What is your data processing policy? (Including GDPR-specific information)

Signed copies and physical paperwork

If you require a formally signed copy of this policy, signed by a director of Simba Hosting Ltd., then please print it out, provide the date, the signature, the name and position of the signer within your company, and then post it to us with a stamped and addressed envelope for the return, using the address on our contact form. You must not amend any details of this policy without prior agreement before sending the document, and without clearly highlighting the changed sections. You must be willing to pay, in advance, any costs we incur in processing or legal evaluation of them. The same willingness to pay costs shall apply to any other formal legal procedures, or physical paperwork, which you request us to handle.

Validity

This policy applies during the time that you have a paid account with us. All of your data will be deleted when, for whatever reason, your account with us is closed. When you no longer have a paid account with us, all appropriate regulations (e.g. the GDPR) continue to apply for as long as we still hold your data, but after an appropriate time (e.g. in which we inquire if you wish to continue services, and encourage you to pay any outstanding invoices), all your data stored with us will eventually be deleted (including that retained in automated backups until they are automatically deleted), and all our obligations in relation to your data (and any capacity we previously had to process it) will thereby end.

Data processing policy

Simba IT Services Ltd. (the owners of www.simbahosting.co.uk) are registered as a data processor with the Information Commissioner's Office (ICO) in the UK. We aim to comply with both the letter and the spirit of all relevant laws, including the General Data Protection Regulation (GDPR).

In respect of website and email hosting services (i.e. if this applies to you, having purchased such services), our systems (i.e. computers belonging to us) will process data as a necessary part of providing your purchased services. If this applies to you, then you should read the following details. Note that in relation to services provided, we are a **data processor**, not a **data controller**. i.e. We do not inherit the responsibilities of a "data controller" in respect of the running of your business (your website, associated database, email accounts, etc.). Those responsibilities remain with the website owner, not with us. We are a data controller only in respect of our own website/business (not yours). In particular, the data processing liabilities and responsibilities for **all** code (or equivalent – e.g. email filter settings, webserver settings or the like) that you upload into your web hosting account or set as settings, remains with you, notwithstanding that processing having been carried out using our rented facilities. As part of this, it is entirely the responsibility of the customer to ascertain that he has purchased the correct facilities to satisfy any legal requirements on their side (e.g. appropriate facilities for PCI card processing compliance for a website that processes online payments).

Unwritten yet existing liabilities

As a UK-based company, we are subject to the relevant privacy laws (e.g. the GDPR). Note that there are various data processing practices which it is only mandated to formally describe when an EU entity contracts with an entity **outside** the EU. For entities in the UK, it is not formally necessary to write down obligations which already exist by virtue of these laws. It is understood that therefore this policy does not attempt to duplicate the mention of every obligation under the GDPR (e.g. the obligation to notify of breaches).

Modifications to this document

Some customers may have purchased services with a specific configuration – e.g. a tailored VPS to a particular specification. In such cases, this document should be read with appropriate modifications in mind where any specifics or technical details are supplied.

Activities performed

As part of providing our services, we may perform these activities:

- Process incoming web (HTTP/HTTPS or any other future protocol) or email (POP3, IMAP, SMTP, HTTP/HTTPS (webmail) or any other protocol), and respond to them in accordance with the protocols, the incoming data and your account configuration.
- Automatically log details of these incoming requests and of the results. These logs may include IP addresses, browser user agents, dates, times, usernames and other technical details. We automatically delete logs after an appropriate time period (by default on web hosting, the current week's logs and 4 weeks' of past logs are kept, then automatically deleted).
- Some technical activities may involve passing data to third-party services in order to provide our essential services – e.g. passing the name of your website to an SSL certificate provider in order to obtain an SSL certificate.
- We use helpdesk software provided by HelpScout. As such, filling in any form requesting any kind of information or assistance will usually result in data being copied to their systems. HelpScout's GDPR and privacy policies are contained on or linked from this page. Help requests going through our website may also be logged in our database. This is purged automatically on a weekly basis of old entries (any older than 90 days old).
- Any other activities unwittingly omitted from the above list which are technically essential to the provision of your purchased services, necessary monitoring, logging or auditing (whether necessary for the integrity of our services, the measurement of performance, legal compliance, or any other similarly compelling reason).

Other than these, we do not make data available to any third parties, except by the account owner's explicit request.

