CORNERSTONE BUSINESS RECOVERY ("CORNERSTONE")
PRIVACY NOTICE

This notice and the information contained herein is provided to meet the requirements of the European General Data Protection Regulations and the Data Protection Act 2018 (together the "GDPR").

This policy describes how Cornerstone and, where applicable, Engin Faik (together **"We," "Us," "Our" (as appropriate)**) collect and use personal data and why We collect such personal data. The policy also provides information about individuals' rights.

It applies to personal data provided to Us by individuals themselves and by other parties. W e may use personal data provided for any of the purposes described in this document or otherwise in accordance with any explanations given at the time the data is collected.

Identity of the data controller and the data protection officer	Where an insolvency practitioner of Cornerstone Business Recovery is not appointed as office holder, the data controller is either the company/individual on whose instructions Cornerstone is acting or it is Engin Faik. The contact details of Cornerstone Business Recovery is 136 Hertford Road, Enfield, Middlesex, EN3 5AX, telephone 020 3793 3338 or email: info@cornerstonerecovery.co.uk Where an insolvency practitioner from Cornerstone is appointed as an office holder and the data processing is carried pursuant to his statutory duties, Engin Faik is the data controller. Engin Faik can be contacted at Cornerstone Business Recovery, 136 Hertford Road, Enfield, Middlesex, EN3 5AX, telephone: 020 3793 3338 or email: info@cornerstonerecovery.co.uk Cornerstone Business Recovery is not required to appoint a Data Protection Officer. However, Engin Faik is responsible for matters relating to Data Protection can be contacted using the details stated above.
How we use your Personal Data	The purpose for which personal data is processed may include, but may not be restricted to, any or all the following: • to deliver services and/or meet legal responsibilities; • verify the identity of an individual where this is required by law (e.g. the Money Laundering Regulations); • to communicate by post, email, fax or telephone; • to understand needs and how they may be met • to maintain records in accordance with legal, professional and/or business requirements; • to process financial transactions; • to prevent and detect crime, fraud or corruption; We may also need to use data to defend or take legal actions related to the above

	The overwhelming majority of data processing carried out by Cornerstone or Engin Faik, as the case may be, in order to comply with a statutory, regulatory or professional obligation in relation to an insolvency process. The manner in which we process such data is also intended to meet the legitimate interests of all stakeholders in the insolvency process, as they are entitled to be kept informed of and engage in the insolvency process. Where Cornerstone Business Recovery has engaged with a client to perform a service, we will be required to process data to provide the service in accordance with the contractual terms.
What Personal Data do we process	The categories include but are not limited to: • contact details, • financial information; and • location In exceptional cases, Cornerstone or Engin Faik may hold some special category data, e.g. trade union membership or information about individuals' health, which will be necessary to administer the insolvency process in accordance with our legal obligations.
With whom do we share Personal Data	We may use third parties located outside the UK and the European Union ("EU") to help us operate our business. As a result, personal data may be transferred outside the countries where We and our clients are located. This includes countries outside the EU and countries that do not have laws that provide specific protection for personal data. We have taken steps to ensure all personal data is provided with adequate protection and that all transfers of personal data outside the EU are done lawfully. Where we transfer personal data outside of the EU to a country not determined by the European Commission as providing an adequate level of protection for personal data, the transfers will be under an agreement which covers the EU requirements for the transfer of personal data outside the EU. Personal data held by us may be transferred to: **(a) Third party organisations that provide applications, data processing, IT services or data storage services to us** We use third parties to help us deliver our services and to operate our internal IT systems. This may include providers of: cloud-based software, document management software programs, programs or applications which assist with identity management, website hosting and management, data analysis, data back-up, security and storage services (both electronic and paper copies). The servers powering and facilitating that cloud infrastructure may be located in secure data centres around the world, and personal data may be stored in any one of them.

	(b) Third party organisations that otherwise assist us in providing goods, services or information **(i) Accountants, solicitors and other professional advisers** We necessarily provide information to our professional advisers in order to comply with our statutory, regulatory or professional duties or for some other legitimate business reason. (ii) **Law enforcement or other government and regulatory agencies or to other third parties as required by, and in accordance with, applicable law or regulation** Occasionally, We may receive requests from third parties with lawful authority to require the disclosure of personal data. This could include: • to check that We are complying with applicable law and regulation; • to investigate an alleged criminal offence; • to establish, exercise or defend legal rights. We will only fulfil requests for personal data where We are authorised or obliged to do so in accordance with applicable law or regulation.
How long we hold your Personal Data	We retain personal data for as long as is necessary to fulfil the purposes listed in this document and/or for any other lawful purpose. For example, we retain most records to comply with statutory or regulatory requirements regarding the retention of such records for insolvency appointment.
Your rights	The GDPR provides the following rights for individuals: **Right to inform** This privacy notice meets the legal requirement to inform you of the manner in which We process personal data. **Access to personal data** You have a right of access to personal data held by us as a data controller. This right may be exercised by contacting the relevant Insolvency Practitioner acting as office holder, using the contact details provided in this privacy notice. We will aim to respond to any requests for information promptly, and in any event within one calendar month or receiving a written request.

	Amendment of personal data You may also request that we amend any personal data we hold by submitting a written request to do so using the contact details provided in this privacy notice. Alternatively, you may may amend the personal details held on relevant applications with which you registered e.g. the IPS Portal. **Rights that do not apply in these particular circumstances** Not all of the rights under the GDPR are available as one of the reasons we are holding your data is on the basis of it being a legal obligation and therefore the right to erasure, data portability and to object do not apply.
Right to withdraw consent	The data received was not based upon obtaining consent and therefore the right to withdraw consent does not apply.
Changes to this privacy notice	We keep this privacy statement under regular review and will upload any updates or amendments on our website, www.cornerstonerecovery.co.uk. Paper copies of the privacy statement may also be obtained by writing to us at Cornerstone Business Recovery, 136 Hertford Road, Enfield, Middlesex, EN3 5AX. This privacy statement was last updated on 11 November 2019.
Complaints	Should you wish to complain about our use of personal data, please contact us by email at info@cornerstonerecovery.co.uk. You also have the right to lodge a complaint with the Information Commissioner's Office ("ICO") (the UK data protection regulator). For further information on your rights and how to complain to the ICO, please refer to the **ICO website**.
Who provided the Personal Data	The personal data we have used to contact you was provided by the company/individual (or persons acting on their behalf) on whose instructions we are acting or in relation to which our insolvency practitioner has been appointed. We may also have extracted the information from the business or personal records of the party who has instructed us. We also access information from the Registrar of Companies and other similar public-access data providers.

CORNERSTONE BUSINESS RECOVERY ("CORNERSTONE")
PRIVACY NOTICE

GDPR POLICY

The EU General Data Protection Regulation (GDPR) came 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.

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.

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.

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, Cornerstone 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 cybersecurity 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).