KONČAR
DIGITAL

PRIVACY INFORMATION MANAGEMENT SYSTEM (PIMS) POLICY

The Management of KONČAR – Digital d.o.o. (hereinafter: the Company) is committed to lawful, transparent and accountable govern personally identifiable information (PII) across all business processes, information systems, services and relationships with interested parties. The Company recognizes that the processing of PII is an integral and unavoidable part of modern business operations and that the manner in which privacy and the protection of PII are managed has a direct impact on the trust of customers, employees, business partners, supervisory authorities and the wider community, as well as on the Company's reputation, legal certainty and long-term sustainability.

Based on this responsibility, the Company commits to establish, implement, maintain and continually improve a Privacy Information Management System (PIMS) in accordance with the requirements of ISO/IEC 27701, as an extension and enhancement of the existing Information Security Management System and in integration with other applicable management systems. The PIMS is established as an integral component of the Company's overall governance and management framework, with the objective of ensuring consistent, repeatable and demonstrable management of privacy throughout the entire life cycle of personally identifiable information.

The Company is committed to processing PII lawfully, fairly and transparently, solely for clearly defined, explicit and legitimate purposes, while ensuring that the scope of processing is adequate, relevant and limited to what is necessary to achieve those purposes. Particular attention is given to ensuring the accuracy, completeness and timeliness of PII, as well as to limiting retention to the period necessary in view of applicable legal, regulatory, contractual and business requirements. Once the purpose of processing has ceased, PII is deleted, anonymized or otherwise permanently disposed of in accordance with defined retention and disposal rules.

Within the PIMS framework, the Company systematically identifies its role in specific PII processing activities, whether acting as a PII controller, PII processor or joint PII controller, and clearly defines responsibilities, authorities and relationships with other involved parties. Special attention is given to the contractual governance of relationships with PII processors and sub-processors, in order to ensure that PII processing is carried out exclusively in accordance with documented instructions and supported by appropriate technical and organizational measures for the protection of privacy.

The Company is committed to respecting and enabling the exercise of the rights of PII principals in relation to the processing of their PII, including the rights to information, access, rectification, erasure, restriction of processing, objection and data portability, within the timeframes and in the manner prescribed by applicable legislation. For this purpose, clear, accessible and documented procedures are established for the receipt, handling and response to requests from PII principals, ensuring transparent communication and appropriate records of actions taken.

In the development and operation of information systems, digital solutions and business processes, the Company applies the principles of privacy by design and privacy by default, ensuring that the

protection of PII is considered from the earliest stages of planning and design, and that default system settings are aligned with the minimum necessary processing of PII. The processing of PII is systematically assessed from the perspective of risks to the rights and freedoms of PII principals, through privacy risk assessments and, where applicable, privacy impact assessments, with the definition and implementation of measures to reduce identified risks to an acceptable level.

The Company ensures the implementation of appropriate technical and organizational measures to protect PII against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, including measures related to access control, identity management, encryption, backup, logging of activities and incident management. In the event of a personal data breach, the Company acts in accordance with predefined procedures, ensuring timely identification, mitigation and documentation of the incident, as well as fulfilment of applicable notification obligations towards supervisory authorities and PII principals, where required.

In order to ensure the continued effectiveness of the Privacy Information Management System, the Company continuously monitors, measures and evaluates its performance, conducts internal audits and regular management reviews, and implements corrective and preventive actions in response to identified nonconformities or opportunities for improvement. Particular emphasis is placed on awareness-raising, education and training of employees and relevant external parties, so that all persons involved in PII processing understand their obligations and responsibilities with regard to privacy protection.

This Policy applies to all organizational units, employees, processes, information systems, products and services of the Company that involve the processing of personally identifiable information, and is binding on all employees and third parties acting on behalf of or for the account of the Company. The Policy is publicly available to interested parties, and non-compliance may constitute grounds for disciplinary, contractual or other appropriate measures. The Company's Management retains overall responsibility for the establishment, implementation and continual improvement of the Privacy Information Management System, hereby confirming its ongoing commitment to the protection of privacy and personally identifiable information as one of the Company's fundamental values.

In Zagreb, 10 October 2025.

Stjepan Sučić, CEO

KONČAR
DIGITAL