

As many organizations have implemented an Information Security Management System (ISMS) based on ISO/IEC 27001 and using the guidance from ISO/IEC 27002, it's a natural step to provide guidance for the protection of privacy that builds on this strong foundation.

ISO/IEC 27701 is a privacy extension to ISO/IEC 27001 and ISO/IEC 27002 and provides additional guidance for the protection of privacy, which is potentially affected by the collection and processing of personal information. The design goal is to enhance the existing ISMS with additional requirements in order to establish, implement, maintain and continually improve a Privacy Information Management System (PIMS). The standard outlines a framework for personally identifiable information (PII) controllers and PII processors to manage privacy controls so that risk to individual privacy rights is reduced (see Table 1). These additional requirements and guidance are written in such a way that they are practical and usable by organizations of all sizes and cultural environments.

Table 1 – Personal information management roles

PII Controller	**PII Processor**
Collects personal information and determines the purposes for which it is processed. More than one organisation can act as PII controller often known as co-controller, and this is where data-sharing agreements may be necessary.	Processes personal information on behalf of and only according to the instruction of the PII controller.
How ISO/IEC 27701 helps PII Controllers	**How ISO/IEC 27701 helps PII Processors**
• Provides best practice guidance • Gives transparency between PII controllers • Provides an effective way to manage PII processes	• Provides best practice guidance • Gives reassurance to customers that PII is effectively managed

ISO/IEC 27701 developing the standard

ISO/IEC 27701 was drafted by the ISO/IEC Working Group responsible for 'Identity Management and Privacy Technologies'. Its development was led by a BSI-nominated Project Editor and BSI was appointed by the UK Government as the National Standards Body and represented the UK interests at both the ISO and the IEC.

It's intended that organizations will certify to ISO/IEC 27701 as an extension to ISO/IEC 27001 management system. In other words, organizations planning to seek an ISO/IEC 27701 certification will also need an ISO/IEC 27001 certification. This demonstrates commitment to both information security and privacy management.

How ISO/IEC 27701 fits in

Requirements and guidance for the protection of personal information vary depending upon the context of the organization and where national laws and regulations are applicable. ISO/IEC 27001 requires that this context be understood and taken into account. ISO/IEC 27701 gets more specific. It includes mappings to:

- the privacy framework and principles defined in ISO/IEC 29100
- ISO/IEC 27018 and ISO/IEC 29151, which both focus on PII

However, all these mappings need to be interpreted to take into account local laws and regulations. It is also worth noting that ISO/IEC 27701 is applicable to all organizations that act as processors, controllers or both; ISO/IEC 27018 applies specifically to public cloud providers.

BS 10012:2017+A1:2018* is a published standard specific to the UK. It provides a best practice framework for a personal information management system that is aligned to the principles of the European Union (EU) GDPR. One of the key distinctions between ISO/IEC 27701 and BS 10012 is that ISO/IEC 27701 is structured so that the PIMS can be considered an extension to ISMS requirements and controls.

ISO/IEC 27701 can be used by PII controllers (including those who are joint PII controllers) and PII processors (including those using subcontracted PII processors).

An organization complying with the requirements in ISO/IEC 27701 will generate documented evidence of how it handles the processing of personal information. This evidence may be used to facilitate agreements with business partners where the processing of personal information is mutually relevant. This might also assist in relationships with other stakeholders. The use of ISO/IEC 27701 in conjunction with ISO/IEC 27001 can, if desired, provide independent verification of this evidence, although compliance with these documents cannot be taken as compliance with laws and regulations.

Benefits of ISO/IEC 27701

- Gives transparency between stakeholders
- Helps build trust
- Provides a more collaborative approach
- More effective business agreements
- Clearer roles and responsibilities
- Reduces complexity by integrating with ISO/IEC 27001

*An amendment to BS10012:2017 was published 2018 (BS 10012+A1:2018). This amendment covers minor changes to some clauses of BS10012:2017; these changes have been made to reflect the UK Data Protection Act 2018.

