

Data Protection Policy

Table of Contents

Data Protection Officer
Commencement

Our Use(s) Of Personal Data and our Purpose(s)
Our Specific Data Protection Measures

Section A: Overview
Section B: Data Protection Principles
Section C: Data Subject Rights
Section D: Our Other Obligations

This Policy has been approved and authorised by:

Name: Nigel Freemantle
Position: Managing Director
Date: 25th May 2018
Due for Review by: 25th May 2019

Signature:

Data Protection Officer

Our data protection officer is Julie Abbott who can be contacted by email at privacy@brandfusionltd.co.uk

Commencement of this policy

This Policy shall be deemed effective as of 25th May 2018; however, it will not have effect retrospectively and will apply only to matters occurring after this date.

Our specific data protection measures

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- our own servers;
- any third-party servers;
- email accounts;
- desktops and laptops;
- potential backup storage; and/or
- paper files.

In relation to our use of personal data we take the following measures:

Erasure, destruction and or deletion	<p>We shall delete confidential or sensitive records categorised as requiring high protection and very high protection. We may either delete or anonymise less important documents.</p> <p>The destruction of confidential, financial, and personnel-related records shall be securely destroyed electronically or by shredding if in paper files. Non-confidential records or records not containing personal data may be destroyed by recycling.</p>
Transmission via email	<p>We use the Google G Suite email system which is fully GDPR compliant. All email accounts are password protected.</p>
Transmission of hard copies	<p>Any confidential or sensitive data is scanned and uploaded directly to a designated email account which is password protected, or if being sent by post or courier, it is marked for the attention of the intended recipient and marked private and confidential.</p>
Transmission via networks	<p>Third party servers and networks are password protected, secure 'closed' systems which only authorised users have access to.</p> <p>Any locally held servers operate via a VPN (Virtual Private Network) connection. A VPN provides a connection which is encrypted and secure and allows for our data traffic to be anonymous online and kept private and safe.</p> <p>Servers are located in data centres and/or cabinets that are physically secure with permitted access only by authorised personnel.</p>
Storage of emails and email content	<p>We use the Google G Suite email system and all emails and any data are stored in line with Google's GDPR compliance policies and procedures.</p> <p>Emails downloaded onto local hard drives or</p>

	servers are password protected with access only by authorised personnel.
Access of employees	We require all employees to respect the security of any personal or sensitive data and to treat it in accordance with the law and our policies on data protection and privacy.
Access of third parties	All third parties must demonstrate their compliance with security obligations equivalent to those imposed on them under the GDPR, by way of written and published policies (or a legally binding contract issued in-line with our own GDPR policy and procedures).
Storage of hardcopies	Locked and secure filing cabinets and archive storage are used to store all sensitive data. Access to personal information is limited to those employees, agents, contractors and other third parties who have a business need to know and treat it in accordance with the law and our own policies on data protection and privacy.
Storage of electronic copies	Storage is on HDD, servers and third party systems, all of which are password protected. Access is limited to those employees, agents, contractors and other third parties who have a business need to know and treat it in accordance with the law and our own policies on data protection and privacy.
Sharing	Any personal information is only shared with those employees, agents, contractors and other third parties who have a business need to know. We require all parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.
Sub-processing	A third party shall not engage another processor ('Sub-processor') in processing of the Personal Data without the written consent of the Controller. The Processor shall inform the Controller of any intended changes concerning addition or replacement of any Sub-processors, and the Controller has the right to object to such changes. Personal data will only be transferred to a data processor if there is agreement by them to comply with our procedures and policies, or if there are adequate measures in place.

Viewing on systems and devices	All authorised persons must ensure that individual monitors do not show confidential information to passers-by and that they log off from their system when it is left unattended.
Passwords	All locally accessed electronic devices and remote servers are password protected. Access to any password is limited to only those employees and certain third parties who have a business need to know and treat it in accordance with the law and our own policies on data protection and privacy.

Our use of personal data and our purpose

We may collect, hold and/or process the following personal data:

- information you put into electronic and written forms or surveys any time, including your personal contact details such as name, title, addresses, telephone numbers and email addresses and bank account details;
- a record of any correspondence between us;
- details of any transactions carried out;
- details of your visits to our website and the resources you use; and
- information about your computer (e.g. your IP address, browser, operating system, etc.) for system administration.

How we will use information about you

Under GDPR we will ensure that your personal data is processed lawfully, fairly, and transparently, without adversely affecting your rights. We will use your personal information only when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- when processing is necessary for the performance of a contract to which you are a party or in order to take steps at the request of you prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which we are subject;
- processing is necessary for the purposes of the legitimate interests pursued by us or by a third party such as our credit card payment processing, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

We may also use your personal information in the following situations, which are likely to be rare:

- where we need to protect your interests (or someone else's interests);
- where it is needed in the public interest or for official purposes.

