EBIS – DATA PROTECTION POLICY

Content

I

GENERAL PRINCIPLES

1. This document entitled "Policy on the protection of data" (hereinafter referred to as the **Policy**) is intended as a map of the requirements, rules and regulations concerning personal data protection in EBIS Sp. z o.o [Ltd.] with its registered seat in Cracow.

2. The Policy is a personal data protection policy within the meaning Of Regulation (Eu) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3. The Policy incorporates:

3.1 a description of data protection rules in force at the Company;

3.2 references to supplementary appendixes (reference procedures or instructions concerning individual areas in the scope of personal data protection that need to be specified in separate documents);

4. The Management Board of the Company is responsible for the implementation and maintenance of this Policy. The Company ensures compliance of the Company's contractors' conduct with this Policy to the extent applicable when personal information is transferred to them by the Company.

5. Definitions:

5.1 **„The Company"** means EBIS Sp. z o.o [Ltd.] with its registered seat in Cracow ul. Samuel Lindego 1C, 30-148 Kraków, entered in the Register of Entrepreneurs kept by the District Court for Kraków-Śródmieście in Kraków, XI Commercial Department of the National Court Register, under number 0000459760, NIP: 6762464669, REGON: 1228439070, share capital: PLN 51.000.00.

5.2 "**Data**" means personal data, unless it is otherwise clear from the context.

5.3 **"Data export"** means the transfer of data to a third country or an international organization.

5.4 **"GDPR"** means Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

5.5 **"The Individual"** means the individual to whom the data relates, unless it is otherwise clear from the context.

5.6 **"The Policy"** means this Policy for the protection of personal data, unless it is otherwise clear from the context.

5.7 "**Profiling"** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

5.8 "**The Processor**" means an organization or a person entrusted by the Company with the processing of personal data (eg an IT service provider, external accounting).

5.9 **"Sensitive data"** means data listed in art. 9.1 GDPR personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

II

PROTECTION OF DATA IN THE COMPANY

6. Pillars of data protection in the Company are:

6.1 **Legality** - the Company ensures the protection of privacy and processes data in accordance with the law.

6.2 **Security** - the Company ensures an adequate level of data security by constantly taking action in this area.

6.3 **Rights of the Entity** - the Company enables persons whose data it processes to exercise its rights and implements these rights.

6.4 **Accountability** - The Company documents fulfillment of its obligations in order to be able to demonstrate compliance at any time.

7. The Company processes personal data respecting the following principles:

7.1 based on the legal basis and in accordance with the law (**legalism**);

7.2 fairly and honestly (**fairness**);

7.3 in a transparent manner for the data subject (**transparency**);

7.4 for specific purposes and not for "spare" (**minimization**);

7.5 no more than necessary (**adequacy**);

7.6 with due care for the correctness of data (**correctness**);

7.7 no longer than necessary (**temporality**);

7.8 ensuring adequate data security **(security**).

8. The system of data protection in the Company consists of the following elements:

8.1 Handling of individual rights. The Company fulfills the information obligations towards the Individuals whose data it processes, and ensures the service of their rights, implementing the requests received in this regard, including:

(a) Information obligations. The Company provides the Individuals with the law with the required information when collecting data and in other situations, and organizes and ensures documenting the implementation of these obligations.

(b) Ability to make requests. The Company verifies and ensures the possibility of effective execution of each type of request by itself and its processors.

(c) Handling of requests. The Company ensures appropriate expenditures and procedures to ensure that people's requests are made on time and in the manner required by the GDP and documented.

(d) Notification of violations. The Company uses procedures to determine the need to notify people affected by the identified data protection breach.

8.2 Minimization. The Company maintains principles and methods of managing the minimization (privacy by default), including:

(a) data adequacy management principles;

(b) principles of regulation and management of data access;

(c) principles for managing the period of data storage and verification of further suitability;

8.3 Security. The Company ensures an adequate level of data security, including:

(a) carries out risk analyses for data-processing activities or categories thereof;

(b) carries out impact assessments on data protection where the risk of violation of the rights and freedoms of persons is high;

(c) adapts data protection measures to the risks identified;

(d) has an information security management system;

(e) uses procedures to identify, assess and report identified data breaches to the Data Protection Authority - manages incidents.

