Privacy Information Management with ISO 27701

Patrick Soenen, Partner, Qualified Audit Academy

GDPR

The application of the **General Data Protection Regulation (GDPR)** on 25th May 2018 means that all organisations, wherever they are established, must now comply with this regulation if they process the personal data of EU citizens. Therefore, an organisation must carefully consider how to handle the personal information of customers, employees and visitors. However, the regulation doesn't provide much guidance on what the measures to protect personal data should look like.

Overview of the ISO 27701

The ISO/IEC 27701:2019 standard is the first international privacy standard, which outlines the requirements for implementing a **Privacy Information Management System (PIMS)**, to govern the handling of personal data, called Personally Identifiable Information (PII) in ISO 27701.

Who should implement ISO 27701?

ISO 27701 has been designed to be used by all data controllers and data processors. Like ISO 27001, it advocates a risk-based approach so that each conforming organisation addresses the specific risks it faces, as well as the risks to personal data and privacy.

GDPR certification

While ISO 27701 is not yet governed by accreditation bodies, it is expected that certification bodies will begin to audit against this new ISO standard despite no established scheme has yet been defined at the International Accreditation Forum (IAF) level.

ISO 27701 - an extension to ISO 27001

Since many organisations already have an ISO 27001 ISMS, it reduces the complexities around establishing a Privacy Information Management System (PIMS), since the ground has already been laid. Those organisations familiar with ISO 27001 will be able to extend their ISMS to address privacy and support them in GDPR compliance by providing a means to demonstrate commitment to privacy information management.

Terminology differences between GDPR and ISO 27701

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 data subject, called PII principal.

The major differences in terminology between the ISO 27701 standard and GDPR are outlined in the table below:

ISO 27701	GDPR
Personally identifiable information (PII)	Personal data
PII controller	Data controller
PII processor	Data processor
Joint PII controller	Joint controller
PII principal	Data subject
Privacy by design	Data protection by design
Privacy by default	Data protection by default

To make this publication easier to read, we have replaced the above ISO 27701 terms by the GDPR terminology.

Information security

Adequate information security is necessary for privacy of personal data but is not enough by itself. Preventing the disclosure, loss or corruption of personal data cannot be effective unless the entire life cycle of the personal data processing is protected through information security controls. The ISO standard defines information security as the result of adequate controls to preserve the confidentiality, integrity and availability of information.

Good practice supports the identification of control objectives to address 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 organisational,

some technical – that with effective operation addresses the privacy risk to personal data.

Understanding the context

The organisation shall determine its role as a data controller and/or a data processor.

The organisation shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include:

- applicable privacy legislation;
- applicable regulations;
- applicable judicial decisions;
- applicable organisational context, governance, policies and procedures;
- applicable administrative decisions;
- applicable contractual requirements.

Where the organisation acts in both roles (e.g. data controller and a data processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

Information security risk assessment

Following requirements are applicable to information security risk assessments:

- 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.
- The organisation shall apply privacy risk assessment process to identify risks related to the processing of personal data, within the scope of the PIMS.
- The organisation shall ensure throughout the risk assessment processes that the relationship between information security and PII protection is appropriately managed.

When assessing the applicability of control objectives and controls from ISO/IEC 27001 for the treatment of risks, the control objectives and controls shall be considered in the context of both risks to information security as well as risks related to the processing of personal data.

PIMS-specific guidance related to ISO 27002

Below we are summarising these control activities which come on top of the ISO 27002 guidance. As already mentioned, the terminology has been adjusted to GDPR.

Information security policies

The organisation should support and commit to comply with GDPR and with the contractual terms agreed between the organisation and its partners, its subcontractors and its relevant third parties, either by the developing separate privacy policies, or by extending information security policies.

Organisation of information security

Information security roles and responsibilities

The organisation should designate a customer point of contact regarding the processing of personal data.

