

Data Privacy and protection Policy- Public

Public Version

Author: CEO

Validated: DPPO

Release Date: 10/08/2017

Revision Number: 1.0

1 TABLE OF CONTENTS

1	Table of contents	2
2	Introduction	3
3	Policy applicability	3
4	Definitions	4
5	Principles of personal data privacy & protection	4
6	Adequate Organizational and technical measures	5
6.1	Organizational Responsibilities	5
6.2	Appropriate measures for Data protection	5
7	Data Breach notification	6
8	Our Suppliers and commissioned sub-contractors	7
9	Territorial scope - Data storage	7
10	DATA subject rights	7
11	Complaint procedure	8
	Document Information	9

2 INTRODUCTION

e-BO Enterprises and affiliates, hereafter “e-BO Enterprises Group of companies” abbreviated as “e-BO Group” is bound by data protection and privacy laws. e-BO Group respects and protects the rights of individuals, in particular the right to data protection and privacy during the processing, use and storage of information as well as the right to privacy. e-BO Enterprises may also share personal data with another member of the e-BO Group or affiliates. The protection of information comprises the personal data of employees, applicants, customers, suppliers, partners, and all other persons within the e-BO Group area of responsibility. To adhere to this obligation, e-BO Group has adopted an e-BO Group Data Protection and Privacy Policy and reviews it regularly.

e-BO Group has its headquarters in Belgium, a member state of the European Union (EU). Therefore, the basic principles established through this Policy are based on the requirements of European data protection and privacy legislation, 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). If, on a case-by-case basis, applicable local law outlines stricter data protection and privacy requirements than this Policy, personal data must be handled in compliance with those stricter laws. Additional standards and/or guidelines within the e-BO Group that are issued as a result of this Policy must also take the applicable law into account in this respect.

Questions on applicable law can be directed to the Data Protection and Privacy Officer (DPPO) (privacy@ebo-enterprises.com).

3 POLICY APPLICABILITY

This public policy is part of the e-BO Group corporate governance framework and outlines the e-BO Group wide minimum framework for handling personal data in compliance with data protection and privacy laws. It defines requirements for all operational processes that affect personal data, as well as clear responsibilities and organizational structures. As soon as a process at e-BO Group involves collecting, processing, usage or storage of personal data, the provisions of this Policy are to be adhered to. Management of e-BO Enterprises and affiliates and the relevant process owners are responsible for ensuring that all processes – during which personal data is collected, processed, used or stored– are designed such that the provisions of this Policy are fulfilled. It is the duty of all e-BO Group employees to comply with the provisions of this Policy when handling personal data in their daily work for e-BO Group.

Personal data that is subject to this Policy includes data on employees, applicants, former employees, customers, interested parties, suppliers, partners, users of e-BO Group services and products, and any other person of interest.

e-BO Group is controller for the personal data of all its own employees, candidates, former employees, customers, suppliers, partners and other persons of interest, meaning e-BO Group makes decisions on the purposes and means of processing the personal data of the above mentioned data subjects.

e-BO Group is always data processor in providing its services and products to their customers. The customer is the data controller for the personal data that is processed on e-BO Group products and services. e-BO Group processes the personal data of the data controller only on behalf of and only according to the instructions given by the data controller, enforced by a processor-controller agreement. The personal data of the data controller may be contained in a system operated by the data controller themselves, or in systems of third parties that operate these on behalf of the data controller. Data controller systems – that e-BO Group or third parties on behalf of e-BO Group operate – are also relevant – as are systems operated by the data controller themselves

whereas e-BO Group employees can access the personal data stored in these systems while providing services, support, or consulting services.

4 DEFINITIONS

The terms used in this policy have the meaning as described in 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 PRINCIPLES OF PERSONAL DATA PRIVACY & PROTECTION

e-BO Group is committed to complying with the data protection principles set out in REGULATION (EU) 2016/679, as personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (**'purpose limitation'**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**). This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**).
- processed in accordance with the **rights of Data Subjects**
- **not transferred** to a country or territory **outside** the European Economic Area unless adequate protection is in place.

e-BO Group adds the following principle, although not required by the data privacy and protection legislation, to not sell personal data to third parties.

