



Privacy Policy

May 2018

ROASTERS, BAKERS, ARTISAN TASTE MAKERS

Introduction

SOHO Coffee Co. (which we'll refer to as 'SOHO', 'we' or 'us' in this document) is proud to have been offering 100% Fairtrade organic, arabica coffee and delicious, handmade food, freshly prepared in our own kitchens for nearly two decades.

Our entire business is built on the trust you place in us and we are equally committed to processing your personal information fairly and transparently and in accordance with data protection law, including the General Data Protection Regulation ("GDPR") ("Data Protection Law").

This Privacy Notice explains in detail the types of personal data we may collect about you when you interact with us. It also explains how we'll store and handle that data, and keep it safe.

We know that there's a lot of information here, but we want you to be fully informed about your rights, and how SOHO Coffee Co. uses your data.

We hope the following sections will answer any questions you have but if not, please do just drop us a line and we'll be happy to help.

The legal bit

The law on data protection sets out a number of different reasons for which a company may collect and process your personal data, including:

Consent

In specific situations, we can collect and process your data with your consent. For example, when you tick a box to receive email newsletters, or sign up to our instore Wi-Fi or App.

When collecting your personal data, we'll always make clear to you which data is necessary in connection with a particular service.

Contractual obligations

In certain circumstances, we need your personal data to comply with our contractual obligations.

For example, if you order an item such as a Working Lunch, we'll collect your contact details and payment to ensure your order has been acknowledged and processed.

Legal compliance

If the law requires us to, we may need to collect and process your data.

For example, we can pass on details of people involved in fraud or other criminal activity affecting the business to law enforcement.

Legitimate interest

In specific situations, we may require your data to pursue our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests.

For example, we will use your purchase history to send you or make available personalised offers.

We also combine the shopping history of many customers to identify trends and ensure we can keep up with demand or develop new products.

What type of information do we collect?

We aim to give you the best possible service and, as part of this, we sometimes collect information directly or indirectly from you.

For example, when you visit our website, <http://www.sohocoffee.com/> or log into our free instore Wi-Fi you may choose directly to sign up to receive newsletters and marketing from us. In which case, you may be asked for details such as your name, date of birth and email address.

Some personal data is collected indirectly. Like most website operators and Wi-Fi providers, this data helps improve our understanding of how we can improve your experience of our website and instore Wi-Fi. This information may include your location, your computer's Internet Protocol (IP) address, your browser type and version, the pages you visit on our website, the time and date of your visit, and the time spent on each page.

When you engage with us on social media and make a comment or complaint about our services via Facebook, Twitter, Instagram, or any other public domain, we may use that information to get in touch with you so that we can respond to your comments. We may equally ask you for permission to use a lovely photo you may have posted! Where you have posted a blog or an article about us we may also wish to get in touch with you.

Where we hold your information

You can trust us to store and maintain any personal information of yours that we may have collected safely and securely, as if it were our own.

We have a secure internal database that is shared with no-one but ourselves and we do not share your information with anyone but those companies who we trust to carry out business on our behalf.

Any information that you have given us directly is stored with these trusted business partners, such as our App provider, Wi-Fi data controller or Mailchimp, all of which are GDPR compliant and take as much care as we do to ensure your information is safe. None of our business partners will ever share your information with any third party, unless required for legal compliance with law enforcement bodies for fraud management or illegal activity; nor will they contact you directly for marketing purposes.

How we may use your information

We may use your information for some or all of the following activities: For customer services purposes, so that we can interact with you; to process any order made via our stores; to process any request you may have made; to process any entries that you make to competitions run by us; for marketing purposes; for market research purposes, so that we can understand your needs better; to improve your user experience across all digital platforms; to seek your views on the services we provide; to notify you of changes to our services; for crime and fraud prevention, where we have a legal duty or right to disclose your information; to process a job application; to verify your identity.

Your Rights

We use Mailchimp for our mailouts, allowing all contact details to be updated with ease. Mailchimp also gives you the option to unsubscribe from our mailing list at any time, and this can be found at the bottom of every mailing/newsletter we send.

You can also email us directly at talktous@sohcoffee.co.uk if you would like to be removed from our database at any time.

If you have not opted-in to receive marketing from us, none of your personal data will be stored.

You have the right to request a copy of any information about you that we hold, also to have that information corrected if it is inaccurate, or have it deleted from our database at any time.

SOHO Coffee Co. HR privacy policy as an employer

The GDPR is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with employees about the use of information held about them, and by following good data handling procedures.

For the purposes of this policy, Personal data is data that relates to an identified or identifiable individual and is:

- processed electronically
- kept in a filing system
- part of an accessible record, for example an education record
- held by a public authority

This includes data that does not name an individual but could potentially identify them, for example a payroll or staff number. All colleagues should ensure they are aware that any personal data they have in their possession will also be subject to the regulation. For example, if a manager has a written copy of contact details for their team or an employee keeps customer names and numbers on notes on their desk.

The regulation contains 6 principles.

- Personal data should be processed fairly, lawfully and in a transparent manner.

All personal data stored is accessible to any colleague who wishes to view his / her personal information. The Company will make not inappropriate use of personal data; all files are protected and access is restricted to authorised personnel only.

- Data will only be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.

All personal data requested and received is done so for the business to carry out its legislative duties; examples of this would be to ensure compliance with an employee's Right to Work, HMRC regulations and other legislative requirements. This ensures, among other things, that we can pay our team, and provide HMRC with all the required information and payments required. The data will also be shared in response to any law enforcement request that is properly requested within the confines of the Act.

- The data should be adequate, relevant and not excessive.

All our payroll data is stored securely by us and our third-party payroll provider, Numerii. Under no circumstances will Numerii request personal information from our team unless it is required under this or other legislation.

- The data should be accurate and where necessary kept up to date.

The business will ensure that all data is relevant and up to date. Any changes to personal information must be authorised by the individual concerned, with a signature, to recognise the changes are accurate and as requested.

- Data should not be kept for longer than necessary.

All personal data will be held for a maximum of 36 months in line with current payroll legislation.

- Data should be kept secure.

Only authorised personnel have access to employee files. These individuals will have been given permission as part of their specific job role and authorised by the Board. Our current third-party payroll data storage companies, Numerii and Quinyx, have detailed GDPR policies and are fully compliant.

All in-house systems are password protected and access is granted to authorised personnel only. If an individual wants to see the information held on them they will need to request access.

All staff have a responsibility to ensure that their activities comply with the data protection principles. Authorised personnel have responsibility for the type of personal data they collect and how they use it. Colleagues should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

The company and our staff are already complying with the Data Protection Act 1998, and as such the new legislation will be further security for the business.

Monitoring employees

We monitor our staff, for example to detect crime, and we are required to make our workers aware of the nature and reason for the monitoring. This forms part of the company CCTV policy. This is applicable whether the monitoring is taking place using CCTV, accessing a worker's email or telephone calls, or in any other way.

A worker's right to request their personal data

Our staff have a right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes.

If a worker wants to see their personal data, they should speak to their line manager or an HR representative of the company. Most requests for personal data can be provided quickly and easily, and in any event within the one-month time limit stipulated by GDPR. If we have reason to refuse a request for access to personal information, we will inform the individual within one month to confirm (i) why the request has been refused; and (ii) that the individual has the right to complain to the supervisory authority and to a judicial remedy.



Privacy Policy 2018