The Skill Set Needed to Implement a Global Privacy Standard:

ISO/IEC 27701 alignment with IAPP CIPM and CIPP/E certifications

Caitlin Fennessy, CIPP/US

iapp

In August 2019, the International Standards Organization released its first global privacy standard, ISO/IEC 27701. To offer insight into the professional skill set necessary to implement this new global privacy standard, the International Association of Privacy Professionals' Westin Research Center mapped ISO/IEC 27701 to the bodies of knowledge for a Certified Information Privacy Professional/Europe and a Certified Information Privacy Manager. These bodies of knowledge were created by the IAPP's certification advisory boards to reflect the skill set and knowledge required by a privacy professional working in the relevant field. They are annually updated, as required by IAPP's ANSI accreditation, through a formal process to determine what professionals in the field are currently doing, under what conditions and with what levels of knowledge and skill. Certification exams are then updated to align with these bodies of knowledge.

ISO/IEC 27701 is a standard designed to guide organizations in establishing, implementing, maintaining and continually improving a privacy information management system. Given its focus on privacy management, the body of knowledge for IAPP's CIPM certification is closely aligned with the standard's requirements. In addition to providing the structure to build a privacy management system, ISO/IEC 27701 was designed with an eye toward future certification of compliance with the EU General Data Protection Regulation. For this reason, the detailed privacy controls ISO/IEC 27701 outlines for controllers and processors map directly to the GDPR, as well as the body of knowledge for IAPP's CIPP/E certification.

This new global privacy standard was developed by a technical committee comprised of privacy experts from around the world, including data protection authorities, security agencies, academia and industry. This breadth of knowledge helped ensure that this ISO/IEC 27701 was informed not only by GDPR, but also by other data protection laws from around the world. While the standard itself presents a mapping to the GDPR, industry efforts are underway to map ISO/IEC 27701 to other national and sub-national privacy laws. This work should assist organizations working to develop a global privacy management system that serves their local compliance efforts.

The authors of ISO/IEC 27701 also aimed to help organizations translate principles-based legal requirements into technical privacy controls that can be implemented in tandem with appropriate security controls. ISO/IEC 27701 is a privacy information management extension to ISO's widely adopted and globally recognized ISO/IEC 27001, "Information Technology – Security techniques – Information security management systems – Requirements." With more than 60,000 organizations certified to ISO/IEC 27001, this alignment offers thousands of organizations the opportunity to better integrate their privacy and security programs.

The IAPP's Westin Research Center developed the following table to document how an ISO privacy standard designed to achieve the above goals aligns with IAPP's certifications. This mapping serves the dual purpose of informing privacy professionals seeking to understand the skill set needed to implement a global privacy standard and IAPP's ongoing work to ensure its certifications are continually refined to meet the needs of the privacy profession around the world.

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
PMS-specific requirements related to ISO/IEC 27001	
5.2.1 Understanding the organization and its context	**CIPM Domain I. A. c. ii.** Identify the source, types, and uses of personal information (PI) within the organization and the applicable laws **CIPM Domain I. C. b.** Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework • Understand when national laws and regulations apply (e.g. GDPR, CCPA) • Understand when local laws and regulations apply • Understand penalties for noncompliance with laws and regulations • Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.) • Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws • Maintain the ability to manage a global privacy function • Maintain the ability to track multiple jurisdictions for changes in privacy law • Understand international data sharing arrangement agreements
5.2.2 Understanding the needs and expectations of interested parties	**CIPM Domain I. A. c. iii. 1. b.** Develop a privacy strategy • Business alignment • Identify stakeholders

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
5.2.3. Determining the scope of the information privacy management system	**CIPM Domain I. A. c. i.** Establish a privacy program • Define program scope and charter

5.2.4. Information security management system	**CIPM Domain I. B.**
	Develop the Privacy Program Framework
	• Develop organizational privacy policies, standards and/or guidelines
	• Define privacy program activities
	  • Education and awareness
	  • Monitoring and responding to the regulatory environment
	  • Internal policy compliance
	  • Data inventories, data flows, and classification
	  • Risk assessment (Privacy Impact Assessments [PIAs]) (e,g., DPIAs etc.)
	  • Incident response and process, including jurisdictional regulations
	  • Remediation
	  • Program assurance, including audits