To validate that the adequate operational controls from the standard are implemented consistently, to carry out the compliance requirements of relevant privacy regulations, measures must be taken to:

1. map the relevant regulatory requirements against the standards controls
2. enumerate specific regulatory requirements that are not already fully captured by the standard controls and the conditions to which the requirements become applicable
3. incorporate the above into the risk assessment process in the audit cycle

A good example to examine is the data breach management controls in ISO/IEC 27701 and the breach notification requirements (article 33) in GDPR. By all measures, the standard's security incident management controls mapping squarely with the GDPR data breach requirements. But the standard does not contain a specific 72-hour notification as required by the law. In order for the practitioners to demonstrate that the organization has implemented a management system that fulfils this particular GDPR requirement, they must show the auditors that the organizations either have a uniform process in place that would notify the data subjects and the privacy regulators within 72 hours of breach confirmation or has a process to determine if the breach involves European citizens or if the breached data processing took place in Europe and, if so, trigger the notification within the required timeframe.

The mapping of standard against regulations and enumerating of unique regulatory requirements and applicable conditions are the necessary mechanisms to which controllers and processors can use ISO/IEC 27701 to verify regulatory compliance against multiple privacy regulations.

Data privacy laws

As the challenge increases for organizations to keep data secure and minimize the risk of a breach, it's unsurprising to see privacy laws evolving to keep up with the changing business landscape. Most notably, the EU GDPR has received a lot of attention.

The GDPR is EU law for the preservation of fundamental rights and freedoms that everyone has the right to the protection of personal information concerning them. These rights must also be preserved in respect of data processing activities and the free flow of personal information between EU Member States. The processing of data should be for the benefit of the natural persons that the data belongs to. Similar laws exist around the world to protect the personal information and rights of citizens, including some sector-specific requirements such as healthcare, retail and banking.

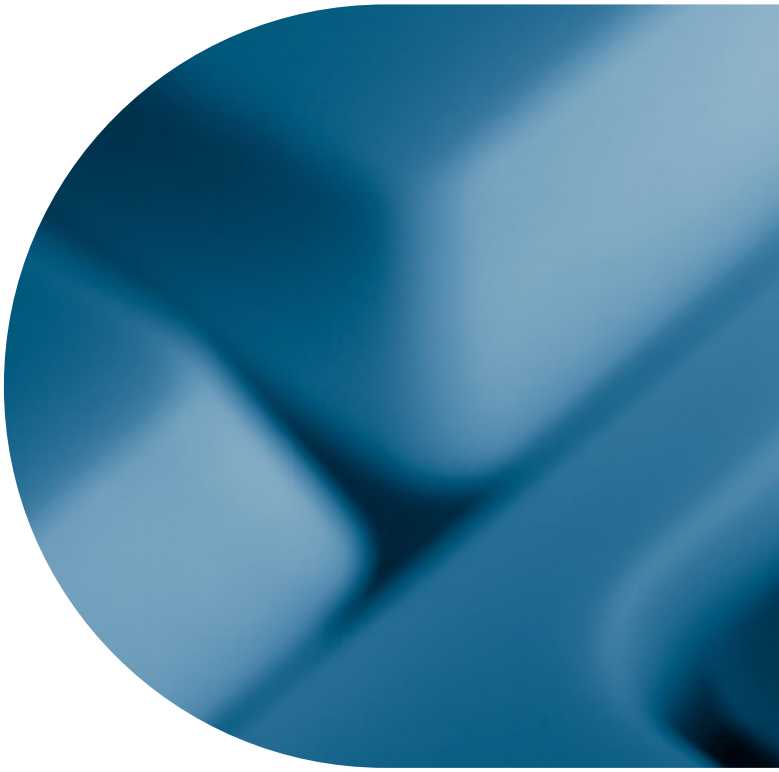
Healthcare sector

As a sector that collects some of the most sensitive personal information, healthcare-specific data protection laws are very prominent. For example, there is the French Public Health Code (Article L.1111-8) that requires service providers who host certain types of health/medical data to be accredited for this activity. And the Health Insurance Portability and Accountability Act in the United States sets the standard for sensitive patient data protection and requires U.S. health plans, healthcare clearing houses and healthcare providers, or any organization or individual who acts as a vendor or subcontractor with access to personal health information, to comply.

