bsi.

...making excellence a habit.™

Privacy regulation

Understanding the role of ISO/IEC 27701

By Kieran McDonagh, Riskscape Law Ltd

A white paper

Contents

Introduction

The privacy of individuals' personal data is very topical. An organization must carefully consider how to handle the personal information of customers, employees, visitors and neighbours; for many organizations this is a challenge. The application of the GDPR (General Data Protection Regulation) in May 2018 meant that all organizations, no matter where they were based, now have to comply with the GDPR if they handle the personal data of citizens of the EU. Beyond the EU, at least 132 countries now have a privacy law in place. Organizations that transfer personal data between these countries must take each relevant law into account when considering controls to protect privacy.

Implementing and monitoring controls to support compliance with such laws can be a complex challenge. To make this more manageable, having standards in place can give organizations more confidence in the steps they have taken in fulfilling regulatory compliance. Such standards include ISO/IEC 27701 which is an internationally agreed standard that enables organizations to extend their existing ISO/IEC 27001 Information Security Management System (ISMS) to address privacy requirements.

This white paper sets out an overview on regulations related to privacy, the role ISO/IEC 27701 can play and what this means for businesses and consumers.

The European privacy landscape

The personal data of millions of European consumers have been protected by law through the GDPR since 25 May 2018. All organizations, of whatever size, that handle personal data must be compliant with the GDPR, or with a local law that incorporates the GDPR. For example, in the UK this means complying with the Data Protection Act 2018 (DPA 2018).

The EU's Charter of Fundamental Rights, which was given legal power through the Treaty of Lisbon in 2009, includes individuals' right to privacy. The GDPR is built on this right to privacy, and so requires that privacy must be taken into account when individuals' personal data is collected, analysed, shared, stored and deleted (collectively 'processed'). The GDPR includes a series of principles that require the processing of personal data to be:

- processed lawfully, fairly and transparently for the individual
- collected for specific purposes and not reused for other purposes
- minimized in its collection and processing
- kept up to date
- stored for the shortest time possible
- secured against unauthorized processing, and loss, destruction or damage

The GDPR sets out the types of controls that must be in place if the privacy of individuals' personal data is to be protected. When reviewing how personal data is processed, the GDPR requires an assessment of whether such processing represents a high risk to the rights and freedoms of the individuals whose personal data is being processed. This assessment needs to be applied in many different circumstances where personal data is processed. Some organizations have found it difficult to assess these risks and have sought advice and guidance from regulators about how to carry out this assessment.

The role of ISO/IEC 27701

The ISO/IEC 27701 standard extends the ISO/IEC 27001 ISMS to incorporate privacy requirements. Since many organizations already have an ISO/IEC 27001 ISMS, it reduces the complexities around establishing a Privacy Information Management System (PIMS), since the ground has already been laid. Those organizations familiar with ISO/IEC 27001 will be able to extend their ISMS to address privacy and support them in GDPR compliance, as well as other privacy laws, by providing a means to demonstrate commitment to privacy information management.

The standard identifies controls that must be in place to allow the management of personal data, or Personally Identifiable Information (PII) to be systematic and transparent. It sets out controls that are required if the organization is acting as a controller or a processor of PII.

Controls in the standard cover the entire life cycle of PII collection, analysis, sharing, storage and deletion. The individual, which the PII relates to, is placed at the centre of these controls, just as the GDPR requires.

The benefits of the standard

Global consistency

Organizations often operate in more than one country and so have many privacy and information security requirements from different jurisdictions. By using an internationally recognized standard, the organization can gather all the requirements together so that only one set of actions is needed to help achieve and maintain compliance. This is particularly important when organizations transfer PII across borders where different laws and control requirements exist on either side of the border.

Stakeholder management

A standard can also provide a structure to incorporate the additional requirements set by the organization's stakeholders such as the Board or customer representatives.

A standardized approach for privacy and information security compliance, based on a best practice standard, provides a clearly signposted beginning, middle and end to a compliance programme. Meeting the requirments of a standard can be used to support the business case for achieving or maintaining compliance, helping to make the issue tangible for senior management. Strong stakeholder buy-in is an essential element in the success of such a programme.