5.3.1 Leadership and commitment	**CIPM Domain I. A. a.** Create a company vision • Acquire knowledge on privacy approaches • Evaluate the intended objective • Gain executive sponsor approval for this vision
5.3.2 Policy	**CIPM Domain I. A. b.** Establish Data Governance model • Centralized • Distributed • Hybrid **CIPM Domain I. B. a.** Develop organizational privacy policies, standards and/or guidelines

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge

5.3.3. Organizational roles, responsibilities and authorities	**CIPM Domain I. A. c. iii. 1. a-d**
	Business alignment
	• Finalize the operational business case for privacy
	• Identify stakeholders
	• Leverage key functions
	• Create a process for interfacing within organization
	
	CIPM Domain I. A. d.
	Structure the privacy team
	• Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization
	  • Large organizations
	  • Chief privacy officer
	  • Privacy manager
	  • Privacy analysts
	  • Business line privacy leaders
	  • "First responders"
	  • Small organizations/sole data protection officer (DPO) including when not only job
	• Designate a point of contact for privacy issues
	• Establish/endorse the measurement of professional competency

5.4.1 Actions to address risks and opportunities	**CIPM Domain I. B. b.** Define privacy program activities • Risk assessment (Privacy Impact Assessments [PIAs]) (e.g., DPIAs etc.) • Incident response and process, including jurisdictional regulations • Remediation • Program assurance, including audits
5.4.2 Information security objectives and planning to achieve them	**CIPM Domain I. A. c. iii. 2-3** • Develop a data governance strategy for personal information (collection, authorized use, access, destruction) • Plan inquiry/complaint handling procedures (customers, regulators, etc.)

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
5.5.1 Resources	**CIPM Domain I. A. c. iii. 1.** Business alignment • Finalize the operational business case for privacy • Identify stakeholders • Leverage key functions • Create a process for interfacing within organization • Align organizational culture and privacy/data protection objectives • Obtain funding/budget for privacy and the privacy team **CIPM Domain II. C. b.** Integrate privacy requirements and representation into functional areas across the organization • Information security • IT operations and development • Business continuity and disaster recovery planning • Mergers, acquisitions and divestitures • Human resources • Compliance and ethics • Audit • Marketing/business development • Public relations • Procurement/sourcing • Legal and contracts • Security/emergency services • Finance • Others
5.5.2 Competence	**CIPM Domain I. A. d. iii.** Establish/endorse the measurement of professional competency

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
5.5.3 Awareness	**CIPM Domain I. B. a, b. i.** Develop the Privacy Program Framework • Develop organizational privacy policies, standards and/or guidelines • Define privacy program activities • Education and awareness **CIPM Domain I. C. d. i. 1, 4** • Create awareness of the organization's privacy program internally and externally • Identify, catalog and maintain documents requiring updates as privacy requirements change

5.5.4 Communication	**CIPM Domain II. C. d. i. 3. & ii.**
	• Develop internal and external communication plans to ingrain organizational accountability
	• Targeted employee, management and contractor training
	  • Privacy policies
	  • Operational privacy practices (e.g., standard operating instructions), such as Data creation/usage/retention/disposal
	  • Access control
	  • Reporting incidents
	  • Key contacts

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge

5.5.5 Documented information	**CIPM Domain I. B. a.**
	Develop organizational privacy policies, standards and/or guidelines
	
	CIPM Domain I. D. b.
	Define reporting resources
	
	CIPM Domain II. A. a.
	Document current baseline of your privacy program
	• Education and awareness
	• Monitoring and responding to the regulatory environment
	• Internal policy compliance
	• Data, systems and process assessment
	  • Map data inventories, flows and classification
	  • Create "record of authority" of systems processing personal information within the organization
	  • Map and document data flow in systems and applications
	  • Analyze and classify types and uses of data
	• Risk assessment (PIAs, etc.)
	• Incident response vii. Remediation
	• Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)
	• Program assurance, including audits
	
	CIPM Domain II. C. d. i. 4.
	Identify, catalog and maintain documents requiring updates as privacy requirements change

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
5.6.1 Operational planning and control **5.6.2. Information security risk assessment**	**CIPM Domain II. A. a. v, vii, viii** • Risk assessment (PIAs, etc.) • Remediation • Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)