8.4 The processors. The Company has rules for the selection of data processing for the benefit of the Company, requirements regarding the terms of processing (entrustment agreement), rules for verifying the performance of entrustment agreements.

8.5 Data export. The Company has rules for verifying that the Company does not transmit data to third countries or international organizations and to ensure the lawful terms of such transfer, if it takes place.

8.6 Privacy by design. The Company manages changes affecting privacy. To this end, the procedures for launching new projects and investments in the Company take into account the need to assess the impact of changes on data protection, ensuring privacy

(including compliance of processing goals, data security and minimization) already at the design stage of changes, investments or at the beginning of a new project.

8.7 Cross-border processing. The Company has rules of verification of cross-border processing and rules for determining the leading supervisory body and the main organizational unit within the meaning of the GDPR.

III

CATALOGUING

9. The Company identifies personal data resources in the Company, data classes, relationships between data resources, and identification of data usage methods (cataloguing).

9.1 **Sensitive data.** The Company identifies cases in which it processes or can process Sensitive data and maintains dedicated mechanisms to ensure compliance with the law of processing sensitive data. If the cases of sensitive data processing are identified, the Company follows the accepted rules in this respect.

9.2 **Unidentified data**. The Company identifies cases in which it processes or can process unidentified data and maintains mechanisms to facilitate the implementation of the rights of persons affected by unidentified data.

9.3 **Profiling.** The Company identifies cases in which profiling of processed data and maintains mechanisms that ensure compliance of this process with the law. In the case of identifying cases of profiling and automated decision-making, the Company complies with the adopted rules in this respect.

9.4 **Jointcontrollers.** The Company identifies cases of co-administering data and acts in this respect in accordance with the adopted rules.

IV

HANDLING INDIVIDUAL RIGHTS

10. The Company ensures the readability and style of information provided and communication with the people whose data it processes.

10.1 The Company simplifies for Individuals to exercise their rights through various activities, including: posting information or links on the Company's website to information on the rights of individuals, how to use them in the Company, including identification requirements, methods of contacting the Company, including order, optional price list of "additional" requests, etc.

10.2 The Company ensures keeping the legal deadlines for the performance of obligations towards persons.

10.3 The Company introduces adequate methods of identification and authentication of persons for the purposes of the implementation of individual rights and information obligations.

10.4 In order to exercise the rights of the entity, the Company provides procedures and mechanisms to identify the data of specific persons processed by the Company, integrate these data, introduce changes to them and delete them in an integrated manner.

10.5 The Company documents the handling of information obligations, notifications and requests of individuals.

10.6 The Company has a procedure to fulfill third party requests.

V

INFORMATION OBLIGATIONS

11. The Company defines lawful and effective means of performing information obligations.

11.1 The Company informs the Individual about:

(a) the extension of over one month deadline for considering the request of that person;

(b) the processing of its data when collecting data from that person;

(c) the processing of its data when collecting data about that person indirectly from it;

(d) the planned change of the purpose of data processing;

(e) the recipients of data about rectification, deletion or limitation of data processing (unless it will require a disproportionately large effort or will be impossible);

(f) about the right to object to the processing of data at the latest at the first contact with that person.

11.2 The Company defines the method of informing Individuals about the processing of unidentified data, where it is possible (eg a tablet about the area covered by video surveillance).

11.3 The Company shall without undue delay notify the Individuals about the violation of personal data protection, if it may cause a high risk of violating the rights or freedoms of that person.

VI

MINIMIZATION

12. The Company ensures the minimization of data processing in terms of: (i) the adequacy of the data for purposes (data volume and scope of processing), (ii) access to data, (iii) data storage time.