It is also important to highlight the European Digital Single Market. This is a policy, announced in 2015, that covers digital marketing, e-commerce and telecommunications. It aims to open up opportunities for people and businesses, breaking down existing barriers. It has three core pillars:

- Access to online products and services
- Conditions for digital networks and services to grow and thrive
- Growth of the European digital economy

It facilitates cross-border data processing and commerce. However, differences in data privacy laws across member states of Europe were recognized as a barrier to the European Digital Single Market being a success. Therefore, the introduction of GDPR to help harmonize data privacy across all of Europe is a positive step change.



Certification mechanisms to help demonstrate compliance with data protection laws

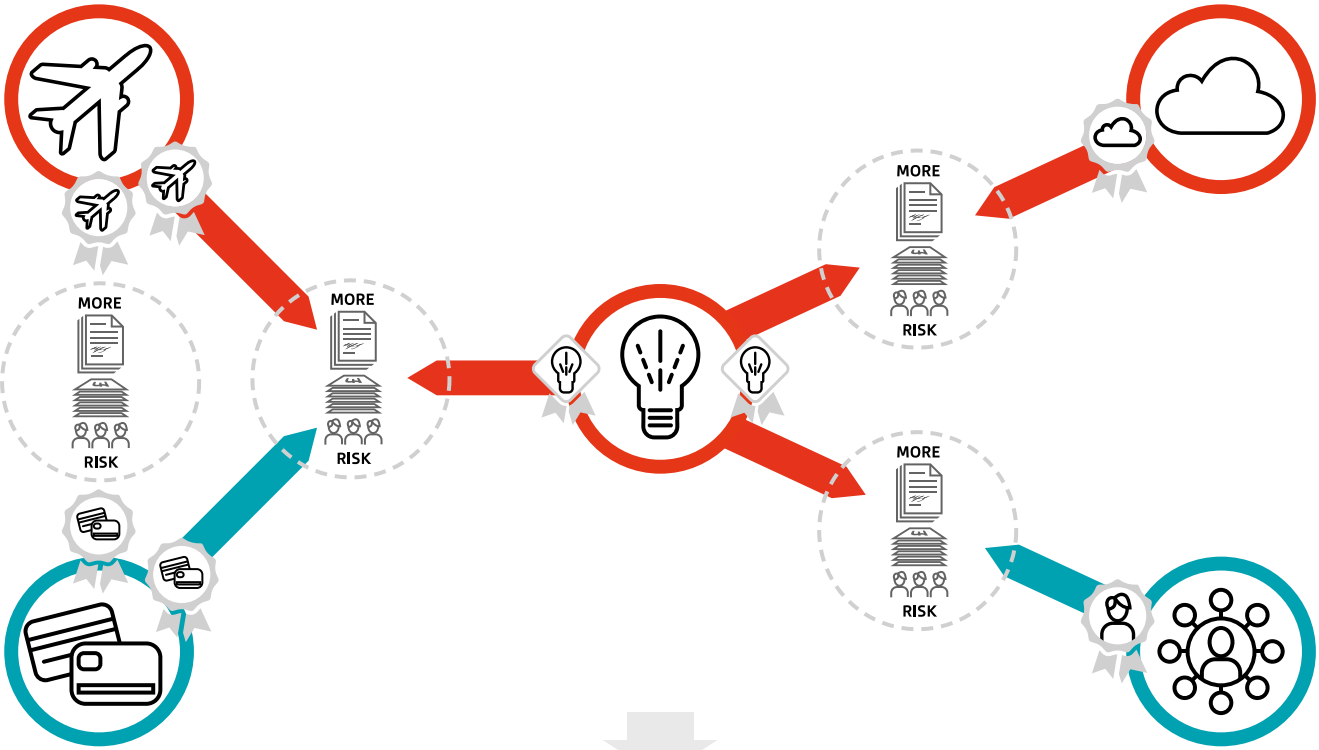
The GDPR encourages data protection certification mechanisms and data protection seals and marks to be established to help demonstrate compliance with the regulations of processing operations by controllers and processors (GDPR (EU) 2016/679, Article 42). Plus, such certification or seals can be used to show that an organization has taken the right measures to handle personal information in a way that aligns with the GDPR.