Further details of how e-BO Group complies with these principles are set out below, distinguishing e-BO Group as Controller and as Processor, whereas in the latter e-BO Group only acts upon instruction of the data controller

and whenever instruction of Controller are lacking, applying data privacy & protection enforced by the e-BO Group internal policies.

6 ADEQUATE ORGANIZATIONAL AND TECHNICAL MEASURES

6.1 ORGANIZATIONAL RESPONSIBILITIES

The legal responsibility for collecting, processing and using personal data within the e-BO Group, lies with the executives of the company that collects, processes or uses the personal data for its own business purposes. Within de e-BO Group the responsibilities are delegated along the organisational structure by means of dedicated and assigned functions and roles, enforced by policies, processes and documented instructions from management to managers at different levels as well as employees, accompanied by sufficient education and training.

The CEO of e-BO Group delegates to the following roles, taken segregation of duties into account, to the management of e-BO Group, presented in the non-exhaustive list below:

- Data Protection and Privacy Officer (DPPO), reporting independently to the highest management, advising CEO and validation of data privacy and protection accountabilities. The DPPO is contact person for all data privacy and protection communication & questions (privacy@ebo-enterprises.com).
- Chief Operation Officer (COO), responsible for the effective execution of policies, guidelines and procedures in operations, service desk and projects.
- Chief Technology Officer (CTO), responsible for R&D of services and products and engineering projects and services.
- Chief Security Officer (CSO) holds the primary responsibility for ensuring the information security.
- HR Officer responsible for personal data privacy and protection in the HR domain.

Roles are dedicated to managers at different levels as well as to employees, taken segregation of duties into account:

- System (information) owner, responsible for purchasing requirements, development and maintenance of information and related information systems.
- System (information) administrator, responsible for implementing, running and maintaining systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is not lost.
- System users, responsible for working in accordance with the instructions.

6.2 APPROPRIATE MEASURES FOR DATA PROTECTION

“ISO 27001:2013 Information security management” is the framework e-BO Group implements for providing the means to ensure adequate data security. In addition to the adopted technical controls, structured documentation, monitoring, and continuous improvement, the implementation of ISO 27001 promotes a culture and awareness of data protection in the e-BO Group.

A non-exhaustive list of ISO 27001 controls are listed, applicable on personal data as on the other information assets e-BO Group is responsible for.

6.2.1 RISK ASSESSMENT & TREATMENT

The data privacy and protection legislations defines personal data and special categories of personal data (ISO control A.8.2.1 : Classification of information), taken into account in the data classification. The data privacy and protection legislation also defines what is to be considered as high risk processing. Based on the data classification and high risk processing, data protection impact assessments are carried out prior to the processing, validated by the DPPO. Our Customers, acting as controller, provide the information of the classification of their personal data , the data processing risk and are by the data privacy and protection law obliged to perform a data protection assessment, which eBO Group takes into account for determination of the technical and organisational measures.

6.2.2 COMPLIANCE

It is mandatory to have a list of relevant legislative, statutory, regulatory, and contractual requirements (ISO control A.18.1.1 : Identification of applicable legislation and contractual requirements), including the data : privacy and protection legislation (ISO control A.18.1.4 (Privacy and protection of personally identifiable information)).

e-BO Group only processes personal data for which it can demonstrate a legitimate legal basis. Compliance with data privacy and protection legislation can be demonstrated by an appropriate accountability framework, installed organizational and technical measures and additional ISO 27001:2013 certification.

6.2.3 ASSET MANAGEMENT

ISO 27001 control A.8 (Asset Management) leads to inclusion of personal data as information security assets, having control on which personal data is involved, where to store it, how long, what is its origin, and who has access.

6.2.4 PRIVACY BY DESIGN & DEFAULT

e-BO Group adopts privacy by design & default in the development of products and systems as part of an integral part of information systems across the entire product and service lifecycle. Privacy by design & default is also adopted in the design of new processes and process activities, supported by information systems. The ISO 27001 control A.14 (System acquisitions, development and maintenance) ensures that “information security” is a requirement as functional and technical requirements for the design and build of information systems.

