Welocalize Information Security Policy

Introduction

The purpose of this document is to demonstrate the management board's commitment to information security and privacy and to provide the over-arching policy statements to which all subordinate policies and control must adhere.

Policy

The Board of Directors and management of Welocalize operates primarily in the business of language services.

We are committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information and information-related assets to meet the purpose and goals of the organization as summarized in our Information Security Context, Requirements and Scope.

We are also committed to achieving compliance with applicable legislation, regulation and contractual requirements in relation to Personal Identifiable Information (PII) protection.

Additionally, we recognize the importance of data privacy and are dedicated to upholding the principles of data protection and privacy rights in our practices and policies.

Information security and privacy requirements will continue to be aligned with the organization's business goals and will take into account the internal and external issues affecting the organization and the requirements of interested parties.

For the processing of personal information, we are acting both as a PII Controller and as a PII Processor. We are acting as PII Processor to our customers for the scope of the services we provide. Our role as PII Controller is related to our role as an employer and the provision of agreed services, for which we are collecting and processing general contact information from our customers and suppliers. We also act as PII Controller for the PII principals that may request information via our Website.

Our Privacy Information Management System (referred to as PIMS henceforth) objectives are outlined and measured in accordance with the requirements of the ISO/IEC standard 27701:2019. The Data Privacy Policy specifically addresses the handling, processing, and protection of personal data in accordance with data protection regulations.

The PIMS is intended as a mechanism for managing information security and privacy related risks and improving the organization to help deliver its overall purpose and goals.

Our system, including our approach to risk management, provides the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of a PIMS.

The approach taken towards Risk Assessment and management, our Statement of Applicability and the wider requirements set out for meeting ISO 27701:2019, identify how information security and privacy as well as related risks are addressed.

The PIMS Board is responsible for the overall management and maintenance of the risk treatment plan with specific risk management activity tasked to the appropriate owner within the organization. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks, for example during special projects that are completed within the context.

Control objectives for each of these areas are supported by specific documented policies and procedures in the online environment and they align with the comprehensive controls listed in Annex A of the ISO 27001:2013 and Annexes A and B or the ISO 27701:2019 standard.

All employees and relevant Interested Parties associated with the PIMS have to comply with this policy. Appropriate training and materials to support it are available for those in the scope of the PIMS, and communication forums such as the PIMS communications group are available to ensure engagement on an ongoing basis.

The Data Privacy Policy is applicable to all individuals processing personal data on behalf of the organization, outlining their responsibilities and the consequences of not adhering to data protection principles. Training specific to data privacy is provided to individuals within the scope of the Data Privacy Policy.

The PIMS is subject to review and improvement by the PIMS Board, which is chaired by the VP of Global IT and has ongoing senior representation from appropriate parts of the organization. Other executives/specialists needed to support the PIMS framework and to periodically review the security policy and broader PIMS are invited to Board meetings and complete relevant work as required, all of which is documented in accordance with the standard.

We are committed to achieving and maintaining certification of the PIMS to ISO 27701:2019 along with other relevant accreditations against which our organization has sought certification.

The Data Privacy Policy aligns with the organization's commitment to achieving and maintaining certification of the PIMS to ISO 27701:2019, specifically focusing on data privacy aspects.

This policy will be reviewed regularly to respond to any changes in the business, its risk assessment or risk treatment plan, and at least annually.

Legal and Regulatory Compliance

Definitions

In this policy and the related set of policies contained within the environment that incorporate our PIMS, ‘information security and privacy’ is defined as:

preserving

This means that all relevant Interested Parties have, and will be made aware of, their responsibilities that are defined in their job descriptions or contracts to act in accordance with the requirements of the PIMS. The consequences of not doing so are described in the Code of Conduct. All relevant Interested Parties will receive information security and privacy awareness training and more specialized resources will receive appropriately specialized information security and privacy training.

the availability

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The environment must be resilient, and the organization must be able to detect and respond rapidly to incidents or events that threaten the continued availability of assets, systems, and information.

confidentiality

This involves ensuring that information is only accessible to those authorized to access it and preventing both deliberate and accidental unauthorized access to the organization’s and relevant Interested Parties information, proprietary knowledge, assets and others systems in scope.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data.

as well as the privacy

Our commitment to privacy extends to the responsible processing of personal information. This includes safeguarding the rights of individuals and ensuring that the handling of personal data adheres to applicable legal clauses and data protection regulations. We acknowledge the importance of securing the privacy of individuals and are dedicated to upholding the principles of data protection and privacy rights in our practices and policies.

of information and other relevant assets

The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information-based processing devices owned by the organization or those of relevant Interested Parties and BYOD in scope that are processing organization related information.

of our organization

The organization and relevant Interested Parties that are within the scope of the PIMS have signed up to our security policy and accepted our PIMS.

Data Privacy Policy

This Data Privacy Policy outlines the organization's commitment to the responsible handling, processing, and protection of personal data. It specifically addresses the principles of data protection regulations and privacy rights.

All individuals processing personal data on behalf of the organization are bound by this policy, and non-compliance may lead to consequences outlined in the Code of Conduct. Training is provided to ensure awareness and compliance with data protection principles.

Document Owner and Approval

The VP of Global IT is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements set out in ISO 27701:2019.

A current version of this document is available to all members of staff in the PIMS controls environment and accessible via the various Business, HR, and Technical Policy Groups.

This information security and privacy policy was approved by the PIMS Board and is issued on a version-controlled basis.