SISO GDPR STATEMENT

v2.1 3rd July 2020

Introduction

Siso is committed to respecting the privacy and data protection rights of its clients and users of our services. This document, therefore, sets out Siso's data protection compliance, to provide the assurances to our clients and prospective clients that we take such compliance seriously and to address some of the common questions we are asked about our company and services, with regards to the protection of personal data.

Siso is governed by UK data protection laws which include the EU General Data protection Regulation (GDPR) and the UK's implementation thereof, the Data Protection Act 2018 and any subsequent data protection law introduced in the UK. Throughout this statement terms like "personal data", "processing", "data subject", "data controller" and "data processor" have the same meaning as defined in UK data protection legislation.

This statement applies to our SaaS (Software as a Service) products.

Our GDPR commitment to our clients

As a UK company, Siso are committed to ensuring our business, services and internal processes are GDPR compliant, that we continue to maintain that compliance and ensure it meets the full requirements of the law. We are also committed to safeguarding any personal data we process on behalf of our clients and apply the same compliance standards to our clients' data, as we do our own.

Our services are compliant because:

- We check all our systems and processes to ensure they meet the requirements of GDPR, particularly in terms of ensuring appropriate technical and organisational measures are in place to ensure the security of our clients' data at all times.

- We do not allow all members of staff to access client data and what access is available, is limited to specific circumstances.

- Our staff are trained in GDPR compliance and understand their responsibilities for managing the systems that process our clients' personal data.

- We have internal policies which set out the data protection responsibilities across the whole of our business.

- We do not transfer client data outside the EEA.

- We only process data that is inputted into our systems by our clients. It is our client's responsibility to ensure it is lawful for them to process the data in the way our systems allow.

- We have implemented the appropriate contractual obligations required by Article 28 of the GDPR (in our terms of service and accompanying documentation).

- We do not make use of sub-processors or other third-party processors.

- We ensure we maintain this compliance at all times.

Our role as a Data Processor

When a client's data is placed on our servers, the client is the Data Controller and Siso, the Data Processor. We only use the data our client provides to us for the purposes of delivering the services and only as agreed in any terms and data processing agreements that have been signed.

We do not use our client's data in any way other than to provide the agreed services. We do not share any client data with third parties unless required to do so by law. Where law enforcement or other authorised parties request access to the data we store on our servers, we follow strict internal policies for dealing with such requests. Furthermore, the third parties are required to demonstrate they have a lawful reason to access the data and under what authority.

What data is processed by our services?
This will depend on the client's requirements and the service used, but typically login credentials (name, email address) for users and admin staff. Given the nature of our services it is unlikely we will ever be needed to process special category data.

Uploading client data to our services
Data will be inputted into our service via import routines, importing data from the client or manually inputted by the client's admin member of staff.

Data location

Our clients' data is stored on our own dedicated servers, hosted by Webcore at a Viatel Data Centre in Dublin, Ireland. No data is stored or transferred outside the EEA.

Security

Our Managing Director has ultimate responsibility for ensuring appropriate information security standards are applied to the technology we use and the services we provide.

Only limited members of our staff have access to our client’s data and no other third-party will have access. We do not share our client’s data with any third-party unless required to do so by law.

Our technology
Our services run on privately tenanted hardware with each client’s system using separated databases and code.

Servers are a LAPP stack in a dedicated hardware VM environment utilising vMotion and running Linux / Apache / PostgreSQL / PHP.

We can provide our clients with server diagrams and details of the Webcore infrastructure, if required.

We have three main first line security measures in place across our infrastructure:

1. Firewall
2. Malicious page request and injection attack monitoring with IP blocking
3. Failed Login monitoring with robot checker and login blocking

All sites include a 128bit SSL certificate to encrypt all data.

Maintaining security
All our employees keep up to date with all technical aspects of security and ensure the ongoing security of our systems. This means that any security patches are applied to our systems as a matter of priority (and some automatically).

We continually monitor our servers for suspicious activity. Any issues identified are fixed accordingly with the utmost priority.

Any changes or updates to our own systems are done so, always, with data protection and privacy in mind and where appropriate, in discussion with our clients.

Examples of the kinds of security hardening implemented:

- Dynamic IP blocker to protect against unauthorised access.
- Malicious page request and injection attack monitoring with IP blocking.
- Secure SSH limited to the office IP address range.
- Logins by certificate only.
- Ubuntu Unattended security patching (with email notification before rebooting).
- All data communications to and from the servers are via secure channels.
- FTP is not utilised. All file uploads are by WebDAV over HTTPS.
- Disabled Apache SSLv3.
- PostgreSQL DB servers are not externally accessible.
- Webcore monitor our servers and services via the VM infrastructure.
- Firewall and load balancing implemented.
- CGI disabled in apache.
- No cPanel or similar admin tools installed so hackers cannot exploit GUI and backend tools.
- We carry out vulnerability testing from time to time and can be tested by our clients.

