TÜVNORD

Inspired by Knowledge

ISO/IEC 27701 Privacy Information Management System

Self assessment questionnaire

The purpose of this document is to help your company assess its readiness for ISO/IEC 27701 certification. By using this self-assessment checklist, you can evaluate your current data privacy management practices, identify areas for improvement, and ensure you meet the required standards for certification. This tool aims to simplify the preparation process, giving you a clear path to achieving ISO/IEC 27701 compliance and bolstering your organization's data protection capabilities.

Please fill in the questions below. Place a **check mark (✓)** in the box if the requirement has been applied, and **leave it blank** if it has not.

Contact : Text
Company : Text
Address : Text
Country : Text
Telp (Incl. Ext) : Text
Job Title : Text
No. of employee Text
Town : Text
Postcode : Text
Email :

General

Is your organization ISO/IEC 27001 (ISMS) certified?	□
Has your organization extended its ISO/IEC 27001 (ISMS) certification to include ISO/IEC 27701 (PIMS)?	□
Is the scope of the PIMS defined to be identical to, or within, the scope of the ISO/IEC 27001 (ISMS)?	□
Has your organization established a privacy risk assessment process to identify risks associated with the processing of Personally Identifiable Information (PII)?	□
Does the risk assessment process identify and evaluate threats and vulnerabilities related to PII?	□
Are responsibilities for the protection of PII integrated into your organization's information security policies and procedures?	□
Does your organization have specific risk treatment strategies in place to protect PII?	□
Do these risk treatment strategies integrate the protection of PII with overall information security measures?	□
Are the security controls implemented by your organization specifically designed to protect PII?	□
Does your organization ensure that these security controls are effective and appropriate for the identified risks?	□
Have your organization's information policies been extended to mention the protection of privacy potentially affected by the processing of PII?	□
Does your organization have established privacy policies?	□
Does your organization have a Data Protection Officer (DPO) responsible for developing, implementing, maintaining, and monitoring an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the processing of PII?	□
Does your organization's mobile device policy include appropriate controls to ensure that the use of mobile devices does not compromise the protection of PII?	□
Are information security awareness, education, and training programs conducted periodically for personnel who have access to PII and PII principles?	□
Does your organization's information classification scheme explicitly consider PII as part of the scheme it implements?	□

Has your organization implemented labeling mechanisms to ensure that individuals under its control are aware of the definition of PII and can recognize information that constitutes PII?	□
Has your organization implemented encryption for the use of removable physical media and/or devices that store PII?	□
Does your organization have procedures for the secure disposal of removable media on which PII is stored?	□
Does your organization have procedures in place to ensure that PII is not accessible to unauthorized personnel?	□
Does your organization have procedures for the registration and de-registration of users who administer or operate systems and services that process PII?	□
Does your organization maintain an accurate and up-to-date record of user profiles for those authorized to access the information system and the PII contained therein?	□
Does your organization have procedures for secure log-on for any user accounts under customer control?	□
Does your organization have policies on the use of cryptographic controls to protect specific types of personal data or PII?	□
Does your organization have procedures for the secure disposal or reuse of equipment containing PII?	□
Has your organization established procedures to limit the creation of hardcopy materials containing PII to the minimum necessary to fulfill the identified processing purpose?	□
Does your organization have processes and procedures to continuously review event logs to identify irregularities and propose remediation efforts?	□
Does your organization have security monitoring and operational diagnostics procedures for log information containing PII to ensure that logged information is used as intended?	□
Does your organization have policies and procedures to enforce the processing of PII both within and outside of the system?	□
Does your organization have confidentiality agreements or obligations to ensure that individuals operating under its control with access to PII maintain confidentiality?	□

Does your organization ensure that PII transmitted over untrusted data transmission networks is encrypted?	□
Does your organization have policies for privacy in systems design that provide control considerations for the processing of PII?	□
Does your organization ensure that the processing of PII adheres to principles of privacy by design and privacy by default, particularly to ensure that the collection and processing of PII are conducted following these principles?	□
Are the principles of privacy by design and privacy by default applied to outsourced information systems, if any?	□
Does your organization use PII for testing purposes?	□
Does your organization have agreements with suppliers regarding the processing of PII and the minimum technical and organizational measures that the suppliers must meet to ensure that the organization meets its information security and PII protection obligations?	□
Has your organization established responsibilities and procedures for the identification and recording of breaches of PII?	□
Does the organization have procedures for responding to information security incidents involving PII?	□
Does the organization identify any potential legal sanctions related to the processing of PII?	□
Are the current and historical policies and procedures reviewed periodically?	□
Has the information security related to PII processing been audited by an independent auditor?	□

