PERSONAL DATA PROTECTION POLICY

I. Introduction

In carrying out its work activities, Evrika-GT Ltd., UIC 813188229, based in Res. complex „Sv. sv. Konstantin i Elena“, “Manastirski rid” area 689, P.O.B. 43, 9006 Varna, processes information containing personal data.

This Policy aims to provide information about the way we, as a data controller, process personal data, as well as about the rights of the data subjects whose data we process.

This Policy is applied to all employees and to all interested parties involved with Evrika-GT Ltd., such as clients, suppliers, and partners.

General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) has a direct effect on the personal data protection laws of the EU Member States. It aims to protect the rights and freedoms of natural persons and to ensure that their personal data shall not be processed without their consent, and – whenever possible – that they are processed with their consent.

Scope according to the GDPR

Material scope – this Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data, which form part of a filing system or are intended to form part of a filing system.

Territorial scope – the rules of the General Data Protection Regulation apply to all data controllers based in the Union (i.e., the EU) that process personal data of natural persons in carrying out their work activities. It also applies to data controllers outside of the Union that process personal data with either the goal of offering goods or services, or if they monitor the behaviour of data subjects residing in a Member State.

II. Definitions

“Controller” – the natural or legal person, public authority, agency, or other body, which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

“Child” – any natural person under 16 years of age, although this may be reduced to 13 years of age, according to Member State law. The processing of the personal data of a child is considered lawful only in the case of provided consent from the holder of parental responsibility. The controller makes reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child;

“Personal data” – any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

"Personal data breach" – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

"Processing" – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"Main establishment" – the headquarters of the controller in the Union would be where the decisions on the purposes and means of the processing of personal data are taken. As regards the controller, its main establishment would be the place of its central administration;

"Recipient" – a natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

"Profiling" – 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;

"Pseudonymisation" – the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"Filing system" – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"Special categories of personal data" – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

"Data subject" – natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

"Consent of the data subject" – any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data;

"Third party" – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

III. Sharing personal data

Evrika-GT Ltd. is committed to protecting all personal data gathered and processed. This involves working solely with trusted partners that are engaged in this process.

Evrika-GT Ltd. may share personal data either in order to fulfil its legal obligations, to prevent misuse and fraud, to protect its interests, and to improve its services, or after receiving the data subject's consent to this. It may also share personal data in a pseudonymised way, i.e., without providing direct information.

Evrika-GT Ltd. does neither offer, nor sell personal data in any form.

Evrika-GT Ltd. shares personal data with third parties in cases when:

- There is an existing obligation to disclose and share personal data in order to comply with a legal requirement;
- It aims to fulfil contractual obligations or other conditions, which you have accepted;
- It aims to protect the rights, property, or safety of Evrika-GT Ltd., and those of our employees, clients, and partners;
- The data subject has consented to this;
- There are other circumstances that give us the legal right to do so.

Partners and other third parties who work with or for Evrika-GT Ltd., and who have or might have access to personal data, are expected to make themselves acquainted with, understand, and observe this Policy. No third party may have access to personal data stored by Evrika-GT Ltd., without concluding an agreement about data confidentiality, which imposes obligations on the third party that are no less restrictive than those taken on by Evrika-GT Ltd., and which gives Evrika-Ltd. the right to conduct inspections on the way the agreed upon obligations are fulfilled.

IV. Obligations and roles according to Regulation (EU) 2016/679

1. Evrika-GT Ltd. is a data controller and it processes personal data according to Regulation (EU) 2016/679.
2. The senior management is responsible for the development, integration, and promotion of good practices in the processing of information in Evrika-GT Ltd. It is also responsible for the management of personal data within the organization, and for ensuring the ability of demonstrating compliance with data protection legislation and good practices.
3. These obligations include:
    - developing and implementing rules according to the requirements of Regulation (EU) 2016/679, as required by this Policy;
    - security and risk management in terms of compliance with this Policy.
4. Compliance with data protection legislation is a responsibility of all employees of Evrika-GT Ltd., who process personal data.
5. The training procedure in Evrika-GT Ltd. determines the specific training and information requirements related to the specific roles of the employees of Evrika-GT Ltd.

V. Principles of data protection

All processing of personal data shall be carried out in accordance with the data protection principles referred to in Article 5 of Regulation (EU) 2016/679. The policies and procedures of Evrika-GT Ltd. are designed to ensure compliance with these principles.

1. Personal data shall be processed lawfully, fairly, and in a transparent manner.

    "Lawfully"—a legal basis shall be identified before processing personal data. The legal basis is often referred to as "basis for the processing", e.g., "consent".

"Fairly"—in order for the processing to be fair, the controller shall provide the data subjects specific information, as far as practicable. This applies regardless of whether the personal data is provided directly by the data subjects or by other sources.

