Fraud Business SolutionsPrivacy Policy – Fraud Business Solutions

Introduction

Fraud Business Solutions (FBS) is committed to protecting and respecting your privacy. We collect information about individuals ("**Data**") when they use our website and services. This privacy policy describes how we collect, use and disclose Data. References in this Policy to "FBS", "us", "Our" and "we" mean Fraud Business Solutions.

Please read the following carefully to understand our use of personal data. Please note that the Privacy Policy "Policy" relates only to living individuals and personal data relating directly to themselves, and not to persons in any other capacity.

**Personal data is data relating to a living individual who can be identified, or is identifiable, using this data or if this data is used in conjunction with other data that is in Fraud Business Solutions possession, or could come into its possession.*

Our Products and Services

FBS provide tailored consultancy solutions for its clients that cover the area of in house or off-site fraud awareness training, risk assessments and internal investigations. The focus of our work is around internal or staff malpractice.

Who is the Data Controller?

For the purposes of Data Protection Laws, FBS, Newbridge, Co Kildare are the Data Controller covered by this policy.

How can you contact the controller?

Email info@fraudbusinesssolutions.com or phone +353 876259071

Information we may collect from you

When you use the Website: We will collect any personal data that you choose to send to us or provide to us. If you submit your personal data to us (e.g. using the contact form; registering for a training event): We use your personal data for purposes made clear to you at the time you submit your information.

When you engage as a client of Fraud Business Solutions: We receive and store personal data that you provide directly to us. The types of personal data we may collect directly from you include: names, email addresses, postal addresses, phone numbers, job titles, transactional information (including invoices due / paid), as well as any other contact or other information they choose to provide us in connection with our engagement.

How do we use your Personal Data?

Services: We may use the information we collect from our customers in connection with the services we provide (e.g. mailing list signup; training registration) for a range of reasons, including to:

- Provide, operate and maintain the services we offer;
- Process and complete transactions, and send related information, including transaction confirmations and invoices;
- Manage our customers' use of the services, respond to enquiries and comments and provide customer service and support;
- Send customers technical alerts, updates, security notifications, and administrative communications;
- Investigate and prevent fraudulent activities, unauthorized access to the services, and other illegal activities; and
- For any other purposes about which we notify customers and users.

The legal basis for this processing will range from contract (performance, establishment, or legal defence of a contract between us and you), consent, and legitimate business interest.

Where you have provided your consent, we may also use the information you send to us via the website and/or services, to communicate with you via email and, possibly, other means, regarding products, services, offers, promotions and events we think may be of interest to you or to send you our newsletter.

You will always be able to opt-out of such communications at any time using a one-click UNSUBSCRIBE option within every marketing email.

Unless we tell you differently and you consent, our 3rd parties do not have any right to use the personal data we share with them beyond what is necessary to assist us. We do not rent or sell your personal data to anyone.

Vendors, consultants and other service providers*:* We may share your information with third party vendors, consultants and other service providers who we employ to perform tasks on our behalf. These companies include, email platform (e.g. Microsoft Office 365), mail service providers (e.g. MailChimp), event registration providers (e.g. Event Brite) and others. Appropriate controls are in place to ensure data is only disclosed to these 3rd parties in compliance with data protection law.

Unless we tell you differently and you consent, our 3rd parties do not have any right to use the personal data we share with them beyond what is necessary to assist us.

Security and where we store your personal data

We use appropriate technical, organisational and administrative security measures to protect any information we hold in our records from loss, misuse, and unauthorized access, disclosure, alteration and destruction.

For example, on our website:

- Uses regular Malware Scanning on our site to confirm it is safe to use.
- Uses a range of security tools to monitor activity on the site and identify unusual activity.
- Your personal information is only accessible to a limited number of persons who have special access rights to such systems and are required to keep the information confidential.
- In addition, all information you supply through the website is encrypted via Secure Socket Layer (SSL) technology between your browser and the site.

In terms of local devices, FBS, has implemented a range of security measures to protect the information we hold in our records. For example:

- All devices (including backup devices) use disk encryption so data is secure at rest.
- Devices automatically lock after a short period of inactivity to reduce the risk of unauthorised access.
- Devices are 'patched' (updated with the latest security updates) on a regular basis.

The 3rd party service providers who we employ to perform certain tasks also commit to implementing appropriate security measures to protect the data that we disclose to them.

Unfortunately, no company or service can guarantee complete security. Unauthorised entry or use, hardware or software failure, and other factors, may compromise the security of user information at any time.

How long do we retain your data?

Different types of personal data is retained for different periods of time. For example, we will hold any investigation material for a period that covers any possibility of a court case or tribunal.

At a high level, personal data is retained for only as long as FBS has a legitimate basis to retain the data. This could include

- Personal data you provide when signing up for our email marketing lists is retained until such time as you unsubscribe. After you unsubscribe, we retain minimal information to ensure we do not forget that you have unsubscribed.
- Personal data provided as part of a contract between us and that we require to establish, perform, or defend a legal action relating to the contract is retained for a period of 7 years after the contract has ended.

Disclosure of your information

Disclosures for National Security or Law Enforcement: Under certain circumstances, we may be required to disclose your personal data in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

Is personal data transferred outside the EEA?
Yes. A small number of our 3rd party service providers explicitly state that they transfer personal data outside of the EEA.
The service providers are listed below, along with their legal basis for each transfer:

- **MailChimp** (email automation): EU-US Privacy Shield.
- **Event Brite** (event registration): EU-US Privacy Shield.
- **Google Analytics** (website analytics) – EU-US Privacy Shield.

Your rights

As an individual, under EU law you have certain rights to apply to us to provide information or make amendments to how we process data relating to you. These rights apply in certain circumstances and are set out below: -
1. The right to access data relating to you ('access right').
2. the right to rectify/correct data relating to you ('right to rectification').
3. The right to object to processing of data relating to you ('right to object').
4. The right to restrict the processing of data relating to you ('right to restriction').
5. The right to erase/delete data relating to you (i.e. the "right to erasure"), and
6. The right to 'port' certain data relating to you from one organisation to another ('right to data portability').

How to exercise your rights

Please contact us at info@fraudbusinesssolutions.com and provide us with as much information as possible to enable us to complete your request.
Right to complain

If you believe FBS is breaching your data protection rights, you have the right to complain to the data protection authorities. In Ireland, this is the Office of the Data Protection Commissioner (Click here to visit the ODPC's website).

Changes to this policy

We reserve the right to change this Policy from time to time in our sole discretion. If we make any changes, we will post those changes here so that you can see what information we gather, how we might use that information and in what circumstances we may disclose it. By continuing to use our site or our services or otherwise provide data after we post any such changes, you accept and agree to this Policy as modified.