Business & Finance Consulting

GDPR Personal Data Protection Policy

September 2024

Business & Finance Consulting
Max-Högger-Strasse 6
CH-8048 Zürich
Switzerland

+41 44 784 22 22
info@bfconsulting.com
www.bfconsulting.com

INTRODUCTION

In its everyday business operations, Business & Finance Consulting GmbH (BFC) makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees and freelancers
- Clients
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Business & Finance Consulting GmbH (BFC) is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Business & Finance Consulting GmbH (BFC) systems.

PRIVACY DATA PROTECTION POLICY

THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a standout amongst the most noteworthy bits of enactment influencing the way that Business & Finance Consulting GmbH (BFC)does its data preparing exercises. Huge fines are relevant if a break is esteemed to have happened under the GDPR, which is intended to secure the individual information of nationals of the European Union. It is Business & Finance Consulting GmbH (BFC)'s strategy to guarantee that our consistence with the GDPR and other important enactment is clear and verifiable consistently.

GDPR FUNDAMENTAL CONCEPTS

The most important concepts from GDPR regulation that are consistent within our organization and apply properly for this policy are the following:

Personal data is defined as:

> 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;

‘processing’ means:

> 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;

‘controller’ means:

> 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;

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

As per GDPR regulation, 2016 version, there are 7 principles involving personal data and how companies should treat these aspects. These are as follows, as per Chapter II, Article 5.1

1. Personal data shall be:

> (a) processed lawfully, fairly, and in a transparent manner, with clear documentation of the legal basis for each type of processing activity undertaken by the company (‘lawfulness, fairness and transparency’);
>
> (b) 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
>
> (d) 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’);
>
> (e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
>
> (f) 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’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Business & Finance Consulting GmbH (BFC)adheres to these principles through stringent business workflows, which include specific security measures at each step of data handling to ensure the protection of personal data against unauthorized access, alteration, or destruction.based on technology that use metadata in order to search, discover, classify, label, protect and apply actions at all levels of personal data. Also, Operational Security Procedures defined support and provide the specific guidelines for all business units involved including Finance, Talent Management, Business Development, Project Management, Marketing & PR.

OUR STAFF RESPONSIBILITIES

Any staff member of Business & Finance Consulting GmbH (BFC)who is involved in the collection, storage or processing of personal data has responsibilities under the legislation.

Any staff member involved in the processing/storing of personal data should make sure:

- to obtain and process personal data fairly.
- to keep such data only for explicit and lawful purposes.
- to disclose such data only in ways compatible with these purposes
- to keep such data safe and secure.
- to keep such data accurate, complete and up-to-date.
- to ensure that such data is adequate, relevant and not excessive.
- to retain such data for no longer than is necessary for the explicit purpose.

Any data access requests received should be forwarded immediately to the Manager of Compliance & Privacy Management.

RIGHTS OF THE INDIVIDUAL

Each data subject has specific rights under the GDPR, as listed below. Detailed procedures on how these rights can be exercised are available upon request and are provided to data subjects at the time of data collection. The rights consist of::

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within Business & Finance Consulting GmbH (BFC)that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown below:

Data Subject Request	Deadline
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling.	Not specified

CONSENT

Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. Transparent information about our usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data is not obtained directly from the data subject then this information must be provided within a reasonable period after the data are obtained and definitely within one month.

PRIVACY BY DESIGN

Business & Finance Consulting GmbH (BFC) rigorously applies the principle of privacy by design, systematically incorporating data protection and privacy considerations into the planning and operation of all new or significantly altered systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymization should be considered where applicable and appropriate.

TRANSFER OF PERSONAL DATA

Transfers of personal data outside the European Union are subjected to thorough reviews to ensure compliance with GDPR. This includes assessing the adequacy of protections in the recipient country as determined by the European Commission.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

DATA PROTECTION OFFICER

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on current operational and data processing criteria, BFC GmbH does not require the appointment of a Data Protection Officer. However, this requirement is subject to annual review, and adjustments will be made based on any changes in regulatory requirements or business operations.

BREACH NOTIFICATION

It is Business & Finance Consulting GmbH (BFC)'s policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. Breach notifications are managed in strict accordance with our comprehensive Information Security Incident Response Procedure, which outlines specific steps and responsibilities for rapid response and mitigation of any data breaches.

Under the GDPR the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million Euros, whichever is the higher, for infringements of the regulations.

ADDRESSING COMPLIANCE TO THE GDPR

The following actions are undertaken to ensure that Business & Finance Consulting GmbH (BFC) always complies with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for
- following good data protection practice
- All staff receive mandatory data protection training upon induction and annually thereafter, with the training program updated regularly to reflect the latest data protection standards and practices

- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal
- data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- Comprehensive documentation of all data processing activities is maintained and regularly updated, reflecting any changes in processing activities or compliance requirements. This documentation is reviewed bi-annually by the compliance team:
    - Organization name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organizational controls in place

These compliance actions undergo a structured review semi-annually as part of the management review process, ensuring ongoing alignment with GDPR and other relevant data protection legislation.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Amendment to EU GDPR Compliance Policy in Accordance with the New Federal Act on Data Protection (FADP) Effective September 1, 2023

Key Changes in the New Swiss Data Protection Law (revDSG)

As per the **revised Swiss Data Protection Act (revDSG)**, which came into effect on **September 1, 2023**, several significant updates have been made to align data protection practices with evolving technology and the European Union's **GDPR**.

1. **Focus on Natural Persons' Data Protection**:

   We have updated our internal data management policies to focus solely on the **protection of personal data of natural persons**. All staff have been trained to ensure compliance with the revised regulations, which no longer apply to legal persons.

2. **Handling of Sensitive Personal Data**:

   Sensitive data has been classified separately and is now subject to enhanced protection measures. We have implemented **strict access control** to safeguard this data and prevent unauthorized use.

3. **Conducting Data Protection Impact Assessments (DPIAs)**:

   DPIAs have been made mandatory for all projects involving high-risk data processing activities. A risk assessment team has been established to evaluate and manage any potential impacts on individual privacy or rights.

4. **Transparency and Information Obligation**:

   Our **privacy policies** have been revised to ensure full transparency in data collection and processing. Clients and users can be informed of the purpose and scope of data usage, with updated privacy notices accessible on all our platforms.

5. **Reporting Data Breaches**:

   A formal **data breach response plan** has been implemented. In the event of a breach, we now promptly notify the **Federal Data Protection and Information Commissioner (FDPIC)** and take immediate corrective action to mitigate risks.

6. **Artificial intelligence (AI):**

   The company's use of **artificial intelligence (AI) technologies**, in any capacity, is subject to strict compliance with the revised Data Protection Act (revDSG). This ensures that all AI-related activities are carried out responsibly, ethically, and with full transparency, upholding the stringent data protection standards set forth in the legislation.