Programme management

An organization that insists that any capital expenditure is managed through a formal project can also use a standard as a framework for programme management, incorporating the risk assessment, mitigation and monitoring activities of both change and 'business as usual' activities.

Programmes often use a formal process for identifying requirements and project objectives that together can add real value. A standard provides a structure for doing precisely this and, when coupled with an internal or external assessment, it provides a tight framework for co-ordinating compliance activities. This helps avoid distractions and digressions on peripheral issues, ensuring a focus on achieving and maintaining compliance.

Using a standard as part of a programme management discipline can help different departments, geographies and technical functions to work together on a single transparent set of requirements. This is essential if cross-border data transfers are to be controlled in more than one country.

Also, using a project delivery approach means that simple metrics can be used to explain progress to senior management in a way that gives credibility to the work of achieving and maintaining compliance. Providing senior management a simple view of the progress towards privacy and information security compliance is essential for the management of the legal risks associated with new laws such as the GDPR. This is particularly the case as fines for non-compliance can be measured in the millions.

Internal education

A standard document can also be used to educate non-specialists in the technical discipline of the standard. It can also help to structure training programmes that provide awareness training across the organization, as well as accredit technical staff as experts in their field. Privacy and information security controls must be successfully implemented and followed by every member of staff, consultants, contractors, visitors and third parties if an organization is to be compliant. Each group needs specific training programmes aligned to their needs to ensure that they are fully aware of their responsibilities and how to operate controls effectively. A standard provides a framework that allows training programmes to be comprehensive, while sharing common messages across different groups.

Assurance

A standard can also be used to provide a framework for testing controls and providing assurance on privacy and information security using successful test results. It helps establish requirements that translate into control objectives and can support the identification of particular controls that an organization must have in place to comply with privacy and information security requirements. Tests of the controls can then be planned, carried out and reported to provide assurance to internal and external stakeholders. A standard allows this workflow to be organized systematically and to be managed as a project to meet senior management objectives.

Demonstrating the achievement and maintenance of compliance with a recognized standard can help to provide assurance to internal and external stakeholders such as regulators and suppliers throughout the supply chain. Both will insist on assurance from an organization on their compliance with privacy and information security requirements, with suppliers needing this before accepting components or services. This requirement is becoming an increasingly important part of supply chain assurance. A standard provides a baseline of controls that allows both upstream and downstream supply chain partners to understand the risks of sharing information, and allows them to mitigate any residual risks by implementing additional controls over their data transfers.

Proactive approach

No matter how many privacy and information security controls are in place, organizations will still be at risk of experiencing a data breach. Where an organization complies with a standard, but nonetheless suffers a privacy or information security breach, the organization can claim that they suffered the breach despite compliance with a best practice standard. The alternative is that they cannot demonstrate their best endeavours to comply, putting them at risk.

When reporting such a breach to the relevant regulators, being compliant with a recognized standard can provide assurance to the regulators that controls are organized systematically and can be strengthened easily following the breach. Without demonstrating compliance with a standard, organizations may need to do more to convince regulators that they have a mature control environment and that it takes compliance with privacy and information security requirements seriously.

Discussions with regulators in these situations can often involve sanctions. The organization can use their compliance with a recognized standard as a mitigating factor in argument against sanctions or fines. As fines under the GDPR can be significant, up to four per cent of annual global turnover, the return on investment on complying with a recognized standard could be very positive.

Key concepts

The language of privacy and information security requirements can seem daunting to those new to the field. However, help is available as defining key concepts is central to the work of creating international standards. Some definitions will be widely accepted by practitioners, while others will be disputed, sometimes indefinitely. Nonetheless, standards present an internationally recognized definition of key concepts that practitioners can use in their day-to-day work of implementing controls. ISO/IEC 27701 and associated standards define many of the key concepts that a compliance programme in privacy and information security requires. Some of these key concepts are described below.

Definition: Personally Identifiable Information (PII)

ISO/IEC 27701:2019 uses the vocabulary common to the suite of ISO 2700x standards that cover information security and associated controls. It uses the term Personally Identifiable Information (PII) to describe the information assets that must be protected and managed when providing security and privacy for a PII principle or individual.