Consistent certification mechanisms can bring the all-important 'accountability' factor into the picture, facilitating the reduction of risk and improving the free flow of personal information. This helps organizations provide useful services, whilst increasing transparency of the process and showing integrity to customers on the protection of personal information as illustrated in **Figure 2**.

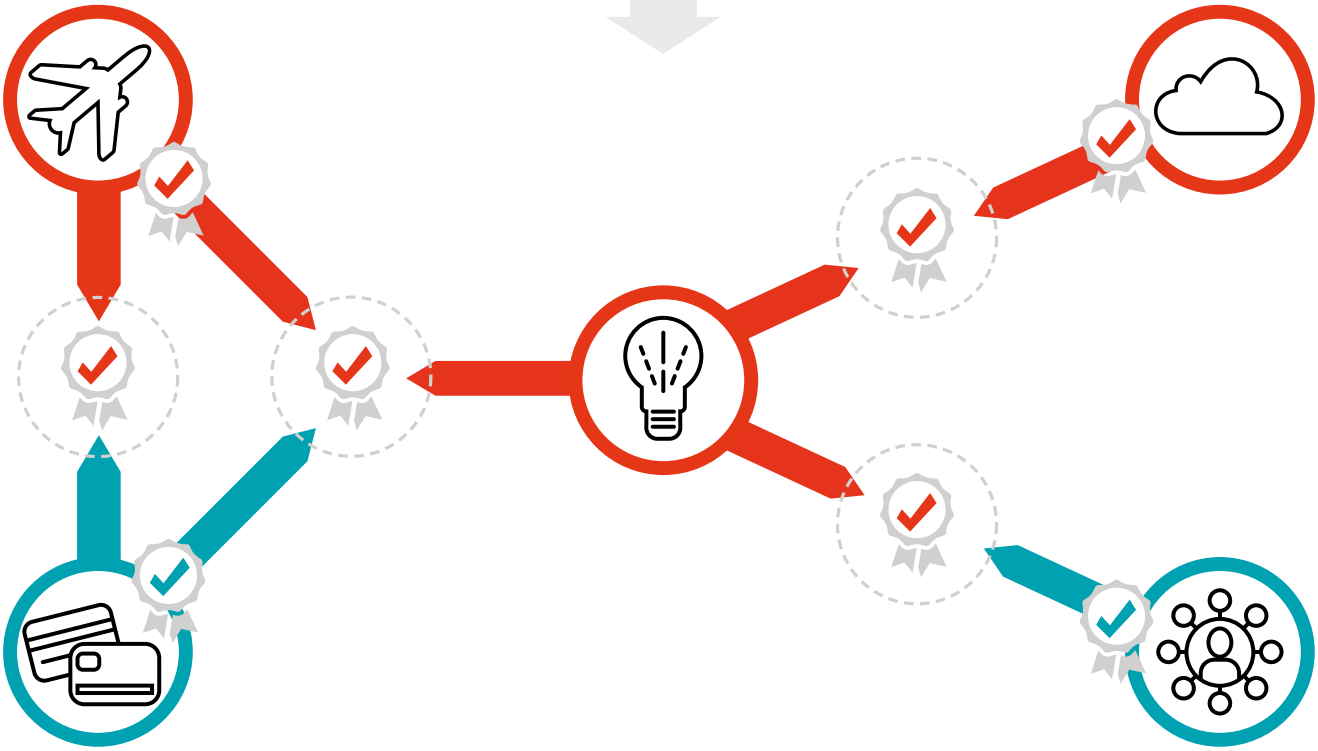
It also brings to the surface the importance of data processing to supply chain management, as the controller is responsible for the data from cradle to grave. Consider a product such as a credit card that is co-branded by an airline and a bank. Customer information from both sides would need to be exchanged to identify which customers are likely to take up such a product. The exchange of a customer's personal information introduces a risk. How does each side verify that the other will adequately protect their customer's data? The risk is exacerbated as further players are involved. A marketing company may be contracted to target customers, perhaps even buying adverts on a social media platform. A cloud service might also be used by the marketing company to store and process data related to this marketing campaign. Certification can serve as an independent verification that will prove the effectiveness of the process and controls the organization uses to assess the risk of exchanging personal information between organizations throughout the supply chain.

