Ryerson University

Privacy by Design
Centre of Excellence

Privacy by Design Certification Program: Assessment Control Framework

Appendix A – Privacy by Design controls framework

Principle 1 – Proactive not Reactive; Preventative not Remedial:

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
1.1 Privacy Governance - Responsibility and Accountability for Policies and Procedures Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating the organization's privacy policies and procedures.	**1.1.1 Contact Person** The organization assigns responsibility for privacy policies to a designated person who is a senior member of the organization, such as a corporate privacy officer. When dealing with EU residents' data, the organization: • Provides the privacy contact's information to the correspondent EU Data Protection Authority; and • Appoints an EU representative (e.g. a law firm) to represent EU operations where there is a privacy issue or complaint. **1.1.2 Documented Roles and Responsibilities for Privacy** The responsibility, authority, and accountability of the designated person or group are clearly documented. Responsibilities include the following: • Establishing with management the standards used to classify the sensitivity of personal information and to determine the level of protection required; • Formulating and maintaining the organization's privacy policies; • Monitoring and updating the organization's privacy policies; • Delegating authority for enforcing the organization's privacy policies; • Monitoring the degree of compliance and initiating action to improve the training or clarification of policies and practices; and • Reporting to the leadership team on the privacy program, privacy incidents/breaches, any relevant metrics, and compliance, on a periodic basis.
1.2 Privacy Impact Assessments or Privacy Risk Reviews Projects undergo a Privacy Impact Assessment (PIA) or a Privacy Risk Review prior to launching a new product or	**1.2.1 Privacy Assessment Process** A process is in place whereby management assesses the impact of new and significantly changed products, services, business processes, and infrastructure (including any such activities outsourced to third parties or contractors).

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
service offering, or to proactively monitor current state of privacy.	When dealing with EU residents' data, consult the correspondent EU Data Protection Authority prior to processing personal information where a privacy assessment identifies a high risk. **1.2.2 Documented Privacy Assessment, Recommendations and Roadmap** A documented PIA exists dated prior to the implementation of the project. The PIA identifies any privacy gaps/risks associated with the project and provides detailed recommendations to address or close the identified gaps/risks and organized within a privacy risk management plan or roadmap. There is evidence that recommendations from these assessments were incorporated and considered in the finally implemented system or service.
1.3 Privacy Incident and Breach Management A documented privacy incident and breach management program has been implemented that includes, but is not limited to, the following: • Procedures for the identification, management, and resolution of privacy incidents and breaches • Defined responsibilities • A process to identify incident severity and determine required actions and escalation procedures • A process for complying with breach laws and regulations, including stakeholders breach notification, if required • An accountability process for employees or third parties responsible for incidents or breaches with remediation, penalties, or discipline as appropriate • A process for periodic review (at least on an annual basis) of actual incidents to identify necessary program updates based on: incident patterns and root cause; and changes in the internal control environment or external requirements (regulation or legislation)	**1.3.1 Breach Management Process/Program** A formal, comprehensive privacy incident and breach management program has been implemented, which specifies the following: • Incidents and breaches are reported to a member of the breach team, who asses if it is privacy or security related, or both, classifies the severity of the incident, initiates required actions, and determines the required involvement by individuals who are responsible for privacy and security. • The Chief Privacy Officer (CPO) has the overall accountability for the program and is supported by the privacy and security steering committees and assisted by the breach team. Incidents and breaches that do not involve personal information are the responsibility of the chief security officer. • The program includes a clear escalation path, based on the type or severity, or both, of the incident, up to executive management, legal counsel and the board. • The program sets forth a process for breach notification of affected individuals and external stakeholders (e.g. privacy regulator) as well as for contacting law enforcement, regulatory, or other authorities when necessary. • Program training for new hires and team members, and awareness training for general staff, is conducted annually, when a significant change in the program is implemented, and after any major incident. **1.3.2 Breach Notification Policy** The organization has a privacy breach notification policy, supported by: • A process for identifying the notification and related requirements of other applicable jurisdictions relating to the data subjects affected by the breach, • A process for assessing the need for stakeholders breach notification, if required by law, regulation, or policy, and • A process for delivering the notice in a timely manner. When dealing with EU residents' data, the organization's Breach Notification Policy includes: • A breach notification template, which is comprised of the following components:

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
• Periodic testing or walkthrough process (at least on an annual basis) and associated program remediation as needed	a) A description of the nature of the data breach (e.g. categories, approximate number of individuals and personal information records concerned); b) The name and contact details of the privacy contact; c) A description of the likely consequences of the data breach; d) A description of the measures taken or proposed to be taken to address the data breach, including mitigation measures; and e) Facts surrounding the breach, its effects and remedial action taken. • A data breach log for record keeping purposes that documents the facts of the breach, impacts, and remedial action taken. **1.3.3 Post-Incident Evaluation Process** The privacy incident and breach management program includes post-incident remediation and prevention activities, including: • After any privacy incident, a formal incident evaluation is conducted by internal audit or outside consultants. • A quarterly review of actual incidents is conducted and required program updates are identified based on: incident root cause, incident patterns, and changes in the internal control environment and legislation. Results of the quarterly review are reported to the privacy steering committee and annually to the audit committee. • Key metrics are defined, tracked and reported to senior management on a quarterly basis. The program and associated breach management policies, procedures and artifacts are refreshed based on the results of these periodic post-incident activities, as appropriate. **1.3.4 Testing Privacy Breach Management Process** There is a process in place to test the privacy incident and breach management program at least every six months and shortly after the implementation of significant system or procedural changes. The program and associated breach management policies, procedures and artifacts are refreshed based on the testing results, as appropriate, and additional training provided to staff, where required.
1.4 Compliance, Monitoring and Enforcement Compliance with privacy policies and procedures, commitments, service-level agreements, and other contracts will be reviewed and documented, and the results of such reviews reported to management. If problems are identified, remediation plans are developed and implemented.	**1.4.1 Review / Approval of Privacy Policies** There is evidence that privacy policies and procedures are reviewed at least annually and updated as needed. New or revisions to existing privacy policies are approved by senior management or a management committee, as appropriate. Updates are communicated to individuals (e.g. posting the notification on the organization's Web site, by sending written notice via postal mail, or by sending an e-mail). **1.4.2 Compliance Review**

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
	Privacy compliance activities and reviews are defined, planned and executed throughout the year through. The results of such reviews are reported to management, including instances of noncompliance. If problems are identified, remediation plans are developed and implemented, and if needed, corrective and disciplinary actions are taken on a timely basis. Systems and procedures are in place to: • Annually review compliance with privacy policies and procedures, commitments and applicable laws, regulations, service-level agreement, and other contracts. • Document periodic reviews, for example, internal audit plans, audit reports, compliance checklists, and management sign offs. • Perform procedures to monitor the effectiveness of controls over personal information on an ongoing basis (e.g., control reports, trend analysis, training attendance an devaluations, complaint resolutions, regular internal reviews, internal audit reports, independent audit reports covering controls at service organizations, and other evidence of controls effectiveness). The selection of controls to be monitored, and the frequency with which they are monitored are based on the sensitivity of information and the risks of possible exposure of the information. • Report the results of the compliance review and recommendations for improvement to management, and implement a remediation plan. • Monitor the resolution of issues and vulnerabilities noticed in the compliance review to ensure that appropriate corrective action is taken on a timely basis (that is, privacy policies and procedures are revised, as necessary) **1.4.3 Tracking Privacy Risks and Remediation Activities** Any identified privacy risks are logged and remediation plans to mitigate these risks are tracked on an ongoing basis.
1.5 Consistency of Privacy Policies and Procedures With Laws and Regulations Privacy policies and procedures are reviewed, updated and approved when there are changes to applicable laws and regulations.	**1.5.1 Consistency of Privacy Policies with Laws, Regulations and Industry Standards** The Privacy function • Determines which privacy laws and regulations are applicable in the jurisdictions in which the organization operates; • Identifies other standards applicable to the organization; and • Reviews the organization's privacy policies and procedures to ensure they are consistent with the applicable laws and regulations and appropriate standards.
1.6 Privacy Training A privacy education and communication program is in place and supported by a monitoring system that confirms all employees and/or contractors are trained.	**1.6.1 Privacy Training** The organization periodically educates staff on privacy matters and current issues. Specialized privacy training is provided to individuals with privileged access to personal information and/or whose job function involves elevated privacy risks. **1.6.2 Privacy Communications** The organization regularly reinforces the importance of privacy to the organization through a privacy communication program aimed at employees.