PII is defined in section 2.9 of ISO/IEC 29100:2011 as information that can be used, on its own or combined with other linked information, to identify a PII principle or individual. This term is most often used in US Federal Laws such as the Health Insurance Portability and Accountability Act (HIPPA), which helps protect medical records and other personal health information. So, for example, an individual's IP address is not in itself PII. However, if it is reasonably possible to combine with other linked information, such as names in IP allocation tables, then this becomes PII.

Sensitive PII is defined in section 2.26 of ISO/IEC 29100:2011 as PII that contains information related to the most intimate details about a PII principle or individual, or whose impact on the individual, if disclosed, would be significant.

Definition: Privacy

'Privacy' can be considered as the term that describes the end result of adequate controls over the 'processing' of PII. Section 2.22 of ISO/IEC 29100:2011 includes the definition of a privacy stakeholder as a PII principle or individual that can be affected by a decision or activity related to the processing of PII. Privacy can therefore be defined as the prevention of adverse impacts on PII principles or individuals as a result of the processing of PII.

The GDPR does not define privacy, but states as its objective in Article 1, as the protection of the fundamental rights and freedoms of individuals with regard to the processing of personal data, and in particular their right to the protection of their personal data.

The risk to privacy of PII is defined in section 2.19 of ISO/IEC 29100:2011 as the effect of gaps in information about an event, its likelihood or consequence for the privacy of PII.

Privacy controls are defined in section 2.14 of I SO/IEC 29100:2011 as organizational, physical and technical measures that treat privacy risks by reducing their likelihood or consequence.

Personal data – EU terminology

In the EU, the term 'personal data' has been used in the GDPR. 'Personal data' is defined in Article 4 as any information relating to an individual that, using reasonable means, allows them to be identified. So, for example, profiling an individual through their IP address, even though their name may not be disclosed, will make this information 'personal data'.

In the EU, special categories of personal data are defined in Article 5 of the GDPR as revealing the most sensitive details about an individual, which might prevent them exercising their rights and freedoms under the Charter of Fundamental Rights of the EU. For example, information about an individual's racial or ethnic origins, religious beliefs or sexual orientation would be considered a special category of personal data. The GDPR would then require this information be protected using additional privacy controls.

Definition: Information security

Privacy is impossible without adequate information security. Adequate information security is necessary for privacy of PII but is not by itself sufficient. Preventing the disclosure, loss or corruption of PII cannot be effective unless the entire life cycle of the PII processing is protected through information security controls. Section 3.28 of ISO/IEC 27000: 2018 defines information security as the end result of adequate controls to preserve the confidentiality, integrity and availability of information.

Confidentiality is defined by section 3.10 of ISO/IEC 27000:2018 as a property of information security where information is not disclosed to those unauthorized to receive it. Disclosure could be the result of a deliberate leak of information outside an organization, an accidental disclosure to the wrong person or a deliberate transfer that was based on inaccurate advice and so was an unauthorized disclosure.

Integrity is defined by section 3.36 of ISO/IEC 27000:2018 as a property of information security where information retains its accuracy and completeness. Controls should also be in place to update the accuracy and completeness of the information in order to provide assurance about these properties to its users.

Availability is defined by section 3.7 of ISO/IEC 27000:2018 as a property of information security where information is made accessible on demand to authorized users. The requirements of users for access to information will vary by the criticality of business process and therefore the sophistication of arrangements required to provide the information under all circumstances will also vary.

The GDPR defines a principle of information security for personal data in Article 5. It requires the use of appropriate technical or organizational measures to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Section 3.28 ISO/IEC 29000:2018 notes that other properties of information security, such as authenticity, accountability, non-repudiation and reliability can also be considered part of information security. Most practitioners see these as sub-properties of confidentiality, integrity and availability.

Definition: Control

A control is an activity that provides a means of treating risk. Section 3.14 of ISO/IEC 29000:2018 defines a control objective as a description of what a control is intended to achieve. While section 3.61 defines a control as a measure that modifies risk, and in the case of privacy controls, modifies privacy risk. The GDPR does not define a control or a control objective.

Good practice supports the identification of control objectives to address particular privacy risks. One privacy risk might apply to more than one privacy control objective. Each control objective requires the design of a suite of controls – some organizational, some technical – that with effective operation addresses the privacy risk to PII. The privacy controls, as defined in section 2.14 of ISO/IEC 29000:2018, reduce the likelihood or consequences of a privacy risk materializing. Compliance against ISO/IEC 27701 would require each control objective to be defined, and controls designed to meet each of these, so providing a framework of controls that together support the privacy of PII.