However, as depicted in **Figure 2(a)**, if one organization uses a certification scheme in one jurisdiction, and another is certified to a different scheme that is applicable in another jurisdiction, this may not provide the necessary assurance or level of trust to business partners that personal information belonging to their customers is being properly treated. Given the global nature of business, a consistent and uniform assurance mechanism is required to show that organizations comply with regulations, protecting personal information and providing an enabler for business growth as depicted in **Figure 2(b)**. A common GDPR certification recognized across jurisdictions and industry verticals is necessary to mitigate risk and lower barriers to trade between commercial partners.

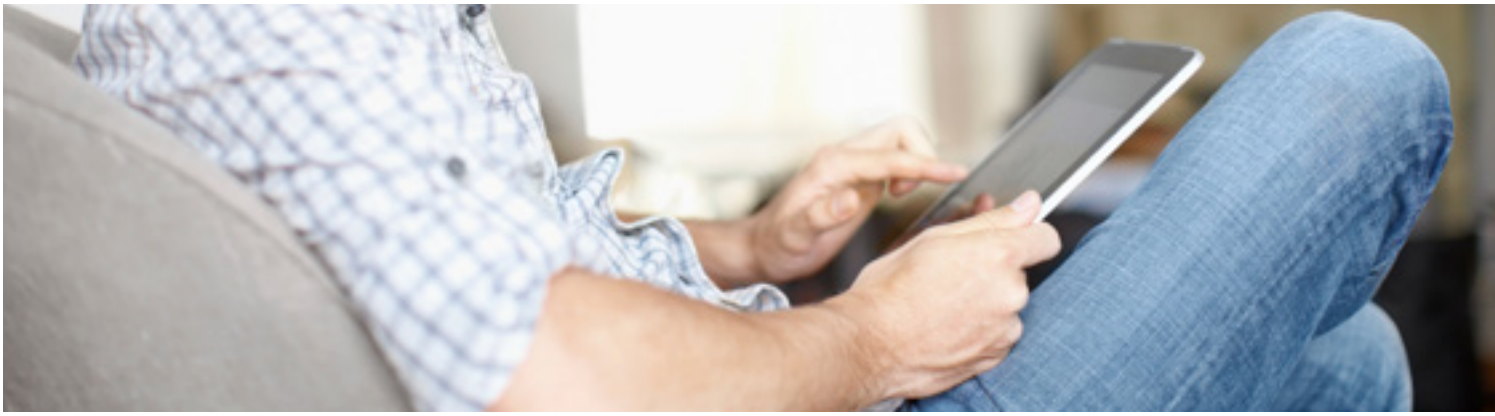
Figure 2 – Enabling commerce through consistent data privacy certification mechanisms.
(a) Fragmented certification between organizations.



(b) Consistent certification



This sentiment is echoed by the European Union Agency for Network and Information Security (ENISA) which recently published recommendations on certification for GDPR [ENISA: Recommendation on European Data Protection Certification, Version 1.0, November 2017; https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification]. ENISA state that certification, seals and marks have a significant role to play in enabling data controllers to achieve and demonstrate compliance of their processing operations with GDPR provisions. ENISA recommends that national certification bodies and supervisory authorities under the guidance and support of the European Commission and European Data Protection Board should pursue a common approach on inception and deployment of GDPR certification mechanisms. They also recommend that the approach is scalable and uses approved and widely adopted criteria. Consistency and harmonization of certification mechanisms across Europe are emphasized, and the trustworthiness and transparency are reinforced as important traits of the certification process.