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
	Privacy policies and changes to such policies are communicated at least annually to employees responsible for collecting, using, retaining, and disclosing personal information. **1.6.3 Qualifications of Privacy Staff** The organization ensures privacy staff, including the Chief Privacy Officer, have established appropriate qualifications (e.g. training and privacy certifications or designations) for the oversight and management of the privacy program's day-to-day operations. Responsibility for protecting privacy and personal information is only assigned to those individuals who meet qualifications and have received training.
1.7 Third Party Protection of Personal Information Personal information is shared only with third parties who have agreements with the organization to protect personal information or in a manner consistent with the relevant aspects of the organization's privacy policies or other specific instructions or requirements. The organization has procedures in place to evaluate that the third parties have controls to meet the terms of the agreement, instructions, or requirements.	**1.7.1 Third Party Agreements** When providing personal information to third parties, vendors or service providers, the organization enters into contracts that require a level of protection of personal information equivalent to that of the organization's. In doing so, the organization: • Limits the third party's use of personal information to purposes necessary to fulfill the contract; • Communicates the individual's preferences to the third party; • Refers any requests for access or complaints about the personal information transferred by the organization to a designated privacy executive, such as a corporate privacy officer. • Specifies how and when third parties are to dispose of or return any personal information provided by the organization. • Addresses the ramifications of third party misuse of personal information provided by the organization. Further, when dealing with EU resident's data, the organization's agreements include provisions requiring third parties to: • Be subject to a confidentiality obligation; • Provide all information necessary to demonstrate compliance with its contractual obligations and to collaborate with audits conducted by the organization; • Notify data breaches; and • Obtain the organization's consent before transferring personal information received from the organization to subcontractors. In addition to all previous requirements, when the third party is a public cloud data processor, the organization's agreements include provisions requiring the public cloud data processor to: • Provide information on its personal information security practices (e.g. log-on, data restoration and data disposal procedures; use of cryptography; frequency of backups); • Document the countries in which personal information might possibly be stored; • Restrict the creation of hardcopy material displaying the transferred personal information;

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
	• Undertake a risk assessment where use of the transferred personal information for testing purposes cannot be avoided; • Notify legally binding requests for disclosure of personal information by a law enforcement authority; and • Define criteria on when and how provide log information and enable the organization to manage access of the cloud service users under its control. **1.7.2 Evaluation of Third Party Controls** The organization evaluates third party compliance with the privacy and security provisions set out in the organization's contract or agreement using one or more of the following approaches to obtain an increasing level of assurance depending on its risk assessment: • The third party responds to a questionnaire about their practices. • The third party self-certifies that its practices meet the organization's requirements based on internal audit reports or other procedures. • The organization performs an onsite evaluation of the third party. • The organization receives an audit or similar report provided by an independent auditor. **1.7.3 Third Parties Pass on Obligations to Service Providers** Third parties require any services providers, vendors, or third parties contracted by the third party to comply with the organization's privacy legal and contractual obligations to which the third party is subject. Third parties have due diligence procedures in place to ensure their service providers are in compliance with these obligations. **1.7.4 Misuse of Personal Information by a Third Party** The organization takes remedial action in response to misuse of personal information by a third party to whom the organization as transferred such information, including for example: • Reviewing complaints to identify indications of any misuse of personal information by third parties; • Responding to any knowledge of third party using or disclosing personal information in variance with the organization's privacy policies and procedures or contractual arrangements; and • Mitigating, to the extent practicable, any harm caused by the use or disclosure of personal information by the third party in violation of the organization's privacy policies and procedures. **1.7.5 Cross-Border Data Transfer Mechanisms** When dealing with EU residents' data, the organization implements appropriate data transfer mechanisms for processing or storing EU residents' data in jurisdictions deemed inadequate by the European Commission. Appropriate mechanisms include: • Adopting standard model clauses approved by the Commission;

Principle 1 – Proactive not reactive; preventative not remedial (7 criteria; 20 controls) The Privacy by Design (*P by D*) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. *P by D* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.	
Assessment criteria	**Illustrative control activities**
	• Self-certifying to the EU/US Privacy Shield; • Adopting Binding Corporate Rules; or • Relying on informed and explicit consent of the individual. The organization Informs EU residents of appropriate safeguards to protect their personal information when that information is transferred to another country.

Principle 2 – Privacy as the default

Principle 2 – Privacy as the default (3 criteria; 14 controls) We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.	
Assessment criteria	**Illustrative control activities**
2.1 Privacy Settings by Default Privacy controls should default to the protected state rather than having to be activated or selected (i.e. controls are built in and automatically switched on).	**2.1.1 Privacy User Settings** Privacy user settings are available to the user and presented in a clear and understandable fashion. **2.1.2 Configuration Defaulted to the Privacy Protected State** The solution is configured such that the default settings protect user privacy (e.g. for a user facing application, prior to the collection of personal information, a user is provided notice/purpose of collection and prompted to consent to this collection utilizing an unchecked box, therefore requiring the user's express, opt-in consent for the collection of his/her personal information).
2.2 Data Minimization: Collection Limited to Identified Purpose The collection of personal information is limited to that necessary for the primary purpose identified in the notice.	**2.2.1 Systems and Procedures to Limit Collection** System and procedural controls are in place to specify the personal information essential for the purposes identified in the notice and differentiate it from optional personal information. **2.2.2 Periodic Review to Ensure Limited Collection** System and procedural controls are in place to periodically review the organization's program or service needs for personal information (for example, once every five years or when significant changes to the program or service are made). **2.2.3 Explicit Consent for Sensitive PI** System and procedural controls are in place to obtain explicit consent when sensitive personal information is collected. **2.2.4 Monitoring Activities to Limit Collection** System and procedural controls are in place to monitor that the collection of personal information is limited to that necessary for the purposes identified in the privacy notice; and, that all optional data is identified as such and requires positive consent. **2.2.5 Anonymization** System and procedural controls are in place to alter personally identifiable information (PII) in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone in collaboration with any other party. **2.2.6 De-Identification** System and procedural controls are in place when data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data. For example, it could be accomplished by removing account numbers, names, SSNs, and any other identifiable information from a set of financial records. **2.2.7 Privacy Aware Data Analytics**

