Updated in February 2022

EVIOSYS GUIDELINES ON DATA PROTECTION

1. Objective

The aim of these Eviosys Guidelines on Data Protection (the "**Guidelines**") is to provide:

- adequate and consistent safeguards for the processing of personal data (as defined below) by all Eviosys entities in the EU; and
- clear instructions to anyone working for Eviosys who, in the execution of his/her role, processes personal data as defined in the Guidelines.

The Guidelines are drafted in order to ensure compliance with the European General Data Protection Regulation 2016/679 of 27 April 2016 ("**GDPR"**). Any questions about the GDPR or compliance thereto should be addressed to:

- Juliana Castillo: Legal & Overall Coordination
- Didier Callet : Finance and administration
- Fabrice Ouedraogo : Human Resources
- Karl Enthoven : IT.

For whom?

The Guidelines have been drafted for any and all people employed by a Eviosys entity established in the European Union and in Switzerland who, in the execution of their role within Eviosys, process personal data of data subjects as defined in these Guidelines. Data subjects are:

- Job Applicants
- Employees
- Contacts at Customers
- Contacts at Suppliers.

2. Definitions

The GDPR includes a list of definitions, the most important terms are explained below:

- **"Controller"** means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. In the context of these Guidelines, any Eviosys legal entity is a Controller.
- **"Employee"** – For practical reasons, the word 'employee' will have a broad scope in the Guidelines and will include any current or former employee, temporary workers and intern.
- **"European Economic Area** ("**EEA**")" currently including the countries if the European Union plus: Iceland, Liechtenstein and Norway.
- **"Eviosys Europe entities ("Eviosys")"** means all affiliates or entities of the Eviosys European Division located in the European Union and Switzerland.
- **"Personal data"** means any information relating to an individual from which s/he can be identified ("data subject"). For example, name, email address, bank details. Other information, such as location data, an identification number, an online identifier (IP address), can also be considered as personal data if it can be linked to a person.
- "**Sensitive personal data**" means Personal Data revealing a person's:
    - racial or ethnic origin,
    - political opinions,
    - religious or philosophical beliefs,
    - trade-union membership
    - data concerning health or sex,
    - criminal convictions and offenses.
- **"Processing"** is defined in the GDPR as '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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' The term 'processing' thus has a very broad scope.

- **"Data breach"** is defined in the GDPR as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

3. Principles for processing personal data

Eviosys will observe the following principles when processing personal data:

- The data will be processed *lawfully*, *fairly* and in a *transparent* manner in relation to the data subject; in particular, in Eviosys, the processing will be based on one of the following legal basis:
  - ✓ The processing is necessary for the performance by Eviosys of its contractual obligations;
  - ✓ The purpose is necessary for the purposes of Eviosys's legitimate interests, provided such interests are not overridden by interests or fundamental rights and freedoms of data subjects;
  - ✓ The processing is necessary for Eviosys to comply with its legal obligations.
- The data will be collected for *specified, legitimate purposes* (*e.g.*, for personnel management); the data will not be processed further in ways that would be incompatible with those purposes;
- The data will be *adequate, relevant to and not excessive for* the purposes for which they are processed (*data minimization*).
- The data will be *accurate* and, where necessary kept up *up-to-date*. Reasonable steps will be taken to *rectify or delete* any data that is inaccurate or incomplete;
- The data will be *kept only as long as it is necessary* for the purposes for which it was collected and processed.
- The data will be *deleted or amended* following a justified request by the data subject;
- The data will be processed in accordance with the *individual's legal rights* as described in the Guidelines or as provided by law;
- Appropriate *technical, physical and organizational measures* will be taken to prevent unauthorized access, unlawful processing and unauthorized or accidental loss, destruction or damage to data. In the event of any violation or accidental data breach, Eviosys will take appropriate steps to end the violation and/or eliminate the breach and determine liabilities in accordance with the GDPR, as well as cooperate with the competent authorities where necessary, should they be involved as a result of such violation or breach.