Access to data by Siso employees

Furthermore, only two people (company directors) within our organisation have direct access to the database that stores your data. There are strict security protocols in place to limit access to the database for maintenance purposes plus the databases themselves, can only be accessed from within our offices (no remote access is possible).

Frontend and backend data may be accessed during a support call, if required.

No other members of staff (just the two directors) can access the database.

Service access

All access to our services is via https Secure Socket Layer (SSL) connections ensuring access to the systems via a web browser is encrypted.

Accounts on our systems are accessible either via our clients' central login services or via a local system login. If a local login option is chosen the password must be a minimum of 8 characters with at least one UPPERCASE, one lowercase and one number.

Generally speaking, our services are accessible from anywhere, unless specified otherwise by our clients. This includes being able to limit admin access to their place of work, whilst users are able to access from anywhere.

Continuity and backups

Backups are carried out on a 21-day rolling backup cycle and are stored in a secure location and encrypted. Only Siso has access to these backups from within our offices.

In terms of disaster recovery, we make use of internal VMWare solutions which we test quarterly, with backups every night and snapshots taken throughout the day. We also take backups of the server settings, code and database outside the VMWare environment. So, if there is a server outage we can easily migrate from the failing server or recover from the backups.

Siso employees

All Siso employees are trained and made aware of their responsibilities under GDPR. This includes their responsibilities with regards to access, security and processing of personal data made available by our clients through the use of our systems.

Security and data governance are covered in our employee handbooks and actively discussed as part of quarterly meetings to ensure all staff are up to date.

Physical security

Only our employees have access to our working offices. Our clients' data is stored on servers only accessible from our offices. Our servers are managed by Webcore and only Webcore staff can access the servers physically.

Third-party processors

Siso does not use any third-party processors or services for the purposes of processing the data as part of our service.

The only third-parties we use are:

- Webcore for the maintenance of our servers, but they have no access to any data. We do not have access to the servers ourselves, this is managed by Webcore.

- Our servers are hosted in Viatel's secure Data Centre (see http://www.viatel.com).

Changes to our approach

Should our approach to any aspect covered by this statement change we will make sure, where a client's data is impacted, we will notify our clients within a reasonable timeframe.

Data breaches

In the unlikely event of a breach occurring (as defined in the GDPR) we will notify you within 48 hours of the breach coming to our attention.

How our own compliance with GDPR helps our clients

Our approach to our own compliance also helps our clients with their own GDPR compliance requirements. This statement should go some way to explain our approach to GDPR compliance. By using our services, clients can be assured their use is GDPR compliant.

Data protection contact

Any questions, queries or requests for further information regarding our GDPR compliance should be sent to:

Siso Software Limited
Data Protection Officer
61c Ashley Drive South
Ashley Heath
Ringwood
Dorset
BH24 2JP

info@siso.co.uk

FAQ

What happens to client data if they cancel their contract?
We would perform a secure deletion of the data and code form our servers. After 20 days the data will have expired from the backup files.

Is data on your servers encrypted at rest?
No, we do not encrypt data at rest on the servers. Access is restricted to two managing directors of Siso and only via devices running on our internal office network. Only our provider Webcore has physical access to the servers which are racked in a secure data centre within a dedicated locked cabinet, but they are not able to access the data stored upon them. If there is a problem with the server, Webcore will replace the hardware and securely destroy any server component's which contain data. There is, therefore, no requirement to encrypt the data. We do encrypt our backups.

However, any communications to and from the hardware is via SSL, with any of our client's data entry in/out of our services being via HTTPS.

Do your services make use of any cookies or similar technology?
Yes, our services make use of cookies. But we only use essential cookies, necessary for the functioning of the service (such as managing logins to the service, screen resolution settings and display options within the interface).

How do you ensure our data is not accessible to other clients?
We use a bash build script which standardises each server instance of our HA cluster. Each system instance per client is maintained independently (separate database) and kept in its own silo and only accessible via our systems in our office.

Are you ISO27001 certified or compliant?
No.

Are you Cyber Essentials or Cyber Essentials Plus accredited?
We are currently undertaking Cyber Essentials Plus accreditation and will update this document with details once completed.

Are you Cloud Security Alliance (CSA) certified?
No.

Have your services been audited according to any particular external standards, such as ISAE 3402?
No.

Have you carried out a Data Protection Impact Assessment (DPIA)?
Our development process for our systems always includes ensuring the most appropriate security and this statement should go some way to allay any concerns of our clients. Generally speaking, though, it would be the Data Controller (i.e. our clients) who need to carry out a DPIA.