Principle 2 – Privacy as the default (3 criteria; 14 controls) We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.	
Assessment criteria	**Illustrative control activities**
	When an organization is linking disparate data sources, the organization ensures that the privacy of the individual is not compromised, and the individual cannot be re-identified through a discrete data element(s).
2.3 Use of Personal Information Personal information is used only for the primary purpose(s) identified and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.	**2.3.1 Systems and Procedures to Limit Use** Systems and procedures are in place to ensure that personal information is used in conformity with the purposes identified in the organization's privacy notice. **2.3.2 Use in Agreement with Consent** Systems and procedures are in place to ensure that personal information is used in agreement with the consent received from the individual. **2.3.3 Use in Compliance with Laws and Regulations** Systems and procedures are in place to ensure that personal information is used for the identified business purposes. **2.3.4 New Purposes and Uses** New purposes or uses are made only with the prior explicit consent of the individual. When dealing with EU residents' data, the organization has a process in place to determine whether personal information may be processed for a new purpose by considering: • Any link between the purposes for which the personal information has been collected and the purposes of the intended further processing; • The context in which the personal information has been collected, in particular regarding the relationship between individuals and the organization; • The nature of the personal information; • The possible consequences of the intended further processing for data subjects; and • The existence of appropriate safeguards, which may include encryption or pseudonymisation. **2.3.5 Access to Personal Information Not in Use** The organization's security program prevents access to personal information in computers, media and paper based information that are no longer in active use (for example, computers, media, paper-based information in storage, sold or otherwise disposed of; upon termination of employee; or acquisition, merger or disposal of business).

Principle 3 – Privacy embedded into design

Principle 3 – Privacy embedded into design (3 criteria; 6 controls) Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.	
Assessment criteria	**Illustrative control activities**
3.1 Consideration of Privacy in Design Documentation Privacy is considered during the technical/solution design	**3.1.1 Technical and Solution Design Documents** Technical design documents, architectural documents, or solution design documents show that privacy was a requirement at the design stage. **3.1.2 Personal Information Life-cycle** Privacy of personal information was considered throughout the full life-cycle, from inception through to destruction. **3.1.3 Scalability Requirements** Scalability requirements were considered to ensure privacy is maintained within the foreseeable volume of records held or processed. **3.1.4 Business Continuity and Disaster Recovery** Privacy requirements were determined as part of the business continuity and/or disaster recovery planning and management process, to ensure privacy continuity during adverse situations (e.g. crisis or disaster).
3.2 Privacy in Operational Procedures and Processes Privacy is considered in the design of operational procedures and processes.	**3.2.1 Operational Procedures and Processes** Technical design documents, architectural documents, or solution design documents show that privacy was maintained in the final solution or product, together with any subsequent operational procedures.
3.3 Privacy in Change Management Privacy is considered in Change Management.	**3.3.1 Change Management** There is evidence that privacy considerations are appropriately included as part of the change management system and that resulting recommendations are implemented.

Principle 4 – Full functionality – Positive Sum not Zero Sum

Principle 4 – Full functionality – positive sum, not zero sum (1 criteria; 2 controls) Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.	
Assessment criteria	**Illustrative control activities**
4.1 Positive Sum The organization can articulate and demonstrate the “positive sum” (e.g. no trade-offs; win/win) characteristics of the solution, product or service.	**4.1.1 Multi-Functional Solution** The organization can attest to the “positive sum” characteristics of the solution, product, or service, and in its development, articulated desired functions (e.g. An HRIS system that includes privacy by design increases employee engagement, or a CRM solution that protects customer privacy increases customer loyalty) and identified that the broad spectrum of requirements have been met in favour of achieving multi-functional solutions. **4.1.2 Limit Unnecessary Trade-Offs** The organization can attest to the “positive sum” characteristics of the solution, product, or service, and in its development, attests that all requirements have been satisfied to the greatest extent required by the organization and that unnecessary trade-offs between requirements were not made. For example, privacy was built into the architecture design with no sacrifice to usability, functionality, or security. The organization can demonstrate that there are no trade-offs between user or system functionality and that privacy is not compromised by security i.e. Win-win.