Definition: Testing

Testing is the activity of assessing the effectiveness of the design of a control or its operation. Without adequate testing, it's impossible to accurately assess whether the control is suitable to achieve the control objective. Similarly, without adequate testing of the operation of the control, it's impossible to accurately assess whether the control is effective in treating risk.

Good practice in testing requires a test plan to be created in advance. This plan should set out:

- the control objectives
- the characteristics of the control design that will be tested
- the criteria against which the design will be assessed
- sample sizes for the output of the control in operation
- threshold acceptance levels that demonstrate effective operation
- reporting lines for acceptable and unacceptable testing results

The testing of privacy controls should consider the central use cases as set out in the analysis of the business process that handles PII. However, no business process works perfectly in all situations, and so testing must also consider use cases where business processes are operated incorrectly or are disrupted by internal or external agents for malicious reasons. Only when the full suite of use cases has been tested successfully can the privacy risk be considered to be under control.

External sources of information can contribute to the risks to the privacy of PII. For example, the principle of minimization can mean that organizations collect very little PII. However, no matter how little PII is collected, when combined with other sources of data, it can allow individuals to be identified and their privacy placed at risk. Testing of privacy risks should also consider scenarios where external sources of data are combined to identify an individual. A celebrated example of this is when a journalist managed to combine different sources of data to allow them to successfully apply for a passport in the name of the Information Commissioner.

Compliance to ISO/IEC 27701 would require an organization to demonstrate that risks to the privacy of the PII that it handles had been assessed, controls put in place and controls shown to be operating effectively through a comprehensive framework of control testing. Testing would therefore be central to this process.

Overview of the global privacy regulation landscape

The key source of information on applying the GDPR is the European Data Protection Board (EDPB). It issues guidance on various topics, such as carrying out Data Protection Impact Assessments, which is available online (https://edpb.europa.eu/guidelines-relevant-controllers-and-processors_en).

The EDPB took on the role of its predecessor organization, the Article 29 Working Group, which had been created by the Data Protection Directive 95/46/EC that was incorporated into UK law as the Data Protection Act 1998. When the EDPB was formed, it adopted all of the guidance published since 1997 covering topics such as employee monitoring and breach notification. All of this guidance is available online (https://ec.europa.eu/justice/article-29/documentation/index_en.htm).

When reviewing an area it believes needs guidance, the EDPB works to establish a consensus between each of the Data Protection Authorities (DPAs) throughout the EU, such as the UK's Information Commissioner's Office (ICO) (www.ico.org.uk) and France's Commission Nationale de l'Informatique et des Libertés (CNIL).

DPAs are responsible for registering organizations that control the processing of personal data, providing advice to organizations and to individuals, responding to complaints from individuals and investigating and fining organizations that have experienced a data breach. The DPA will also prosecute organizations if they believe that their processing of personal data is not compliant with the GDPR.

While there is still ambiguity over how to comply with some aspects of the GDPR, instances where a DPA prosecutes an organization for non-compliance will provide a useful indication about how the DPA and the courts expect organizations to comply with the law. Where a case is appealed to the European Court of Justice, the EU's supreme court, the judgements can be considered definitive. These cases tend to offer an indication of how to implement the GDPR in some of the most complex circumstances. These cases are reported online (https://eur-lex.europa.eu/homepage.html?locale=en).

The global impact of GDPR

The GDPR covers the personal data of European citizens, no matter where their data is processed, and has therefore set a high standard for organizations all over the world. Other countries, when considering how to revise their own data protection laws, have looked to the GDPR as an up to date model for data protection in the age of global social media. Brazil has introduced a new data protection law (LGPD) that comes into force in 2020 which adopts many of the principles of the GDPR. In addition, the new California Consumer Privacy Act (CCPA), which also comes into force in 2020, adopts some of the concepts of the GDPR. Legislators in Washington DC have been negotiating to introduce a federal data privacy law that may pre-empt the CCPA, and their efforts have centred on achieving similar protections to those in the GDPR. Being compliant with the GDPR therefore means less effort is required to comply with international laws.

