IAPP-OneTrust Research:
Bridging ISO 27001 to GDPR

Introduction

Privacy is hot. Security knows the feeling.

Much as the move to digital products and services necessitated a new profession of information security, so too has the move to personalized products and services created a new profession of privacy professionals.

However, while the two professions often work together, they have long worked differently. Security has traditionally worked in binary states: access or no access. Privacy has traditionally worked along a spectrum that's context dependent. Is it personal data? Well, that depends.

J. Trevor Hughes
CIPP,
CEO and President, IAPP

Privacy has largely been a matter of law and policy. Security has largely been a matter of technology and policy. Now, that's all changing.

With the European Union's General Data Protection Regulation, and other more stringent pieces of privacy regulation coming into force the world over, "adequate security" is now mandated by law. And with these complex pieces of legislation has now come a class of technologies to help privacy teams understand and comply with them operationally.

Increasingly, this means the professional lives of information security and privacy professionals are overlapping, captured perhaps in the European idea of "data protection." It's clear these two classes of professionals need better ways to work together, better methods of communication, and common tools.

Kabir Barday
CIPP/E, CIPP/US, CIPM, CIPT, FIP
CEO, OneTrust

Thus, the IAPP and OneTrust have undertaken the task of mapping the most common security operations standard, ISO's 27001, to the world's most influential piece of privacy legislation, the GDPR, so as to create a framework for understanding just how closely they align and how much of the work toward GDPR compliance that security has likely already done.

With this research project, we have identified six main areas of common ground that should help every organization align their security and privacy operations in a way that will create efficiencies and, hopefully, reduce the risk of a damaging incident while increasing productivity and customer trust.

We hope you find it useful and worthwhile.

Bridging ISO 27001 to GDPR:

Where security and privacy share common ground

Executive Summary

According to the International Standards Organization, in 2016 more than 33,000 organizations globally held certification to the ISO 27001 standard, which relates to information security management systems and security controls. That same year, the European Union's General Data Protection Regulation was finalized, launching a two-year scramble for compliance by May 25, 2018, for companies of all sizes around the world.

There is significant common ground between the GDPR and ISO 27001 requirements. Although they come from different perspectives, ISO 27001 and the GDPR at their core are both about reducing risk to people and organizations caused by misuse of personal data, with demonstrable overlap in both principles and requirements. On the one hand, ISO 27001 focuses on reducing risks to information security by compelling organizations to produce information security management systems that are continuously maintained and improved. On the other hand, the GPDR focuses on reducing risks for data subjects by providing them with rights, placing clear privacy responsibilities on organizations processing personal data, and holding them accountable through legal and administrative enforcement mechanisms.

Both the GDPR and ISO 27001 call for organizations to invest in knowledgeable leadership and develop organization-wide awareness for data protection and security. ISO 27001 requires organizations to take a holistic approach to data security, developing clear, comprehensive policies and procedures based on considerations of organizational scope (including the nature and amount of data processed) that must be maintained through reviews and audits. One of ISO 27001's fundamental requirements is the appointment of leadership with defined responsibilities for information security management. Similarly, the GPDR requires many organizations to appoint data protection officers with expert knowledge of the Regulation and sufficient authority within the organization to advocate for data subject rights as well as implement and oversee comprehensive privacy and security policies.

This whitepaper demonstrates how that collaboration can involve fewer pain points and be more productive by showing how the ISO 27001 information security management framework correlates to the goals, objectives, and even specific requirements of the GDPR. It is a tool for security and privacy professionals to use for improved communication and mutual understanding.

Privacy professionals will need to work closely with security professionals in helping organizations comply with the GDPR. This whitepaper demonstrates how that collaboration can involve fewer pain points and be more productive by showing how the

ISO 27001 information security management framework correlates to the goals, objectives, and even specific requirements of the GDPR. It is a tool for security and privacy professionals to use for improved communication and mutual understanding.

Specifically, this whitepaper identifies six critical areas of common ground between ISO 27001 and the GPDR:

- Security.
- Breach notification.
- Vendor management.
- Recordkeeping.
- Privacy by design.
- Data subject rights.