The responsible person - the DPO in GDPR - should, where appropriate:

- be independent and report directly to the appropriate management level of the organisation in order to ensure effective management of privacy risks;
- be involved in the management of all issues which relate to the processing of personal data;
- be expert in data protection legislation, regulation and practice;
- act as a contact point for the Data Protection Authorities;
- inform top-level management and employees of the organisation of their obligations with respect to the processing of personal data;
- provide advice in respect of data protection impact assessments (DPIA) conducted by the organisation.

Mobile devices and teleworking

The organisation should ensure that the use of mobile devices does not lead to a compromise of personal data.

Human resource security

Information security awareness, education and training

Measures should be put in place, including awareness of incident reporting, to ensure that relevant staff are aware of the possible consequences to the organisation (e.g. legal consequences, loss of business and brand or reputational damage), to the staff member (e.g. disciplinary consequences) and to the data subject (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of personal data.

Asset management

Classification of information

The organisation's information classification system should explicitly consider personal data as part of the information classification it implements.

The organisation should ensure that people under its control are made aware of the definition of personal data and how to recognize information that is personal data.

Labelling of information

The organization should ensure that people under its control are made aware of the definition of personal data and how to recognize information that is personal data.

Media handling

The organisation should document any use of removable media for the storage of personal data. Removable media which is taken outside the physical confines of the organisation is prone to loss, damage and inappropriate access.

Wherever feasible, the organisation should use removable physical media that permit encryption when storing personal data. Encrypting removable media adds a level of protection for personal data which reduces security and privacy risks should the removable media be compromised.

Where removable media on which personal data is stored is disposed of, secure disposal procedures should be included in the documented information and implemented to ensure that previously stored personal data will not be accessible.

If physical media is used for information transfer, a register should be put in place to record incoming and outgoing physical media containing personal data.

The organisation should subject physical media containing personal data before leaving its premises to an authorisation procedure and ensure the personal data is not accessible to anyone other than authorised personnel.

Access control

User access management

Procedures for registration and de-registration of users who administer or operate systems and services that process personal data should address the situation where user access control for those users is compromised, such as the corruption or compromise of passwords or other user registration data.

The organisation should not reissue to users any de-activated or expired user IDs for systems and services that process personal data.

In the case where the organisation is providing personal data processing as a service, the customer can be responsible for user ID management. Such cases should be included in the documented information.

The organisation should maintain an accurate, up-to-date record of the user profiles created for users who have been authorised access to the information system and the personal data contained therein. This profile comprises the set of data about that user, including user ID, necessary to implement the identified technical controls providing authorised access.

Implementing individual user access IDs enables appropriately configured systems to identify who accessed personal data and what additions, deletions or changes they made.

In the case where the organisation is providing personal data processing as a service, the customer can be responsible for some aspects of access management. Where appropriate, the organisation should provide the customer the means to perform access management, such as by providing administrative rights to manage or terminate access. Such cases should be included in the documented information.

Where required by the customer, the organization should provide the capability for secure log-on procedures for any user accounts under the customer's control.

Cryptography

The use of cryptography may be required to protect sensitive or critical personal data, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

Physical and environmental security

Secure disposal or re-use of equipment

The organisation should ensure that, whenever storage space is re-assigned, any personal previously residing on that storage space is not accessible.

On deletion of personal data held in an information system, performance issues can mean that explicit erasure of that personal data is impractical. The risk that another user can access the personal data should be avoided by specific technical measures.

The organisation should ensure that, whenever storage space is re-assigned, any personal data previously residing on that storage space is not accessible.

For secure disposal or re-use, equipment containing storage media that can possibly contain personal data should be treated as though it does contain personal data.

Clear desk and clear screen policy

The organisation should restrict the creation of hardcopy material including personal data to the minimum needed to fulfil the identified processing purpose.

Operations security

Backup

The organisation should have a policy which addresses the requirements for backup, recovery and restoration of personal data and any further requirements (e.g. contractual and/or legal requirements) for the erasure of personal data contained in information held for backup requirements.

Where the organisation explicitly provides backup and restore services to customers, the organisation should provide them with clear information about their capabilities with respect to backup and restoration of personal data.