Other European privacy laws

The GDPR was created at the same time as two parallel laws, Regulation (EU) 2018/1725, that require good data protection practices in EU institutions, and the specific data protection Directive (680/2016) that requires good data protection practices in EU law enforcement bodies. The Regulation (EU) 2018/1725 came into effect for EU institutions on 11 December 2018, while the Directive came into effect in each jurisdiction through local enabling laws. It was incorporated into the UK's DPA 2018, which came into effect on 23 May 2018. A copy is available online (http://www.legislation.gov.uk/ukpga/2018/12/contents).

ePrivacy regulation challenges AdTech business model

In addition to the GDPR and the Directive, the EU is creating a new law to update the Privacy and Electronic Communications Directive 2002 (2002/58/EC) or the ePrivacy Directive. The Directive was given legal force in the UK through the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and became known as the 'cookie law'.

When introduced, the 'cookie' law required Internet sites to ask permission from users to place cookies on their computers. However, the law was not clear how this might work. Companies were concerned that in order to establish whether a user had previously opted out of having cookies placed on their computer, they would have to had already placed a cookie which could then inform the company about the user's preferences. The law also was unclear about whether a user had to opt-in to having cookies placed on each visit to a website, or just the first visit. As a result of this confusion, the law was interpreted widely, and many sites failed to comply with the spirit of the law.

The revision of the ePrivacy Directive is intended to respond to the changes in the processing of personal data on the Internet since the previous law in 2002, and to align requirements with the GDPR. This new law will be a regulation, just like the GDPR, and so will be uniformly applicable across the EU. The latest draft of the Regulation (13 March 2019) makes the processing of any personal data as part of electronic 'interpersonal communication' subject to privacy controls similar to the GDPR.

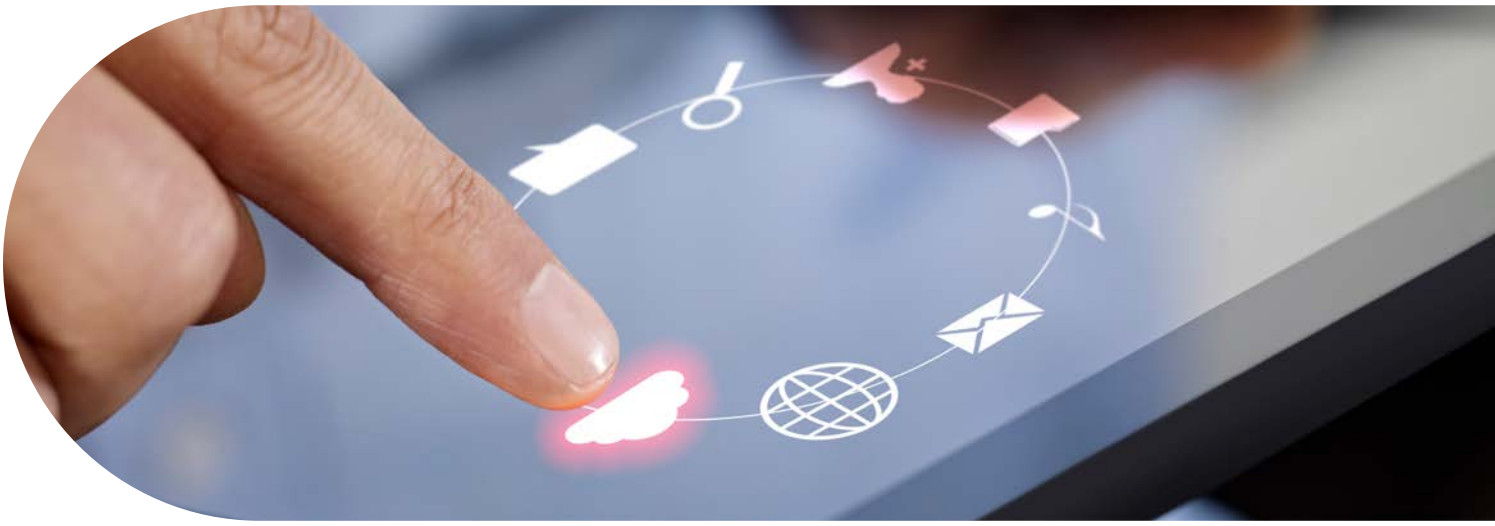
The processing of metadata has also been considered during the drafting of the Regulation. Whether the metadata associated with the processing of personal data online is also classified as personal data is an issue that has not yet been settled, but case law seems to be pushing towards this outcome. This would mean that metadata would also need to be protected by similar privacy controls to those for personal data.

