responsebusinessfinance.co.uk
22 Walker Avenue, Milton Keynes, MK12 5TW
+44 (0)3333 580 444

# 1 Purpose Response Business Finance - GDPR Policy

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018.

It replaces the Data Protection Directive 95/46/EC and was designed to reshape the way organisations approach data privacy.
Its aim is to harmonise data privacy laws across Europe.

**DEFINITIONS**

**Personal Data**

"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The special categories of personal data are personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership.

They also include the processing of:

- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health;
- Data concerning a natural person's sex life or sexual orientation.

**Sensitive Personal Data**

"Sensitive Personal Data" is personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).

**Data relating to Criminal Offences**

Data relating to criminal offences and convictions may only be processed by national authorities. National law may provide derogations, subject to suitable safeguards. A comprehensive register of criminal offences may only be kept by the responsible national authority. Data relating to criminal offences are therefore treated separately from Sensitive Personal Data.

responsebusinessfinance.co.uk
22 Walker Avenue, Milton Keynes, MK12 5TW
+44 (0)3333 580 444

# 1 Purpose Response Business Finance - GDPR Policy

**Anonymous Data**

Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) by any means or by any person.

The GDPR does not apply to data that are rendered anonymous in such a way that individuals cannot be identified from the data.

**Pseudonymous Data**

Some sets of data can be amended in such a way that no individuals can be identified from those data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

A good example of pseudonymous data is coded data sets used in clinical trials.

Pseudonymous data are still treated as personal data because they enable the identification of individuals (albeit via a key). However, provided that the "key" that enables re-identification of individuals is kept separate and secure, the risks associated with pseudonymous data are likely to be lower, and so the levels of protection required for those data are likely to be lower.

**Processing**

"Processing" means any operation or set of operations performed upon personal data or 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.

**Data Controller**

"Controller" means the natural or legal person, public authority, agency or any 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 processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.

**Data Processor**

"Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

**Consent**

In general, the validly obtained consent of the data subject will permit almost any type of processing. "The consent of the data subject" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

**Data Breach**

"Data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Notice of a Breach**

Under the GDPR, we as Data Processors will be legally obligated to notify our clients of a Data Breach where said breach is likely to "result in a risk for the rights and freedoms of individuals".

If, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This must be done within 72 hours of first having become aware of the breach.

**Data Breaches concerning Health (both Physical & Mental Health)**

The idea that health data should be treated as Sensitive Personal Data is well-established.

"Data concerning health" means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status. It expressly covers both physical and mental health.

responsebusinessfinance.co.uk
22 Walker Avenue, Milton Keynes, MK12 5TW
+44 (0)3333 580 444

**The Client's Right to Access Data**

As Data Subjects, clients will have the right to ask us for confirmation as to whether or not personal data concerning them is being processed and for what purpose.

A copy of the information being held for processing will be provided to our clients freely, in an electronic format. The Client's Right to be Forgotten.

**Clients will have the right to be "forgotten".**

This means, in layman's terms, that Data Subjects have the authority to request that we erase their personal data.

The GDPR goes further and also places an obligation on us to cease further dissemination of the data, and potentially have third parties halt processing of the same.

The data will be erased on the condition that (a) it is no longer relevant to original purposes for processing; or (b) the Data Subject withdraws consent for us to use the data.

We are further required to compare the Data Subjects' rights to "the public interest in the availability of the data" when considering such requests.

**Data Portability**

GDPR introduces data portability.

This means that our clients have the right to request the data we hold against them and then transfer that data to another - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

responsebusinessfinance.co.uk
22 Walker Avenue, Milton Keynes, MK12 5TW
+44 (0)3333 580 444

responsebusinessfinance.co.uk
22 Walker Avenue, Milton Keynes, MK12 5TW
+44 (0)3333 580 444

**Privacy by Design**

Privacy by design as a concept is now a legal requirement with the GDPR. Regular Privacy Impact Assessments (PIAs) are part of our contingency plan for ensuring data protection.

We, as Data Controllers, are obligated to "implement appropriate technical and organisational measures in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects."

Article 23 calls for us, as Data Controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

**Data Protection Officers**

DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

As such, RBF will not be required to appoint a DPO.

**Cyber-Security Preparedness**

This is an issue that is front and centre in the news currently following accusations against Cambridge Analytica and Facebook.

Personal data breaches are likely to be one of the major catalysts for many investigations by the Information Commissioner.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

The government's Cyber Aware programme provides cyber security advice for small businesses and individuals. We highly recommend you familiarise yourself with these resources.

**Data Preparation and Integrity**

We are now required to provide the personal data in a structured commonly used and machine readable form.

The GDPR explicitly refers to pseudonymisation and encryption of data as potentially appropriate mechanisms for ensuring the security of personal data. Amongst other measures it mentions are:

(1) ensuring the ongoing confidentiality, integrity, availability and resilience of your processing systems and services;

(2) having the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

(3) having a process for regularly testing, assessing and evaluating the effectiveness of your technical and organisational measures for ensuring the security of your processing.

**Subject Access Requests (Changes)**

(1) Clients will no longer have to pay a fee to have their request processed;

(2) We will have a month (28 days) to comply, rather than the previous 40 days;

(3) We now have a right to refuse or charge for requests that are manifestly unfounded or excessive. However, if we refuse a request, we are obliged to tell the individual why. They then have the option/right to complain to the supervisory authority and to a judicial remedy.

We have to do so without undue delay and at the latest, within one month (28 days).

responsebusinessfinance.co.uk
22 Walker Avenue, Milton Keynes, MK12 5TW
+44 (0)3333 580 444