Privacy Statement

I. Privacy Protection

DB informatika d.o.o. undertakes to keep confidential the personal data you provide when placing an order, collected for accounting purposes, for creating quotes and invoices, and solely for business contact with you during the use of our services.

All data in the ordering process is protected by the SSL security protocol—that is, it is encrypted during transmission—ensuring a secure transfer of data to our database. DB informatika d.o.o. does not record credit card data.

DB informatika d.o.o. undertakes not to sell, rent, or share your data with third parties without your consent, except in the following situations:

- when providing domain registration services, where your data must be supplied for the domain registration process itself;
- when selling SSL certificates, where entering your accurate data is a precondition for obtaining a certificate;
- when processing business data in our accounting;
- in the event of a transfer of business to another company;
- in the event of an official request for data from state institutions of the Republic of Croatia, in which case—in addition to data about the legal/natural person—access to the website (activity logs, databases, programs, etc.) may be requested.

II. Confidentiality Statement

By this statement, DB informatika d.o.o. undertakes, in accordance with Article 18, paragraph 2 of the Personal Data Protection Act, to maintain the confidentiality of all personal data to which it has the right and authorization to access, which are contained in the company's personal data filing systems, and to use such personal data exclusively for a specific (prescribed) purpose.

DB informatika d.o.o. further undertakes not to deliver/make available such personal data for use, nor in any other way make them accessible to third (unauthorized) persons, with the exception of the situations mentioned above where such data are essential for the provision of the service, and undertakes to keep the confidentiality of such personal data even after the termination of authorization to access personal data.

DB informatika d.o.o. is aware that any unauthorized handling of personal data to which it has access in its work constitutes a breach of work obligations.

III. General Data Protection Regulation (GDPR)

A. Introduction

The GDPR (General Data Protection Regulation) has applied since 25 May 2018 and represents the most significant change related to personal data protection in the last two decades. It has been devised and designed to fully meet the needs of the digital age. The twenty-first century brings broader application of technology in everyday life, as well as new definitions of personal data. The aim of the GDPR is to standardize data protection laws across the EU and thus provide individuals

with greater and more consistent rights regarding access to and control over their personal information.

B. Our Commitment to Data Protection

DB informatika d.o.o. (also referred to as we/our) is fully committed to ensuring the security and protection of the personal data (of users) that are processed, as well as to providing our users with a consistent approach to data protection. We have always sought to maintain a robust and effective data protection program in line with current laws and the core principles of data protection. Nevertheless, we recognize the need to enhance it so that it fully meets GDPR guidelines and the laws of the Republic of Croatia.

C. How We Prepare for the GDPR

DB informatika d.o.o. has a consistent level of data protection policies and processes across all organizational levels; however, in order to be fully aligned with GDPR guidelines by 25 May 2018, we implemented the following steps:

- **Information audit** – An audit of collected personal data was carried out at all organizational levels: the content of the data, how it was collected, why it is processed, and to whom it is disclosed.
- **Policies and procedures** – We reviewed and introduced new data protection policies and procedures that meet all GDPR and related legal requirements, including:
    - **Data protection** – The main data protection policy and procedure document was revised to meet GDPR standards and requirements. Responsibilities and governance measures have been established to ensure that we understand, appropriately disseminate, and demonstrate our obligations and responsibilities, with a special focus on privacy by design and the rights of individuals.
    - **Data retention and deletion** – We updated retention rules and schedules to ensure compliance with the principles of "data minimization" and "storage limitation," and to ensure that personal data are stored, archived, and destroyed ethically and in accordance with those principles. We have specific deletion procedures to meet the new "right to erasure" obligation and are aware when other data subject rights apply—including exceptions, response time frames, and notification responsibilities.
    - **Breach management** – Our breach management procedures set out safeguards and steps to identify, assess, investigate, and report personal data breaches as quickly as possible. These procedures are robust, available to all employees, and outline a series of concrete actions to take.
    - **International data transfers and disclosures to third parties** – Where DB informatika d.o.o. stores or transfers personal data outside the EU, robust procedures and safeguards are in place to secure, encrypt, and maintain the integrity of the data. Our procedures include ongoing reviews of countries with adequacy decisions, provisions on binding corporate rules, as well as standard data protection clauses or approved codes of conduct for countries without such decisions. We conduct strict due-diligence checks on all recipients of personal data to assess and confirm that they have appropriate safeguards to protect information, ensure enforceable data subject rights, and provide effective legal remedies for data subjects where applicable.