ISO/IEC 27701 is a potential certification mechanism

ISO/IEC 27701 addresses the recommendations above, and it's anticipated, could be used as the basis of a certification mechanism (as stipulated by Article 42). If used in such a way, it would provide the necessary proof that an organization treats the personal information of its customers in compliance with the law, including for the case of cross-border data flows. ISO/IEC 27701 is applicable to organizations of all sizes and cultural environments. It is for the collection and processing PII of both employees and customers. The set of controls being developed extends technical measures for implementing information security to also address privacy requirements and, if implemented by an organization, can assist in demonstrating compliance with data privacy laws such as GDPR.

Therefore, demonstrating compliance with the controls in ISO/IEC 27701 and generating the required documentation as evidence of how an organization handles PII can:

- significantly reduce compliance workloads by negating the need to support multiple certifications
- increase trust between organizations and customers by demonstrating compliance with data privacy laws
- generate evidence that Data Protection Officers can provide to senior management and board members to show their progress in privacy regulatory compliance
- increase the opportunities for business and commerce through the EU Digital Single Market and cross-border data flows

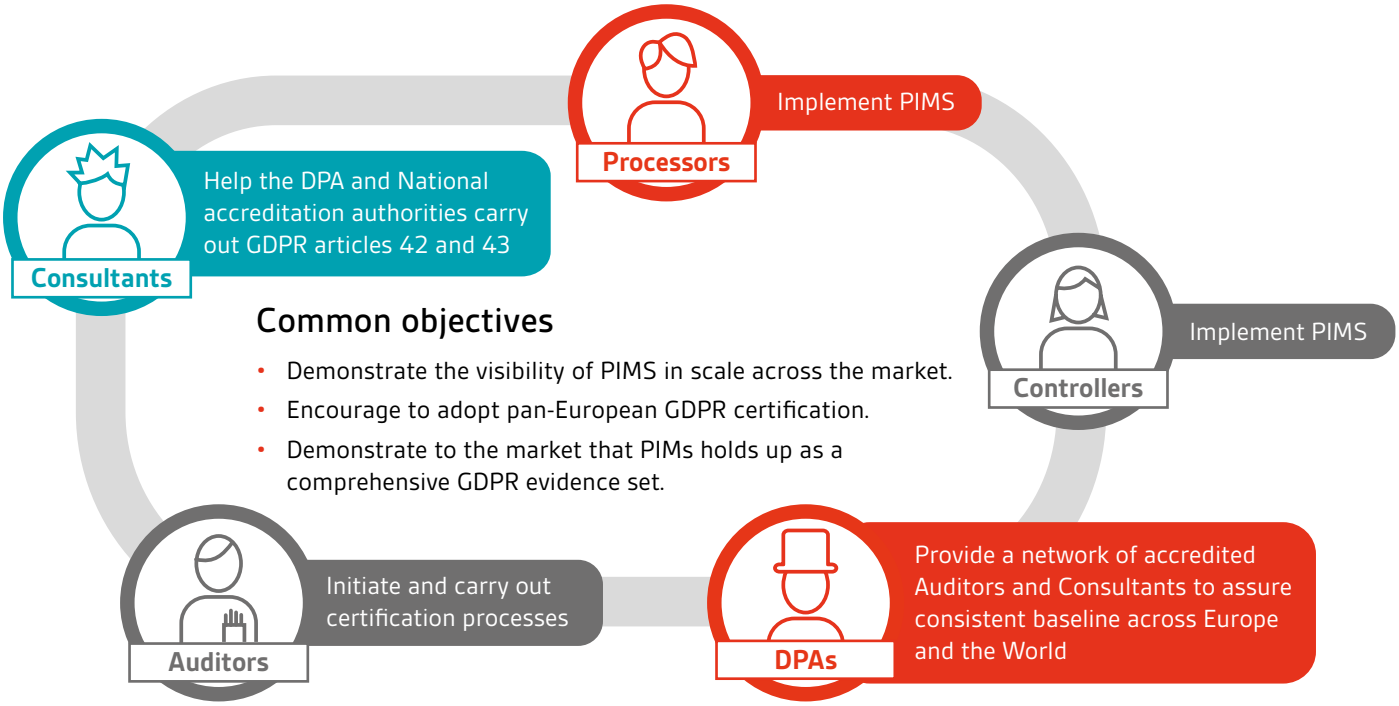
Furthermore, the intended application of ISO/IEC 27701 is to augment the existing ISMS with privacy-specific controls and create a PIMS that enables effective privacy management within an organization. With a well-established network of auditors providing certification against ISO/IEC 27001, which is commonly accepted as a successful standard for information security, ISO/IEC 27701 is in a very good position to be integrated into existing audit processes.