There can be occasions where personal data needs to be restored, perhaps due to a system malfunction, attack or disaster. When personal data is restored, the integrity should be ensured.

Logging and monitoring

A process should be put in place to review event logs to identify irregularities and propose remediation efforts. Where possible, event logs should record access to personal data.

Data processors should define criteria regarding if, when and how log information can be made available to or usable by the customer.

Log information recorded for, for example, security monitoring and operational diagnostics, can contain personal data. Measures such as controlling access should be put in place to ensure that logged information is only used as intended.

A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in the retention schedule.

Communications security

Information transfer

The organisation should consider procedures for ensuring that rules related to the processing of personal data are enforced throughout and outside of the system, where applicable.

The organisation should ensure that individuals operating under its control with access to personal data are subject to a confidentiality obligation. The confidentiality agreement, whether part of a contract or separate, should specify the length of time the obligations should be adhered to.

When the organisation is a data processor, a confidentiality agreement, in whatever form, between the organisation and its staff should ensure that staff members comply with the policy and procedures concerning data handling and protection.

Systems acquisition, development and maintenance

Security requirements of information systems

The organisation should ensure that personal data that is transmitted over untrusted data transmission networks is encrypted for transmission. Untrusted networks can include the public internet and other facilities outside of the operational control of the organisation.

Security in development and support processes

Policies for system development and design should include guidance for the organisation's processing of personal data needs, based on obligations to data subjects and/or any applicable legislation and/or regulation and the types of processing performed by the organisation. The policies should contribute to privacy by design and privacy by default.

Systems and/or components related to the processing of personal data should be designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls, in particular such that the collection and processing of personal data in those systems is limited to what is necessary for the identified processing purposes.

The same principles of privacy by design and privacy by default should be applied, if applicable, to outsourced information systems.

Test data

Personal data should not be used for testing purposes, but false or synthetic data should be used. Where the use of personal data for testing purposes cannot be avoided, technical and organisational measures equivalent to those used in the production environment should be implemented to minimise the risks. Where such equivalent measures are not feasible, a risk-assessment should be undertaken and used to inform the selection of appropriate mitigating controls.

Supplier relationships

Addressing security within supplier agreements

The organisation should specify in agreements with suppliers whether personal data is processed and the minimum technical and organisational measures that the supplier needs to meet in order for the organisation to meet its information security and personal data protection obligations.

Supplier agreements should clearly allocate responsibilities between the organisation, its partners, its suppliers and its applicable third parties taking into account the type of personal data processed.

The agreements between the organisation and its suppliers should provide a mechanism for ensuring the organisation supports and manages compliance with all applicable legislation and/or regulation. The agreements should call for independently audited compliance, acceptable to the customer.

The organisation should specify in contracts with any suppliers that personal data is only processed on its instructions.

Information Security incident management

Management of information security incidents and improvements

As part of the overall information security incident management process, the organisation should establish responsibilities and procedures for the identification and recording of personal data breaches. Additionally, the organisation should establish responsibilities and procedures related to notification to required parties of these breaches (including the timing of such notifications) and the disclosure to the Data Protection Authorities.

Guidance for data controllers

An incident that involves personal data should trigger a review by the organisation, as part of its information security incident management process, to determine if a breach involving personal data that requires a response has taken place. When a personal data breach has occurred, response procedures should include relevant notifications and records.

Where a breach involving personal data has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as a description of the incident; the time period; the consequences of the incident; the name of the reporter; to whom the incident was reported; the steps taken to resolve the incident; the fact that the incident resulted in unavailability, loss, disclosure or alteration of personal data.

Guidance for data processors

Provisions covering the notification of a breach involving personal data should form part of the contract between the organisation and the customer. The contract should specify how the organisation will provide the information necessary for the customer to fulfil their obligation to notify relevant authorities. This notification obligation does not extend to a breach caused by the customer or data subject or within system components for which they are responsible. The contract should also define expected and externally mandated limits for notification response times.

The data processor should notify the data controller of the existence of a breach without undue delay (i.e. as soon as possible), preferably, as soon as it is discovered so that the data controller can take the appropriate actions.

