ISO 27701:2019

Privacy Information Management Systems

kiwa | Compass Assurance Services

Self Assessment Checklist

Context

The Organisation

□ Have we determined and documented our role as PII Controller and/or Processor?

Interested Parties

□ Have we determined internal and external issues that will impact on our Privacy Information Management System? including applicable legislation, judicial decisions, organisational context, contractual requirements etc.)

Scope

□ Have we included the processing of PII in our ISMS scope?

Planning

Risk and Opportunity

□ Have we applied our information security risk assessment process to identify risks associated with confidentiality, integrity, and availability of PII and other information?

□ Have we ensured the relationship between information security and PII protection is appropriately managed?

□ Have we considered when assessing the applicability of control objectives from Annex A, in the context of both risks to information security as well as risks related to processing of PII?

Information Security Policies

□ Have we considered our commitment to achieving compliance to applicable PII regulations in our Privacy Policies and our contractual agreements?

□ Have we produced a statement (either in existing policies or as a standalone policy) concerning support or and commitment to achieving compliance with applicable PII protection legislation /regulations and with any contractual obligations?

Organisation of Information Security

Internal Organisation

□ Have we designated a point of contact for the customer with regards to their PII?

□ Have we developed and implemented an organisation-wide governance and privacy program for staff to understand and comply with applicable privacy regulations?

□ Have we appointed at least one person to be responsible for the maintenance of the governance and privacy program and are they are aware of their responsibilities?

Human Resource Security

□ Have we made relevant staff aware of incident reporting and the consequences to themselves, the organisation and the PII principal in the case of a breach of privacy or security?

Asset Management

□ Has our information classification system explicitly considered PII, where it is stored and the systems through which it can flow?

□ Are we documenting any use of removable media and/or devices used for the storage of PII?

□ Are we disposing of PII on removable media such that it will no longer be accessible?

Access Control

□ Do we have documented procedures for registration and de-registration of users who administer or operate systems that process PII?

Cryptographic Controls

□ Do we communicate to our customers the circumstances in which cryptography is used to protect PII?

Physical and Environmental Security

□ Are we ensuring that when storage space is re-assigned, any previously stored PII is no longer accessible?

□ Are we restricting the production of hard copy material including PII to the minimum?

Operations Security

Backup

□ Do we have a documented policy that includes the requirements for backup, recovery and restoration of PII that is communicated and available to all relevant staff?

□ Do we have processes in place to identify incompleteness/inaccuracy and to resolve this?

□ Do we have responsibilities in relation to communicating with customers about PII back up and restoration?

□ Is there a procedure for and log of PII restoration efforts?

□ Do we have external obligations with respect to back up and are we compliant?

□ Are we able to document and demonstrate all of our compliance with external obligations in relation to restoring log content?

□ Do we have processes in place to ensure PII is restored to a state where integrity can be assured?

□ Do we have a process to review event logs either using continuous automated monitoring and alerting processes or manually?

For PII Processors Only

□ Do we have a documented set of criteria that defines if, when and how log information can be made available to the customer?

□ Have we put controls in place to ensure customers can only access their own logs and not that of others?

Protection of Log Information

□ Have we put in place a procedure (preferably automatic) to ensure logged information is either deleted or de-identified?

□ Have we put controls in place to ensure log information is used only as intended?

Communications Security

Information Transfer

□ Have we put procedures in place to ensure that rules regarding PII are enforced throughout the organisation?

Confidentiality or Non-Disclosure Agreements

□ Do we ensure everyone with access to PII signs and agrees to a non-disclosure agreement or similar?

Systems Acquisition, Development and Maintanence

Securing Application Services on Public Networks

□ Do we ensure that PII is only transmitted over trusted networks, or where it must be transmitted over untrusted networks it is encrypted?

Security in Development and Support Processes

□ Do our system development and design policies consider PII needs based on local regulations?

□ Do our policies contribute to privacy by design and privacy by default and consider the following aspects:

□ Guidance on PII protection through the software development cycle

□ Privacy and PII protection requirements in the design phase, which can be based on the risk assessment

□ PII protection checkpoints and miles stones

□ Required privacy knowledge

□ Minimise PII processing by default

Secure Systems Engineering Principles

□ Are our systems and components involved in the processing of PII designed in alignment with local privacy regulations?