For each topic, we identify overlap between the two systems and suggest how security professionals can work more effectively with privacy professionals toward GDPR compliance. These areas of commonality are non-exhaustive, of course; they are simply intended to demonstrate how ISO 27001-certified organizations are well positioned to respond to many GDPR priorities. Each section also has a short list of "agenda items" for security team meetings designed to help enhance communication with the privacy team around data protection and the GDPR.

GDPR Terminology

Having a mutual understanding of "GDPR vocabulary" – set forth in GDPR Article 4 – will facilitate communication between security and privacy professionals.

Personal data: Any information relating to an identified or identifiable natural person (known as a data subject); this includes name, identification number, location data, online identifier, and physical, physiological, genetic, mental, economic, cultural or social identity factors relating to that person.

Processing: Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, and erasure or destruction.

Controller: The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor: A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Consequences of a personal data breach under the GDPR include requirements to provide notice of the breach to data protection regulators called "supervisory authorities" as well as to data subjects when there is a "high risk" to their rights and freedoms.

Pseudonymization: The processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Security

The ISO 27001 Security Roadmap

ISO 27001 creates a roadmap for the development, implementation, and maintenance of a comprehensive information security program. Starting in Clause 4, Context of the Organization, ISO 27001 guidelines require that organizations determine both the internal and external issues that may affect their security programs. This determination must include consideration of potential issues regarding third parties and should identify the scope and limitations of the security program.

Next, Clause 6 requires organizations to plan and structure a security program that can achieve the goals and match the scope identified in Clause 4. Clause 6 also calls for the creation of an information security risk assessment methodology, which includes the identification of risk levels and risk acceptance, the assignment of responsibility, plans for the treatment of identified security risks, and the setting of security objectives.

Finally, Clause 8 calls for the implementation of the processes created by Clause 6, and sets standards for the continued maintenance of the program. Clause 8 focuses heavily on the documentation of the risk assessments, risk treatments, and security program functions generally, to demonstrate compliance with regulations. Clause 8 also calls for periodic review to ensure that progress is being made on the security objectives called for in Clause 6.

GDPR: Appropriate Safeguards and Oversight

Article 5 of the GDPR sets out the Regulation's fundamental principles governing data processing, including ensuring "appropriate security of personal data" and the protection against "unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures." Additional guidance on appropriate "technical and organizational measures" is found in Article 32, which requires that organizations "ensure a level of security appropriate to the risk" of the data held and processed. These measures include pseudonymization and encryption of personal data; the CIA triad (ensuring the confidentiality, integrity and availability of data) familiar to security professionals; the ability to restore personal data access shortly after a physical or technical incident; and a process for "regularly testing, assessing and evaluating the effectiveness" of technical and organizational security measures.

Article 32 also requires the use of personal data access restrictions to prevent employees and contractors from gaining unauthorized access to data. Related to Article 32 security obligations are the responsibilities data protection officers have under Article 39 to inform and advise the organization regarding their GDPR obligations (including security) and monitoring the organization's compliance with GDPR's data processing provisions.

ISO 27001	GDPR	Collaboration
Clause 6.1.2: The organization shall identify the risk associated with the loss of "confidentiality, integrity and availability" of information. **Clause 6.1.2:** The organization shall identify risk owners. **Clause 6.1.2:** The organization shall determine the levels of risk. **Clause 6.2:** The organization shall establish information security objectives that result from risk assessments and risk treatments **Clause 8:** The organization shall oversee and manage the implementation of the various aspects of the security program in a plan and routinely reassess risk. **Control A.10:** Policies should be developed and implemented for the use of cryptographic controls and protection of cryptographic keys.	**Article 5(1)(f)** and **Article 32:** Data controllers and processors shall implement technical and organizational measures to ensure a level of security appropriate to the risk. **Article 32:** In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. **Article 32:** Security appropriate to the risk may include: • Pseudonymization and encryption of personal data. • Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services. • Ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident. • Process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring security of processing.	Conformity with ISO 27001 provides strong evidence of compliance with GDPR Article 32 security requirements. Both regimes focus on the risk associated with loss of confidentiality, integrity and availability of protected data. Both regimes require internal leadership to work with other professionals throughout the organization to map data processing activities and assess risk to the organization – and data subjects – by understanding the sensitivity of the information. Security professionals will work closely with the privacy team to provide documentation that security systems are appropriate to the risk.