5.6.3. Information security risk treatment	**CIPM Domain II. A. b. i, iii**
	Processors and third-party vendor assessment
	• Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
	  • Privacy and information security policies
	  • Access controls
	  • Where personal information is being held
	  • Who has access to personal information
	• Risk assessment
	  • Type of data being outsourced
	  • Location of data
	  • Implications of cloud computing strategies
	  • Legal compliance
	  • Records retention
	  • Contractual requirements (incident response, etc.)
	  • Establish minimum standards for safeguarding information

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
	CIPM Domain II. A. c, d, e Physical assessments - Identify operational risk • Data centers and offices • Physical access controls • Document destruction • Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.) • Device forensics • Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls) Mergers, acquisitions and divestitures • Due diligence • Risk assessment Conduct analysis and assessments, as needed or appropriate • Privacy Threshold Analysis (PTAs) on systems, applications and processes • Privacy Impact Assessments (PIAs) • Define a process for conducting Privacy Impact Assessments • Understand the life cycle of a PIA Incorporate PIA into system, process, product life cycles

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge

5.7.1 Monitoring, measurement, analysis and evaluation	**CIPM Domain I. D.**
	Metrics
	• Identify intended audience for metrics
	• Define reporting resources
	• Define privacy metrics for oversight and governance per audience
	  • Compliance metrics (examples, will vary by organization)
	  • Collection (notice)
	  • Responses to data subject inquiries
	  • Use
	  • Retention
	  • Disclosure to third parties
	  • Incidents (breaches, complaints, inquiries)
	  • Employees trained
	  • PIA metrics
	  • Privacy risk indicators
	  • Percent of company functions represented by governance mechanisms
	  • Trending
	  • Privacy program return on investment (ROI)
	  • Business resiliency metrics
	  • Privacy program maturity level
	  • Resource utilization
	• Identify systems/application collection points
	
	CIPM Domain II. A. e.
	Conduct analysis and assessments, as needed or appropriate
	• Privacy Threshold Analysis (PTAs) on systems, applications and processes
	• Privacy Impact Assessments (PIAs)
	  Define a process for conducting –
	  • Privacy Impact Assessments
	  • Understand the life cycle of a PIA
	  • Incorporate PIA into system, process, product life cycles

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge

	CIPM Domain II. C. a.
	Measure
	• Quantify the costs of technical controls
	• Manage data retention with respect to the organization's policies
	• Define the methods for physical and electronic data destruction
	• Define roles and responsibilities for managing the sharing and disclosure of data for internal and external use
	
	CIPM Domain II. C. e.
	Monitor
	• Environment (e.g., systems, applications) monitoring
	• Monitor compliance with established privacy policies
	• Monitor regulatory and legislative changes
	• Compliance monitoring (e.g. collection, use and retention)
	  • Internal audit
	  • Self-regulation
	  • Retention strategy
	  • Exit strategy

5.7.2 Internal audit	**CIPM Domain I. B. b. viii.**
	Define privacy program activities
	• Program assurance, including audits
	
	CIPM Domain II. A. a. ix.
	Document current baseline of your privacy program
	• Program assurance, including audits
	
	CIPM Domain II. C. c.
	Audit
	• Align privacy operations to an internal and external compliance audit program
	  • Knowledge of audit processes
	  • Align to industry standards
	• Audit compliance with privacy policies and standards
	• Audit data integrity and quality and communicate audit findings with stakeholders
	• Audit information access, modification and disclosure accounting

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
5.7.3 Management review	**CIPM Domain II A. a. iii** Document current baseline of your privacy program • Internal policy compliance **CIPM Domain II. C. c. ii. & e. ii.** • Audit compliance with privacy policies and standards • Monitor compliance with established privacy policies
5.8.1 Nonconformity and corrective action	**CIPM Domain I. B. b. vii.** Define privacy program activities i. Education and awareness • Remediation **CIPM Domain II. A. a. vii.** Document current baseline of your privacy program • Remediation
5.8.2 Continual improvement	**CIPM Domain I. C. b.** Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework • Understand when national laws and regulations apply (e.g. GDPR, CCPA) • Understand when local laws and regulations apply • Understand penalties for noncompliance with laws and regulations • Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.) • Maintain the ability to manage a global privacy function • Maintain the ability to track multiple jurisdictions for changes in privacy law • Understand international data sharing arrangement agreements **CIPM Domain II. B. c.** Privacy by Design • Integrate privacy throughout the system development life cycle (SDLC) • Establish privacy gates as part of the system development framework