Where a breach involving personal data has occurred, a record should be maintained with sufficient information to provide a report for regulatory and/or forensic purposes, such as a description of the incident; the time period; the consequences of the incident; the name of the reporter; to whom the incident was reported; the steps taken to resolve the incident; the fact that the incident resulted in unavailability, loss, disclosure or alteration of personal data.

In the event that a breach involving personal data has occurred, the record should also include a description of the personal data compromised, if known; and if notifications were performed, the steps taken to notify the customer.

Compliance

Compliance with legal and contractual requirements

The organisation should identify any potential legal sanctions related to the processing of personal data, including substantial fines directly from the Data Protection Authority.

Review of current and historical policies and procedures can be required e.g. in the cases of customer dispute resolution and investigation by a Data Protection Authority. The organisation should retain copies of its privacy policies and associated procedures for a period as specified in its retention schedule. This includes retention of previous versions of these documents when they are updated.

Information security reviews

Where an organisation is acting as a data processor, and where individual customer audits are impractical or can increase risks to security, the organisation should make available to customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the organisation's policies and procedures. A relevant independent audit, as selected by the organisation, should normally be an acceptable method for fulfilling the customer's interest in reviewing the organisation's processing operations, if it covers the needs of anticipated users and if results are provided in a sufficient transparent manner.

As part of technical reviews of compliance with security policies and standards, the organisation should include methods of reviewing those tools and components related to processing personal data.

Additional guidance for data controllers

The PIMS specific guidance for data controllers consists of the "PIMS-specific guidance related to ISO 27002" (previous topic) together with his additional guidance.

Related to the additional guidance, the table contains the categories having a control objective, following with the proposed controls. The implementation guidance is included in the ISO 27701 standard.

Cat	C.O/ctl	A	PIMS specific guidance for Data Controllers	
Conditions for collection and processing	Control Object.	**A.7.2**	To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.	
	Control	A.7.2.1	Identify and document purpose	The organization shall identify and document the specific purposes for which the *personal data* will be processed.
	Control	A.7.2.2	Identify lawful basis	The organization shall determine, document and comply with the relevant lawful basis for the processing of *personal data* for the identified purposes.
	Control	A.7.2.3	Determine when and how consent is to be obtained	The organization shall determine and document a process by which it can demonstrate if, when and how consent for the processing of *personal data* was obtained from *data subjects*.
	Control	A.7.2.4	Obtain and record consent	The organization shall obtain and record consent from *data subjects* according to the documented processes.
	Control	A.7.2.5	Privacy impact assessment	The organization shall assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing of *personal data* or changes to existing processing of *personal data* is planned.
	Control	A.7.2.6	Contracts with personal *data* processors	The organization shall have a written contract with any *data* processor that it uses, and shall ensure that their contracts with *data* processors address the implementation of the appropriate controls numbered B. (see below)
	Control	A.7.2.7	Joint *data* controller	The organization shall determine respective roles and responsibilities for the processing of *personal data* (including *personal data* protection and security requirements) with any joint *data* controller.