12.1 **Minimizing the scope:**

(a) The Company verified the scope of acquired data, the scope of their processing and the amount of data processed in terms of adequacy for purposes of processing as part of the implementation of the GDPR.

(b) The Company periodically reviews the amount of data processed and the scope of its processing at least once a year.

(c) The Company performs verification of changes in the amount and scope of data processing under the change management procedures (privacy by design).

12.2 **Minimizing access:**

(a) The Company applies restrictions on access to personal data: legal (confidentiality obligations, authorization limits), physical (access zones, closing premises) and logical (restrictions on the rights to systems processing personal data and network resources in which personal data reside).

(b) The Company applies physical access control.

(c) The Company updates the access rights for changes in the composition of staff and changes in the roles of persons, as well as changes in the processing entities.

(d) The Company periodically reviews established system users and updates them at least once a year.

(e) Detailed rules for physical and logical access control are included in the physical security and information security procedures of the Company.

12.3 **Minimizing time:**

(a) The Company implements life-cycle data protection mechanisms in the Company, including verification of the further suitability of the data in relation to the dates and control points indicated in the Register.

(b) Data which scope of use is limited with the passage of time are removed from the Company's production systems, as well as from handheld and main files. Such data may be archived and be stored on back-up systems and information processed by the Company. Procedures for archiving and using archives, creating and using backup copies take into account the requirements of control over the life cycle of data, including the requirements for data deletion.

VII

SECURITY

13. The Company provides a level of security corresponding to the risk of violating the rights and freedoms of individuals as a result of the processing of personal data by the Company.

13.1 The Company carries out and documents the adequacy analysis of personal data security measures. For this purpose:

(a) The Company ensures an appropriate state of knowledge on information security, cybersecurity and business continuity - either internally or with the support of specialized entities.

(b) The Company categorizes data and processing activities in terms of the risk they present.

(c) The Company conducts analyzes of the risk of violation of the rights or freedoms of individuals for data processing activities or categories of data. The Company analyzes possible situations and scenarios of personal data breach taking into account the nature, scope, context and purposes of processing, the risk of violation of the rights or freedoms of individuals with varying likelihood of occurrence and the severity of the threat.

(d) The Company determines the organizational and technical security measures that can be applied and assesses the cost of their implementation. The Company determines the suitability and applies such measures and approach as:

(i) pseudonymisation,

(ii) encryption of personal data,

(iii) other cyber security measures consisting of the ability to continually ensure the confidentiality, integrity, availability and resilience of processing systems and services,

(iv) measures to ensure business continuity and to prevent the consequences of disasters, i.e. the ability to quickly restore the accessibility and access to personal data in the event of a physical or technical incident.

13.2 The Company evaluates the effects of planned processing operations for the protection of personal data where, in accordance with the risk analysis, the risk of violating the rights and freedoms of persons is high.

13.3 The Company applies security measures established as part of risk analyzes and the adequacy of security measures and impact assessments for data protection. Personal data security measures are part of information security and cyber security measures in the Company and are described in more detail in the procedures adopted by the Company for these areas

13.4 The Company uses procedures to identify, assess and report an identified data breach to the Data Protection Authority within 72 hours of the establishment of the breach.

VIII

PROCESSORS

14. The Company has the principles of selection and verification of data processors for the Company designed to ensure that the processors provide sufficient guarantees to implement appropriate organizational and technical measures to ensure security, implementation of individual rights and other data protection obligations on the Company.

15. The Company accounts processors using sub-processors, as well as other requirements arising from the Principles of entrusting personal data.

IX

PRIVACY IN DESIGN

16. The Company manages changes affecting privacy in such a way as to enable adequate security of personal data and minimize their processing.

17. To this end, the principles of project and investment management by the Company refer to the principles of personal data security and minimization, requiring an impact assessment on privacy and data protection, consideration and design of security and minimization of data processing from the beginning of the project or investment

X

FINAL PROVISIONS

18. The Policy is effective since 01.05.2018