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
PIMS-specific guidance related to ISO/IEC 27002	**Note:** Only ISO/IEC 27002 controls with additional PII-specific implementation guidance are mapped

6.2.1 Management direction for information privacy	**CIPM Domain I B – C**
	Develop the Privacy Program Framework
	• Develop organizational privacy policies, standards and/or guidelines
	• Define privacy program activities
	  • Education and awareness
	  • Monitoring and responding to the regulatory environment
	  • Internal policy compliance iv. Data inventories, data flows, and classification
	  • Risk assessment (Privacy Impact Assessments [PIAs]) (e.g., DPIAs etc.)
	  • Incident response and process, including jurisdictional regulations
	  • Remediation
	  • Program assurance, including audits
	Implement the Privacy Program Framework
	• Communicate the framework to internal and external stakeholders
	• Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework
	  • Understand when national laws and regulations apply (e.g. GDPR, CCPA)
	  • Understand when local laws and regulations apply
	  • Understand penalties for noncompliance with laws and regulations
	  • Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.)
	  • Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws
	  • Maintain the ability to manage a global privacy function
	  • Maintain the ability to track multiple jurisdictions for changes in privacy law
	  • Understand international data sharing arrangement agreements

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
	CIPM Domain II. A. b. iv. Processors and third-party vendor assessment Contractual requirements
6.3.1 Internal organization	**CIPM Domain I. A. d.** Structure the privacy team • Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization Large organizations • Chief privacy officer • Privacy manager • Privacy analysts • Business line privacy leaders • "First responders" Small organizations/sole data protection officer (DPO) including when not only job • Designate a point of contact for privacy issues Establish/endorse the measurement of professional competency
6.3.2 Mobile devices and teleworking	**CIPM Domain II A. c. i. 6** Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls)
6.4.2 During employment	**CIPM Domain II. C. d. ii.** Targeted employee, management and contractor training • Privacy policies • Operational privacy practices (e.g., standard operating instructions), such as • Data creation/usage/retention/disposal • Access control • Reporting incidents • Key contacts

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
6.5.2 Information classification	**CIPM Domain I. B. b. iv.** Define privacy program activities • Data inventories, data flows, and classification **CIPM Domain II. A. a. iv.** Data, systems and process assessment • Map data inventories, flows and classification • Create "record of authority" of systems processing personal information within the organization • Map and document data flow in systems and applications • Analyze and classify types and uses of data
6.5.3 Media handling	**CIPM Domain II. A. c. i.** Identify operational risk • Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.) **CIPM Domain II. B. b. ii.** Technical security controls
6.6.2 User access management **6.6.4 System and application access control**	**CIPM Domain II. A. b. i. 2, 4** Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer • Access controls • Who has access to personal information **CIPM Domain II. A. c. i. 2** Physical assessments • Identify operational risk • Physical access controls **CIPM Domain II. B. b. i, iii** Access controls for physical and virtual systems • Access control on need to know • Account management (e.g., provision process) • Privilege management Implement appropriate administrative safeguards **CIPM Domain II. C. c. iv** Audit information access, modification and disclosure accounting

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
6.7.1 Cryptographic controls	**CIPM Domain II. B. b. ii.** Technical security controls **CIPM Domain II. C. d. i. 1-2** • Create awareness of the organization's privacy program internally and externally • Ensure policy flexibility in order to incorporate legislative/ regulatory/market requirements
6.8.2 Equipment	**CIPM Domain II. A. c. i.** Identify operational risk • Data centers and offices • Physical access controls • Document destruction • Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.) • Device forensics • Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls) **CIPM Domain II. C. d. ii. 2. a.** Operational privacy practices (e.g., standard operating instructions), such as • Data creation/usage/retention/disposal
6.9.3 Backup	**CIPM Domain II. C. c. iii.** Audit data integrity and quality and communicate audit findings with stakeholders **CIPM Domain II. D. a. iv.** Respond • Managing data integrity

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
6.9.4 Logging and monitoring	**CIPM Domain II. A. b. i. 2.** Processors and third-party vendor assessment • Access controls **CIPM Domain II. B. b. i.** Access controls for physical and virtual systems • Access control on need to know • Account management (e.g., provision process) • Privilege management **CIPM Domain II. C. c. iv.** Audit information access, modification and disclosure accounting