Principle 5 – End-to-end lifecycle protection

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
5.1 Security in Privacy Policies The organization's privacy policies (including any relevant security policies), address the security of personal information.	**5.1.1 Information Security Policy** The organization has defined an information security policy which is approved by management and sets out the organization's approach to managing its information security objectives, principles, and security management roles and responsibilities. The information security policy should be supported by topic-specific security policies, including but not limited to: • Access control. • Acceptable use of information and assets • Mobile devices and teleworking • Security assessments • Information transfer and supplier relationships • Vulnerability management • Network security • Logging and monitoring • Data loss prevention and data leakage These policies are communicated to employees and relevant third parties in a form that is relevant, accessible and understandable to the intended audience. **5.1.2 Documented Security Safeguards** Privacy policies adequately address security measures to safeguard the protection of personal information whether in electronic, paper, or other forms. Security measures are consistent with the sensitivity of the personal information. **5.1.3 Acknowledgement of Privacy and Security Responsibilities** All employees and relevant third parties are required to review the organization's privacy policy and information security policy and related policies and procedures upon hire and confirm their understanding of their roles and responsibilities and agreement to comply with these policies and procedures. The privacy and security policy review and acknowledgement process is refreshed on an annual basis for existing employees. This process can also be aligned with the organization's privacy and security awareness activities, as appropriate
5.2 Safeguarding of Personal Information	**5.2.1 Accountability for Security**

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
Personal information is protected, from start to finish, using administrative, technical and physical safeguards to prevent loss, misuse, unauthorized access, disclosure, alteration, and destruction.	The organization has defined, documented and allocated information security accountability and responsibilities in accordance with its security policies and practices, including: • Overall accountability for the development, implementation and management of the information security program (for example a CISO who may delegate certain responsibilities to a Security Manager) • Responsibilities for the protection of individual assets and carrying out specific information security processes; • Responsibilities for information security risk management activities • Authorization levels • Responsibility for coordination and oversight of supplier relationships in so far as they relate to information security. **5.2.2 Information Security Awareness and Training** All employees and relevant third parties, receive appropriate security awareness, education and training to ensure staff are aware of the organization's security policies and their responsibilities for information security. Updates to security policies and procedures are communicated to staff in a timely manner, as relevant for their job function. **5.2.3 Security Program** A security program has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect personal information from loss, misuse, unauthorized access, disclosure, alteration and destruction. The organization's security program addresses the following matters related to the protection of personal information: • Periodic privacy impact assessments or privacy risk reviews [criteria 1.2]. • Identification of all types of personal information and the related processes, systems, and third parties that are involved in the handling of such information. • Identification and documentation of the security requirements of authorized users. • Allowing access, the nature of that access and who authorizes such access [criteria 5.3]. • Preventing unauthorized access by using effective physical and logical access controls [criteria 5.3]. • The procedures to add new users, modify the access levels of existing users, and remove users who no longer need access [criteria 5.3]. • Assignment of responsibility and accountability for security [criteria 5.2]. • Assignment of responsibility and accountability for system changes and maintenance [criteria 3.3]. • Protecting operating systems and network software and system files. • Protecting cryptographic tools and information.

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
	• Implementing system software upgrades and patches. • Testing, evaluating, and authorizing system components before implementation. • Addressing how complaints and requests relating to security issues are resolved. • Handling errors and omissions, security breaches, and other incidents [criteria 1.3]. • Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing). • Allocating training and other resources to support its security policies. • Provision for the handling of exceptions and situations not specifically addressed in its system processing integrity and related system security policies. • Business continuity management and disaster recovery plans and related testing [criteria 3.1]. • Provision for the identification of, and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contracts [criteria 1.4]. • A requirement that users, management, and third parties confirm (initially and annually) their understanding of an agreement to comply with the organization's privacy policies and procedures related to the security of personal information. • Procedures to cancel access privileges and ensure return of computers and other devices used to access or store personal information when personnel are terminated. **5.2.4 Personal Information Identification and Classification** The organization has both an information classification policy and process, which include the following: • A classification process which identifies and classifies information into one or more of the following categories: business confidential, personal information, business general, and public. • Identifying processes, systems and third parties that handle personal information. Specific security and privacy policies and procedures that apply to each category of information.
5.3 Logical Access to Personal Information Logical access to personal information is restricted by procedures that address the following matters: a. Authorizing and registering internal personnel and individuals	**5.3.1 "Need to Know" and "Least Privileged"** Systems and procedures are in place to establish the level and nature of access that will be provided to users based on the sensitivity of the data and the user's legitimate business need to access the personal information. **5.3.2 User Authentication**

