Stroud Office Supplies – Full Privacy Policy

Purpose of this privacy policy

This privacy policy sets out on how and why Stroud Office Supplies collects and processes personal data while conducting its day-to-day business operations.

Company information

Stroud Office Supplies Limited ("we", "us", "our") is incorporated and registered in England and Wales with company number 5510697 whose registered office is at 701 Stonehouse Park, Sperry Way, Stonehouse, Glos., GL10 3UT. Our main trading address is Unit F2B, Bath Road Trading Estate, Stroud, Glos, GL5 3QF. Our VAT number is 448465615.

Definitions

Data Controller – A Data Controller determines the purposes and means of processing (personal) data. In this instance, Stroud Office Supplies is the data controller.

Data Processor – A data processor is responsible for processing personal data on behalf of the controller. For the most part, Stroud Office Supplies is the data processor with the exceptions given below where a third-party processes data on our behalf.

Processor/Processing – Broad terms indicating that 'something' is being done to data; be it collecting, storing, or deleting, for example.

Data Subject – An identifiable human who can be identified by reference to data collected or stored.

Personal Data – Any data which is identifiable to a human, or data subject.

EU Regulation 2016/679 – General Data Protection Regulation ("GDPR")

The GDPR, which came into force on 25th May 2018 and applies to all individuals and organisations residing and operating in the EU, is a regulation based in EU law which focuses on data protection and the privacy of individuals. It seeks to give EU citizens more control of the data organisations holds about them and to simplify the regulatory frameworks in which both citizens and organisations within the EU operate.

Article 5(1) of the GDPR sets out seven key principles pertaining to personal data. It requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

We believe that compliance with the above principles is not only a reasonable legal obligation but also best practice for ensuring that individuals' rights and privacy are protected.

Transfers of personal data outside of the European Economic Area

Personal data provided to us may be transferred and processed outside of the EEA if any of the below listed organisations have servers/offices based in such locations.

Where personal data is transferred outside of the EEA, we will, to all reasonable standards, ensure that

(a) The European Commission has made an "adequacy decision" with respect to the data protection laws of the country to which it is transferred; or (b) where we use providers based in the US, we may transfer data to them if they adhere to the relevant Privacy Shield frameworks. These were co-designed by the US Department of Commerce, European Commission, and Swiss Administration, and ensures US-based organisations provide similar levels of protection to personal data shared between Europe and the US; or (c) we have entered into a suitable data processing agreement with the third party situated in that country to ensure the adequate proception of your data. In all cases, transfers outside of the EEA will be protected by appropriate safeguards.

Data Subjects' Rights

Under certain circumstances, a data subject has the following rights in relation to their personal data:

- To access: The right to be provided with access to all their personal data and also confirmation as to whether or not any personal data is or is not being processed
- To rectification: The right to require any mistakes or inaccuracies in their data held are corrected and rectified without undue delay
- To erasure ("the right to be forgotten"): The right to require the deletion of their personal data
- To object: The right to object to processing of their personal data, at any time.
- Of restriction of processing: The right to require the restriction of processing their personal data, often where the data subject prefers not to have their data erased
- Of data portability: The right to receive a copy of their personal data held by us, in a structured, commonly-used and machine-readable format and/or transmit data to a third party in certain situations.
- To withdraw consent: The right to withdraw consent as easily and as freely as it was given initially.

If anyone wishes to exercise any or all of the rights set out above, please contact Ben Cook on 01453 750419 or by email at ben@stroudofficesupplies.co.uk.

The data subject will not have to pay a fee to access their personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if the request if clearly unfounded, repetitive, or excessive. Alternatively, we may refuse to comply with your request in these circumstances.
We may need to request specific information from the data subject to help us confirm their identity and ensure their right to access their personal data (or to exercise any of the other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it.
We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if the request I particularly complex or excessive. In these cases, progress updates will be given at reasonable intervals.

Why do we need to process data about individuals and organisations?

We need to hold certain basic details of customers to conduct our business; to provide them with the products and/or services they have purchased – as well as relevant information to these - and to be able to maintain their accounts and sales records accordingly. Our lawful basis for processing this data is *legitimate interest*; we have a legitimate interest and reasonable cause to collect and process this data to be able to provide customers with the products and/or services they have asked for.