"Transparently"—the Regulation includes rules about disclosing confidential information to data subjects in Articles 12, 13, and 14. These rules are detailed and specific, emphasizing on the understandability and accessibility of the confidentiality notices. The information shall be conveyed to the data subjects in a comprehensible form, by using clear and understandable language.

The rules for notification of the data subject by Evrika-GT Ltd. are defined in the internal procedures of the company, and the notification is presented through this Policy.

The specific information to be provided to the data subject shall include at minimum:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer (DPO);
- the purposes of the processing, for which the personal data are intended, as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the following rights—to request from the controller access to personal data, rectification, erasure (the right "to be forgotten"), restriction of processing, as well as the right to object to the conditions (or lack thereof) in connection with the exercise of these rights;
- the categories of personal data;
- the recipients or the categories of recipients of personal data, where applicable;
- where applicable, whether the controller intends to transfer personal data to a third party recipient and information about the level of protection of the data.
- any additional information needed to ensure a fair processing.

2. Personal data are collected for specific, explicit, and legitimate purposes. Personal data collected for specific purposes shall not be further processed for purposes different than those officially declared.
3. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes, for which they are processed ('data minimisation'):
    - the DPO is responsible for ensuring that Evrika-GT Ltd. does not collect information that is not strictly necessary for the purpose, for which it was received.
    - the DPO ensures that all data collection methods are reviewed annually (e.g., through internal audit, or external experts), to ensure that the data collected are still adequate, relevant, and limited to what is necessary.
4. Personal data must be accurate and kept up-to-date at all times; every reasonable step shall be taken to ensure that personal data can be erased or rectified without delay (insofar as technical limitations permit).
    - Data stored by the collector shall be reviewed and updated when needed. Data shall not be stored in cases when they are unlikely to be accurate.
    - The data protection officer is responsible for ensuring that all of the staff are instructed on the importance of accurate data collection and maintenance.
    - It is the duty of the data subject to declare that the data they submit for storage to Evrika-GT Ltd. are accurate and up-to-date.
    - The employees and clients of Evrika-GT Ltd. shall be required to notify the company about any changes in circumstances, so personal data records could be kept up-to-date. Evrika-GT Ltd. is responsible for ensuring that each notification about changes in circumstances is recorded and acted upon.

- The DPO is responsible for ensuring that adequate procedures and policies are in place for maintaining personal data accurate and up-to-date, by taking into account the volume of data collected and other relevant factors.
- The DPO refers to the filing system to review the storage periods of all personal data processed by Evrika-GT Ltd. at least on an annual basis, and shall identify all data that are no longer required in the context of the registered purpose. These data shall be securely destroyed in accordance with the procedures and rules of the controller.
- The DPO is responsible for compliance with data correction requests within one month (according the relevant procedure). This deadline may be extended by two further months in cases of complex requests. If Evrika-GT Ltd. decides not to comply with the request, the DPO shall answer the data subject, in order to explain their reasons, and to inform them on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
- The DPO is responsible for taking appropriate measures in cases when the organizations of third parties have inaccurate or outdated personal data, to inform them that this information is inaccurate or outdated, so it will not be used for making decisions regarding the data subjects, and to forward any corrections of personal data to the third parties, where necessary.

5. Personal data shall be stored in such a form that the data subject can only be identified for as long as is necessary for processing.
    - When personal data are kept after the processing date, they shall be stored in an appropriate manner (minimised, encrypted, pseudonymised), in order to protect the identity of the data subject in case of personal data breach.
    - Personal data shall be kept in accordance with (according the relevant procedure), and after their storage period has expired, they shall be securely destroyed in the manner defined by this procedure.
    - The DPO shall specifically approve each retention of data beyond their storage period defined in (according the relevant procedure), and shall ensure that its justification is well complies with the requirements of the data protection legislation. This approval must be made in writing.
6. Personal data shall be processed in a manner that ensures appropriate security of the data (Articles 24 and 32 of GDPR).

The DPO shall carry out an impact assessment (risk assessment) taking into account all circumstances related to the management or processing operations of Evrika-GT Ltd.

In determining the suitability of processing, the DPO shall also assess the extent of any damage or loss that may be caused to natural persons (e.g., personnel or clients), if a data breach was to occur, as well as any possible damage to the reputation of the controller, including a possible loss of customer confidence.

When assessing appropriate technical safeguards, the DPO shall consider the following:

- Password protection;
- Locking of idle workstations;
- Removal of access permissions for flash drives and other removable storage media;
- Antivirus software and firewalls;
- Role-based access rights, including those of temporary appointed staff;
- Security of the devices leaving the premises of the organization, such as laptops or others.
- Security of local- and wide-area networks;
- Privacy-enhancing technologies, such as pseudonymisation and anonymisation;

- Identification of international standards for information security appropriate for Evrika-GT Ltd.

