*Updated May 2019*

# STARBOOKS LIMITED - DATA PROTECTION PRIVACY NOTICE

## Purpose

This Notice outlines the data protection policies and procedures we have adopted and to which we abide to ensure we are GDPR compliant. The purpose of this Notice and any other documents referred to in it, is to clearly list and identify the legal requirements, procedures and rights which must be established when we obtain, process, transfer and/or store your personal data. This Notice will assist you in understanding the obligations, responsibilities and rights which arise from the Data Protection Laws.

## Introduction

Everyone has rights with regard to the way in which their personal data is handled. In order to operate efficiently we need to collate and use information about the people with whom we work. This includes current, past and prospective employees, clients, and others with whom we communicate.

We regard the lawful and correct treatment of personal information as integral to successful operation and to maintaining the confidence of the people we work and communicate with. To this end we fully endorse and adhere to the principles of the relevant Laws.

We are registered as a Data Controller on the Register kept by the Information Commissioner's Office.

## Definitions in this Privacy Notice

| | |
|---|---|
| **Data:** | Information stored electronically, on a computer, server or in certain paper-based filing systems. |

| | |
|---|---|
| **Data Controller:** | Starbooks Ltd has determined the purposes for which, and the manner in which, your Personal Data is processed. The Data Controller has overall responsibility for compliance with the Data Protection Laws. Any questions about the operation of this Notice or any concerns that the Notice has not been followed should be referred in the first instance to our data privacy manager using the details below. |
| **Privacy Manager:** | Our data privacy manager is responsible for awareness-raising, training staff and informing and advising the Data Controller, Data Processors and Data Users how to ensure compliance with the enactments, and to monitor that compliance. If you have any questions about this Notice, including any requests to exercise your legal rights, please contact the data privacy manager via datarequest@starbooks.co.uk. |
| **Data Processor:** | Any person or organisation that is not a Data User that processes personal data on our behalf and in accordance with our specific instructions. Our staff will be excluded from this definition but, the definition could include suppliers who handle personal data on our behalf. |
| **Data Subjects:** | All living individuals about whom we hold Personal Data. All Data Subjects have legal rights concerning the processing and storage of their personal information. |
| **Data Users:** | Our employees whose work involves processing your Personal Data. Data users are responsible for the proper use of the data they process and must protect the data they handle in accordance with this Notice. |
| **The Enactments:** | The Data Protection Act 1998 (the Act) up to and until 25 May 2018 after which The General Data Protection Regulations 2017 (GDPR) will apply, both of which regulate the way in which all Personal Data is held and processed. |
| **Personal Data:** | Information which can be used to directly or indirectly identify a living individual. |

| | |
|---|---|
| **Processing:** | Any activity in which the data is used, including (but not limited to) obtaining, recording, organising, amending, retrieving, using, disclosing, erasing, destroying and/or holding the data. The term "processing" also includes transferring personal data to third parties. |
| **Supervisory Authority:** | The Authorised Body which is empowered to govern and manage how the GDPR is implemented and abided by in a particular EU state. In the case of the UK the Supervisory Authority is the: Information Commissioner's Office. |
| **Sensitive Personal Data:** | This includes information about a person's race, ethnicity, political opinions, convictions, religion, trade union membership, physical and/or mental health, and sexual preference. Sensitive personal data can only be processed with the express written consent of the person concerned. |

**Notice Statement**

In accordance with the GDPR anyone processing Personal Data must comply with the six principles of good practice. These provide that Personal Data must:

1. Be processed fairly, lawfully and transparently;
2. Only be used for the purpose for which it was collected;
3. Be adequate, relevant and not excessive for the purpose for which it is being processed;
4. Be accurate and kept up-to-date;
5. Not be kept longer than necessary to fulfil the purpose of its collection; and
6. Be kept secure and protected from unauthorised processing, loss, damage or destruction.

**1. Fair, Lawful and Transparent Processing**

For Personal Data to be processed lawfully, the basis for the processing must be one of the legal grounds set out in the Enactments. These include, among other things, your written consent to the processing, or that the processing is necessary for the performance of our bookkeeping contract with you.

In the event we collect Personal Data directly from you, this Notice should assist in informing you about:

- The purpose or purposes for which we intend to process your Personal Data.
- The types of third parties, if any, with which we may share or disclose your Personal Data.
- The means with which you can limit our processing and disclosure of your Personal Data.

If we receive Personal Data about you from other sources, we will provide you with this information as soon as possible thereafter.

When sensitive personal data is being processed, additional conditions and securities must be in place to ensure protection.

**2. Processing for Limited Purposes**

In the course of our business, we shall process the Personal Data we receive directly from you (for example, by you completing forms, sending us papers or from you corresponding with us by mail, phone, email or otherwise) and your Personal Data which we receive from any other source.

We shall only process your Personal Data to fulfil and/or enable us to satisfy the terms of our obligations and responsibilities in our role as your Bookkeeper or for any other specific purposes permitted by the Enactments. Should we deem it necessary to process your Personal Data for purposes outside and/or beyond the reasons for which it was originally collected, we will contact you first, to inform you of those purposes and our intent and may also apply for your consent.

