Group Data Protection
POLICY

Bufab Group

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Bufab Group ("**Bufab**" or "**we**") recognise the importance of protecting the personal data and privacy of the individuals whose personal data we process, and of acting in accordance with applicable data protection and privacy laws. Therefore, this Group Data Protection Policy (the "**Policy**") has been adopted in order to establish essential knowledge and awareness across Bufab regarding data protection and privacy issues.

1.2 The Policy is based on the General Data Protection Regulation applicable within the EU and the EEA (the "**GDPR**")[1] and serves as a framework document, setting down basic principles on processing of personal data, and applies to everyone within Bufab. All employees are obliged to ensure that they understand the Policy and their related responsibilities. If you have any questions relating to the Policy, please contact your local contact for GDPR or your Managing Director.

2. INTERNAL RESPONSIBILITY, ORGANISATION AND REPORTING

2.1 It is the responsibility of the respective Managing Director of each Bufab company to ensure timely compliance with the Policy, all applicable data protection and privacy regulations (including GDPR) relevant for the Bufab company in question.

2.2 Each Bufab company shall appoint an employee (as a general rule the Managing Director) responsible for data protection within the respective company. This function shall be equipped with the resources and authority reasonably necessary to ensure implementation and compliance with applicable data protection regulation as well as monitoring, supporting and training of the same on a continuous basis.

2.3 Each Bufab company is expected to ensure that any individual who has access to personal data, collected or processed by the company, acts in accordance with the Policy. Each Bufab company shall also provide appropriate training to its employees, as needed, on the Policy and applicable laws.

2.4 Any participation in a violation of the Policy or applicable law, including retaliating against an employee who has in good faith reported a potential violation, will be grounds for disciplinary action up to and including termination of employment.

2.5 Any actual or potential violation of the Policy or of applicable data protection and privacy laws must promptly be reported to your local contact for GDPR or your Managing Director.

3. SCOPE OF GDPR

3.1 GDPR applies to personal data, which means information directly or indirectly relating to a living natural person.

3.2 GDPR applies to:

[1] 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).

(a) Companies located in the EU/EEA even if the processing of the data takes place outside the EU/EEA; and

(b) Companies located outside the EU/EEA when the companies market goods or services to individuals in the EU/EEA or engage in monitoring activities of individuals' behaviour in the EU/EEA (such as profiling activities).

3.3 GDPR does not apply to information which is completely anonymous. It does, however, apply to information that has undergone so-called pseudonymisation, i.e. information that can be linked to an individual with the use of another set of information (such as a "key"). Personal data which has undergone encryption, and no longer can be related to a natural person without the encryption key, is considered to be pseudonymised.

4. KEY DEFINITIONS

4.1 "*Controller*" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing. For example, when a Bufab company processes personal data concerning its customers or employees, it is the "controller" of that data.

4.2 "*Personal data*" means any information directly or indirectly relating to an identifiable natural person, such as name, bank details, identification number, location data, digital identifier, biometric data or any information relating to the physical, genetic, mental, economic, cultural or social identity of that individual.

4.3 "*Processing*" means any operation performed on personal data, manually or by automation, such as collection, recording, organisation, viewing, reading, structuring, storage, adaption, use, disclosure by transmission or dissemination.

4.4 "*Processor*" means a natural or legal person which processes personal data on behalf of the controller. For example, if a Bufab company is processing personal data on behalf of another Bufab company, it will be the "processor" with respect to that data.

5. PRINCIPLES OF GDPR

5.1 Basic principles

5.1.1 All processing of personal data taking place within Bufab must be conducted in accordance with the following seven basic principles:

(a) ***Lawfulness, fairness and transparency*** – We will always have a legal basis for our processing and be transparent in relation to the individuals whose personal data we process and, clearly communicate how and why their personal data is being processed.

(b) ***Purpose limitation*** – We will only collect personal data for clearly specified and legitimate purpose(s) and the personal data must be managed in a way that is compatible with the original purpose for which the personal data was collected.

(c) ***Data minimisation*** – We will only collect and process the personal that is actually necessary to fulfil a particular purpose. In other words, we must not

collect personal data on a “nice-to-have” basis or collect superfluous personal data.

(d) ***Accuracy*** – We will take all reasonable steps to ensure that any personal data in our possession is accurate, kept up-to-date and that any inaccurate or outdated personal data shall be deleted or corrected without delay.