We may process personal data to inform customers of special offers, competitions, newsletters, or new products and services. Our lawful basis for processing this data is our *legitimate interests* in promoting the growth of our business. This means that we do not usually need their explicit consent to send them correspondence. However, where consent is required, we will ask for this separately and clearly.
Anyone has the right to opt-out of receiving promotional communications from us and can do so at any time by contacting us or using the 'unsubscribe' link contained within every email of a promotional nature.

What data is involved?

Overview

	Where is it held?	Who has access?	How is it secured?	How long is it kept?
Customer database	Pulse, main server	All office staff	Password protected	6 years after last purchase
Accounts database	Sage, main server	Accounts dept., Director	Password protected	6 years after last purchase
Paper documents	Locked filing cabinets	All office staff	Lockable cabinets and locked office	6 years after last purchase

Details

	Details
Customer database	Some, or all of the following data may be collected and held in Pulse, our back-office system: Business name and address and phone/fax number, the names and email addresses of contacts in sales and accounts departments, as well as non-personal data such as sales activity which includes the date, quantity and price of items bought, and account-specific information such as credit limits, discounts, and payment terms.
Accounts database	Some, or all of the following data may be collected and held in Sage, our back-office accounts software: Business name and address and phone/fax number, the names and email addresses of contacts in accounts departments as well as non-personal data such as sales activity including the date, quantity and price of items bought, and account-specific information such as credit limits, discounts, and payment terms.
Paper documents	We maintain a record of both handwritten and printed order forms for each order placed, as well as paper copies of each invoice produced.

What security do we have?

Digital - Offline

Our computers are password-protected to ensure no unauthorised access. After a period of inactivity login and re-entry of password are required. Both Pulse and Sage programs also require correct credentials to be entered to allow access.

Digital - Online

Our computers are protected in real-time against unauthorised access by both antivirus and firewall systems. These are both automatically kept up-to-date. All our passwords are randomised and held securely in an online password manager. This itself is further protected by the use of two-factor authentication.

Physical

Our offices are private and not open to the public, with the exception of a trade counter which has no access or line-of-sight to any personal data held. The office is always staffed during office hours, and securely locked in the evenings and weekends. Filing cabinets and mobile pedestals containing data are all locked. A clean desk policy ensures no data is left out in the open and is always filed and locked away when not in use. We have by our printer a professional cross-cut shredder which is used to securely destroy any documents which are no longer needed.

Who else has access to data we control/process?

The following organisations (with links to their own privacy policies) may also process data on our behalf:

Organisation	Details
Mailchimp	What data? Business name, email address, contact name. Why? We use Mailchimp to design and send emails quickly to our existing customers. Privacy policies: https://mailchimp.com/legal/privacy/
Heart Systems	What data? Business name and address and phone/fax number, the names and email addresses of contacts in sales and accounts departments, as well as non-personal data such as sales activity including the date, quantity and price of items bought, and account-specific information such as credit limits, discounts, and payment terms. Why? Heart Systems created and manage Pulse, our back-office system. Occasionally, they may need to access our systems in order to provide support or fix any software issues that arise. Privacy policies: http://www.heartsystems.co.uk/privacy-policy
2020Prosoftware	What data? Business name and address, email address, contact name, history of orders (and the orders' contents) placed online through our website, stroudofficesupplies.co.uk. Our systems and theirs are separate and there is no link, automatic or otherwise, between the two organisations. Only customers who have themselves manually requested and/or created an online account will have any data processed by 2020prosoftware. Why? 2020prosoftware host our website and therefore process the minimum amount of data for a web-ordering system to reasonably function. Privacy policies: https://www.2020prosoftware.com/privacy/index.html
Pickaweb	We use Pickaweb's servers to send and receive routine emails from and to @stroudofficesupplies.co.uk email addresses. Privacy policies: https://www.pickaweb.co.uk/privacy-policy/

Other than under those specific circumstances given above, we will never sell, distribute, or lease any personal information or data to third parties without your explicit permission or unless we are required to do so by law.

If you require further information, please contact Ben Cook on 01453 750419 or ben@Stroudofficesupplies.co.uk