Introduction

The intention of this policy is to clearly define to any individual how Stone Computers Ltd processes 'Personal data' for which it has responsibility.

The definition of 'Personal data' is that as defined by the General Data Protection Regulation 2016 – this is primarily pieces of data that identify you as an individual

In circumstances where any individual supplies 'Personal data' about themselves to Stone Computers Ltd, we will become responsible for it legally as the 'Data Controller'.

In circumstances where data is supplied to Stone Computers Ltd about individuals by another party who is legally the 'Data Controller', we will legally have responsibility as the 'Data Processor' and conduct processing of that data under a legal contract with the Data Controller.

The definition of a 'Data Controller' or 'Data Processor ', is that as defined by the General Data Protection Regulation 2016.

Contact Details:

Stone Computers Ltd

Granite One Hundred, Acton Gate, Stafford, Staffordshire. ST18 9AA

Tel: 01785 786 700

The appointed Data Protection Officer for Stone Computers Ltd is

Chris Hykin - Technical Services Director

Why do we need your data?

We require Personal data from you to be able to supply any products or services which you have requested from us. We will only ask for and keep the data needed to ensure we provide you with an efficient level of service and support and any legal commitments we have as a business.

We will use Personal data we have gathered to contact and inform you of products and services which we believe will be of genuine interest to you and/or your organisation.

We may also request your consent to use your data to send you information about our products and services or collect data on use of our websites and E-Commerce portals (our online shops).

The Privacy Notice Matrix at the end of this policy gives details of what types of data we may store about you.

What do we do with your data?

We have a responsibility to protect data we hold about you and ensure it is not accessed by anyone who is not authorised to use it for the reasons legitimately hold it. We also have a responsibility to ensure that your data is accurate, retrievable and is not kept any longer than is necessary or legally required.

If your data held on hard copy documents (Paper), it is held securely at the address above until it is no longer required and destroyed by securely shredding it. Data held electronically will be stored on servers located at our own site and in the UK or the European Union; but never outside the European Union. Electronic data is erased to recognised standards from these servers when it is no longer required.

We have assessed the risks to the security of your data and implemented many physical and electronic controls to keep it protected. These controls are updated regularly to ensure that any new risks or threats can be countered. The controls and policies we have in place meet recognised standards such as ISO27001, ADISA and Cyber Essentials and we are regularly tested by external assessors against these standards.

Access to your data will be limited to only those who need it to provide you with the services you have requested or consented to receiving, or have legal authority to request access to it. We will ensure that we have in place a Confidentiality Agreement with anyone having access to your data.

We will need to pass your data to other parties (Businesses) sometimes, who we use for specific parts of supplying products & services to you or provide us with data storage and disposal services. These third parties will only receive your data from us when we have assessed the risks in giving them access to it, are assured they have an adequate level of data security and have agreed a legal contract detailing how they should protect your data. They will not be permitted to store your data outside of the European union.

We will not pass your data to third parties to use for marketing of their own services. The Privacy Notice Matrix at the end of this policy gives details of how long we may need to keep your data.

What happens if we lose your data or it is accessed by unauthorised persons?

If we detect that 'Personal data' we are holding as a Data Controller, has been lost or accessed by unauthorised persons (a Data Breach) and that this will potentially infringe your rights or cause you damage; we will inform you immediately of the data breach. We will also be required legally to inform the Information Commissioners Office (the Governments data protection regulator) within 72Hrs of detecting the breach; who may then investigate our compliance with data protection legislation and effectiveness of our controls.

If your data has been passed to us for processing by another organisation (Data Controller) we will contractually be required to inform them of the breach immediately and the ICO within 72Hrs of detecting it. We will work with the Data Controller to ensure that all individuals who might be affected by the breach are informed as quickly as possible.

We will also ensure that as a business we are able to meet any liabilities for which we would be responsible.

What rights do you have?

Data protection regulations give you a legal right to:

A) Request information on what data is held about you.

To make a request for this information please use the following:

Email: subjectaccessrequests@stonegroup.co.uk

To assist us in making a response to you, please ensure you provide the following information:

Full name & address, contact telephone number, description of the data which you would like information about and any relevant dates or time scales related to this data.

B) The right to have your data changed or deleted from our records.

To make this type of request please use the above contact details and we will advise you if this will affect our ability to provide agreed products or services.

C) The right to complain to the regulator (ICO) about how we have handled your data.

To make a complaint to the ICO (Information Commissioners Office) use the link below or call their hotline on Tel No.: 0303 123 1113.

https://ico.org.uk/concerns/

D) Complain to use about our handling of your data.

To make this type of complaint please use the contact details listed in A).

E) The right to withdraw your consent for receiving product & service information or inform us that you do not want to be sent this type of information.

To make this type of request please use the following contacts:

E Mail- marketing@stonegroup.co.uk

Under normal circumstances we will not charge you for processing these requests and will respond to you within 30 working days. If we believe your request is complex and will be chargeable; we will first contact you before proceeding.

Questions?

If you would like to make any general enquiries about our data protection policies please contact Hannah Palacio (Risk & Compliance Manager)

Email – hannah.palacio@stonegroup.co.uk

Telephone – 07384 830985

Privacy Notice Matrix

Processing Activity	Personal Data required / held	Retention Time	Reason to hold data
Supply of Products & Services	Name, phone number (s), work or home address, E - Mail address(s)	7 Years	Legitimate – in order to provide the products or services you have ordered.
Marketing	Name, E - Mail address(s), Job Title, Business name & Profile of contact history	Until notified to stop Marketing by you	Legitimate Interest - we will provide information which we believe is of genuine interest to you or your organisation and based on your job role.
Marketing	Name, phone number (s), work or home address, E - Mail address(s)	Until consent withdrawn by you	Consensual – you have given your consent to receive information about products & services which are of interest to you.
Website Browsing	Internet Protocol Address (IP)	7 Years	Consensual – you have read & accepted our Website Policies which explain the use of trackers & cookies on the website you visited
Credit / Debit Card Payments	Card holder name, card number, security number	Duration of the transaction	Consensual – you have agreed to give these details in order to pay for products or services ordered
Remote& Managed Service Support	During remote access to customer devices or networks – all activity is recorded for security purposes, there is potential for data to be recorded. Files cannot be accessed without permission & supervision.	30 Days	Consensual – you will have agreed to allow us access your device in order for us to resolve technical issues remotely. Data may be captured during this process.
Repair Services	We may require your PC password to access devices to test. Data is not copied or viewed.	Duration of repair	Consensual – you will have agreed to supply the password in order for us to repair your device. You have the option to remove it prior to collection for repair. ** Ensure you have a backup copy of your data held on the device.
IT Recycling / Data Disposal Services	We may require your Bios password to erase data. Data is not accessed or copied during disposal process.	Duration of data disposal process Max: 25 Working Days	Legitimate – in order to provide effective Recycling & Data disposal services. We will work under a Data Processing contract agreed with the Data Controller (Customer) for all data disposal services.