continued

Clause 5.1: Management shall ensure information security policies and objectives are set, integrated, compatible with the organization's strategic direction, and achieve desired outcomes.	**Article 39:** The data protection officer shall inform and advise the controller or processor and its employees of their obligations under the GDPR, and shall monitor compliance with the Regulation, including assignment of responsibilities, awareness-raising and training of staff, and related audits. **Article 32:** The controller and processor shall take steps to ensure that any natural person acting under their authority who has access to personal data does not process the data except on their instructions.	In many organizations, the privacy leader — whether a chief privacy officer, a DPO, or someone who serves both roles — will regularly meet with the chief information security officer or equivalent. Privacy working groups will involve security personnel, while security working groups will ideally also involve privacy professionals.

Article 32 Compliance Through ISO 27001

As one of the most widely adopted security standards in the world, ISO 27001 compliance is a strong means of demonstrating compliance with GDPR Article 32 security requirements. Of course, the final control in ISO 27001 Annex 1 requires that security professionals be knowledgeable of all relevant legal requirements, document these requirements, and incorporate them into security plans, so that ISO 27001 compliance requires updating policies and procedures to reflect the requirements of the GDPR. Security and privacy professionals will benefit from working together to identify relevant data protection legal requirements, as well as to classify information assets by "risk" as contemplated in the GDPR.

Internal Discussion Items

- What types of personal data are being collected, processed, and stored?
    - Is any sensitive personal data (racial or ethnic identifiers, biometric, healthcare, financial data, etc.) included in the above?
    - Is sensitive data treated with a higher level of protection?
- How are security controls and protocols documented? Are specific controls identified for specific categories of data or specific data processing activities?
- What methods are currently used to determine risk of loss of confidentiality, integrity, and availability? Do they include an assessment of the rights of the data subjects?
- Is personal data encrypted at rest and in transit? Does the organization have the capacity and practice to anonymize or pseudonymize personal data?
- Are privacy professionals invited to security team meetings and vice versa?

Breach Notification

ISO 27001 Data Breach Response Plans

ISO 27001 requires mechanisms both to quickly identify security incidents and to report them through the necessary established channels. This control (A.16) is designed to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. The fundamental elements underpinning an ISO 27001 compliant response plan are a clear chain of command, established identification and reporting procedures, and the reporting of any unusual activity or incidents by employees and contractors. As with all ISO 27001 requirements, documentation and continued updating are key.

GDPR Articles 33 and 34 Data Breach Notifications

The GDPR contains two separate data breach notification requirements. The first, Article 33, requires data controllers to provide notice of any data breach "likely to result in a risk to the rights and freedoms of a natural person" to the relevant supervisory authority "without undue delay" and not later than 72 hours after becoming aware of the breach. Article 33 also requires that data processors notify data controllers of any breaches "without undue delay."

GDPR Article 34 requires notification to data subjects following a breach, but only when the breach will result in a "high risk to the rights and freedoms of natural persons." Notification must include the DPO's contact information, the likely consequences of the breach, and the measures taken or considered to address the breach (including measures to mitigate its possible adverse effects). Article 34 exempts controllers from notifying data subjects when they have implemented appropriate technical and organizational protection measures that render the personal data unintelligible, where the high risk to data subjects has been effectively mitigated, or when such notification would involve "disproportionate effort." Finally, Article 34 provides data protection authorities with the discretion to compel organizations to notify affected data subjects.