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
b. Identifying and authenticating internal personnel and individuals c. Making changes and updating access profiles d. Granting privileges and permissions for access to IT infrastructure components and personal information e. Preventing individuals from accessing anything other than their own personal or sensitive information f. Limiting access to personal information to only authorized internal personnel based upon their assigned roles and responsibilities g. Distributing output only to authorized internal personnel h. Restricting logical access to offline storage, backup data, systems, and media i. Restricting access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls) j. Preventing the introduction of viruses, malicious code, and unauthorized software	Systems and procedures are in place to authenticate users, for example, by user name and password, two-factor authentication, certificate, external token, or biometrics before access is granted to systems handling personal information. Capabilities to assign different access privileges to different persons depending on their roles and responsibilities in the organization. **5.3.3 User Authorization Process** User authorization processes consider the following: • How the data is accessed (internal or external network), as well as the media and technology platform of storage • Access to paper and backup media containing personal information • Denial of access to joint accounts without other methods to authenticate the actual individuals Note: Some jurisdictions require stored data (at rest) to be encrypted or otherwise obfuscated. **5.3.4 Role-Based Access Control** Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. **5.3.5 Segregation of Duties** Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organizations information and assets. **5.3.6 Remote Access to Personal Information** Systems and procedures are in place to require enhanced security measures for remote access, such as additional or dynamic passwords, callback procedures, digital certificates, secure ID cards, virtual private network (VPN), or properly configured firewalls. **5.3.7 User Access Logs** User access to personal information (e.g. viewing, modification, deletion of records) both from a front-end (e.g. business user) perspective and a back-end (e.g. system or database administrator) perspective is logged and monitored on a regular basis, and unauthorized access or suspicious user activity is flagged accordingly. **5.2.8 System Logging and Monitoring** Event logs recording user activities, exceptions, faults, and privacy and information security events are produced, maintained, monitored and reviewed on an ongoing basis. **5.2.9 Protection of Log Information**

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
	Logs are protected against tampering and unauthorized access, and appropriate privacy safeguards are in place to protect sensitive information contained within logs.
5.4 Physical Access Controls Physical access is restricted to personal information in any form (including the components of the organization's system(s) that contain or protect personal information).	**5.4.1 Physical Security** Physical safeguards (e.g. locked file cabinets, card access systems, physical keys, and sign in logs) are in place to control access to offices, data centres, and other locations in which personal information is processed or stored. **5.4.2 Physical Access to Personal Information** Systems and procedures are in place to manage, log and monitor logical and physical access to personal information, including hard copy, archival, and backup copies, and to prevent the unauthorized or accidental destruction or loss of personal information. There is a process in place to investigate breaches and attempts to gain unauthorized access to physical records, assets and information storage/processing locations; and to communicate investigation results to the appropriate designated privacy executive. **5.4.3 Reports Containing Personal Information** Systems and procedures are in place to maintain physical control over the distribution of reports containing personal information.
5.5 Environmental Safeguards Personal information, in all forms, is protected against accidental disclosure due to natural disasters and environmental hazards.	**5.5.1 Protection Against Environmental Factors** Management maintains measures to protect against environmental factors (for example, fire, flood, dust, power failure, and excessive heat and humidity) based on its risk assessment. The organization's controlled areas are protected against fire using both smoke detectors and a fire suppression system. In addition, the organization maintains physical and other safeguards to prevent accidental disclosure of persona information in the event of an environmental incident.
5.6 Transmitted Personal Information Personal information collected and transmitted over the Internet, over public and other non-secure networks, in the cloud and over wireless networks is protected.	**5.6.1 Encryption for Personal Information Transmitted Electronically** Systems and procedures are in place to define minimum levels of encryption and control and to employ industry standard encryption technology over secure links (e.g. VIPNs) for transferring and receiving personal information. Personal information is encrypted when transmitted via mobile or removable media devices or across communication lines. **5.6.2 External Network Connections** Systems and procedures are in place to approve external network connections. **5.6.3 Wireless Transmissions** Systems and procedures are in place to encrypt personal information collected and transmitted wirelessly to protect wireless networks from unauthorized access.