4. Types of data processed

Information notices shall be sent to employees and made available on Eviosys's intranet. The privacy policy is available online on Eviosys's website for job applicants, customers, and suppliers. Each notice will list the type of data that Eviosys processes for each category of data subject: for example, identification data, personal data, data regarding education and professional experience for candidates; name of contact person and contact details, data required for payment of invoices for suppliers and customers; identification and contact data, personal and professional data, bank account data, occupational health data, connection data for employees.

5. Purposes for personal data processing

Privacy policies and information notices to each category of data subject shall also disclose the purposes for which Eviosys processes personal data, as well as the legal basis for such processing. Examples of purposes for which Eviosys processes personal data are listed below.

For HR matters:
Eviosys, for example, processes personal data, in order to manage its personnel, for the performance of the employment agreements, to comply with applicable legal obligations (*e.g.*, regarding social security and tax matters, work permits) and also to pursue certain legitimate interests, (*e.g.*, providing reliable and secure HR management, personnel administration).

For Non HR matters (suppliers, customers etc.): Any personal data that is necessary for the execution of an agreement with any customer, prospective customers or supplier will be processed only by the employees who, in

the execution of their role within Eviosys, are required to have access to such information. These personal data are in principle limited to standard data (name, gender, phone number(s), business email address, etc.). The suppliers and customers will receive information on this personal data in the updated general sales and purchase conditions and/or in the privacy policy available on Eviosys' website.

If Eviosys introduces a new process or application that will result in the processing of personal data for purposes that go beyond the purposes it already disclosed, Eviosys will inform the concerned data subjects of such new process or application, new purposes for which the personal data are to be used, and the categories of recipients of the personal data. It will also update the register which sets out its data processing activities and will assess whether it needs to undertake a so-called DPIA (Data Protection Impact Assessment). This would be required if the processing is likely to result in a high risk to the rights and freedoms of individuals. Different criteria exist to assess whether a DPIA is necessary and certain supervisory authorities have determined that certain data processes require a DPIA (such as the CNIL for whistleblowing schemes).

6. Security/confidentiality

Eviosys is committed to taking appropriate technical, physical and organizational measures to protect personal data against unauthorized access, unlawful processing, accidental loss or damage and unauthorized destruction.

Equipment and Information Security:
To protect against unauthorized access to personal data by third parties outside Eviosys, all electronic personal data held by Eviosys are maintained on systems that are protected by up-to-date secure network architectures that contain firewalls and security monitoring services. The data saved in servers is "backed up" (*i.e.*, the data are recorded on separate media) to avoid the consequences of any inadvertent erasure, destruction or loss otherwise. The servers are stored in facilities with high security, access protected to unauthorized personnel, fire detection and response systems. The location of these servers is known to a limited number of Eviosys's employees.

Access security:
The importance of security for all personally identifiable information associated with Eviosys's employees is of highest concern. Eviosys is committed to protecting the integrity of personal data and preventing unauthorized access to information maintained in Eviosys's databases. These measures are designed and intended to prevent corruption of data, block unknown and unauthorized access to our computerized systems and information, and to provide reasonable protection of personal data in Eviosys's possession. All employee files are confidentially maintained in the HR department in secured and locked file cabinets or rooms. Access to the computerized database is controlled by a log-in sequence and requires users to identify themselves and provide a password before access is granted. Users may only access data required to perform their job function. Security features of our software and developed processes are used to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

Training:
Eviosys will conduct adequate training sessions regarding the GDPR and data protection principles, in particular the lawful purposes of processing personal data, the need to protect and keep information accurate and up-to-date, and the need to maintain the confidentiality of the data to which employees have access. Authorized users will comply with these Guidelines and Eviosys will take appropriate actions in accordance with applicable law, if personal data are accessed, processed, or used in any way that is inconsistent with the requirements of the Guidelines.

General instruction:
Any and all individuals working at Eviosys who, in the execution of their role, have access to personal data (such as, but not limited to, individuals working in the HR, IT, SSC, Sourcing, Commercial and legal departments must comply with the rules set out in these Guidelines so that Eviosys is compliant with European current and future privacy rules and regulations. Non-compliance with privacy rules may lead to serious negative consequences for Eviosys (notably high penalties imposed by Supervisory Authorities, reputational damages) but also possible impacts for data subjects. Employees must therefore in particular handle personal data with utmost care and in strict compliance with the Guidelines so as to ensure its correct and lawful treatment.