**3. Adequate, Relevant Non-Excessive Processing**

We will only collect and process your Personal Data as required to fulfil the specific purpose/s of our contract and agreements with you as set out in the terms agreed upon engagement.

**4. Accurate and up to date data**

We shall ensure that all Personal Data held is accurate and up to date and will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. If you become aware that any of your Personal Data is inaccurate, you are entitled to contact us and request that your Personal Data is amended. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

**5. The Timely Processing of the Data**

We will not keep Personal Data longer than is necessary for the purpose or purposes for which it was collected. Once Personal Data is no longer required, we will take all reasonable steps to destroy and erase it.

## 6. Keeping Your Personal Data Secure

Our employees and contracted personnel are bound to our privacy policies, procedures and technologies which maintain the security of all your Personal Data from the point of collection to the point of destruction.

We maintain data security by protecting the confidentiality, integrity and availability of your Personal Data, and when we do so we abide by the following definitions:

**6.1** **Confidentiality:** We ensure that the only people authorised to use your personal data can access it. Employees are prohibited from accessing and viewing your personal data unless it is necessary to do so.

**6.2** **Integrity:** We will make certain that your Personal Data is accurate and suitable for the purpose for which it is processed.

**6.3** **Availability:** We have established procedures which mean only our authorised Data Users should be able to access your Personal Data if they need it for authorised purposes.

**6.4** Secure lockable desks and cupboards. Desks and cupboards shall be kept locked if they hold your personal data.

**6.5** Methods of disposal. Paper documents containing Personal Data are shredded and digital storage devices shall be physically destroyed when they are no longer required.

**6.6** Data Users shall be appropriately trained and supervised in accordance with this Notice which includes requirements that computer monitors do not show confidential information to passers-by and that Data Users log off from or lock their PC/electronic device when it is left unattended.

**6.7** Our computers have appropriate password security, boundary firewalls and effective anti-malware defences. We routinely back-up electronic information to assist in restoring information in the event of disaster and our software is kept up-to-date with the latest security patches.

**6.8** One or all of the following measures shall be applied to the personal data held; separating the personal data and/or pseudonymisation and/or the encoding of the data.

Our Privacy Manager will ensure that this Notice is kept updated in response to any amendments to the Law.

We shall take appropriate security measures against unlawful and/or unauthorised processing of personal data, and against the accidental loss of, or damage to, your Personal Data.
We shall only transfer your Personal Data to a Data Processor (a Data User outside our business) if the Processor agrees to comply with our procedures and policies, or if the Processor puts in place security measures to protect Personal Data, which we consider adequate and are in accordance with the Enactments.

## Transferring the Personal Data out of the EEA

We shall only transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), if one of the following conditions applies:

- The country to which your Personal Data shall be transferred ensures an adequate level of protection and can ensure your legal rights and freedoms.
- You have given your consent that your Personal Data is transferred.
- The transfer is necessary for one of the reasons set out in the Enactments, including the performance of a contract between you and us, or to protect your vital interests.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
- The transfer is authorised by the ICO and we have received evidence of adequate safeguards being in place regarding the protection of your privacy, your fundamental rights and freedoms, and which allow your rights to be exercised.

The Personal data we hold will not be processed by staff operating outside the EEA.

## How We Will Use Your Personal Data

We will only collect and process your Personal Data to the extent that it is needed to fulfil our operational and contractual needs or to comply with any legal requirements.

We shall access and use your Personal Data in accordance with your instructions and as is reasonably necessary:

- To fulfil our contractual obligations and responsibilities to you;
- To provide, maintain and improve our bookkeeping services;

- If we intend to use your personal data for the advertising and marketing of our services and/or the services of our affiliates. We shall seek your separate express consent and you are entitled to opt out of these services at any time; and

- To respond to your requests, queries and problems;

- To inform you about any changes to our services and related notices, such as security and fraud notices.

**When We May Share Your Personal Data**

There are times when we may need to share your Personal Data. This section discusses how and when we might share your Data.

In the course of us fulfilling our role as your bookkeeper it will be necessary for us to disclose your Personal Data in certain situations:

- In our role as your bookkeeper we may need to share your Personal Data with certain bodies to fulfill our contract with you such as your suppliers, contractors and sub-contractors, HMRC, ICB and other governmental, regulatory bodies.

- We use the following software provider to process electronic data, including personal data, Xero (UK) Limited. This provider states that it is GDPR compliant and/or applies equivalent/adequate safeguards. It's privacy notice can be found here:

  www.xero.com/uk/about/terms/privacy/

- We use secure external servers to process/store our electronic records, including your Personal Data which are maintained by Drop Box and Xero. Their privacy notices can be found here:

  www.dropbox.com/en_GB/privacy

  www.xero.com/uk/about/terms/privacy/

- There may also be situations in which it is necessary for us to disclose your Personal Data to other third parties, which include but are not limited to: HMRC requests, ICO requests and ICB requests.

- If we are under a duty to disclose or share your Personal Data in order to comply with any legal obligation, lawful requests, court orders and legal process.

- To enforce or apply any contract or other agreement with you.