ISO 27001	GDPR	Collaboration
Control A.16: Information security events shall be reported through the proper internal channels immediately, assessed to determine if they are "incidents," documented, and investigated.	**Article 33:** The controller must notify the relevant supervisory authority without undue delay, and, where feasible, not later than 72 hours after becoming aware of the personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of a natural person. Notice to the supervisory authority must include, when feasible: • Nature of personal data breach including categories and approximate number of data subjects concerned.	The managerial reporting structure created by the ISO 27001 requirements can be adapted to incorporate the necessary data protection authority. Security personnel will often be the first to discover a security incident – or at least the first contacted. Proper management channels for reporting a security event includes notifying the DPO or privacy leader. The DPO or privacy leader will also be involved in determining if the event rises to the level of a personal data breach.

continued

ISO 27001	GDPR	Collaboration
	• Contact details of controller's DPO. • Likely consequences of breach. • Response plan, including mitigation measures. **Article 34:** When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the affected data subjects without undue delay. Notice must include, when feasible: • Description of the personal data involved. • The number of data subjects. • The DPO's contact information. • Likely consequences of the breach. • The controller's response plan, including mitigation measures.	Privacy and security teams will also need to work together on crafting the notice to the supervisory authority and, if necessary, data subjects. The notice will need to include information about the personal data breach discovered during security investigations as well as security's plans to mitigate harm and prevent future additional incidents.
Control A.18: Security management includes complying with legal, regulatory and contractual obligations relating to information privacy.	**Article 33:** Data processors must notify data controllers without undue delay of a personal data breach.	Privacy professionals will need to assist the security team with identifying contracts that might be relevant to the data affected by the security incident and providing proper notice pursuant to those agreements as necessary.

Implementing GDPR Breach Notification Compliance

The GDPR Article 33 and 34 requirements are complementary to the ISO 27001 standards. There is perhaps no time when inter-departmental communication is more crucial than following discovery of a security incident. Through proper incident response planning, training, and practice, a live security incident should be accompanied by productive communication between security and privacy professionals. Current policies should include the relevant reporting structure and personal data risk inventories to allow for incidents to be investigated, evaluated against the definition of "personal data breach" under the GDPR, and readied for notification without delay.

Internal Discussion Items

As these policies are updated, IT professionals should consider the following questions:

- Is the organization functioning as a data controller or a data processor?
    - There may be multiple answers to this question. For example, an organization may function as a processor while handling customer information and a controller while handling HR information.
- Are data inventories managed in such a way that the appropriate reporting metrics can be easily identified in the event of a breach?
- Do plans and procedures include the involvement of the DPO (notably to identify whether an incident qualifies as a personal data breach within the definition of GDPR)?
- In the event of a breach, are any controls in place to mitigate the risk for affected data subjects?
- How can incident response plans accommodate the 72-hour notification period?

Vendor Management

ISO 27001 Vendor Control

ISO 27001 includes vendor oversight and control as critical components of appropriate data security protocols. Clause 8 requires organizations to identify what processing actions are outsourced and ensure that these processes are a controlled part of the security program. Clause 9 builds off Clause 8, requiring organizations to review, document, and maintain oversight of security programs which may include scheduled risk assessments and audits to confirm that customer data is secure. Additional, more specific guidance is found in controls A.15, governing "supplier relationships," and A.18.1, governing compliance with contractual requirements. Control A.15 addresses security concerns where the organization is vulnerable to vendor ("supplier") access to personal data. It requires risk mitigation by limiting data access and by entering agreements to impose security responsibility and assign liability. Control A.18 contemplates compliance with agreements where the shoe is on the other foot and the organization is acting as the supplier, requiring compliance with the customer's security requirements.

GDPR Article 28: Data processors

Article 28 of the GDPR sets forth detailed requirements for vendor management, placing clear responsibilities on both data controllers and processors that must be embodied in contracts. Controllers are restricted to using only those processors who can guarantee technical, administrative, and organizational safeguards at levels equal to or exceeding those required by the GDPR. Processors have defined security requirements and are restricted from using sub-processors without consent from the relevant data controller. A major focus of Article 28 is the requirement that controllers secure contractual terms and assurances from processors, creating a form of agreement known as a "data protection agreement." Article 28 suggests the types of controls a data protection agreement should contain.