Section A: Overview

1. The reason for this policy

1.1 You have legal rights with regard to the way your personal data is handled.

1.2 In the course of our business activities we collect, store and process personal data about our customers, suppliers and other third parties and therefore, in order to comply with the law and to maintain confidence in our business, we acknowledge the importance of correct and lawful

treatment of this data.

- 1.3 All people working in or with our business are obliged to comply with this policy when processing personal data.

2. Introduction

- 2.1 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects; for example customers and business contacts, or personal data that is provided to us by data subjects or other sources.
- 2.2 In this policy when we say 'you' or 'your' we are generally referring to the data subjects unless the context requires otherwise.
- 2.3 It also sets out our obligations in relation to data protection under the General Data Protection Regulation 2016 ('the **GDPR Rules**').
- 2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.
- 2.5 We agree to ensure that all of our directors, employees, consultants and agents comply with this policy.
- 2.6 We aim to ensure the correct, lawful, and fair handling of your personal data and to respect your legal rights.

3. The meaning of key data protection terms

- 3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.
- 3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
- 3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.
- 3.4 **Data controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.
- 3.5 **Processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4. Summary of the data protection principles

This Policy aims to ensure compliance with the GDPR Rules. The GDPR Rules set out the following principles with which any party handling personal data must comply. All personal data must be:

- a) **Processed fairly and lawfully** – it must be processed fairly and lawfully and it must be processed - in relation to you as the data subject - in a transparent manner;
- b) **Processed for limited purposes and in an appropriate way** - the purposes for which it is collected must be explicit, specified and legitimate;
- c) **Adequate, relevant and not excessive for the purpose;**

- d) **Accurate** – as well as being accurate it must be kept up to date with inaccurate data deleted;
- e) **Not kept longer than necessary for the purpose;**
- f) **Processed in line with data subject's rights;**
- g) **Security** – there must appropriate technical or organisational measures to ensure appropriate security.

In addition, personal data must not be transferred outside the European Economic Area (the “EEA”) without adequate protection.

Section B: Data Protection Principles

5. Notifying data subjects

5.1 As part of complying with the principles in paragraph 4 above, if you provide us with personal data we will always try to tell you:

- 5.1.1 the purpose or purposes for which we intend to process that personal data;
- 5.1.2 the types of third parties, if any, with which we will share or to which we will disclose that personal data;
- 5.1.3 how you can limit our use and disclosure of the personal data;
- 5.1.4 if we receive personal data from other sources.

6. Lawful, fair and transparent data processing

The GDPR Rules are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting your rights. The processing of personal data is lawful if one (or more) of the following applies:

- a) **(Consent)** the data subject has consented for a specific purpose;
- b) **(Contract)** if the data subject requests the processing with a view to entering into a contract or the processing is necessary for the performance of a contract;
- c) **(Legal Obligation)** if the processing is necessary for the compliance with a legal obligation to which the data controller is subject;
- d) **(Protection)** processing is necessary to protect your vital interests or those of another natural person;
- e) **(Public Interest)** it is in the public interest for a task to be carried out which requires such processing, or the task is to be carried out as a result of the exercise of any official authority held by the data controller;
- f) **(Legitimate Interests)** for the legitimate interest of the data controller or the party to whom the personal data is disclosed.

7. Processed for limited purposes and in an appropriate way

- 7.1 In the course of our business, we may collect and process the personal data set out above. This may include personal data we receive directly from you (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).
- 7.2 We will only process personal data for the specific purposes set out above or for any other purposes specifically permitted by the GDPR Rules. We will notify those purposes to you when we first collect the personal data or as soon as possible thereafter.

8. Adequate, relevant and not excessive for the purpose

We will only collect and process personal data for the specific purpose(s) set out above.

9. Accuracy of data and keeping data up-to-date

We will keep your personal data accurate and up-to-date. We will check its accuracy regularly. When we find inaccurate or out-of-date data we will take reasonable steps to amend or erase that data. It is important that you let us know as soon as possible of any changes to your personal information, so we can amend our records accordingly.

10. Timely processing

We will only keep your personal data for a period of time which we judge is relevant and necessary, taking into account the purpose(s) of collecting the personal data which are specified above.

11. Processing that is secure

In addition to the measures above:

- 11.1 we will make sure that the personal data we collect is securely kept and we stop unauthorised processing and prevent its loss, destruction or damage;
- 11.2 we will ensure that only people who are authorised to use personal data can access it and that we have entry controls to our premises and systems, lockable filing cabinets and cupboards for confidential personal data and destruction of hard copy documents and digital storage devices;
- 11.3 All authorised persons must ensure that individual monitors do not show confidential information to passers-by and that they log off from their system when it is left unattended.