ISO/IEC 27701 was developed through recognized consensus-driven processes; this is one of the key tasks in developing the standard. There has been input and review from a range of industry and regulatory stakeholders; this includes participation and review by the European Data Protection Board (previously, the Article 29 Working Party), consisting of Data Protection Authorities (DPA) from all EU countries. DPAs, as well as accreditation bodies for auditors, will need to be satisfied that a certification mechanism based on ISO/IEC 27701 adequately assists organizations from all industry sectors and of all sizes to demonstrate compliance with privacy regulations. Additionally, a certification mechanism must address the needs of controllers and processors, both of which have numerous controls defined for them in ISO/IEC 27701.

Importance of stakeholder engagement

As previously mentioned above, ISO/IEC 27701 is an extension to ISO/IEC 27001, and the standard is structured in the ISO management systems convention (commonly referred to as 'Annex SL'), allowing multiple management systems to be implemented more efficiently by an organization. **Figure 3** shows the landscape of stakeholders and the importance of their roles. By already working with the existing ISO/IEC 27001 ISMS, all these stakeholders will be in a very good position to work with ISO/IEC 27701. They all share common objectives on personal information management and the need for a recognized approach to show it is being taken seriously, which is where the role of ISO/IEC 27701 comes in.

Figure 3 – Stakeholder landscape for certification based on ISO/IEC 27701 (source: Microsoft).



Conclusions

To conclude, managing personal information in compliance with the evolving regulatory landscape is complex but cannot be ignored. The protection of an individual's personal information is one of their fundamental human rights. Laws exist around the world to protect these rights in an environment where business and data related to personal lives are becoming increasingly globalized. The European GDPR has been introduced to ensure that collection and processing of PII are conducted lawfully, and it supports the cross-border data flows required to enable the EU Digital Single Market.

The European GDPR recognizes that certification mechanisms for demonstrating compliance with regulations go a long way to increasing trust in how organizations treat personal data, whilst creating business opportunities through providing assurance between organizations. This is especially true if certification is implemented consistently between EU member states and beyond the borders of Europe to enable global commerce and business.

The introduction of ISO/IEC 27701 is a necessary addition to the existing standards portfolio. Implementing the controls specified in ISO/IEC 27701 should enable an organization to document evidence on of how it handles the processing of personal information. Such evidence may be used to facilitate agreements with business partners where the processing of personal information is mutually relevant and in the event of gaining a widely accepted certification mechanism, can assist in demonstrating compliance with data protection laws such as GDPR.

Why BSI?

BSI has been at the forefront of information security standards since 1995, having produced the world's first standard, BS 7799, now ISO/IEC 27001, the world's most popular information security standard. And we haven't stopped there, addressing the new emerging issues such as privacy, cyber and cloud security. That's why we're best placed to help you

Working with over 86,000 clients across 193 countries, BSI is a truly international business with skills and experience across a number of sectors including automotive, aerospace, built environment, food, and healthcare. Through its expertise in Standards Development and Knowledge Solutions, Assurance and Professional Services, BSI improves business performance to help clients grow sustainably, manage risk and ultimately be more resilient.

BSI/AU/1591/SC/0819/EN/GRP

Our products and services

Knowledge

The core of our business centres on the knowledge that we create and impart to our clients.
In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels.
In fact, BSI originally created eight of the world's top 10 management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools which help facilitate this process.

bsi.

BSI Australia
15 Talavera Road
Macquarie Park NSW 2113
Australia

T: 1300 730 134
E: info.aus@bsigroup.com
bsigroup.com/en-au

Find out more about
ISO/IEC 27701 with BSI

Call **1300 730 134**
or visit **bsigroup.com/en-au**