7. Rights of data subjects

Information:
Any person whose personal data are being processed by Eviosys has the right to be provided with information such as the nature of the personal data stored or processed about him/her, the purpose of the processing, the recipients of the data, the retention period, whether Eviosys transfers data outside the EEA. This information will be notified in the following manner:

- to employees and job applicants: by means of an information notice;
- to customers and suppliers: in the general terms and conditions.

Procedure for responding to requests:
All data subjects whose data Eviosys processes will also receive information on the exercise of the following rights. If a data subject exercises these rights, Eviosys is required by law to provide him/her with a response within **30 days**. This period may be extended by up to two months if the request is complex or numerous. Given this short time frame, any written request submitted via any channel (email, text, letter, but not verbal requests), made by an individual or a third party on behalf of an individual, should be transmitted to one of the data protection contact persons listed in Section 1, so that Eviosys may timely respond. Requests relating to HR matters should be transmitted to HR.

Eviosys will in any event need to respond to the data subject, if not only to indicate why it is not taking action following a request. Eviosys must also keep traces of the requests and responses thereto.

Access request:
Any data subject has a legal right to make an access request and request a copy of any or all personal data concerning him/her that Eviosys holds and processes. S/he is not entitled to any information which is not about him/her and concerns the business, its products or any third party.

Rectification, restriction or erasure:
If any information is inaccurate or incomplete, the data subject may request that the data be corrected.

Under certain circumstances, the data subject can ask Eviosys to erase the personal data pertaining to him/her, amongst others if the personal data are no longer necessary for the purposes for which they are collected or processed or if the data subject objects to the processing for legitimate reasons. In certain cases, Eviosys may however refuse to erase these data, particularly if it needs it to defend a legal claim.

Under certain circumstances, for example when the accuracy of the data is contested or when the data subject has objected to the processing, he/she can ask that the processing of his/her personal data be restricted, meaning that the stored personal data are marked and that this will be clearly indicated in the file.

Restrict or object to the processing and transfer of personal data:
Under certain circumstances, the data subject also has the right to object to the processing of his/her personal data. Eviosys does not have to accept such objection, if compelling justified grounds can be invoked and which override the employee's rights, or if these data are necessary to support a legal claim.

Data portability [For information purposes as this should not apply to Eviosys]:
If necessary and in so far as applicable, a data subject may ask to receive certain personal data that he/she has provided to Eviosys, and even request to transfer these data to another data controller, if this is technically possible and if the processing is based on consent or a contract and the processing is automated. This right may however not violate the rights and freedoms of others. This only applies to limited employee data processed based on the contract (for example, data regarding certain benefits, pension schemes).

Complaint:
If a data subject has complaints relating to Eviosys's processing of their personal data, s/he should raise these in the first instance with:

- The HR department for job applicants and employees, including former employees;

- The Shared Services Center or Sourcing department for suppliers;
  The Sales department or Shared Service Center for customers.

Alternatively, the data subject may also raise complaints with the local Supervisory Authority.

8. Retaining personal data

The retention rules regarding the processing of personal data are provided in the Data Retention Policy to be made available on the intranet in the Policy Centre.

9. Transfer of data outside the EEA

The transfer of personal data within the EEA is allowed pursuant to the GDPR. Eviosys may also transfer personal data to *non-EEA* Eviosys entities, if a sufficient level of protection is guaranteed as set out below. Eviosys transfers personal data to Switzerland and to the United Kingdom, which have been recognized as granting an adequate level of protection by the EU Commission. It transfers limited data to KPS in the United States and relies on such data transfer on derogations provided by Article 49 of the GDPR.