Section C: Data Subject Rights

12. You, as a data subject, have the right to information about:

- a) who we are;
- b) the purpose(s) of collecting your personal data and the legal basis for collecting it and what our legitimate interest is for processing your personal data;
- c) the categories of personal data collected and where it is to be transferred, especially if outside the EEA;
- d) the length of time we hold personal data (or, where there is no predetermined period, details of how that length of time will be determined);
- e) your rights as a data subject including your right to withdraw your consent to processing, the right to complain to the Information Commissioner and also things such as details of any legal requirement for processing personal data that may exist and any automated decision-making that we carry out.

We will try to provide this information when we collect the personal data or, if we collect the personal data from another party, when we communicate with you after the personal data is received.

13. Data subject access

- 13.1 You may request access to any data held about you by us. This is called a subject access request ('SAR').
- 13.2 We reserve the right to charge reasonable fees for onerous or repetitive requests.
- 13.3 Data subjects must make a formal request for information we hold about them. This must be made in writing.
- 13.4 When receiving telephone enquiries, we will only disclose personal data we hold on our

systems if the following conditions are met:

- a) we will check the caller's identity to make sure that information is only given to a person who is entitled to it, and/or
- b) we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14. Accuracy of personal data: right to rectification

- 14.1 We will do our best to ensure that all personal data held about you is accurate and complete. We ask that you notify us of any changes to information held about you.
- 14.2 You have the right to request that any incomplete or inaccurate information held about you is rectified and to lodge a complaint with us and the Information Commissioner's Office (ICO).
- 14.3 We will respond to requests to rectify within one month.

15. Right to be forgotten

You have the right to request the deletion or removal of personal data. However, requests for erasure can be rejected in certain circumstances.

16. Right to restriction of processing

You can block the processing of your personal data. This means we may be able to store it, but cannot process it further without consent. Restricting data is required where the accuracy of data is challenged - but only until the accuracy has been verified.

17. Right to data portability

- 17.1 If you have provided personal data to us, you have the right to transfer it from us to someone else.
- 17.2 If you request it, we may be required to transmit the data directly to another organisation if feasible. We must respond without undue delay and within one month, or two months if the request is complex.

18. The right to object

You have a right to object to the processing of your data. We must stop processing unless we can demonstrate a legal ground for the processing.

19. Automated decision-making

- 19.1 You have the right not to be subject to a decision based on automated processing and it produces a legal effect or other significant effect on you.
- 19.2 You can request human intervention where personal data is processed using automated decision-making and can ask for an explanation of the decision to use automated decision-making.

20. Profiling

If we use your personal data for profiling purposes:

- a) we will give you information fully explaining the profiling which will be carried out, including its importance and the likely results of that profiling;
- b) we will make sure that appropriate mathematical or statistical procedures will be used;
- c) we will implement technical and organisational measures which are required to minimise the risk of mistakes and to enable such mistakes to be easily corrected; and
- d) we will make sure that all personal data processed by us for profiling purposes will be kept secure so as to avoid discriminatory effects resulting from such profiling.

Section D: Our Other Obligations

21. How we deal with personal data internally

We will:

- a) train our employees in relation to our responsibilities under the GDPR Rules;
- b) ensure that only appropriately trained, supervised and authorised personal have access to personal data held by us; and
- c) regularly evaluate and review our collection and processing of personal data and the performance of employees and third parties working on our behalf to ensure that it is in accordance with the GDPR Rules.

21.1 We will keep internal records of personal data that we collect and process including, in relation to that personal data, details of the categories, any transfers, our security measures, our purpose of collection and the duration of retention of that personal data. We will also retain details of all third parties that either collect your personal data for us or that we use to process your personal data.

21.2 As required by law, we will carry out privacy impact assessments for any project where the processing of data is likely to result in a high risk to the individual.

22. Transferring personal data to a country outside the EEA

We may transfer personal data to countries outside of the EEA; however, we will ensure that the transfer is:

- a) to a place that the EU has judged to provide adequate levels of protection for personal data;
- b) to a place that provides adequate safeguards under either an agreement with a public body, rules that bind companies or standard data protection clauses adopted by the EU or some other form of approved code of conduct approved by a supervisory authority or certification or other contractual clauses or regulatory provisions;
- c) necessary for the performance of a contract between you and us, or with a view to creating that contract;
- d) made with your consent;
- e) necessary for important public interest reasons, legal claims, to protect your vital interests.

23. Notification of personal data security breach

23.1 If a personal data security breach occurs, we will manage and respond to it effectively in accordance with GDPR and it must be reported immediately to our Data Protection Officer.

23.2 We will notify the Information Commissioners Office (**ICO**) and any data subject of personal data security breaches to the extent we are required to do so by GDPR.

23.3 If disclosure is not required by GDPR, we will nevertheless investigate closely all the circumstances surrounding the breach and examine the seriousness of the breach and the benefits that might be obtained by disclosure (such as limiting risks of fraud), and we will give careful consideration to any decision to notify the ICO or you, especially if your rights and freedoms as data subjects are affected.