6.10.2 Information transfer	**CIPM Domain II. A. b. iii.-v.**
	Processors and third-party vendor assessment
	• Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
	  • Privacy and information security policies
	  • Access controls
	  • Where personal information is being held
	  • Who has access to personal information
	• Understand and leverage the different types of relationships
	  • Internal audit
	  • Information security
	  • Physical security
	  • Data protection authority
	• Risk assessment
	  • Type of data being outsourced
	  • Location of data
	  • Implications of cloud computing strategies
	  • Legal compliance
	  • Records retention
	  • Contractual requirements (incident response, etc.)
	  • Establish minimum standards for safeguarding information
	• Contractual requirements
	• Ongoing monitoring and auditing

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
6.11.1 Security requirements of information systems	**CIPM Domain II. B. b. ii.** Technical security controls

6.11.2 Security in development and support processes	**CIPM Domain II. B. a. & c.**
	• Data life cycle and governance (creation to deletion)
	• Privacy by Design
	  • Integrate privacy throughout the system development life cycle (SDLC)
	  • Establish privacy gates as part of the system development framework

6.11.3 Test data	**CIPM Domain II. A. e. ii. 1. b.** Incorporate PIA into system, process, product life cycles **CIPM Domain II. B. c. i.** Integrate privacy throughout the system development life cycle (SDLC)

6.12.1 Information security in supplier relationships	**CIPM Domain II. A. b. i, iii-v.**
	Processors and third-party vendor assessment
	• Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
	  • Privacy and information security policies
	  • Access controls
	  • Where personal information is being held
	  • Who has access to personal information
	• Risk assessment
	  • Type of data being outsourced
	  • Location of data
	  • Implications of cloud computing strategies
	  • Legal compliance
	  • Records retention
	  • Contractual requirements (incident response, etc.)
	  • Establish minimum standards for safeguarding information
	• Contractual requirements
	• Ongoing monitoring and auditing

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
6.13.1 Management of information privacy incidents and improvements	**CIPM Domain II. D. b.** Privacy incidents Legal compliance • Preventing harm • Collection limitations • Accountability • Monitoring and enforcement Incident response planning • Understand key roles and responsibilities • Identify key business stakeholders • Information security • Legal • Audit • Human resources • Marketing • Business development • Communications and public relations • Other • Establish incident oversight teams • Develop a privacy incident response plan • Identify elements of the privacy incident response plan • Integrate privacy incident response into business continuity planning Incident detection • Define what constitutes a privacy incident • Identify reporting process • Coordinate detection capabilities • Organization IT • Physical security • Human resources • Investigation teams • Vendors

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
	Incident handling • Understand key roles and responsibilities • Develop a communications plan to notify executive management Follow incident response process to ensure meeting jurisdictional, global and business requirements • Engage privacy team • Review the facts • Conduct analysis • Determine actions (contain, communicate, etc.) • Execute • Monitor • Review and apply lessons learned Identify incident reduction techniques Incident metrics—quantify the cost of a privacy incident
6.15.1 Compliance with legal and contractual requirements	**CIPM Domain I. C. b.** Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework • Understand when national laws and regulations apply (e.g. GDPR, CCPA) • Understand when local laws and regulations apply • Understand penalties for noncompliance with laws and regulations • Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.) • Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws • Maintain the ability to manage a global privacy function • Maintain the ability to track multiple jurisdictions for changes in privacy law • Understand international data sharing arrangement agreements

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge

6.15.2 Information security reviews	**CIPM Domain II. C. c.**
	Audit
	• Align privacy operations to an internal and external compliance audit program
	  • Knowledge of audit processes
	  • Align to industry standards
	• Audit compliance with privacy policies and standards
	• Audit data integrity and quality and communicate audit findings with stakeholders
	• Audit information access, modification and disclosure accounting

Additional ISO/IEC 27002 guidance for PII controllers	
7.2.1 Identify and document purpose	**CIPP/E Domain II. A. 1, 2, 4** • Personal data • Sensitive personal data • Processing **CIPP/E Domain II. C. 2.** Purpose limitation
7.2.2 Identify lawful basis	**CIPP/E Domain II. C. 1.** Fairness and lawfulness **CIPP/E Domain II. D.** Lawful Processing Criteria • Consent • Contractual necessity • Legal obligation, vital interests and public interest • Legitimate interests Special categories of processing
7.2.3 Determine when and how consent is to be obtained	**CIPP/E Domain II. D. 1.** Consent **CIPP/E Domain II. F. 5.** Consent, including right of withdrawal