- To protect our rights, property, or safety and that of our employees, members, or others, in the course of investigating and preventing money laundering and fraud.

## Your Rights and Requests Concerning Your Personal Data

We will process and manage all your Personal Data in line with your rights; in particular your rights to:

- Request access to any data we hold about you;

- Prevent the processing of your Personal Data for direct-marketing purposes, if so instructed;

- Ask to have inaccurate Personal Data amended;

- Be forgotten, and have all relevant Personal Data erased (subject to our overriding legal obligations);

- Prevent processing which is likely to cause damage or distress to you or anyone else;

- Request certain restrictions on the processing of your Personal Data;

- Receive a copy of your Personal Data and/or request a transfer of your Personal Data to another Data Controller;

- Not be subject to automated decision making;

- Be notified of a data security breach which affects your rights and freedoms, without undue delay;

- If you have provided your express consent that your Personal Data may be processed for marketing and advertising purposes, you are entitled to withdraw that consent. Such a withdrawal will not affect any processing of the data completed before consent was withdrawn; and

- To make certain requests to us concerning how your Personal Data is managed.

## Access and Portability Requests

You are entitled to request access to your Personal Data unless providing a copy would adversely affect the rights and freedoms of others.

You can also request information about the different categories and purposes of data processing; recipients or categories of recipients who receive your Personal Data, details on how long your Personal Data is stored for, information on your Personal Data's source and whether the Data Controller uses automated decision-making.

You also have "Data Portability" rights which includes the right to request a copy of your Personal Data be sent to you or transmitted to another Data Controller.

**Correction Requests**

You are entitled to request we correct or complete your inaccurate or incomplete Personal Data without undue delay and we will update the information and erase or correct any inaccuracies as required.

**Erasure Requests**

You can exercise your "right to be forgotten" and can request we erase your Personal Data. Once receiving a request we must erase the Personal Data without delay, unless an exception applies that permits us to continue processing your data. Details of such exceptions are contained in the Enactments and include situations where we might need to retain the information to carry out our official duties and/or comply with legal obligations and/or for the establishment of exercising or defending legal claims, or it is in the public interest to retain your Personal Data.

**Restriction Requests**

You may request restrictions be applied to the processing of your Personal Data for some specific reasons such as you contest the accuracy of the data, the processing is unlawful or if we no longer need to process your Personal Data. You can also request restrictions be applied if the processing is being done for public interest or third party reasons.

If such a request is received we can continue to store your Personal Data, but may only process it under certain circumstances, such as: you give consent for us to continue processing your data, we need to establish, exercise, or defend legal claims or we need to protect the rights of another individual or legal entity or for important public interest reasons.

**Objection Requests**

You may also object to your Personal Data being processed under certain circumstances, including for direct marketing purposes and profiling related to direct marketing.

If we receive such an objection we will stop processing your Personal Data unless we can show a compelling legitimate ground for processing your Personal Data which overrides your interests and the basis of your request.

**Your Telephone Queries and Requests**

When receiving telephone enquiries, in which Personal Data is requested we will only verbally disclose Personal Data held on our systems if we can confirm the caller's identity so as to ensure that the data is only given to a person who is entitled to receive it.

We may suggest that a caller put their request in writing to assist in establishing the caller's identity, and to enable us to clearly record the nature of the request and to assist in further identity checks.

If we have reasonable doubts about the identity of the person making the request, we may request additional information to confirm the caller's identity.

In difficult situations our Data Users may refer a request to their line manager for assistance.

**Your Written Queries and Requests**

When responding to written requests Personal Data will only be disclosed if we can confirm the identity of the sender and/or sufficient supporting evidence is provided by the sender establishing their identity.

**Responding to Your Requests**

Upon receiving a request from you concerning your Personal Data, we will respond within one month of receiving the request by email (unless you request a response in an alternative format).

If we are unable to immediately comply with your request we will inform you within our response stating whether we need to extend our response time (for up to a maximum of two months), along with an explanation for the delay.

If we do not take any action within one month after receiving your request, you are entitled to request an explanation from us as to why no action was taken and you may make a complaint to the ICO: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow Cheshire SK9 5AF (Tel: 0303 123 1113) (email. casework@ico.org.uk)

Under the GDPR we are not entitled to charge for the provision of your personal data, unless the requests are manifestly unfounded or excessive, particularly if it is repetitive in which case we may refuse to act on the request, or apply further fees to cover the associated administrative costs.

**Your Complaints**

If you feel that your questions or concerns regarding your Personal Data have not been dealt with adequately or that your request has not been fulfilled by us, you can use our complaints procedure, by emailing us at *info@starbooks.co.uk*

If, at the conclusion of our complaints procedure you do not feel that we have adequately dealt with your complaint you may make a complaint directly to ICO: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow Cheshire SK9 5AF (Tel: 0303 123 1113) (email. casework@ico.org.uk).

**Changes to our Data Protection Policy**

We keep our privacy policy under regular review and reserve the right to amend and update the policy as required. Where appropriate, we will notify you of those changes by mail, email and/or by placing an updated version of the policy on our website.