nqa.

ISO/IEC 27701 IMPLEMENTATION GUIDE

50,000 CERTIFICATES GLOBALLY

100% TRANSPARENT FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OVER 90 OPERATING COUNTRIES

MANAGING PERSONAL INFORMATION WITH ISO/IEC 27701

Since 2016, within a relatively short period, Data Protection legislation has been passed both in the UK and in the EU which shaped the requirements necessary to ensure the privacy of personal data which is taken by organisations. Both the EU General Data Protection Regulation (GDPR) and UK Data Protection Act 2018 (DPA) are now applicable to all organisations, regardless of sector, in the United Kingdom. The relative speed at which this legislation has been established has left some organisations unable to adequately respond, and well publicised breaches have occurred.

Despite the well signposted roll out of both pieces of legislature, neither regulation provides specific guidance on what measures should be taken to ensure compliance with their requirements. Further, existing standards do not have, in most cases, a robust enough set of clauses or controls to ensure data privacy is addressed in full through implementation of management systems.

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) have developed a new standard to provide the necessary guidance for businesses to effectively address data privacy and ensure the gap between existing management systems requirements and privacy data legislation is effectively bridged.

GDPR – An overview of legislation

The GDPR was adopted by the EU in April 2016 and replaced the EU Data Protection Directive 95/46/EC. This new legislation has initiated obligations to any organisation with data processing responsibilities, and is applicable to organisations outside of the EU too. The penalties for failure to comply can be severe. Fines of up to 4% of annual global turnover or €20million await any organisation which breaches the legislation.

Primarily the goal can be perceived as being an EU data privacy harmonisation. As previously mentioned any non-EU entity offering goods or services to individuals located in the EU are also bound by the requirements of the GDPR. Business sectors with sizeable personal data processing requirements are uniquely affected and ensuring conformity to the legislation is paramount.

Organisations are required to confirm explicit and unambiguous consent from customers, based on specific purposes for use of their data and for specific periods of time. Individuals have the right to request a copy of all data that is held on them, including an explanation of how such data is used and if third parties have access. Individuals may request for their data profile to be passed to another data processor; furthermore, individuals also have the right to withdraw consent and to request for data that is no longer required to be erased.

Data responsible processes or individuals are now required to have appropriate security controls in place to ensure confidentiality of the data they hold or process and have mechanisms in place to measure that effectiveness.

Notifications of data breaches must be submitted to the supervisory authority; for the UK this is the Information Commissioners Office (ICO) within 72 hours of recognition of a breach being identified. The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Further international data transfer rules from the Data Protection Directive are continued within the GDPR. Personal data can be transferred outside of the EU, but only to countries which are considered to have comparable protection mechanisms.

Further guidance can be found through the UK Government Data Protection Act 2018 page.

WHAT IS ISO 27701 AND WHY IS IT NEEDED?

As previously indicated there has been no guidance on how to effectively implement processes within an organisations existing structure to adhere to GDPR. ISO 27701:2019 is a privacy extension to the international information security management standard, ISO 27001 (ISO 27701 Security techniques – Extension to ISO 27001 and ISO 27002 for privacy information management – Requirements and guidelines).

ISO 27701 details the requirements for and gives the required guidance for the establishment, implementation, maintenance and improvement of a Privacy Information Management System (PIMS). The standard is based on the requirements, control objectives and controls of the ISO 27001 standard, and includes a suite of privacy requirements, controls and control objectives.

Concepts of information safety are familiar to organisations which already have an operational Information Security Management System (ISMS). The new PIMS will ensure that organisations have comprehensive and universal data governance which directly map to the legislative requirements.

Instances of GDPR breaches have been well publicised and have affected organisations with both national and global mandates. A recent Capgemini report outlines that up to 70% of all organisations believe that they are not currently compliant to GDPR requirements. The severity of the penalties which organisations attract through non-compliance has necessitated the creation of this standard.

BOLT ON TO ISO 27001

ISO 27701 differs slightly in that the standard requires an existing management system to attach to. Not every clause and control is applicable in all instances.

The requirements of the standard are split in to the four groups listed below:

1. PIMS requirements related to ISO 27001 are outlined at clause 5
2. PIMS requirements related to ISO 27002 are outlined at clause 6
3. PIMS guidance for Personally Identifiable Information (PII) Controllers are outlined at clause 7
4. PIMS guidance for PII Processers are outlined at clause 8

Additionally, applicable controls are outlined within Annex constructs to the main body of the standard.

The following can be used as a guide for relevance:

1. Annex A lists all applicable controls for PII Controllers.
2. Annex B lists all applicable controls for PII Processors.
3. Annex C maps the provisions of ISO 27701 against ISO 29100.
4. Annex D maps the provisions of ISO 27701 against the GDPR.
5. Annex E maps the provisions of ISO 27701 against ISO 27018 and ISO 29151
6. Annex F provides guidance for applying ISO 27701 to ISO 27001 and ISO 27002.

In most circumstances, organisations with existing certification to ISO 27001 should start at Annex F to understand how the application of PIMS fits in to their existing ISO 27001 ISMS. This annex refers to three instances for application of the standard to protection of privacy of PII principals when processing PII:

- Application of security standards as is
- Additions to security standards
- Refinement of security standards

The clause areas within PIMS extend the requirements of ISO 27001 to incorporate PII considerations. Clause 5 provides a PIMS-specific guidance set concerning the information security requirements in ISO 27001 appropriate to an organisation which acts as either a PII controller or processor.