ISO 27001	GDPR	Collaboration
Clause 8: Control and oversee outsourced processes. **Clause 9:** Review the impact of vendor contracts and performance on security concerns. **Control A.15:** Mitigate risks to the organization presented by suppliers that have access to personal data; supplier agreements should address information security risks and impose privacy and security responsibilities. **Control A.18:** Avoid breaches of contractual responsibilities to maintain privacy and security of personal information.	**Article 28:** Controllers shall use only processors guaranteeing appropriate technical and organizational safeguards. Processing must be governed by a compliant contract. **Article 28:** Processors may not subcontract to other processors without controller consent and an appropriate contract. Processors share responsibility for security and access requirements.	Because GDPR Article 28 burdens controllers with selecting processors that have appropriate technical and organizational security measures, controllers' privacy teams will need to work with security teams to vet potential processors, and processors' teams will need to collaborate to respond to controller demands. ISO 27001's expectations regarding supplier security and respecting contractual obligations are compatible with these goals.

Using Contracts as "Controls"

According to a 2017 IAPP report, 50 percent of privacy professionals look for ISO 27001 compliance when trying to determine if vendors provide appropriate levels of security for personal data. With GDPR Article 28 explicitly requiring privacy professionals to incorporate security assurances into data processor contracts, a vendor's ability to demonstrate ISO 27001 compliance becomes even more relevant.

GDPR Article 28 prohibits data controllers from transferring data to processors who cannot guarantee appropriate technical and organizational safeguards in a written agreement. Article 28's contractual requirements are also critical to structuring relationships between controllers and processors. Security professionals may need to assist their privacy team with vetting potential vendors to evaluate the vendors' security regimes and with responding to customers' security questionnaires.

Internal Discussion Items

- Does your organization have a comprehensive list of vendors and third-party processors?
- Does your supplier risk assessment include data protection-related questions, including Article 28 requirements?
- Does your organization have standard data privacy contractual language?
- If yes, is this language present in all third-party contracts?
- When and if your organization is functioning as a controller, do you require processors to seek permission prior to using sub-processors?
- When and if your organization is functioning as a data processor, are GDPR Article 32 security requirements part of your data security policies?

Record Keeping

ISO 27001 Record-Keeping Requirements

The stated goal of ISO 27001 Clause 8 is to develop and maintain appropriate safeguards for organizational assets. Specifically, Clause 8.1 requires that organizations identify and clearly label important data assets. This inventory protocol includes requirements for clear definitions of ownership and acceptable uses for the data. Clause 8.2 continues by requiring data sensitivity classifications, labeling, and access controls based upon these sensitivity levels. Clause 9 also contains relevant guidance on the creation and maintenance of an access control policy.

GDPR Record-Keeping Requirements

GDPR Article 30 requires data controllers and processors alike to maintain records of their processing activities, identifying how different categories of data are processed, safeguarded, and retained by an organization. For controllers, these records are required to contain: the categories of data subjects; the categories of data collected; the types of processing activities that have and are likely to occur; the legal purpose or grounds of the processing; potential recipients of disclosures; information regarding cross-border transfers of the data; retention plans; and security controls. For processors, the contents of the records are more limited and include: categories of processing activities; information regarding the data controller; and information regarding security safeguards and cross border data transfers.

ISO 27001	GDPR	Collaboration
Clause 8: The organization shall document its security processes, and the results of security risk assessments and risk treatment. **Control A.8:** Information assets shall be inventoried and classified; asset owners shall be assigned, with procedures defined for acceptable data use, labelling, and handling. **Control A.8.3:** Prevention of unauthorized disclosure includes securely disposing of media on which information is stored when it is no longer required. **Control A.13.2** Information transferred to an external party shall be appropriately secure, subject to agreements addressing security, and consistent with formal policies, procedures and controls.	**Article 30(1):** A controller shall maintain a record of processing activities under its responsibility, which shall contain: • The name and contact details of the controller and its DPO. • The purposes of the processing. • Categories of data subjects and of personal data. • Transfers of personal data to any third country and documentation of suitable safeguards for such transfers. • Time limits for data erasure; data retention policies. • A general description of the technical and organizational security measures used.	Compliance with Article 30 record-keeping requirements involves considerable inter-departmental communication. The security team's documentation of security procedures and classification of information assets will assist with this effort. Conversely, the privacy team's categorization of data subjects and personal data may be relevant to information classification kept by security professionals. Privacy professionals also engage in data inventory and mapping, a task that will be aided by the security team's identification of information asset location and ownership. Current lists of acceptable uses for information assets required by ISO 27001 will also provide the privacy team with important insight into data retention and processing. *continued*

