



## PRIVACY POLICY

### Introduction

At bf1systems we are committed to protecting and respecting your privacy. Please read this Privacy Policy carefully as it provides guidance on the basis on which we collect, store, and process your personal data.

In this Privacy Policy, a reference to “you” means the person whose personal information we collect, use and process. We will use your personal data only for the purposes and in the manner set out below to ensure we process any of your personal data is in compliance with the Data Protection Acts 1998 and 2018 and the General Data Protection Regulation (the “GDPR”) and any subsequent amendments to data protection legislation.

By using our website, you agree to the collection, use and transfer of the information you provide to us in line with this Privacy Policy. We will update this Policy from time to time as the need arises.

### Data Controller – Contact Details

For the purposes of the Data Protection Legislation, the Data Controller is bf1systems Limited, which is registered with the ICO with registration number ZA664037.

### Information we collect, hold and how we use it

This Privacy Policy applies to personal information that we collect, you have provided to us, use, and otherwise process about you in connection with your relationship with us as a customer or potential customer, potential employee, or supplier.

We may collect and process the following but are not limited to:

- ✓ Personal information - name, gender
- ✓ Contact details – business or personal address, email, phone number;
- ✓ Financial information – purchase order details and payment details
- ✓ IT information –login information

It is unlikely that we will need to collect Sensitive Personal Information about you unless you apply to an advertised vacancy via our website. **Sensitive Personal Information** is defined as your racial or ethnic origin, religious, political, or philosophical beliefs, genetic data, and biometric data for the purposes of unique identification, trade union membership or information about your health/sex life and personal information relating to criminal convictions or offences. However, in some circumstances we may need to collect or request voluntarily some Sensitive Personal Information for legitimate purposes.

## How do we use your personal information?

The main purposes for which we use your personal information are:

- to provide you with information about our products, services, and systems;
- to carry out our obligations arising from any contracts between us;
- to ask you to partake in our customer surveys, to improve our customer service or make other services available to you;
- to help us develop and market other products, services, and systems;
- to answer your technical and support queries;
- to third parties in order that we comply with all legal and regulatory requirements.

## Purposes for processing personal information

- where you have given your consent to the processing of your personal data;
- to enable us to perform our obligations under any contract with you;
- for legitimate interests provided these are not overridden by your interests and fundamental rights and freedoms e.g., to respond to your enquiries;
- where we must comply with a legal obligation to disclose your personal information to a government and/or regulatory bodies and other third parties where required to do so by applicable law, e.g., to comply with a court order, for taxation purposes etc.;
- In the event of a merger, acquisition, or any form of sale of some or all of our assets to a third party, we may also disclose your personal information to the third parties concerned or their professional advisors. In the event of such a transaction, the personal information held by bf1systems will be among the assets transferred to the buyer.

## Data Retention

Your personal data will not be kept for longer than is necessary to fulfil the specific purposes outlined in this Privacy Policy and to allow us to comply with our legal requirements, including, without limitation, any tax, and commercial obligations.

The criteria we use to determine data retention periods include the following:

- In case of queries - we may retain your personal data for a reasonable period after you have enquired about our products and services, in case of a follow up query from you.
- In case of claims - we may retain your personal data for the period in which you might legally bring claims against us (this means we will retain it for at least 7 years) if and to the extent this is relevant.
- In accordance with legal and regulatory requirements - we will consider whether we need to retain your personal data after the period of retention in the case of queries or claims (above) because of a legal or regulatory requirement. Some or all of these criteria may be relevant to retention of your personal data collected from you in connection with our products and services.

- Permitted under applicable law - we will continue to retain personal data where necessary to provide our products and services to you and where the retention of such personal data is necessary for the purposes of pursuing our legitimate interests or where it is necessary for public interest purposes.

Please note that, although reasonable efforts will be taken, it may not always be possible to completely remove or delete all of your personal information from our databases because of back-ups and other technical reasons. Where this is the case, we will take steps to ensure that your personal data is suppressed in order to render it unusable.

## Your data privacy rights

You may exercise the rights available to you under data protection laws as follows:

1. The right to **withdraw your consent** to the processing of your personal data. However, we may continue to process your personal information if there is an alternative legal basis for the processing;
2. The right to **request access** to or obtain a copy of the personal data we hold about you. Any request will be processed within 30 days in accordance with the GDPR;
3. The right to **rectification** including to require us to correct inaccurate personal data;
4. The right to request **restriction of processing** concerning you or to object to processing of your personal data if processing is based on legitimate interests or direct marketing etc.,
5. The right to request the **erasure** of your personal data where it is no longer necessary for us to retain it;
6. The right to **data portability**; and
7. The right to object to **automated decision making** including profiling (if any) that has a legal or significant effect on you as an individual;
8. The right to complain to a data protection authority e.g., the Information Commissioners Office (ICO) if you consider that we have infringed applicable data privacy laws when processing your personal data.

## Security

We endeavour to use appropriate technical and physical security measures to protect your personal data, which is collected, stored, or otherwise processed by us, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access. These measures include storing personal data in a secure database which is protected with the username and password of our authorised users. Our service providers are also selected carefully and required to use appropriate protective measures.

As effective as modern security practices are, no physical or electronic security system is entirely secure. The transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted over the internet. Any transmission of data is at your own risk. Once we receive your data, we will use appropriate security measures to seek to prevent unauthorised access. We will continue to revise policies and implement additional security features as new technologies become available.



In the event that there is an interception or unauthorised access to your personal data, we will not be liable or responsible for any resulting misuse of your personal information.

We may monitor the use and content of emails, calls and secure messages sent from and received by us so that we can identify and take legal action against unlawful or improper use of our systems e.g., transmitting computer viruses and attempts to prevent our website or other systems from working.