The sub-clauses outline detailed requirements. This is perhaps the most pertinent area for those with existing ISMS to consider and dwell on requirements.

ADDITIONAL CONSIDERATIONS

Detailed below are the additional considerations within clause 5 of the ISO 27701 standard which may be observed as extra to existing ISMS requirements:	
5.1	The requirements of ISO 27001 must be extended to the protection of privacy as potentially affected by the processing of PII. A glance at Annex F provides a table which gives visual indication of how this will look.
5.2.1	An additional requirement to ISO 27001 clause 4.1 is to outline that an organisation will determine its role as a PII Controller and/or processer. Additionally external and internal factors that are relevant to context and affect the ability to achieve outcomes of its PIMS require indication. This includes any relevant legislation adherence already in place as a consideration within the existing ISMS or contractual requirements which hitherto had been identified in differing clauses or Annex controls within ISO 27001.
Where an organisation has both PII controller and PII processor roles identified, separate roles must be determined, each of which will be subject to a separate control set.	
5.2.2	A consideration extra to ISO 27001 clause 4.2 is the requirement to include interested parties with responsibilities associated with the processing of PII. This can include customers, which again is not something which may have previously been considered in an ISO 27001 ISMS. Additionally requirements which are relevant to the processing of PII can be determined by legal requirements, contractual obligations or self-identified objectives.
5.2.3	The scope of the ISMS is required by ISO 27001 clause 4.3. Additional PIMS factors for scope include an organisation including processing of PII. PIMS scope determination, therefore, can require a revision of the ISMS because of the extension to interpretation of what constitutes information security in ISO 27701 clause 5.1.
5.2.4	Further to ISO 27001 clause 4.4 an organisation is required within the new standard to establish, implement, maintain and continually improve a PIMS in accordance with the requirements of ISO 27001:2013 Clauses 4 to 10, extended by the requirements in Clause 5.
5.3	Within ISO 27001, organisations are required to demonstrate commitment to the ISMS through leadership initiatives and the creation of policies, roles & responsibilities and guidance. Likewise, the PIMS requires a similar input from the top management along with relevant PIMS specific interpretations as indicated at 5.1 to ISO 27701 which covers all mirrored aspects of clause 5 of the ISMS.
5.4.1	The requirements of ISO 27001 to address risks and opportunities require augmentation with the considerations of clause 5.1 in ISO 27701. Furthermore, Information Security risk assessments identified within ISO 27001 are applicable with the following additional requirements: 1. The organisation shall apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability, within the scope of the PIMS. 2. The organisation shall apply privacy risk assessment process to identify risks related to the processing of PII, within the scope of the PIMS. 3. The organisation shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed. This can be an integrated risk assessment process or parallel processes which are controlled separately; this depends entirely on the organisation to determine. Additionally, ISO 27001 clause 6.1.2.d is refined to include an assessment for potential consequences for both the organisation and PII principals that would result if the risks identified during the 6.1.2.c (ISO 27001) were to materialise. Further considerations are given to the Statement of Applicability which would have been generated by the organisation when implementing the ISO 27001 ISMS. As an organisation would have encountered an “opt out and justify” approach to produce the SoA in the first instance, likewise for the PIMS, not all control objectives and controls listed within Annex areas need to be included during PIMS implementation. Justification for exclusion where controls are not deemed necessary can be identified.
5.4.2	Information security objectives from the organisations ISMS from clause 6.2 augmented by the interpretation of ISO 27701 clause 5.1 must be considered.
5.5	Support considerations from ISO 27001 at clause 7 are applicable along with the additional interpretation specified within ISO 27701 clause 5.1.
5.6	Operational consideration from ISO 27001 at clause 8 including risk treatment planning are similarly required by ISO 27701 along with additional information which is identified through addressing clause 5.1 to the latter standard.
5.7/5.8	Similarly; the Monitoring/Measuring & Improvement considerations which are live within an existing ISMS require further augmentation from the considerations given to clause 5.1 to ISO 27701.

The processes identified above indicated that clause 5.1 to the new standard is a key point to the implementation of a PIMS. The extension to the protection of privacy as potentially affected by the processing of PII is a key element to implementation and guides the consideration given when addressing the further clause areas of ISO 27701.

The following table provides a simple overview of the information on the previous page:	
ISO 27001 Clause	**ISO 27701 Extension**
5.1 **5.2** **5.3** **7.1** **7.4**	Top Level Commitment for Privacy Policy and integration of PIMS to the ISMS of an organisation including: **1.** Resourcing/Establishment of Roles **2.** Communication (Internal/External) **3.** Anticipated outcome **4.** Control and Guidance **5.** Continual Improvement of PIMS
6.2	PIMS/Privacy Objectives
7.2	Competency profiles of individuals assigned to privacy requirements
7.3	Awareness of the PIMS policy and how personnel contribute to the establishment and improvement of the system
7.5	Documentation for PIMS with additional considerations on information and documentation non-organic to the organisation.
8.1	PIMS Risk Treatment activation
8.2	PIMS Risk Assessment process
8.3	PIMS Risk Treatment Plan including amendments to existing risk registers
9.1 **9.2** **9.3**	PIMS Performance and analysis of PIMS effectiveness including: **1.** Internal Audit **2.** Management Review
10	PIMS Continuous Improvement considerations