If an EEA Eviosys entity transfers personal data to a third party located outside the EEA, Eviosys will provide appropriate safeguards by applying one of the following transfer solutions:

(a) The data importer is located in a country recognized by the European Commission as offering an adequate level of data protection as determined by the European Commission (*e.g.*, notably Switzerland, the UK);

(b) Eviosys can rely on the derogations set out by Article 49 of the GDPR, which must be strictly interpreted (for example, consent of the data subject, performance of a contract between the controller and data subject, performance of a contract in the interest of the data subject between the controller and a third party, to establish, exercise or defend legal claims); or

(c) The data importer has agreed to process these data in accordance with the 'Standard Contractual Clauses' ("SCC") approved by the European Commission. Note that new SCCs have been adopted last June 2021, which require a prior assessment of the envisaged data transfer including an assessment of the importing country.

10. Transfer to third parties

Personal data may be disclosed to third parties outside the Eviosys group if disclosure is consistent with a legal basis for processing on which Eviosys relies and doing so is lawful and fair to the data subject. More specifically, Eviosys may disclose personal data if it is necessary for its legitimate interests as an organization or the interests of a third party (but Eviosys will not do this if these interests are overridden by the privacy rights of the data subject).

Eviosys may also disclose personal data:

- if the data subject gives his/her consent,
- if it is required to do so by law, or
- in connection with criminal or regulatory investigations.

HR: HR-cases where personal data may be disclosed to third parties include disclosure to:

- organizations that process data on Eviosys's behalf such as the payroll service, insurers and other benefit providers, the bank and organizations that host Eviosys's IT systems and data;
- external recipients of electronic communications (such as emails) which contain personal data;
- disclosure on a confidential basis to a potential buyer of its business or company for the purposes of evaluation – but only if Eviosys is contemplating selling;

Where disclosure to a third party is necessary, Eviosys shall only use contract processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the data subjects' rights. Eviosys will enter into contracts with such third party, in line with the GDPR.

11. Automated decision

Automated decisions are defined as decisions about individuals that are based solely on the automated processing of data and that produce legal effects that significantly affect the individuals involved. As a rule, Eviosys does not make automated decisions for employee data. If automated decisions were to be made, affected persons would be given an opportunity to express their views on such automated decision and object to it.

12. Data breaches

Eviosys's obligations in case of data breach:
Based on European privacy rules, Eviosys must immediately notify the relevant national Data Protection or supervisory Authority ("DPA") of any data breach that has or is likely to have serious negative consequences for the protection of personal data. Eviosys must notify the Supervisory Authority or the lead supervisory authority within 72 hours after becoming aware of the personal data breach. In certain instances, Eviosys must also inform the data subject affected by the personal data breach.

What is a data breach?
A data breach is a breach of physical or technical security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data. This security breach may be, for example, the theft/loss of an unprotected USB-key/mobile device/laptop that contains personal data, an intrusion to any system containing personal data by a hacker or unauthorized physical access to paperwork that contains personal data (*e.g.*, break-in to a filing cabinet, leaving paperwork in a communal area, etc).

Reporting data breaches
In case of suspicion of data breach, individuals should refer to the procedure provided in Eviosys's Security Incident Response Plan to be made available on the Intranet. They should also contact EISS Support.

13. Enforcement of the Guidelines

Eviosys will ensure that the Guidelines are observed and duly implemented. All persons who have access to personal data must comply with the Guidelines.

Violations of the applicable data protection legislation in the EEA may lead to penalties and/or claims for damages imposed by the DPA or the court, to Eviosys.

Eviosys undertakes to register its processing activities and/or keep its register up to date as a data controller in all jurisdictions where Eviosys maintains entities in the EU. Any new processing or use of an application, any modification to its processing will need to be documented in its register.

14. Communication about the Guidelines

These Guidelines have been drafted more specifically for employees that process personal data in their functions, i.e., employees in the HR, IT, SSC, Sourcing, Commercial and Legal Departments. The Guidelines will therefore specifically be communicated to such employees. They will also be posted on Eviosys's intranet and thus made available for all Eviosys employees to consult it to learn more about the GDPR and how Eviosys handles personal data.

15. Modifications on the Guidelines

Eviosys reserves the right to modify the Guidelines as needed, for example, to comply with changes in laws, regulations or requirements introduced by DPAs. Eviosys will post all changes to the Guidelines on its intranet.