When assessing the appropriate organisational measures, the DPO shall consider the following:

- Levels of appropriate training at Evrika-GT Ltd.;
- Employee reliability measures (e.g., appraisal assessments, recommendations, etc.);
- Inclusion of data protection clauses in employment contracts;
- Identification of disciplinary measures for breaches in data processing;
- Regular staff inspections for compliance with relevant security standards;
- Control of physical access to electronic or paper-based records;
- Adoption of "clean desk policy" (when leaving the workplace, all work-related documentation is removed or locked away in suitable restricted areas—special cabinets, locked rooms, no longer necessary documents are destroyed, etc.);
- Paper-based storage of the database in lockable wall-mounted cabinets;
- Restrict the use of portable electronic devices outside the workplace;
- Restrict employee use of personal devices in the workplace;
- Adoption of clear rules for creating and using of passwords;
- Regular backups of personal data and physical storing of media with copies of the data outside of work premises;
- Imposition of contractual obligations on counterparty organizations to take appropriate security measures, when transferring data outside of the Union.

These controls are selected on the basis of identified risks for personal data, as well as the potential for harm to the data subjects.

7. Compliance with the principle of accountability

Evrika-GT Ltd. shall prove compliance with data protection principles: by implementing data protection policies, by joining codes of conduct, by implementing appropriate technical and organizational measures, as well as by the adoption of: data protection techniques at the level of data protection by design and by default, impact assessment on the protection of personal data, data breach notification procedure, etc.

VI. Rights of the data subjects

1. Data subjects shall have the following rights in respect of processing and data stored for them:
   - To obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, to obtain access to the personal data and information about the recipients of this personal data.
   - To request from the controller a copy of their personal data;
   - To request from the controller the rectification of personal data when they are inaccurate or no longer up-to-date;
   - To request from the controller the erasure of personal data (the right "to be forgotten");
   - To request from the controller a restriction of processing of personal data, which in this case shall only be stored, but not processed;
   - The object to the processing of their personal data;
   - To object to the processing of their personal data, where that data are processed for direct marketing purposes;
   - To lodge a complaint with a supervisory authority, if they believe any of the provisions of the GDPR have been infringed;

- To request and to receive their personal data in a structured, commonly used, and machine-readable format;
- To withdraw their consent to personal data processing at any time with a separate request to the controller;
- Not to be subject to a decision that significantly affects them and that is based solely on automatic processing without the possibility of human intervention;
- To oppose automatic profiling carried out without their consent;

2. Evrika-GT Ltd. provides conditions to ensure the exercise of these rights by the data subject:
    - Data subjects can request data access. Evrika-GT Ltd. guarantees that the response to the data subject's requests will be in accordance with the requirements of the General Regulation.

VII. Consent

1. By "consent" Evrika-GT Ltd. shall understand any freely given, specific, informed, and unambiguous indication of the data subject's wishes, by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
2. By "consent" Evrika-GT Ltd. understands only those cases, in which the data subject has been thoroughly informed about the planned processing of their data and has expressed their consent without coercion. Consent given under coercion or due to misleading information shall not be a valid basis for processing of personal data.
3. Consent cannot be inferred by the lack of response to a message to the data subject. There should be active communication between the controller and the data subject, in order to establish consent. The controller shall be able to demonstrate the obtained consent to the processing operations.
4. For special categories of personal data, the consent of the data subject shall be obtained explicitly in writing, unless there is an alternative legal basis for processing.
5. In most cases, the consent to processing of personal data and special categories of personal data is routinely obtained from Evrika-GT Ltd. by using standard consent documents, e.g., when a client signs a contract or when recruiting new staff.
6. When Evrika-GT Ltd. processes personal data of children, consent should be obtained by the holder of parental responsibility (parents, guardians, etc.). This requirement applies for children under the age of 16 years.

VIII. Data security

1. All employees are responsible for ensuring security in storing of the data under their care, which is held by Evrika-GT Ltd., as well as ensuring that the data is not disclosed to third parties under any circumstances, unless Evrika-GT Ltd. has granted these third parties rights, by concluding a contract / confidentiality clause.
2. All personal data shall be accessible only to those that need them, and access can be granted only in accordance with the established access control rules. All personal data shall be treated with the highest security and shall be stored:
    - in a self-contained room with controlled access; and/or in a locked cabinet or in a filing cabinet; and/or
    - if processing is computerized—it shall be password protected and in compliance with the internal requirements specified in the technical and organisational measures for control of the access to information, and/or
    - stored on portable computer media that are protected in compliance with the technical and organisational measures for control of the access to information.
3. All employees are required to undergo training, to accept the relevant contractual clauses, and to declare compliance with the technical and organisational measures for access, before they are granted access to information of any kind.