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
7.2.4 Obtain and record consent	**CIPP/E Domain II. D. 1.** Consent **CIPP/E Domain II. H.3.** Documentation and cooperation with regulators
7.2.5 Privacy impact assessment	**CIPP/E Domain II. H.4.** Data protection impact assessment • Established criteria for conducting
7.2.6 Contracts with PII processors	**CIPP/E Domain II. A. 6.** Processor **CIPP/E Domain II. G. 3-4** Security of Personal Data • Vendor Management • Data sharing **CIPP/E Domain II. H. 1.** • Responsibilities of controllers and processors
7.2.7 Joint PII controller	**CIPP/E Domain II. A. 5.** Controller **CIPP/E Domain II. H. 1.** Responsibilities of controllers and processors • Joint controllers
7.2.8 Records related to processing PII	**CIPP/E Domain II. H.3.** Documentation and cooperation with regulators

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
7.3.1 Determining and fulfilling obligations to PII principals	**CIPP/E Domain II. A. 7** Data subject **CIPP/E Domain II. F.** Data Subjects' Rights • Access • Rectification • Erasure and the right to be forgotten (RTBF) • Restriction and objection • Consent, including right of withdrawal • Automated decision making, including profiling • Data portability Restrictions
7.3.2 Determining information for PII principals **7.3.3 Providing information to PII principals**	**CIPP/E Domain II. E.** Information Provision Obligations • Transparency principle • Privacy notices • Layered notices
7.3.4 Providing mechanism to modify or withdraw consent	**CIPP/E Domain II. F. 5.** Consent, including right of withdrawal
7.3.5 Provide mechanism to object to PII processing	**CIPP/E Domain II. F. 4.** Restriction and objection
7.3.6 Access, correction and/or erasure	**CIPP/E Domain II. F. 1-3** Data Subjects' Rights • Access • Rectification • Erasure and the right to be forgotten (RTBF)

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
7.3.7 PII controllers' obligations to inform third parties	**CIPP/E Domain II. G. 3-4** Security of Personal Data • Vendor Management • Data sharing **CIPP/E Domain II. H. 1.** Responsibilities of controllers and processors
7.3.8 Providing copy of PII processed	**CIPP/E Domain II. F. 1, 7** Data Subjects' Rights • Access Data portability
7.3.9 Handling requests	**CIPP/E Domain II. F. 1.** Access **CIPP/E Domain II. H. 5.** Mandatory data protection officers
7.3.10 Automated decision making	**CIPP/E Domain II. F. 6.** Automated decision making, including profiling
7.4.1 Limit collection	**CIPP/E Domain II. C. 2.** Purpose limitation
7.4.2 Limit processing	**CIPP/E Domain II. C. 3.** Proportionality
7.4.3 Accuracy and quality	**CIPP/E Domain II. C. 4.** Accuracy
7.4.4 PII minimization objectives	**CIPP/E Domain II. A. 3.** Pseudonymous and anonymous data
7.4.5 PII de-identification and deletion at the end of processing	**CIPP/E Domain II. C. 5.** Storage limitation (retention)

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
7.4.6 Temporary files	**CIPP/E Domain II. C. 5.** Storage limitation (retention) **CIPP/E Domain II. H. 2.** Data protection by design and by default
7.4.7 Retention	**CIPP/E Domain II. C. 5.** Storage limitation (retention)
7.4.8 Disposal	**CIPP/E Domain II. C. 5-6** • Storage limitation (retention) Integrity and confidentiality
7.4.9 PII transmission controls	**CIPP/E Domain II. G. 1, 3, 4** Security of Personal Data • Appropriate technical and organizational measures • protection mechanisms (encryption, access controls, etc.) • Vendor Management Data sharing
7.5.1 Identify basis for PII transfer between jurisdictions	**CIPP/E Domain II. I.** International Data Transfers • Rationale for prohibition • Safe jurisdictions • Safe Harbor and Privacy Shield • Model contracts • Binding Corporate Rules (BCRs) • Codes of Conduct and Certifications Derogations
7.5.2 Countries and international organizations to which PII can be transferred	**CIPP/E Domain II. I.** International Data Transfers • Rationale for prohibition • Safe jurisdictions **CIPP/E Domain II. H. 3.** Documentation and cooperation with regulators