Cat	C.O/ctl	A	PIMS specific guidance for Data Controllers	
	Control	A.7.2.8	Records related to processing *personal data*	The organization shall determine and securely maintain the necessary records in support of its obligations for the processing of *personal data*.
Obligations to *data subjects*	Control Object.	**A.7.3**	To ensure that *data subject*s are provided with appropriate information about the processing of their *personal data* and to meet any other applicable obligations to *data subjects* related to the processing of their *personal data*.	
	Control	A.7.3.1	Determining and fulfilling obligations to *data subjects*	The organization shall determine and document their legal, regulatory and business obligations to *data subjects* related to the processing of their *personal data* and provide the means to meet these obligations.
	Control	A.7.3.2	Determining information for *data subjects*	The organization shall determine and document the information to be provided to *data subjects* regarding the processing of their *personal data* and the timing of such a provision.
	Control	A.7.3.3	Providing information to *data subjects*	The organization shall provide *data subjects* with clear and easily accessible information identifying the *data controller* and describing the processing of their *personal data*.
	Control	A.7.3.4	Providing mechanism to modify or withdraw consent	The organization shall provide a mechanism for *data subjects* to modify or withdraw their consent.
	Control	A.7.3.5	Providing mechanism to object to *personal data* processing	The organization shall provide a mechanism for data subject to object to the processing of their *personal data*.
	Control	A.7.3.6	Access, correction and/or erasure	The organization shall implement policies, procedures and/or mechanisms to meet their obligations to data subjects to access, correct and/or erase their personal data.
	Control	A.7.3.7	*Data* controllers' obligations to inform third parties	The organization shall inform third parties with whom p*ersonal data* has been shared of any modification, withdrawal or objections pertaining to the shared *personal data,* and implement appropriate policies, procedures and/or mechanisms to do so.
	Control	A.7.3.8	Providing copy of *personal data* processed	The organization shall be able to provide a copy of the *personal data* that is processed when requested by the *data subject.*

Cat	C.O/ctl	A	PIMS specific guidance for Data Controllers	
	Control	A.7.3.9	Handling requests	The organization shall define and document policies and procedures for handling and responding to legitimate requests from *data subjects*.
	Control	A.7.3.10	Automated decision making	The organization shall identify and address obligations, including legal obligations, to the *datat subjects* resulting from decisions made by the organization which are related to the *data subject* based solely on automated processing of *personal data*.
Privacy by design and privacy by default	Control Object.	**A.7.4**	To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.	
	Control	A.7.4.1	Limit collection	The organization shall limit the collection of *personal data* to the minimum that is relevant, proportional and necessary for the identified purposes.
	Control	A.7.4.2	Limit processing	The organization shall limit the processing of *personal data* to that which is adequate, relevant and necessary for the identified purposes.
	Control	A.7.4.3	Accuracy and quality	The organization shall ensure and document that *personal data* is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the *personal data*.
	Control	A.7.4.4	*Personal data* minimization objectives	The organization shall ensure and document that *personal data* is as accurate, complete and up-to-date as is necessary for the purposes for which it is processed, throughout the life-cycle of the *personal data*.
	Control	A.7.4.5	*Personal data* de-identification and deletion at the end of processing	The organization shall define and document data minimization objectives and what mechanisms (such as de-identification) are used to meet those objectives.
	Control	A.7.4.6	Temporary files	The organization shall either delete *personal data* or render it in a form which does not permit identification or re-identification of *data subjects*, as soon as the original *personal data* is no longer necessary for the identified purpose(s).

Cat	C.O/ctl	A	PIMS specific guidance for Data Controllers	
	Control	A.7.4.7	Retention	The organization shall not retain *personal data* for longer than is necessary for the purposes for which the *personal data* is processed.
	Control	A.7.4.8	Disposal	The organization shall have documented policies, procedures and/or mechanisms for the disposal of *personal data*.
	Control	A.7.4.9	*Personal data* transmission controls	The organization shall subject *personal data* transmitted (e.g. sent to another organization) over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
Personal data sharing, transfer and disclosure	Control Object.	**A.7.5**	To determine whether and document when *personal data* is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.	
	Control	A.7.5.1	Identify basis for *personal data* transfer between jurisdictions.	The organization shall identify and document the relevant basis for transfers of *personal data* between jurisdictions.
	Control	A.7.5.2	Countries and international organizations to which *personal data* can be transferred.	The organization shall specify and document the countries and international organizations to which *personal data* can possibly be transferred.
	Control	A.7.5.3	Records of transfer of *personal data*	The organization shall record transfers of *personal data* to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the *data subjects*.
	Control	A.7.5.4	Records of *personal data* disclosure to third parties.	The organization shall record disclosures of *personal data* to third parties, including what *personal data* has been disclosed, to whom and at what time.

Additional guidance for data processors

The PIMS specific guidance for data processors consists of the "PIMS-specific guidance related to ISO 27002" (previous topic) together with his additional guidance.