The need to warn website visitors about the use of cookies to record activity on a site was the most public aspect of the original Directive. This requirement to warn visitors on every visit is one that some hoped might be discarded in the new Regulation.

The latest draft seeks to reduce the workload on visitors by allowing generic opt-in or opt-out to cookies within the browser settings. However, consent will still be required in most situations, and the level of consent is expected to meet that of the GDPR and so be 'freely given, specific, informed and unambiguous'. Websites will also have to inform visitors how their personal data will be processed and to which third parties it will be transferred. Some websites have already begun to structure their cookie consent banners to reflect this GDPR requirement, but the ICO has already highlighted that the majority of websites are not yet compliant with the GDPR.

For some organizations, the need to restrict processing, inform customers and secure consent will be a challenge. Where this challenge cannot be met, some organizations will have to change their business models. The ICO has warned organizations of this risk in its June 2019 publication on AdTech (https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf).

The ePrivacy Regulation is expected to be finalized later in 2019 or 2020 and become law automatically in all EU states within 24 months. Other countries, in the European Economic Area (Norway, Liechtenstein and Switzerland) would negotiate a timetable for the Regulation to apply to their countries. Third countries would have to negotiate bilaterally and reflect the requirements of the ePrivacy Regulation in local law, such as where certain country organizations wish to process the personal data of EU citizens online.



Competition law challenges for those processing large datasheets

Those organizations that process large amounts of personal data are discovering that their processing may also infringe competition law.

Competition law is designed to prevent a dominant market position being used to reduce competition from other organizations in the same market. Where organizations, such as social media platforms, process the personal data of large numbers of individuals, they might be considered to have a dominant position in the market for gathering market research data, and providing display advertising. New competitors might struggle to compete against an existing social media platform as the new company will not have the benefit of millions of existing customers and their Internet data. Where this dominant position is considered to prevent other organizations also gathering such market research data, reducing competition in the market, the social media platform could be subject to competition law scrutiny.

In the EU, the Commission's Competition Directorate tends to look at the market share of particular organizations in specific markets to determine whether there is a risk to competition in the market. Where competition law finds a dominant position in the market for market research data, sanctions can include fines for anti-competitive behaviour, divestment of subsidiaries or breakup of dominant groups. The European Commission is actively considering how new regulations might help to ensure that social media platforms do not reduce competition from other companies.

Online harm from personal data posted online

Where users post their own material online, in the so-called Web 2.0, this material can be considered personal data. Not only does a hosting site have to protect the privacy of this data, but it must also consider whether hosting this user-generated material will lead to harm to third parties. Calls have grown in a number of countries for social media platforms to be regulated like publishers of individuals' posts rather than merely as technology companies providing the platform's underlying technology.

In New Zealand, the Harmful Digital Communications Act 2015 requires hosts of user-generated material to delete online material if served with a complaint about specific content, even if the complaint is ignored by its author. In April 2019, the UK Government published a white paper that proposed placing a 'duty of care' on hosts of user-generated material (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf). If made law, it would require posts that are considered to contain material that is harmful to children or vulnerable people, to be removed within a strict time frame. Ireland is considering a similar law. Calls have been made in the US for social media platforms to take more responsibility for the user-generated material they host. The US Congress has taken this issue sufficiently seriously to ask the social media platforms to testify about how they deal with online harms.

There appears to be a drift of the law towards seeing the hosts of user-generated material as publishers rather than technologists. This change in status would have significant implications for all online hosting platforms, not just the major social media platforms. Any organization that hosts user-generated material may have to build new business processes to scrutinize posts and promptly delete those considered to be harmful.

Implementing privacy and information security standards

Standards can help to provide a baseline of control objectives for organizations that are seeking to comply with privacy and information security laws and regulations. Where multiple laws must be complied with, a single standard can be used to accommodate each set of legal requirements into a single structure that an organization can use as a focus for its compliance efforts. Implementing standards allows an organization to demonstrate to regulators, suppliers and customers that it not only has privacy and information security controls in place, but that senior management takes these issues seriously.

