Declaration of Compliance with the EU General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) came into effect across the entire European Union on May 25, 2018. From the very first stages of preparation, an approach focused on privacy protection was adopted to ensure that the GDPR requirements meet the demands of the digital age. The 21st century brings extensive use of technology, new definitions of what constitutes personal data, and a significant increase in cross-border processing of such data. The aim of the Regulation is to standardize data protection legislation and data processing across the EU, and to provide individuals with stronger and more consistent rights to access and control their personal data.

Our Commitment

Even before the GDPR came into force, the company had implemented a reliable and effective data protection program compliant with applicable legislation and had long adhered to personal data protection principles. We accept and continuously fulfill the obligations arising from the GDPR, including the requirement to update and expand this program so that it complies with GDPR requirements and the legislation of the Slovak Republic concerning personal data protection and information security.

The company is committed to ensuring the security and protection of the personal data we process while promoting a consistent approach to handling such data. We focus on personal data protection within our scope of activities and on developing data protection practices that are effective, fit for purpose, and demonstrate GDPR compliance.

Our GDPR compliance implementation and objectives are summarized in this declaration and include the creation and implementation of new roles, policies, procedures, controls, and data protection measures, as well as ensuring maximum and continuous compliance with legislation.

How We Apply GDPR Requirements

The company has consistently maintained a high level of personal data protection and security throughout the organization. Our goal is to apply data and information protection principles in accordance with current legislation and the prevailing security environment.

Our implementation of GDPR requirements and principles includes:

- **Information Audit**

An information audit across the entire company to identify and assess what personal data we process and store, where we obtain it from, how and why it is processed, the legal basis for obtaining and processing it, and whether and to whom it is disclosed.

● **Policies, Directives, and Procedures**

Personal data protection policies, directives, and procedures have been implemented to comply with GDPR requirements, standards, and all applicable data and information protection laws, including:

o Personal Data Protection Policy

Our primary policy and procedure document regarding data protection has been developed to meet GDPR standards and requirements. Accountability and management measures are in place to ensure the application of adequate personal data protection principles. The policy also declares our obligations and principles regarding personal data protection, with a particular focus on safeguarding the privacy and rights of individuals during the processing of personal data.

o Personal Data Retention and Disposal Guidelines

We continuously update our data retention and disposal policies, including relevant schedules and plans in accordance with applicable legislation, to ensure GDPR compliance by applying the principles of data minimization and storage limitation. Personal data is retained, archived, and disposed of in compliance with applicable legislation. We have implemented specialized deletion (disposal) procedures to fulfill the "right to erasure." We are aware of when the rights of data subjects apply, including exceptions to erasure, response deadlines, and responsibilities for notifying data subjects.

o Personal Data Breach Procedures

Our security breach and regulatory compliance directives ensure that procedures and measures are in place to identify, assess, investigate, and report any personal data breach as quickly as possible. These directives are regularly updated, and all employees and staff are familiarized with them. The procedures clearly define the steps employees must follow in the event of a security or personal data protection breach.

o International Transfers and Processing of Personal Data Outside the EU by Third Parties

Our company does not transfer personal data to third countries outside the EU.

o Requests for Information Regarding Processed Personal Data

We have implemented procedures for providing information in compliance with the 30-day deadline for responding to requests and for providing such information free of charge to authorized individuals. Our procedures describe how to verify the legitimacy of requests, the steps required to process access requests, applicable exceptions, and standardized response templates to ensure GDPR-compliant, consistent, and appropriate communication with data subjects.

● **Legal Basis for Processing**

All processing activities are reviewed to determine the legal basis for processing and to ensure that each legal basis is appropriate for its intended purpose. We also maintain records of processing activities to ensure compliance with GDPR and applicable legislation.

● **Privacy Notices and Data Protection Principles**

Our privacy notices and data processing principles comply with GDPR requirements. We ensure that all data subjects whose personal data we process are informed why we need their data, how it is used and processed, what their rights are, to whom the data is disclosed, and what protective measures are in place.

● **Consent to Processing**

Our procedures for obtaining consent ensure that data subjects understand what data they provide, why and how it is used and processed, and to whom it is disclosed for clearly defined purposes. The procedures also specify how consent records are maintained and how consent can be withdrawn at any time.

● **Direct Marketing**

Our company does not conduct direct marketing activities.

● **Data Protection Impact Assessments (DPIA)**

Where we process personal data considered high-risk, involving large-scale processing or special categories of personal data (e.g., criminal convictions), we have developed procedures and templates for conducting DPIAs fully compliant with GDPR requirements. Documentation processes are in place to record each assessment, evaluate risks arising from processing activities, and implement mitigating measures to reduce risks to data subjects.

● **Contracts with Processors**

Where we use third parties to process personal data on our behalf (e.g., security services, payroll, recruitment, hosting), we have prepared model agreements and procedures in accordance with legislative requirements to ensure that processors, like our company, comply with GDPR obligations and ensure personal data protection. These measures include initial and ongoing reviews of the provided services and processing activities, taking into account implemented technical and organizational measures.

● **Special Categories of Personal Data**

Where we collect and process special categories of personal data, we do so in full compliance with GDPR requirements for enhanced protection. Such data is processed only when absolutely necessary and only after an appropriate legal basis has been identified.

Rights of Data Subjects

In addition to the above principles and procedures ensuring that individuals may exercise their data protection rights, we provide easily accessible information through requests for exercising an individual's right of access to any personal information we process about them.

Data subjects have the right to obtain confirmation from the controller as to whether personal data concerning them is being processed, including information about:

- What personal data is being processed
- The purposes of processing

- Categories of processed personal data
- Recipients to whom personal data has been disclosed or provided
- How long the personal data is retained
- If the personal data was not collected directly from the individual, information about the source
- The right to rectification or completion of incomplete or inaccurate data and the process for requesting such correction
- The right to request erasure of personal data (unless otherwise required by law) or restriction of processing in accordance with data protection laws, as well as the right to object to direct marketing and to be informed about any automated decision-making used
- The right to lodge a complaint or seek judicial remedy and information on whom to contact in such cases

Information Security and Technical and Organizational Measures

The company is committed to ensuring the security of personal data to prevent unauthorized access, misuse, or disclosure, maintain the accuracy and currency of data, and ensure its effective use.

We have implemented appropriate technical, personnel, organizational, electronic, and managerial procedures to protect and secure collected and processed personal data. When collecting or transferring personal data, we apply security measures according to recognized security standards.

We have extensive information security policies and procedures in place to protect personal data from unauthorized access, alteration, disclosure, or destruction. Security measures are implemented in accordance with Decree No. 158/2018 Coll. of the Office for Personal Data Protection.

The company takes the privacy and security of individuals and their personal data very seriously and therefore adopts and documents all reasonable measures necessary to protect and secure the personal data we process.

Employee Participation in GDPR Compliance

Within the GDPR framework, the company has defined employee roles and responsibilities according to job functions, organizational structure, and workplace regulations. A dedicated team has been established to ensure the implementation of GDPR requirements and the operation of personal data protection processes.

Our company has appointed an external Data Protection Officer (DPO). The legal awareness of our employees and staff is regularly maintained through educational programs and training sessions, including topics related to personal data protection and information security.