4. Paper-based records shall not be left where they can be accessed by unauthorized persons and shall not be removed from the designated work areas without explicit permission. As soon as the paper documents are no longer required for ongoing customer work, and are not subject to storage, they shall be destroyed in accordance with the procedure / rules established for that purpose.
5. Personal data shall be erased or destroyed only in compliance with the documents management procedure. Paper-based records that have reached their date of storage shall be shredded and destroyed. Hard disk data on redundant personal computers shall be erased or the disks shall be destroyed, according to the procedures.
6. Processing of personal data outside work areas has a potentially higher risk of loss, theft, or breach of the privacy policy. The staff should be specially authorized to process data outside the premises of the controller.

IX. Data disclosure

1. Evrika-GT Ltd. shall ensure that personal data are not disclosed to unauthorized third parties, including family members, friends, state authorities, even investigating authorities, if there is reasonable doubt that they are required by the order established for that purpose. All employees should be careful when asked to disclose personal data about another person to a third party. It is important to keep in mind whether the disclosure of information is related to the needs of the company's business.
2. All requests from third parties to provide data should be supported by appropriate documentation and any such disclosure should be specifically authorized by DPO.

X. Storage and destruction of data

1. Evrika-GT Ltd. does not store personal data in a form that permits identification of the data subjects for a longer period than is necessary with respect to the purposes for which the data were collected.
2. Evrika-GT Ltd. keeps data for longer periods only if the personal data will be processed for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, and only when in compliance with the appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
3. The storage period and the criteria used to determine it, for each category of personal data, are determined under the documents management procedure.
4. Personal data should be securely destroyed, in compliance with the principle of ensuring an appropriate level of security (Article 5 of the GDPR)—including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

XI. Data transfer

Any data transfer from within the EU to states outside the EU (referred to in the General Regulation as "third parties") is unlawful unless there is an adequate level of protection to the fundamental rights of the data subjects.

1. Adequacy decision

The European Commission shall decide whether a third country, a territory, and/or one or more specified sectors within that third country ensures an adequate level of protection to the rights and freedoms of natural persons. In these cases, no specific authorisation is required.

Countries that are members of the European Economic Area (EEA), but not of the EU, are considered to be in compliance with the requirements for an adequacy decision.

2. Exceptions

In the absence of an adequacy decision, binding company rules and/or contractual clauses, transfer of personal data to a third party or an international organization shall be made only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers;
- the transfer is necessary for the performance of a contract between the data subject and the controller, or for the performance of pre-contractual measures, taken at the data subject's request;
- the transfer is necessary for the conclusion or the performance of a contract, concluded in the interest of the data subject, between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise, or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or other persons, when the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register, which, according to Union or Member State law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

XII. Data processing registry (filing system)

1. Evrika-GT Ltd. has created a filing system as part of its approach to addressing the risks and possibilities in adhering to the compliance policy with Regulation (EU) 2016/679. In Evrika-GT Ltd.'s process of filing and workflow, the following things are considered:
   - the business processes that use personal data;
   - the sources of personal data;
   - the number of data subjects;
   - a description of personal data categories and of the elements in each category;
   - the processing activities;
   - the purposes of the processing, to which the personal data are intended;
   - the legal basis for the processing;
   - the recipients or the categories of recipients of personal data;
   - the main systems and storage locations;
   - all personal data that are subject to transfers outside the EU;
   - storage and erasure times.
2. Evrika-GT Ltd. is aware of the risks associated with the processing of certain types of personal data.
3. Evrika-GT Ltd. Is assesses the level of risk for persons, related to the processing of their personal data. Impact assessments on data protection, related to the processing of personal data by Evrika-GT Ltd., and in relation to the processing of personal data by other organizations on behalf of Evrika-GT Ltd., are carried out.
4. Evrika-GT Ltd. manages all the risks identified by the impact assessment, in order to reduce the probability of non-compliance with these rules.

Where a type of processing may lead to a high risk to the rights and freedoms of natural persons, in particular by using new technologies, and taking into account the nature, scope, context, and purposes of the processing, before proceeding with processing, Evrika-GT Ltd. can assess the impact of the planned processing operations

on the protection of personal data. A general impact assessment may consider a set of similar processing operations that present similar high risks.

5. Where, as a result of the impact assessment, it is clear that Evrika-GT Ltd. will start processing personal data, which, due to a high risk, could cause damage to data subjects, the decision whether or not to continue processing should be submitted for review by the DPO.
6. If the DPO has serious concerns either about the potential harm or danger, or about the amount of relevant data, they should refer the matter to the supervisory authority.

Effective from: 31.08.2018