The challenge of GDPR certification

The EDPB published guidance in June 2019 (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf) on the requirements for new certification schemes that will allow organizations to demonstrate compliance with the GDPR. In the future, certification schemes are likely to be developed that cover aspects of GDPR compliance such as Data Subject Access Requests, Complaints Processes, Privacy by design and Communications with Data Subjects.

There are currently no certification schemes that cover all aspects of the GDPR. The EDPB has noted that certification schemes that cover only some GDPR controls can help organizations demonstrate their overall compliance with GDPR. A mosaic of certification schemes is therefore expected to form the basis of GDPR certification for most organizations for the foreseeable future.

Privacy governance

Good business governance is important to help organizations respond to changing environments, and there are different types of standards available to support. For example, management system standards help organizations to manage risk and improve performance across a range of areas from quality management and health and safety to privacy and information security.

The benefits of a management systems approach

Complying with any standard for a business process or product helps an organization develop in a specific discipline. However, implementing a management systems standard requires a much more robust approach that impacts all functions across the organization. If the management systems standard is going to be effective, it must be embedded into the existing management of the organization.

A management systems standard is focused on making compliance with the standard robust at any point in time and sustainable in the longer term. This type of standard makes the management of the organization as a whole much more systematic and transparent. Compliance against the standard demonstrates that the organization takes its management responsibilities seriously.

Leadership engagement

A key feature of a management systems standard is the requirement for the organization's senior management to be involved. This can bring significant management attention to issues, such as privacy and information security, and help to raise the profile of the issues within senior management teams. It can also support future conversations about the need for further investment and attention. For most organizations, the progress towards compliance is an everlasting one, and so following against an international standard provides ongoing focus for a programme that can lose focus after the initial burst of energy.

Integration efficiencies

Any management systems standard is also designed to be shared in a modular way, so that the effort of adding a new management systems standard to an organization is minimized. Once an organization has embedded a single management standard, say for quality, the extra effort required to add an additional management standard, say for privacy and information security, is much less than that for the initial standard.

Any organization that seeks to comply with privacy and information security requirements through a management systems standard is therefore investing in the robustness and sustainability of their organization in a way that allows other technical areas such as safety, or quality to be addressed in the future.

Conclusion

This white paper has explored the privacy regulation landscape. It has not only demonstrated a number of differences and similarities globally, but highlights the importance of specific regulatory requirements such as the ePrivacy Directive.

All regulations have positive intentions to support an individual's privacy rights, and the foundation set by GDPR has given a springboard for other countries and states around the world. There are of course nuances between these that can create a challenge for organizations, however that is where international standards can offer support.

ISO/IEC 27701 is a great example of a management systems standard that encourages organizations to put governance around their personally identifiable information activities. It requires jurisdictional differences to be considered and encourages senior management to take privacy seriously. This is of critical importance when new regulations are coming into place, and the impacts can affect the bottom line.

It is also essential to recognize that the regulatory landscape is complex, ever changing and needs to be regularly reviewed. By adopting a management system approach, organizations are encouraged to continually monitor and assess performance in light of the business environment in which they operate; and ISO/IEC 27701 is a great example of organizations, governmental bodies and academics bringing their knowledge together to provide a governance framework that can support this.

Author

Kieran McDonagh, Riskscape Law Ltd

Kieran McDonagh is an experienced data protection and cyber security professional. He has used international standards to audit, risk assess and remediate controls in data protection, cyber security, business resilience and supply chain risk management. He has led regulatory compliance projects for BNP Paribas, BP and Centrica, and he is currently a member of the BSI committee developing the international standard ISO 31700 – Privacy by Design. He has masters' degrees in cyber security, management science and law.

Reviewers

This white paper was peer reviewed by:

Geoffrey Goodell, Senior Research Associate, UCL CBT, UCL Computer Science.

One peer reviewer elected to remain anonymous

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.

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
389 Chiswick High Road
London W4 4AL
United Kingdom

T: +44 345 086 9001
E: cservices@bsigroup.com
bsigroup.com

Find out more about
ISO/IEC 27701 with BSI

Call **0345 080 9000**
or visit **bsigroup.com/iso27701-UK**