(e) ***Storage limitation*** – We will not keep the personal data longer than is necessary to fulfil our purposes. The personal data will be deleted in accordance with our retention routines.

(f) ***Integrity and confidentiality*** – We will ensure that the personal data is processed in a manner which ensures appropriate security and confidentiality of personal data and prevents unauthorised access (such as cyber-attacks) or accidental loss of data.

(g) ***Accountability*** – All our data protection policies and procedures will be properly documented and be provided to data protection authorities upon request.

5.2 Lawful and transparent processing

5.2.1 All processing of personal data must be based on one of the legal grounds stipulated in the GDPR. Before a processing activity is initiated, the legal ground shall be determined and documented. In practice, there are four primary legal grounds which are relevant for Bufab and which establish legitimate reasons for processing of personal data:

(a) ***Performance of a contract*** – Processing of personal data is necessary to fulfil a contract with the data subject, e.g. an employment contract.

(b) ***Legitimate interest*** – In certain cases we have a legitimate interest of processing the personal data. This may be the case when we are processing personal data for direct marketing or business development purposes. When processing is based on this legal ground, a balance of interest test must be conducted where our legitimate interest and the individual’s right to privacy must be weighed against each other. The more extensive the processing activities are, the more compelling reasons are required in order rely on this ground.

(c) ***Legal obligation*** – Processing of personal data may be conducted if it is necessary in order to comply with a legal obligation, for example when we have a legal obligation to file tax income information to tax authorities.

(d) ***Consent*** – In some cases we may obtain an individual’s consent for the processing of his or her personal data. The GDPR stipulates certain requirements in order for a consent to be deemed valid, *e.g.,* it should be documented, specific and freely given. Such requirements shall be carefully considered each time a consent is obtained.

5.3 Categories of personal data that shall be given special protection

Processing of special categories of personal data, such as datarevealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data is generally prohibited and shall not be conducted unless an exception under the GDPR applies. For example, we may process

special categories of personal data if it is required by employment law or if the data subject has consented to the processing.

6. TRANSPARENCY AND INFORMATION

6.1 In order to ensure fair and transparent processing we shall, upon collection of personal data, provide the individual with all information necessary to protect the privacy of the individual and as set forth under the GDPR. The information could be provided, for example, to employees (see Appendix 1 Privacy Notice to Employees), to jobseekers (see Appendix 2 Recruitment Privacy Notice to jobseekers) and via our web pages (see Appendix 3 Newsletter Privacy Notice and Cookie Policy), etc. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6.2 When personal data is collected directly from a data subject, the Bufab company acting as controller must ensure that the data subject is provided with the following information:

(a) *Name and contact details.* The name and contact details of the Bufab company and the function with responsibility for data protection and privacy within that company.

(b) *Purpose.* The purpose for which the data subject's personal data is processed and which legal basis, set out in Section 5.2.1, the Bufab company relies upon for the processing. If the relevant Bufab company later wishes to use the personal data for a purpose other than the one initially specified, the data subject must be provided with information regarding the new purpose prior to processing.

(c) *Recipients.* Any recipients, or categories of recipients, with whom the Bufab company will share the personal data.

(d) *Details of any third country transfers.* If the Bufab company intends to transfer the personal data to a country outside the EU/EEA, this must be stated together with the safeguard relied upon for the transfer (e.g. adequacy decision by the European Commission or "Model Contracts for the transfer of personal data to third countries" adopted by the European Commission).

6.3 To ensure fair and transparent processing of the personal data, the data subject must also be informed of any of the following as far as necessary.

(a) *Contractual or legal necessity.* Whether providing the personal data is necessary under law or in order to enter into/fulfil a contract, and the potential consequences of not providing the personal data.

(b) *Storage time.* Information on how long the personal data will be stored for or, if it is not possible to provide an exact retention period, how the length of storage time will be determined.

(c) *Use of automated decision making.* Whether the personal data will be subject to automated decision-making (including profiling) and necessary information on the process and its possible impact on the data subject.

6.4 *Data subject rights.* The data subjects' rights, e.g., to request access to their personal data, to request its erasure, rectification or restriction, to object to its

processing, to withdraw consent to processing, to data portability, and to lodge a complaint with a data protection authority. When collecting personal data about a data subject from another source than the data subject, the relevant Bufab company should, if possible (without seriously disproportionate effort relative to the personal data concerned), make sure that the data subject is kept informed of the nature and the source of the collected personal data.