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
	5.6.4 Personal Information Transmitted by Physical Means Systems and procedures are in place to protect personal information in both hardcopy and electronic forms sent by mail, courier, or other physical means.
5.7 Retention and Storage of Personal Information Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise, and is stored securely.	**5.7.1 Retention Procedures** The organization documents its retention policies and disposal procedures. **5.7.2 Limit Retention** The organization ensures that personal information is retained only as long as necessary for the intended business purpose for which the information was collected and in accordance to legal retention periods. **5.7.3 Contractual Retention Requirements** Contractual requirements are considered when establishing retention practices when they may be exceptions to normal policies. **5.7.4 Mobile Device Safeguards** The organization personal information stored on mobile devices or on servers is protected from unauthorized access. **5.7.5 Encryption of Personal Information "At Rest"** Personal information is encrypted while "at rest" or in storage, as appropriate (e.g. at the server, database or data element level), including backups containing personal information, in order to protect personal information from unauthorized access, tampering, modification, misuse and/or unauthorized disclosure.
5.8 Disposal, Destruction and Redaction of Personal Information Personal information no longer needed is de-identified, anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	**5.8.1 Destruction in Accordance with Retention Schedules** The organization erases or destroys records in accordance with the retention policies, regardless of the method of storage (for example, electronic, optical media, or paper based). **5.8.2 Destruction in Accordance with Destruction Procedures** The organization disposes of original, archived, backup and ad hoc or personal copies of records in accordance with its destruction policies and using appropriate secure destruction methods for the sensitivity of the data and the media on which it resides. **5.8.3 Certificate of Destruction** The organization documents the disposal of personal information (e.g. certificate of destruction). **5.8.4 Destruction, Removal and Redaction of Personal Information** The organization within the limits of technology, locates and removes or redacts specified personal information about an individual as required, for example, removing credit card numbers after the transaction is complete.

Principle 5 – End-to-end security; full lifecycle protection (9 criteria; 38 controls) Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.	
Assessment criteria	**Illustrative control activities**
	5.8.5 Destruction, Erasing, or Anonymizing of Personal Information Not Required The organization regularly and systematically destroys, erases, or makes anonymous personal information no longer required to fulfill the identified purposes or as required by laws and regulations.
5.9 Testing Security Safeguards Tests of the effectiveness of the key administrative, technical, and physical safeguards protecting personal information are conducted periodically.	**5.9.1 Periodic Testing** Systems and procedures are in place to regularly test the effectiveness of the key administrative, technical, and physical safeguards protecting personal information. **5.9.2 Threat and Vulnerability Testing** Systems and procedures are in place to periodically undertake threat and vulnerability testing, including security penetration and Web vulnerability and resilience. **5.9.3 Periodic Updates to Security Policies and Procedures Based on Evolving Threats and Vulnerabilities** Systems and procedures are in place to make appropriate modifications to security policies and procedures on a periodic basis, taking into consideration the results of tests performed and new and changing threats and vulnerabilities. **5.9.4 Reporting Testing Results** Systems and procedures are in place to periodically report the results of security testing to management.

Principle 6 – Visibility and Transparency

Principle 6 – Visibility and transparency: keep it open (2 criteria; 4 controls) Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.	
Assessment criteria	**Control activities**
6.1 Policies and Commitment Privacy policies are documented in writing, are current and up-to-date, which demonstrate commitments to protect privacy, in user-friendly terms.	**6.1.1 Privacy Policy** The organization defines and documents its information handling practices with respect to the following: • Notice; • Choice and consent; • Collection; • Use, retention, and disposal; • Access; • Disclosure to third parties; • Security for privacy; • Quality; and • Monitoring and enforcement. When dealing with EU residents' data, the organization's privacy policies meet the following criteria: • Are "right sized" to the organization based on size, complexity and scope of operations; • Are drafted in a user-friendly, concise and easy to understand language; • Inform EU residents of the existence of automated profiling (e.g. analysis of performance at work) and provide the option to opt-out of being subjected to a decision based on this profiling; • Inform EU residents of the use of a foreign service provider, the jurisdictions to which personal data might be transferred, and the purposes for which the foreign service provider has been authorized to collect, use or disclose personal information for or on behalf of the organization.
6.2 Openness Information about an organization's privacy policies and procedures, including the name of the Privacy Officer and their responsibilities, are user-friendly, communicated and made readily available to the public, internal personnel and third parties who need them.	**6.2.1 Privacy Inquiries and Complaints Handling** The organization is open about its policies and practices with respect to the management of personal information, how to make privacy inquiries or complaints. **6.2.2 Transparency of Privacy Policies and Practices** There is a mechanism for individuals to acquire information about privacy policies and practices without unreasonable effort. This information is made available in a form that is generally understandable and by a mechanism suitable for the service being provided (e.g. web, brochures, phone etc.) When dealing with EU residents' data, the organization: • Has developed a procedure to verify the identity of individuals that request information about the organization's privacy practices orally; and

Principle 6 – Visibility and transparency: keep it open (2 criteria; 4 controls) Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.	
Assessment criteria	**Control activities**
	• Has developed, documented and implemented a process to maintain a written record of processing activities, which must include: a) Name and contact details of the organization; b) Purposes of the processing; c) Categories of individuals, personal information and recipients; d) Third countries to which personal information is transferred to and the suitable security safeguards (if applicable); and e) Limits for erasure of personal information and organizational security measures (if possible). **6.2.3 Designated Privacy Contact Person and Information** The information made available should include (a) the name/title and address of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded (as well as details of the complaint or dispute process); (b) the means of gaining access to personal information held by the organization; (c) a description of the type of personal information held by the organization, including a general account of its use; (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and (e) what personal information is made available to related organizations (e.g. subsidiaries).