ISO 27001	GDPR	Collaboration
	Article 30(2): A processor shall maintain a record of all categories of processing activities carried out on behalf of a controller, which shall contain: • Name and contact details of the processor and of each controller on whose behalf the processor is acting. • The categories of processing carried out on behalf of each controller. • Transfers of personal data to a third country and documentation of suitable safeguards. • A general description of the technical and organizational security measures used. These records shall be in writing, including in electronic form.	Security's definition of acceptable uses of information assets reflects on the overall technical and organizational security in place for personal data and may fit neatly into the Article 30 records requirements. Finally, although international data transfers are a special case under the GDPR, steps security professionals take to track and ensure the security of transfers to "external parties" can assist the privacy team with recording cross-border transfers as well.

Leveraging ISO 27001 for Article 30 Compliance

Data inventory and mapping have been the first steps in building a privacy program for quite some time. Article 30 requires that records be kept of certain information gained during the inventory and mapping process. This potentially complex task requires considerable lift by many throughout the organization, not just the privacy team, because gathering accurate information about the organization's personal data practices requires working across departments. The security team may already have documented and classified information assets pursuant to ISO 27001 and thus might be the first place to start in a mapping and record-keeping exercise. That said, Article 30 may alter how information is categorized, labeled, and maintained. These changes will require collaboration between the security and privacy teams. Despite these changes, the existing ISO 27001 inventory frameworks are likely to be a strong starting point for achieving Article 30 compliance.

Internal Discussion Items

When reviewing security assets, it can help to document answers to the following basic questions:

- What type of personal data is collected?
- How and from where is the data collected?
- How and where is the data processed?
- How and where is the data being transferred?
- Is the data being stored, protected, and deleted?
- What data retention and destruction policies are already in place? Are they being followed?

Data Protection by Design

ISO 27001: A Flexible Security Framework

Clauses 5 and 6 contain multiple requirements designed to develop and maintain an adaptive security framework while identifying and mitigating operational risks. Clause 5 takes a structural approach to the subject, requiring the development and periodic review of necessary security policies. It also requires the appointment of all necessary managerial staff and the clear delegation of duties and responsibilities. Clause 6 requires that an organization undertake ongoing security risk assessments designed to ensure the efficacy of the security management program, the identification and prevention of risk, and the appropriate treatment of security issues. Combined, these clauses emphasize the importance of establishing a foundational framework that allows for the testing and safeguarding of processing actions.

GDPR Article 25: Privacy by Design

Much like the ISO 27001 standards, Article 25 of the GDPR encourages a system and practice, reinforced by policies overseen by management, of incorporating security and privacy principles into products and processes from the outset and throughout implementation. The GDPR calls this "data protection by design and by default." First, taking into account the cost, scope, and content of the processing, a controller must provide "appropriate" safeguards "both at the time of determination of the means for processing and at the time of the processing itself." Second, Article 25 requires that organizations collect, process, and retain only data that is absolutely necessary, thereby reducing the volume and scope of any data that could be lost, and identify the potential privacy risks associated with a particular processing activity so as to implement measures to mitigate those risks. These requirements encourage a holistic view of data management, identifying exactly what data is required for each step of the process and ensuring that the appropriate safeguards are in place even prior to data collection.

ISO 27001	GDPR	Collaboration
Clause 4: Organizations shall understand the scope and context of the data being collected and processed. **Clause 5:** Professional security leadership should be appointed and given clearly defined responsibilities. **Clause 6:** Security professionals should routinely run risk analyses to determine security threats, risk tolerance, and security objectives.	**Article 25:** Taking account the state of the art, the costs of implementation, the nature and scope of processing, along with the risks to the rights and freedoms of data subjects, the controller shall implement appropriate technical and organizational measures, such as pseudonymization, design to implement data protection principles, such as data minimization, and to integrate the safeguards into processing.	Privacy teams will likely engage security teams with evaluating existing collection and processing practices to determine whether the collection limitation principle is being appropriately considered. Security is a key component of privacy by design and privacy by default in product and system design.

continued

ISO 27001	GDPR	Collaboration
Control A.10: Policies should be developed and implemented for the use of cryptographic controls and protection of cryptographic keys.	The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Collection, processing, and retention are limited to what is necessary.	