6.5 The information should be given to the data subject as soon as possible and no later than the time when the information is used to contact the data subject or, if applicable, disclosed to a third party. The overall maximum time limit for providing the data subject with this information is one month from when the personal data is obtained.

7. RIGHTS OF THE INDIVIDUAL

According to the GDPR, data subjects have certain rights in relation to the processing of their personal data that we must be able to fulfil. All requests from data subjects shall be managed without undue delay and the individuals shall be provided with the information requested at the latest within one month from the receipt of the request.

More specifically, data subjects have the following rights:

Obligation	**Description**
Right to access	The individual has the right to receive a copy of the personal data undergoing processing and certain additional information relating to the processing activity.
Right to rectification	We have an obligation to correct personal data which is inaccurate and outdated upon request from data subjects.
Right to erasure ("Right to be forgotten")	At the request of the individual, we shall erase personal data without undue delay when our retention of the data is not compliant with the requirements of the GDPR, *e.g.*, if the personal data no longer is needed to fulfil the purpose of collection or if retention is not required by law.
Right to restriction	Data subjects may, under certain circumstances, require that the processing of their personal is restricted. This means that we may store the personal data but not process it further without the data subject's consent.
Right to data portability	Data subjects may under certain circumstances require that we provide the data in a commonly used machine-readable format. The individual may also request that we transmit the personal data directly to a new controller.
Right to object	Individuals have the right to object to our processing of personal data where the basis for the processing is our legitimate interest. In case of objection by the individual, we must cease with the processing unless we have compelling legitimate grounds for the processing which override the interests and rights of the individual.

8. CONTROLLER AND PROCESSOR

8.1 Responsibility

It is important for all Bufab companies to identify scenarios (both external and intra-group scenarios) in which they act as controller and as processor, respectively. It is important to understand that companies and central functions within Bufab may act as controller and processor in relation to each other. E.g., when personal data relating to employees is shared between Bufab companies. See the internal document *Personal Data Mapping* for a description of intra-group data flows and the division of responsibilities within the Bufab Group.

8.2 Data protection by design and by default

8.2.1 When acting as a controller the relevant Bufab company must, in respect to each current or proposed data processing activity, implement measures to ensure data protection compliance. For example, the Bufab company should implement appropriate technical and organisational measures which are designed to implement the basic principles described in Section 5.1 above, such as data minimisation and purpose limitation, ("*data protection by design*").

8.2.2 Furthermore, when acting as a controller, the relevant Bufab company must implement appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for the purpose of the processing is processed ("*data protection by default*"). For example, with regard to the amount of data collected, the extent of the processing, the period of storage and data accessibility.

8.3 Data processor agreements

8.3.1 Regardless of whether the relevant Bufab company is acting as a controller and wishes to appoint a processor, or is acting as a processor itself, the Bufab company must enter into a written data processor agreement with the opposite party (e.g., suppliers of services such as IT services, consultants or other companies). For further guidelines on outsourcing and the use of cloud-based services, please consult our CIO at our Global IT function.

8.3.2 We must ensure that the data processor agreement contains the provisions required under the GDPR. Our template agreement for situations where a Bufab company acts as a controller is included in Appendix 4 Template Data Processor Agreement.

8.3.3 We must also enter into data processor agreements where one company within Bufab processes personal data on behalf of another Bufab company. Please be referred to Appendix 5 Data Processor Agreement signed by all companies within the whole Bufab group.

8.4 Records of processing activities

In accordance with the GDPR, all our processing activities shall be listed in an internal record of processing activities. Each Bufab company shall ensure that such record is kept of all of the respective company's personal data processing activities and share it with data protection authorities upon request. The record shall include information on:

(a) The name and contact details of the controller/processor and the function responsible for data protection;

(b) The purposes of the processing;

(c) The categories of data subjects concerned and personal data processed;

(d) The categories of processing conducted on behalf of each controller (in case a Bufab company is acting as processor);

(e) The categories of recipients with whom the personal data may be shared;

(f) Cross-border data transfers (i.e. transfers of personal data outside the EU/EEA) and documentation of suitable safeguards;

(g) The applicable data retention periods; and

(h) A description of the security measures implemented to protect the personal data.