Related to the additional guidance, the table contains the categories having a control objective, following with the proposed controls. The implementation guidance is included in the ISO 27701 standard.

Cat	C.O/ctl	B	Data Processors	
Conditions for collection and processing	Control Object.	**B.8.2**	To determine and document that processing is lawful, with legal basis as per applicable jurisdictions, and with clearly defined and legitimate purposes.	
	Control	B.8.2.1	Customer agreement	The organization shall ensure, where relevant, that the contract to process *personal data* addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).
	Control	B.8.2.2	Organization's purposes	The organization shall ensure that *personal data* processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.
	Control	B.8.2.3	Marketing and advertising use	The organization shall not use *personal data* processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate *data subject.* The organization shall not make providing such consent a condition for receiving the service.
	Control	B.8.2.4	Infringing instruction	The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.
	Control	B.8.2.5	Customer obligations	The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations.
	Control	B.8.2.6	Records related to processing *personal data*	The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of *personal data* carried out on behalf of a customer.
Obligations to *data subjects*	Control Object.	**B.8.3**	To ensure that *data subjects* are provided with appropriate information about the processing of their *personal data* and to meet any other applicable obligations to *data subjects* related to the processing of their *personal data*.	
	Control	B.7.3.1	Obligations to *data subjects*	The organization shall provide the customer with the means to comply with its obligations related to data subjects.

Privacy by design and privacy by default	Control Object.	**B.8.4**	To ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.	
	Control	B.8.4.1	Temporary files	The organization shall ensure that temporary files created as a result of the processing of personal data are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
	Control	B.8.4.2	Return, transfer or disposal of *personal data*	The organization shall provide the ability to return, transfer and/or disposal of *personal data* in a secure manner. It shall also make its policy available to the customer.
	Control	B.8.4.3	*Personal data* transmission controls	The organization shall subject *personal data* transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.
Personal data sharing, transfer and disclosure	Control Object.	**B.8.5**	To determine whether and document when *personal data* is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.	
	Control	B.8.5.1	Basis for *personal data* transfer between jurisdictions	The organization shall inform the customer in a timely manner of the basis for *personal data* transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.
	Control	B.8.5.2	Countries and international organizations to which *personal data* can be transferred.	The organization shall specify and document the countries and international organizations to which personal data can possibly be transferred.
	Control	B.8.5.3	Records of personal data disclosure to third parties.	The organization shall record disclosures of *personal data* to third parties, including what *personal data* has been disclosed, to whom and when.
	Control	B.8.5.4	Notification of *personal data* disclosure requests.	The organization shall notify the customer of any legally binding requests for disclosure of *personal data*.

	Control	B.8.5.5	Legally binding *personal data* disclosures.	The organization shall reject any requests for *personal data* disclosures that are not legally binding, consult the corresponding customer before making any *personal data* disclosures and accepting any contractually agreed requests for *personal data* disclosures that are authorized by the corresponding customer.
	Control	B.8.5.6	Disclosure of subcontractors used to process *personal data*.	The organization shall disclose any use of subcontractors to process *personal data* to the customer before use.
	Control	B.8.5.7	Engagement of a subcontractor to process *personal data*.	The organization shall only engage a subcontractor to process *personal data* according to the customer contract.
	Control	B.8.5.8	Change of subcontractor to process personal data	The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process *personal data*, thereby giving the customer the opportunity to object to such changes.

Conclusion

Benefits

Organisations often operating in several countries, may have privacy and information security requirements from different jurisdictions. By using an internationally recognised ISO standard, the organisation can gather all the requirements together so that only one set of actions is needed to help achieve and maintain compliance.

Upcoming

In addition to the GDPR, the EU is creating a new law to update the Privacy and Electronic Communications Directive 2002 (2002/58/EC) or the ePrivacy Directive.

The European Data Protection Board (EDPB) published guidance in June 2019 on the requirements for new certification schemes that will allow organisations 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.

Implementing today ISO 27701 may already be an interesting step in the good direction….