Principle 7 – Respect for user privacy

Principle 7 – Respect for user privacy – keep it user-centric (5 criteria; 11 controls) Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.	
Assessment criteria	**Control activities**
7.1 Purpose of Collection - Notice The primary purpose of collecting personal information is identified and documented (e.g. notice) prior to collection of any personal information, which is clear, easy to read and find.	**7.1.1 Privacy Notice** The organization has a privacy notice that describes the personal information collected, the sources of such information, and purposes for which it is collected, use and disclosed. The organization privacy notice also indicates the purpose for collecting sensitive personal information (if collected) and whether such purpose is part of a legal requirement. When dealing with EU residents' data, the organization posts at the time of the collection a written privacy notice (e.g. via a website), that also informs of: • The recipients of the personal information; • The intention of the organization to transfer the information to a third country and the correspondent data transfer mechanism (when applicable); • The storage period of the personal information; • Whether the provision of personal information is a statutory or contractual requirement; • The existence of automated decision-making and the consequences of such processing; and • The categories of personal data concerned (when personal information is not obtained from the individual).
7.2 Consent and Notice Individuals are informed about (a) the choices available to them with respect to the collection, use, and disclosure of personal information, and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law specifically requires or allows otherwise.	**7.2.1 Clear and Concise Notice for Privacy Choices Available to Individuals** The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, the choices available to the individual regarding the collection, use, and disclosure of personal information. The organization provides the individual with a summary of the applicable consent applied to them (i.e. consent receipt) after their information has been collected. **7.2.2 Updating an Individual's Contact Preferences** The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, the ability of, and process for, an individual to change contact preferences. **7.2.3 Notice of the Consequences for Failing to Provide Personal Information** The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, the consequences of failing to provide personal information required for a transaction or service. **7.2.4 Changing of Individual Preferences and Withdrawal of Consent**

Principle 7 – Respect for user privacy – keep it user-centric (5 criteria; 11 controls) Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.	
Assessment criteria	**Control activities**
	The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, that preferences may be changed, and consent may be withdrawn at a later time, subject to legal or contractual restrictions and reasonable notice. **7.2.5 Type of Consent Required** The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, the type of consent required depends on the nature of the personal information and the method of collection (for example, an individual subscribing to a newsletter gives implied consent to receive communications from the organization). **7.2.6 Explicit Consent for Sensitive Information** The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, that explicit consent is used for sensitive information. **7.2.7 Consent for New Purposes** The organization's privacy notices or privacy preferences/user settings describe, in a clear and concise manner, that consent is re-obtained for any new purposes or uses.
7.3 Access to and Correction by Individuals of Their Personal Information Individuals are informed about how they may obtain access to their personal information to review, update, and correct that information.	**7.3.1 Individual Access to and/or Correction of His / Her Personal Information** The organization's privacy notice describes the organizations process for handling individual access and/or correction requests. Specifically, the privacy notice: • Explains how individuals may gain access to their personal information and any costs associated with obtaining such access; • Outlines the means by which individuals may update and correct their personal information (for example, in writing, by phone, by e-mail, or by using the organization's Web site); and • Explains how disagreements related to personal information may be resolved. The organization provides EU residents (when the organization deals with their data) with the requested personal information in a structured, commonly used and machine readable format and, if requested, transmits that personal information to another controller.
7.4 Right to deletion ("right to be forgotten") and right to object	**7.4.1 Individual Deletion and/or Objection to the Processing of His / Her Personal Information**

Principle 7 – Respect for user privacy – keep it user-centric (5 criteria; 11 controls) Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.	
Assessment criteria	**Control activities**
Individuals are informed about how they may request the organization to delete their information or to stop processing it.	When dealing with EU residents' data, the organization has developed and implements a process and/or an automated system to delete personal information when: • The individual requests it; • The information has been unlawfully processed or is no longer necessary for the purposes it was collected; or • A legal obligation requires it. When dealing with EU residents' data, the organization has developed and implements a process and/or an automated system to: • Stop processing personal information in the following cases: a) When the individual requests it (e.g. withdraws consent or objects to the processing of his/he personal information); b) If verification of overriding grounds is pending, in the context of an erasure request; c) During dispute procedures; d) When the individual contests the accuracy of his/her personal information; or e) When the organization no longer needs the data for their original purpose, but the data are still required by the organization to establish, exercise or defend legal rights. • Communicate the deletion and/or objection to the processing of an individual's personal information to third parties.
7.5 Accuracy Personal information is accurate and complete for its intended purposes.	**7.5.1 Accuracy of Personal Information** The organization's solution, product, or service incorporates controls to ensure that personal information is kept sufficiently accurate and updated for the stated purposes and risks to the information owner are minimized.