Controller

Has the organization identified and documented the specific purposes for which PII is processed?	□
Has your organization determined, documented, and complied with the relevant lawful bases for the processing of PII?	□
Has the organization determined when and how consent for the processing of PII was obtained from PII principals?	□
Has the organization obtained and documented consent from PII principals according to established processes?	□
Has the organization conducted a privacy impact assessment for the processing of PII?	□
Does the organization have a written contract with any PII processor that it uses?	□
Has the organization determined the respective roles and responsibilities for the processing of PII with any joint PII controller?	□
Has the organization determined and maintained records necessary to support its obligations for the processing of PII?	□
Is the organization fulfilling obligations related to the processing of PII principals' data?	□
Has the organization determined and documented the information to be provided to PII principals regarding the processing of their PII?	□
Does the organization provide mechanisms for PII principals to object to the processing of their PII?	□
Does the organization have policies, procedures, and/or mechanisms to meet the obligations to PII principals to access, correct, and/or erase their PII?	□
Does the organization inform third parties with whom PII has been shared about any modifications, withdrawals, or objections pertaining to the shared PII, and implement appropriate policies, procedures, and/or mechanisms to do so?	□
Does the organization have the ability to provide a copy of the PII that is processed when requested by the PII principals?	□

Does the organization have policies and procedures for handling and responding to legitimate requests from PII principals?	□
Has the organization identified and addressed obligations to PII principals resulting from decisions made by the organization based solely on automated processing of PII?	□
Does the organization have policies, procedures, and/or mechanisms to limit the collection and processing of PII?	□
Does the organization have procedures and controls to ensure and document that PII is accurate, complete, and up to date?	□
Has the organization defined and documented data minimization objectives?	□
Does the organization have procedures and mechanisms for the de-identification and deletion of PII at the end of processing?	□
Does the organization have policies, procedures, and/or mechanisms to ensure that temporary files created as a result of the processing of PII are disposed of appropriately?	□
Does the organization have policies, procedures, and/or mechanisms for the retention and disposal of PII?	□
Does the organization have appropriate controls in place for the transmission of PII over data-transmission networks?	□
Has the organization identified and documented the relevant basis for the transfer of PII between jurisdictions (if applicable)?	□
Has the organization specified and documented the countries and international organizations to which PII can possibly be transferred?	□
Are the transfers of PII to or from third parties recorded with respect to obligations to PII principals?	□
Does the organization have procedures to record disclosures of PII to third parties, including details on what PII has been disclosed, to whom, and when?	□

Processor

Does the organization have contracts with controllers to process PII that address the organization’s role in providing assistance with customers’ obligations?	□
Does the organization have documentation to ensure that PII processed on behalf of a customer is only processed for the purposes specified in the documented instructions of the customer?	□
Does the organization refrain from using PII processed under a contract for the purposes of marketing and advertising without establishing that prior consent was obtained from the appropriate PII principals?	□
Does the organization have procedures or mechanisms to inform the customer if a processing instruction infringes applicable legislation and/or regulation?	□
Does the organization provide the customer with the appropriate information so that the customer can demonstrate compliance with their obligations?	□
Does the organization have procedures and/or mechanisms to determine and maintain the necessary records to demonstrate compliance with its obligations for the processing of PII?	□
Does the organization determine and document the information to be provided to PII principals regarding the processing of their PII?	□
Does the organization have policies, procedures, or mechanisms to ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission/transfer, and disposal) are limited to what is necessary for the identified purposes?	□
Does the organization have appropriate controls designed to ensure that data reaches its intended destination if subject PII is transmitted over a data-transmission network?	□
Does the organization inform the customer in a timely manner of the basis for PII transfers between jurisdictions?	□
Has the organization specified and documented the countries and international organizations to which PII can possibly be transferred?	□

Does the organization record disclosures of PII to third parties, including details on what PII has been disclosed, to whom, and when?	□
Does the organization have procedures and mechanisms to notify the customer of any legally binding requests for the disclosure of PII?	□
Does the organization have mechanisms to reject non-legally binding requests for PII disclosures, consult the corresponding customer before making any PII disclosures, and accept any contractually agreed requests for PII disclosures?	□
Has the organization disclosed the use of any subcontractors for the processing of PII to the customer before use?	□
Does the organization have mechanisms and procedures to ensure that a subcontractor processes PII according to the customer contract?	□
Does the organization have mechanisms to inform the customer of any intended changes concerning the addition or replacement of a subcontractor for the processing of PII?	□

Thank you for completing this readiness certification checklist. If there are still some questions in the questionnaire that are **without check mark**, we highly recommend that you fulfill these requirements first to enhance your organization's readiness for implementing the management system.

This checklist helps to describe your organization's level of readiness for the conformity assessment process in certification. Ensuring that all requirements are fully met will position your organization well for achieving the desired certification.

Information provided will not be disclosed and will be destroyed immediately after use.

Contact

Further information and contact form

TÜV NORD Indonesia
Arkadia Green Park, Tower F 6th Floor, Suite 602-604
Jl. TB. Simatupang Kav.88, Kebagusan, Pasar Minggu,
Jakarta Selatan 12520

T +62 21 78837338
tuv-nord.com/id/
indonesia@tuv-nord.com