Building Privacy out of Security

By requiring organizations to identify the scope, context, and management structure of security programs, ISO 27001 encourages data protection by design. Data minimization is a major consideration added by GDPR's Article 25 that will have to be incorporated into existing security policies. Privacy teams will likely engage security teams with evaluating existing collection and processing practices to determine whether the collection limitation principle is being appropriately considered. Although data protection by design and by default is aimed at programming, marketing, and product development teams, security is always a crucial component of privacy, especially in product and system design.

Internal Discussion Items

- What personal data is required for each processing procedure handled by the organization or its processors?
- Do current policies and procedures limit the amount of personal data that can be collected through form limitations or other structural safeguards?
- Are developers or project managers on the security team? If so, how can they work more collaboratively with the privacy team to incorporate privacy principles into new products and services?

Data Subject Rights

ISO 27001 Data Categorization and Access Control Requirements

ISO 27001 does not explicitly address data subject rights. The combination of data inventory, classification, and operating requirements from Clause 8 and Control A.8, however, empowers security with knowledge of the categories of data the organization collects about data subjects and where the data lives. Control A.9, moreover, addresses access controls, which include how to authenticate data subjects gaining access to their own data through login credentials.

GDPR Data Subject Rights

The GDPR addresses data subject rights in Articles 13 through 22, with each article

focusing on a specific right. Data subjects are entitled to: transparency regarding what personal data about them is collected and how it is processed; the right to access their personal data; the right to correct ("rectify") inaccurate personal data about them and to have their information erased under certain circumstances; to restrict the controller's processing of the data; and to be able to require the controller to port their data to another controller in certain circumstances. In addition, data subjects have the right to know if decisions are made about them through automated means and to object to such processing, as well as to object to direct marketing.

ISO 27001	GDPR	Collaboration
Control A.8: Information assets shall be inventoried and classified; asset owners shall be assigned, with procedures defined for acceptable data use, labelling, and handling. Ownership of assets shall be clearly identified.	**Article 12:** Controllers shall be transparent regarding their processing activities and provide clearly understandable information when data subjects exercise their rights. **Article 13:** Controllers shall share certain information with data subjects at the time of collection, including: • The controller's and DPO's contact information. • The purpose and legal bases for processing personal data. • Third party recipients of the personal data. • Information about any international transfers of the data. • Data retention periods. • The existence of their data subject rights. **Article 14:** Data subjects are entitled to receive certain notifications when their data is obtained from third parties.	For security professionals, sharing information about data processing with consumers is likely counter-intuitive to their information security instincts and training. Yet, the GDPR mandates that controllers be open and transparent about their data processing practices and even allow data subjects the ability to gain access to their data through secure automated means, if feasible. Privacy teams will need to work closely with security professionals to understand the categories of data collected and stored, and respective retention policies. They will also need assistance cataloging the external parties with whom data is shared, including any transfer and storage outside of the EU. The IT processing policies required by ISO 27001 are critical to providing data subjects with accurate information regarding processing activities.