- **Subject Access Request (SAR)** – We amended SAR procedures to comply with the revised 30-day timeframe for providing requested information and to implement this provision free of charge. Our procedures detail verification of data, steps taken to process access requests, applicable exemptions, and a series of response templates to ensure communications with data subjects are compliant, consistent, and correct.

- **Legal basis for processing** – We review all processing activities to identify the legal bases for processing and to ensure that each basis is appropriate for the activity concerned. Where applicable, we keep records of our activities, ensuring that obligations under Article 30 of the GDPR and Annex 1 of the Personal Data Protection Act are met.

- **Privacy notices and policies** – We have amended our privacy notices to comply with the GDPR, ensuring that all individuals whose personal data are processed are informed about why we need the data, how it is used, what their rights are, and what safeguards exist to protect the data.

- **Obtaining consent** – We have revised consent mechanisms for collecting personal data, ensuring that individuals understand what they provide, why, and how we use it, and that we offer clear and defined ways to consent to the processing of personal information. We developed strict procedures for recording consent, ensuring that we can demonstrate affirmative consent together with the date and time of the record. In this way it is easy to see and access how consent can be withdrawn at any time.

- **Direct marketing** – We have revised text and procedures for direct marketing, including clear opt-in mechanisms for direct subscriber marketing (newsletters), as well as clear notice and opt-out features in all subsequent marketing materials.

- **Data Protection Impact Assessments (DPIA)** – Where we process personal data considered to be high risk—including large-scale processing or special category/criminal conviction data—we have developed strict procedures and assessment templates fully aligned with Article 35 GDPR. We have implemented documentation processes that record each assessment, enable us to evaluate the risk posed by processing, and implement mitigation measures to reduce the risk to which the data subject is exposed.

- **Processor agreements** – Where we use a third party to process personal data on our behalf (e.g., payroll, employment, hosting, etc.), we have drawn up appropriate processing agreements and due-diligence procedures to ensure compliance with our and their obligations under the GDPR. These measures include initial and ongoing audits of the service provided, the necessity of processing activities, technical and organizational measures, and GDPR compliance.

- **Special category data** – In situations where we obtain and process special category data, all procedures comply with Article 9, and high-level encryption and protection are applied to all data of this type. Special category data are processed only where necessary and only after first identifying the appropriate basis under Article 9(2) or a condition under Annex 1 of the Personal Data Protection Act. Where we rely on consent for processing, it is explicitly confirmed by signature, with clearly indicated rights to amend or withdraw consent.

D. Rights of the Data Subject

In addition to the rules and procedures above—through which individuals can ensure their data protection rights—we provide access via our website to information on the right of individuals to

access all personal data that DB informatika d.o.o. processes about them. Data subjects have the right to request information about:

- all personal data we hold about them;
- the purpose of data processing;
- the categories of personal data being processed;
- all parties that will have access to the personal data;
- how long the personal data will be stored;
- the source of the data, if we did not collect the data directly from them;
- the right to rectification of incomplete or inaccurate data about them, and the process for initiating correction and supplementation;
- the right to request deletion of personal data or restriction of processing in accordance with all relevant data protection laws, and the right to object to any form of direct marketing and to obtain insight into any automated processes of direct marketing by which it is carried out;
- the right to lodge a complaint or seek a legal remedy, and whom to contact.

E. Information Security and Technical/Organizational Measures

DB informatika d.o.o. takes the privacy and security of individuals—and of their personal data—very seriously and takes all reasonable measures and precautions to ensure the data processed are protected. Robust security policies and procedures are in place to protect personal data from unauthorized access, alteration, disclosure, or destruction, with several layers of security measures, including:

- SSL
- Access control
- Password policies
- Encryption
- Pseudonymization
- Practices
- Restrictions
- IT
- Authentication

F. GDPR Roles and Employees

On behalf of DB informatika d.o.o., **Darko Glujić** has been designated as the person responsible for data security, and a group has been formed to implement policies and procedures in accordance with the GDPR. This group is responsible for promoting GDPR awareness within the organization, ensuring employee understanding, and securing ongoing GDPR compliance. An employee training program has been implemented and will be available to all employees before 25 May 2018, as part of the organization-wide annual training program.