7 DATA BREACH NOTIFICATION

e-BO Group has a data breach assessment, treatment and notification process in place, ensuring “a consistent and effective approach to the management of information security incidents, including communication. The DPPO of e-BO Group is the contact person for all communications on data breaches (privacy@ebo-enterprises.com), as well the contact person towards data privacy authorities and data subjects.

In the business we conduct with our customers, we apply the internal data breach notification process as basis or otherwise defined as part of the processor agreement with our customers to handle data breaches.

8 OUR SUPPLIERS AND COMMISSIONED SUB-CONTRACTORS

e-BO Group informs the customers, acting as controller, on the category of suppliers and commissioned sub-processors. The defined requirements in the processor agreements between e-BO Group and the controller are enforced throughout our commissioned sub-processors and suppliers.

9 TERRITORIAL SCOPE - DATA STORAGE

All personal data where e-BO Group acts as controller or personal data stored, commissioned by the customers as controller, are stored in a secure manner within the EEA and are not transferred outside the EEA, enforced throughout the suppliers and commissioned sub-processors of e-BO Group. Only upon formally written request and decision by the controller, territorial transfers outside de EEA are handled as agreed with the controller, whereas the controller is responsible for the necessary transfer agreements, contractual clauses or Binding Corporate rules with the party the data needs to be transferred to.

The retention of personal data where e-BO Group acts as controller is enforced by the internal e-BO Group retention and deletion policy. The retention of Personal data belonging to the customers and stored by e-BO Group are covered by the retention policies of the controller. If no such retention policy is foreseen by the controller in the processor agreement, the internal e-BO Group retention and deletion policy will be applied.

10 DATA SUBJECT RIGHTS

In the activities where e-BO Group is the controller of the personal data, we organize our policies, guidelines, standards, procedures and instruction in such a way that all data subject rights and freedom rights are respected.

Enhanced right to be informed

Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data. Data subjects, where e-BO Group acts as controller of the personal data, are informed depending on the data subject type, through different channels (e.g. privacy statement, privacy notices on digital touch points, employee data privacy and protection notice).

Right of access

Data subjects have the right to obtain the following:

- confirmation of whether, and where, the controller is processing their personal data;
- information about the purposes of the processing;
- information about the categories of data being processed;
- information about the categories of recipients with whom the data may be shared;
- information about the period for which the data will be stored (or the criteria used to determine that period);
- information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
- information about the existence of the right to complain to the DPA;
- where the data were not collected from the data subject, information as to the source of the data; and
- information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects.
- Additionally, data subjects may request a copy of the personal data being processed.

Right of rectification

Data subjects are entitled to require a controller to rectify any errors in their personal data.

Right to erasure (the "right to be forgotten")

Data subjects are entitled to require a controller to delete their personal data if the continued processing of those data is not justified. Data subjects have the right to erasure of personal data (the "right to be forgotten") if:

- the data are no longer needed for their original purpose (and no new lawful purpose exists);
- the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
- the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
- the data have been processed unlawfully; or
- erasure is necessary for compliance with EU law or the national law of the relevant Member State.

The right to restrict processing

Data subjects have the right to restrict the processing of personal data (meaning that the data may only be held by the controller, and may only be used for limited purposes) if:

- the accuracy of the data is contested (and only for as long as it takes to verify that accuracy);
- the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure);
- the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or
- if verification of overriding grounds is pending, in the context of an erasure request.

Right to object to processing

Data subjects have the right to object, on grounds relating to their particular situation,

- to the processing of personal data, where the basis for that processing is either public interest; or legitimate interests of the controller.
- to processing for the purposes of direct marketing
- to processing for scientific, historical or statistical purposes, , unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right of data portability

Data subjects have a right to:

- receive a copy of their personal data in a structured, commonly used, machine-readable format that supports re-use;
- transfer their personal data from one controller to another;
- store their personal data for further personal use on a private device; and
- have their personal data transmitted directly between controllers without hindrance.

11 COMPLAINT PROCEDURE

You can ask a question or make a complaint about this privacy policy and/or the processing of your personal data by contacting the Data Privacy and Protection Officer. (privacy@ebo-enterprises.com)

DOCUMENT INFORMATION

Filename	Data Privacy and protection Policy- Public		
Revision Number	1.0		
Prepared by	CEO	10/08/2017	signature
Approved by	DPPO	10/09/2017	signature