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
7.5.3 Records of transfer of PII	**CIPP/E Domain II. I.** International Data Transfers
7.5.4 Records of PII disclosures to third parties	**CIPP/E Domain II. G. 3-4** • Vendor Management Data sharing **CIPP/E Domain II. H. 3.** Documentation and cooperation with regulators
Additional ISO/IEC 27002 guidance for PII processors	
8.2.1 Customer agreement	**CIPP/E Domain II. G. 3-4** • Vendor Management • Data sharing **CIPP/E Domain II. H. 1.** Responsibility of controllers and processors
8.2.2 Organization's purposes	**CIPP/E Domain II. A. 1, 2, 4** • Personal data • Sensitive personal data • Processing **CIPP/E Domain II. C. 2.** Purpose limitation **CIPP/E Domain II. G. 3-4** • Vendor Management • Data sharing

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
8.2.3 Marketing and advertising use	**CIPP/E Domain II. G. 3-4** Vendor Management Data sharing **CIPP/E Domain II. C. 2.** Purpose limitation **CIPP/E Domain III. C.** Direct Marketing • Telemarketing • Direct marketing Online behavioural targeting
8.2.4 Infringing instruction	**CIPP/E Domain I. C.** Legislative Framework **CIPP/E Domain II. C. 1.** Fairness and lawfulness **CIPP/E Domain II. D.** Lawful Processing Criteria **CIPP/E Domain II. G. 3-4** • Vendor Management Data sharing
8.2.5 Customer obligations	**CIPP/E Domain II. E.** Information Provision Obligations • Transparency principle • Privacy notices Layered notices
8.2.6 Records related to processing PII	**CIPP/E Domain II. H. 3.** Documentation and cooperation with regulators

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
8.3.1. Obligations to PII principles	**CIPP/E Domain II. E.** Information Provision Obligations **CIPP/E Domain II. F.** Data Subjects' Rights **CIPP/E Domain II. H. 1.** Accountability Requirements Responsibility of controllers and processors
8.4.1 Temporary files	**CIPP/E Domain II. C. 5.** Storage limitation (retention) **CIPP/E Domain II. H. 2.** Data protection by design and by default
8.4.2 Return, transfer or disposal of PII	**CIPP/E Domain II. C. 5-6** • Storage limitation (retention) • Integrity and confidentiality **CIPP/E Domain II. H.** Responsibility of controllers and processors
8.4.3 PII transmission controls	**CIPP/E Domain II. G. 1, 3, 4** Security of Personal Data • Appropriate technical and organizational measures • protection mechanisms (encryption, access controls, etc.) • Vendor Management Data sharing

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
8.5.1 Basis for PII transfer between jurisdictions	**CIPP/E Domain II. I.** International Data Transfers • Rationale for prohibition • Safe jurisdictions • Safe Harbor and Privacy Shield • Model contracts • Binding Corporate Rules (BCRs) • Codes of Conduct and Certifications • Derogations **CIPP/E Domain II. G. 3, 4** • Vendor Management • Data sharing **CIPP/E Domain II. H. 1.** Responsibility of controllers and processors
8.5.2 Countries and international organizations to which PII can be transferred	**CIPP/E Domain II. I.** International Data Transfers • Rationale for prohibition • Safe jurisdictions • Safe Harbor and Privacy Shield • Model contracts • Binding Corporate Rules (BCRs) • Codes of Conduct and Certifications • Derogations **CIPP/E Domain II. H. 3.** Documentation and cooperation with regulators
8.5.3 Records of PII disclosure to third parties	**CIPP/E Domain II. H. 1, 3** Accountability Requirements • Responsibility of controllers and processors Documentation and cooperation with regulators
8.5.4 Notification of PII disclosure requests	**CIPP/E Domain II. H. 1.** Responsibility of controllers and processors

ISO/IEC 27701:2019	IAPP CIPP/E & CIPM Body of Knowledge
8.5.5 Legally binding PII disclosures	**CIPP/E Domain II. G. 3, 4** • Vendor Management • Data sharing **CIPP/E Domain II. H. 1.** Responsibility of controllers and processors
8.5.6 Disclosures of subcontractors used to process PII	
8.5.7 Engagement of a subcontractor to process PII	
8.5.8 Change of subcontractor to process PII	