(Lack of) marketing partners

Since our launch in 2007 we have not bought any marketing services from any third party that involved the passing of any customer identifiers or customer data to them.

Backups

Copies of your data may be stored in our backup systems, for the necessary task of being able to restore services in the event of a catastrophic failure, criminal break-in, or other similar event. These backups are stored encrypted, and deleted after a period of time in the region of two months. They cannot have individual portions deleted from them upon request because this is technically infeasible due to the nature of aggregated, encrypted backups.

Security

We aim to protect all our services using suitable technology and in accordance with best practices. For example:

- Our servers deploy firewalls to prevent unwanted traffic, including automated traffic analysis and blocking.
- We apply anti-spam and anti-virus software, IP blocklists and other associated technical measures to protect mailboxes
- Our mailserver, webmail and FTP server can only be accessed over an encrypted connection. Our website is only available over https (SSL).
- We do not store any card details; payment processing is handled by reputable third parties (PayPal and Stripe).
- Our own computers that we operate the business through are protected with disk encryption and strong passwords.
- Our backups are also stored on encrypted storage, and/or using file-level encryption.
- We regularly apply patches to our server components to block discovered security issues. These are usually automated for the quickest possible application, unless there was a specific technical reason why that was not the best approach.

Note that our performance of these tasks on our own systems does not mean that no similar needs exist for code installed by you in your web hosting space, for which you are liable (e.g. WordPress updates, using a third-party payment processor for payments, using https if appropriate, etc.).

Right to obtain a copy of all your data

EU consumers have the right to request a copy of all the data which we hold upon them. In respect of the data in their web hosting account, this can be obtained by using an FTP client to log in to your account, and to download all the data in that account (which comprises your own uploaded website data, and access logs). In respect of email hosting, this data can be

obtained by using any IMAP client to log in to your mailbox, and downloading a copy of all your mailboxes. We do not maintain any marketing databases and do not build profiles of customer (or visitor) behaviour that contain personal information; other data we hold on you is visible inside your Simba account at https://www.simbahosting.co.uk/s3/client-details/.

Right of deletion

EU consumers have a right to request that all data relating to them is deleted. This is, by its nature, a request to close your account and end services. Note that (as explained in other parts of this document), some data may only be deleted when automated rotation/deletion of old data takes place (e.g. backups and log files). Note that rights to deletion may also be limited by other laws or other essential business needs (e.g. the need to maintain accurate accounting/taxation information) which take precedence over the GDPR's right of deletion.

Privacy breaches

We will inform of data privacy breaches in line with the requirements of the GDPR.

Relevant third party policies

We do not transfer data to third parties except as required to perform technical tasks essential to the provision and maintenance of our services. Please also consult the above section on marketing partners.

- Stripe (our payment processor for card payments) – general policy on data transfers, and privacy shield policy.
- Linode, Inc., who are one of our suppliers to provide server capacity, with whom we have a data processing agreement (which authorises Linode only to provide the contracted technical services, and not to process data for any other purpose).
- Digital Ocean, Inc., who are one of our suppliers to provide server capacity, with whom we have a data processing agreement (which authorises Digital Ocean only to provide the contracted technical services, and not to process data for any other purpose).
- Amazon Web Services (used by us to store backups of our servers) adhere to the Cloud Infrastructure Services Providers in Europe Code of Conduct – https://aws.amazon.com/compliance/cispe/ – as part of their GDPR compliance. Also, see here. Note that we only stored backups that are pre-encrypted, and Amazon have no access to the encryption key. As such, Amazon have no access to the actual data, and are not a data processor.
- We may form arrangements with other data processors, but only on the same, GDPR-compliant, principles.

Limits upon costs

In all circumstances, indemnification against any costs, claims, damages, expenses or any other liability incurred by you due to any failure on behalf of us, our employees or any agents we employ, will be limited to a refund of the total amount paid by you to us for the services purchased from us, from the time that those liabilities were incurred.

Correction of deficiencies

If you find any deficiencies in this policy document, then please let us know using the contact facility available on this website.

Legal authority

Simba IT Services Ltd. is a UK company, and all disputes that cannot be settled by mutual agreement or arbitration mutually agreed to, will be settled under the authority of the courts of England and Wales. All customers agree to make a maximum good faith effort to settle any disputes before entering any formal legal proceedings, or raising the prospect of them, and are willing for any court to look upon their case with prejudice if they have not done so.

Posted in: Small Print