9. DATA SECURITY

9.1 Technical and organisational security measures

We must always have appropriate technical and organisational measures in place to ensure the ongoing confidentiality, integrity, availability, and resilience of our processing activities. When implementing such technical and organisational security measures, we shall consider the technology available, the costs of implementation and the nature, scope, context and purposes of processing. Depending on the nature of the processing these measures may include encryption of personal, limited access rights to systems containing personal data, storage of physical documents in locked archives and back-up systems.

9.2 Personal data breaches

9.2.1 A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that we process (e.g. a cyber-attack, loss of documents containing personal data, sending an email containing personal data to the wrong recipient).

9.2.2 If an employee becomes aware of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, the relevant Bufab company must, without delay, notify the relevant data protection authority and in some cases also notify the data subjects. Where feasible, the personal data breach must be reported to the relevant data protection authority no later than 72 hours after detecting the breach.

9.2.3 If an employee suspects that there has been a personal data breach, see Appendix 6 Personal Data Breach Routine and notify our Global GDPR responsible/our CFO immediately.

9.3 Data protection impact assessment

9.3.1 Where a type of processing (*e.g*. when new technologies will be deployed such as camera surveillance, or when special categories of personal data will be processed) is likely to result in a high risk to the individuals' privacy , the relevant

Bufab company must conduct a data protection impact assessment before commencing the processing. Conducting a data protection impact assessment is an important compliance tool that will allow us to address and mitigate data protection risks before the processing is initiated.

9.3.2 For more information on when and how to conduct a data protection impact assessment, [see Appendix 7 Risk Assessment and Data Protection Impact Assessment and] please contact our Global GDPR responsible/our CFO.

10. DATA ANALYTICS AND PROFILING

Data analytics can be an important tool which makes it possible to discover additional information about data subjects such as customers and employees. However, when using personal data for the purpose of data analytics or profiling, data protection aspects must be considered. This includes application of the basic principles in GDPR, see Section 5.1, as well as other measures such as data protection by design and by default, see Section 8.2.

11. INTERNATIONAL TRANSFERS

11.1 Ensuring adequate protection

We are a global organisation and need to transfer personal data on a global scale. If we transfer personal data to any party in a country outside of the EU/EEA, we must ensure there that the transfer is conducted in accordance with requirements under the GDPR, e.g. enter into Standard Contractual Clauses adopted by the European Commission (a copy of these clauses can be found here) or transfer personal data only to countries which have been deemed to afford adequate protection under its local laws (a list of the EU Commission's adequacy decisions can be found here).

11.2 Exceptions

Nevertheless, we may transfer personal data to a country outside the EU/EEA without an adequate standard of protection in the following circumstances:

(a) *Explicit and informed consent.* The data subject has been informed of the associated risks of such a transfer without adequate protection or safeguards and nevertheless explicitly consents to the transfer;

(b) *Contract.* The transfer is necessary for fulfilling obligations under a contract with the data subject. This can also include preparatory steps that we might make prior to entering into the contract, if done at the data subject's request;

(c) *Legal Claims*. The transfer is necessary for the enactment of legal claims; or

(d) One-off limited transfer for legitimate interests. The transfer is a one-off transfer that:

- concerns a limited number of data subjects;
- is necessary for the relevant Bufab company to pursue a compelling legitimate interest which is not overridden by the rights or interests of the data subjects;

- was done after a careful assessment of the circumstances and with suitable safeguards, both of which are documented; and
- the relevant Bufab company informs the relevant data protection authority of the transfer and also informs the data subject about the transfer and the legitimate interest being pursued.

12. MATERIAL/APPENDICES

Initially, the following appendices provide additional information on data protection within Bufab:

(a) Appendix 1 Privacy Notice to Employees

(b) Appendix 2 Recruitment Privacy Notice

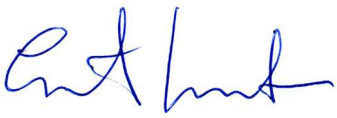
(c) Appendix 3 Newsletter Privacy Notice

(d) Appendix 4 Template Data Processor Agreement (Bufab as Controller)

(e) Appendix 5 Data Processor Agreement

(f) Appendix 6 Personal Data Breach Routine

Erik Lundén, CEO, Bufab Group



Michael Exenberger, CIO