continued

ISO 27001	GDPR	Collaboration
Control A.8: Information assets shall be inventoried and classified; asset owners shall be assigned, with procedures defined for acceptable data use, labelling, and handling. Ownership of assets shall be clearly identified. **Control A.9.2:** Organizations shall have formal systems for user registration and de-registration to enable access right assignment; they shall have processes for authenticating users and revoking access; employees and external parties shall lose access rights upon termination of the relationship. **Control A.9.4:** Secure log-on procedures shall be used to authenticate user access to information and application systems. **Control A.12:** Operating procedures shall be documented. **Control A.13:** Security personnel shall have awareness of and appropriate controls for the security of information transferred to an external party.	**Article 15:** Data subjects are entitled to receive certain information upon request, including: • The purposes of the controller's processing activities. • The categories of personal data processed. • Recipients of the data, including third parties. • Data retention periods. • The existence of their data subject rights. • Information about the original source of the data if not the controller. • Existence of any automated decision-making. The controller shall provide a copy of the data undergoing processing. **Recital 63:** Where possible, the controller should be able to provide remote access to a secure system that would provide the data subject with direct access to his or her personal data. **Recital 64:** The controller should use all reasonable measures to verify the identity of the data subject who requests access. **Article 16:** Data subjects have the right to correct inaccurate personal data about them. **Article 17:** Data subjects may obtain erasure of their data without undue delay when the data is no longer necessary for the purpose for which it were collected, when consent for processing is withdrawn, was the data subject objects to processing on certain grounds, or when the data has been unlawfully processed.	Security professionals can provide crucial support to the privacy team in responding to data subjects seeking access to, or rectification, erasure or portability of, their personal data. Such activities inherently present security risks to information systems if not handled carefully. Thus, the privacy team will need to collaborate with the security team on building systems for responding to data subject requests in a manner that authenticates the data subject – the GDPR of course requires that data subjects be able to see only their own data, and that effort be made to verify their identity should a request be submitted. The privacy team will also need to rely on programmers and security professionals to facilitate automated access, rectification, and perhaps even erasure. The security team may also help with generating records of these requests and the timeliness of response. Security teams following ISO 27001 classification and operating procedures should be well positioned to assist with these endeavors. Still, classification, access rights, and operating procedures may need to be reviewed with the privacy team and updated as necessary to ensure that the appropriate information is provided to data subjects at the time of collection and on request, in a secure manner.

continued

ISO 27001	GDPR	Collaboration
	Article 18: Data subjects have the right to compel the controller to restrict its data processing under specific circumstances. **Article 19:** The controller must provide notice to data subjects in the case of rectification, erasure, or restriction. **Article 20:** Data subjects may request the transfer of personal data between controllers when feasible. **Article 21:** Data subjects may object to the general processing of their personal data, including for profiling and marketing. **Article 22:** Data subjects have the right not be subject to automated decision-making.	

Leveraging Data Infrastructure To Respond to Subject Rights

Organizations with existing ISO 27001 inventories and policies will have a leg up in ensuring more effective responses to data subject rights under the GDPR. The ISO 27001 inventory and categorization requirements will allow security teams to support privacy professionals in data mapping and inventory, and in describing to data subjects the categories of information about them and how it is processed, as well as to whom it is transferred. Security professionals will be essential in managing data assets, ensuring that appropriate permissions are employed, and implementing notice and review policies.

Internal Discussion Items

- Which tags or markers do current data inventories and categorization schemes include?
    - What additional tags would be required to comply with a GDPR data subject request?
- Do current policies and procedures allow for data subjects to securely access any personal data your organization is holding about them? Are there other types of personal data that data subjects cannot automatically access? How will those reports be generated and communicated securely?
- Are there policies in place to review and correct outdated or otherwise incorrect information?
- Is there a policy or procedure in place to ensure that data subjects are notified when their personal data is changed or deleted?
- Does your organization use automated decision-making processes based on personal data?
- What data retention policies are in place and how are they enforced?
- Does the security team have an updated list of all external parties to whom personal data is transferred?

Conclusion

Organizations that achieve ISO 27001 certification send reassuring signals to data controllers seeking to share data with them. They also have security professionals who, through following ISO 27001's clauses and controls, are well positioned to work with privacy professionals building programs for GDPR compliance. Indeed, the frameworks and policies already developed and implemented by security teams may streamline and significantly simplify the development of new GDPR-compliant privacy procedures. What is more, through their collaboration, security professionals will gain insight into new relevant legal requirements relating to information assets and assistance incorporating them into their documentation and security plans.

In sum, security professionals familiar with and following ISO 27001 will find they are already well on the way to understanding and adding value to the privacy team's GDPR programs—and vice versa.

The IAPP offers free access to the OneTrust GDPR Readiness Assessment which includes ISO 27001 annotations in the IAPP-OneTrust PIA and Data Mapping Tool.