Test Data

□ How do we ensure that PII is not used for testing purposes?

Supplier Relationships

Addressing Security Within Supplier Agreements

□ Do we specify in supplier agreements whether PII is processed, and the minimum protection measures the supplier needs to meet?

Information Security Incident Management

Responsibilities and Procedures

□ Have we established responsibilities and procedures for identification and recording of PII breaches that take into consideration local privacy regulation, as part of our overall information security incident management procedures?

For PII Processors

□ Do provisions covering the notification of a breach form part of the contract with our customer?

□ Does the contract specify how this information should be provided?

□ Are there obligations to notify the PII controller of a breach?

□ Do we have processes for recording the following details of a breach?

- □ Description
- □ Time period
- □ Consequence
- □ Who reported it
- □ To whom was it reported
- □ How was it resolved
- □ Description of the loss/unavailability of PII

□ Does the record include a description of the PII compromised?

□ Do we have a process to record all notifications to the customer and/or regulatory agencies?

Compliance

Identification of Applicable Legislation and Contractual Requirements

□ Do we have a documented policy that includes the requirements for backup, recovery and restoration of PII that is communicated and available to all relevant staff?

Independent Review of Information Security

□ Do we have an independent third party contracted to conduct audits on our information security to ensure it is implemented and operated in accordance with our policies and procedures?

Protection of Records

□ Do we retain historical copies of our privacy policies and associated procedures for the time specified by our local privacy regulations?

Technical Compliance Review

□ Have we implemented methods of reviewing tools and components related to processing PII?

Annex A

Additional Guidance for PII Controllers

7.2 Conditions for collecting and processing	Documented legality & purposes for data collection Documented processes for obtaining consent from the PII Roles and responsibilities of any joint PII controller(s)
7.3 Obligations to PII Principals	Documented legal, regulatory, and business obligations to PII principals Method by which the PII Principal can access, correct and/or erase data and modify or withdraw consent or object to processing, and have changes communicated to any third parties Ability to provide a copy of processed data to the PII Principal on request Documented policies and procedures on handling legitimate PII Principal requests
7.4 Privacy by design and privacy by default	Limit data collection and processing to only what information is relevant and necessary Documented data minimisation objectives and mechanisms to meet objectives Delete or de-identify PII upon completion of processing and Only retain PII for as long as necessary Documented policies and procedures for secure disposal of PII
7.5 PII sharing, transfer and disclosure	Documented justification for the transfer of PII between jurisdictions as well as which countries and international organisations PII may be allowed to be transferred. Record transfers of PII between third parties

Annex B

Additional Guidance for PII Controllers

8.2 Conditions for collecting and processing	The contract to process PII addresses our role in providing assistance with the customer's obligations Ensure PII are only processed for the purposes expressed by the customer and inform the customer if a processing instruction infringes any applicable legislation and/or regulation Document and maintain records in support of demonstrating compliance with the obligations as specified in the contract
8.3 Obligations to PII Principals	Provide the customer with the means to comply with obligations related to PII principals Provide PII Principals with the appropriate information relating to processing of their PII
8.4 Privacy by design and privacy by default	Temporary files created as a result of the processing of PII are disposed of securely Documented policy on secure return, transfer, and disposal of PII available to the customer Controls in place for the transmission of PII to ensure the information reaches the intended destination
8.5 PII sharing, transfer and disclosure	Obligation to inform the customer of the justification for any intended transfers between jurisdictions, giving the customer the option to object Maintain records of what PII has been disclosed to third parties as well as to whom and when Obligation to notify the customer of any legally binding requests for PII to be disclosed Reject non-legally binding requests for disclosure of PII or consult the customer before disclosing PII Disclose any use of subcontractors to the customer and engage with subcontractors in accordance with the agreement with the customer, and inform the customer of intended changes regarding the use of subcontractors giving the customer the option to object

So What Now?

Contact us for a quick quote to get a better idea of costs and timings. Visit our website:

www.cas.com.au