SIMPLY.COM

SECURITY ENVIRONMENT

Data Processing Agreement - Appendix 1

Table of Contents

Physical security

Simply.com's data and infrastructure are located at multiple data centres in Denmark. You can therefore be sure that your data remain within Denmark. Our data centre supplier is responsible for the physical framework such as power, cooling, fire extinguishing and access control and we have stringent checks in place to ensure that our subcontractors comply with applicable security regulations at all times.

Only employees who require access for work-related purposes have physical access to the servers. Electronic access cards are used at all entry points to the data centres and this access is logged. All entry points are likewise monitored by CCTV.

Logical access

We allocate rights to employees based on work-related requirements. Only selected employees are given privileged access to the systems. We periodically check whether access to the systems has been allocated correctly.

Networks

We use a high degree of segmentation in our networks to minimise the risk of an attack spreading. Firewalls inspect traffic to client environments and DDoS protection limits the impact that any attack on the servers may have. Advanced network inspection detects patterns and attempted attacks from known, malicious IP addresses and alerts our operations department when required.

Logging

We log all access to management and client environments and use our logs for troubleshooting and investigation of any incidents.

Vulnerability management

We are responsible for the continuous monitoring of new vulnerabilities arising in the systems we operate. We have a process in place for assessing and managing new vulnerabilities. We also install patches as soon as possible after they have been released.

You are responsible for performing vulnerability management of the software/code you place on our servers – i.e. you must keep it updated yourself.

Monitoring

We monitor our infrastructure and applicable services 24 hours a day. All deviations are recorded in our incident management system. As a supplement to our monitoring, we use security 24/7.

Backup

We perform backups of our own internal systems – for client data backup, please see below. Backup data are mirrored between two independent locations in Denmark so that a copy is always available in the event of a critical breakdown.

Web hotel backup incl. e-mail
Daily backups are performed and usually stored for 30 days.

Backing up 'cloud servers'
We do not usually back up cloud servers. Backup is available as a paid option.

Encryption

Access to administrative systems/control panels takes place on encrypted TLS connections.

Web hotel encryption
If data need to be encrypted during transfer (HTTPS), this has to be set up by the user on the Control Panel. Transfer of files to the web hotel can be encrypted if this option is selected in the user's client programme.

E-mail encryption
You must actively select use of an encrypted protocol as the e-mail systems, in order to support legacy e-mail programmes, also provide the option of using non-encrypted connections.

'Cloud server' encryption
You must yourself set up encryption where required.

Data encryption
If data (files, databases etc.) are to be stored in an encrypted form, you must do this yourself within the application. Data are not usually stored in encrypted form by us.

Subcontractors

If subcontractors are able to affect our security environment, we ensure that they comply with the same stringent requirements as we do. We ensure this by using contracts, data processing agreements, audit reports, own checks and confidentiality agreements. We continuously check

that our subcontractors comply with our requirements.

Emergency response capabilities

Emergency response is about being prepared for incidents that may have a critical or catastrophic impact on operations. We therefore have emergency response plans in place that set out our procedures, routines and roles in the event of a catastrophe. Employees are trained in emergency response several times a year.

Part of our emergency response is also that we are prepared if a data breach should occur. For this, we have procedures in place for advising our clients and applicable authorities as is required by the new GDPR.

Customer responsibility

Simply.com handles security on its part of the product, i.e. the IT systems providing the web hotel and e-mail services.

You, the client, are yourself responsible for how you set up these systems and for ensuring that the software and code you place on the systems are secure.

If the data being transferred to/from your website are confidential, you should ensure that you have HTTPS protection.

If you handle sensitive data by e-mail, you should at a minimum use an encrypted connection when accessing the e-mail systems.