SiSo GDPR Statement

v1.1 26th January 2018

Introduction

The new EU General Data Protection Regulation (GDPR) comes into force on 25th May 2018 and will impact every organisation which processes personal data of EU citizens. It introduces new responsibilities, empowers businesses to be accountable for their processing of personal data as well as enabling EU citizens to protect their privacy and control the way their data are processed. Even though the UK will be leaving Europe, the GDPR still applies and will replace the UK's Data Protection Act 1998 when it comes into force.

Data protection definitions

Personal data is any information that relates to a living individual. It also includes any data that can be used with other sets of data to identify an individual. Typical examples of personal data are: name, identification number, location data, online identifier, email address, etc.

Processing relates to any operation carried out on personal data including collection, recording, organising, structuring, storing, using, etc. Processing also doesn't have to be by automated means which means that processing includes paper-based, non-digital systems.

A **Data Subject** is the individual whose personal data is being processed.

A **Data Controller** is the organisation which determines what personal data is collected, how it's processed and supplied.

A **Data Processor** is an organisation which processes data on behalf of a Controller. This typically means a third party who is used by the Controller to process their data (e.g. a marketing company used to send out marketing materials)

For detailed information about the GDPR and data protection, visit the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

info@siso.co.uk
+44 (0)1202 777 210
siso.co.uk

Our GDPR commitment

As a UK company, SiSo are committed to ensuring our business, services and internal processes are GDPR compliant. We engaged a consultant to advise us on elements of our services and how the GDPR changes impact our compliance. As such, this GDPR Statement provides our assurances to GDPR compliance.

By the GDPR implementation deadline, we will have put in place:

- Employee data protection training to ensure all staff understand their role in data protection compliance
- Updated our internal policies relating to data protection and responsibilities within our businesses for ongoing GDPR compliance
- Checked all our systems and processes to ensure they meet the requirements of GDPR, particularly around security of data
- Processes to ensure ongoing compliance past the GDPR deadline

Our services are compliant because:

- We have appropriate technical and personnel protocols in place to ensure the security of your data
- We do not make use of sub-processors or other third-party processors
- We do not allow all members of staff to access your data and what access that is available, is limited to specific circumstances
- We do not transfer your data outside the EEA
- Our staff are trained in GDPR compliance and understand their responsibilities for managing the systems that process your personal data

Our role as a Data Processor

You are the owner of the data you submit to our services (whether they are hosted on your premises or on our servers).

When your data is placed on our servers, you are the Data Controller and SiSo, the Data Processor. We only use the data you provide to us for the purposes of delivering the services you pay us for and only as agreed in any data processing agreements we have signed.

info@siso.co.uk
+44 (0)1202 777 210
siso.co.uk

We do not use your data in any way other than to provide the agreed services provided to you. We do not share any of your 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.

Data location

Where your data is stored externally from your establishment or institution, it will be stored on hardware located at Webcore in Dublin Ireland (https://www.webcore.cloud). No data is transferred outside of the EEA and all data communication to and from the server cluster is sent over secure channels.

Webcore maintains hardware's health of the server cluster but has no access to the data held on the servers. The servers are kept in locked cabinets and there are strict security protocols in place regarding access to the physical hardware within the data centre: No one physically accesses the servers, unless physical hardware maintenance is required and on our strict instruction. At no point is data available to the data centre staff. Any hardware which stores data and experiences a failure, is destroyed to ensure optimal data security.

Security

Maintaining security

All our employees keep up to date with all technical aspects of security and ensure the ongoing security of our systems. Where security patches are not applied automatically, security related patches are applied to our systems as a matter of priority and 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 customers.

Access to data

Furthermore, only two people 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).

There are strict protocols in place to ensure that support staff only access front-end data if required, by yourself, for support purposes.

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

Accounts on our systems are accessible via several authentication methods which rely on yours or your Data Subjects own security controls regarding protecting access to the system via these authentication methods (e.g. password security and adequacy).

Data storage
The data stored within our systems is stored on our secure servers and with full automated system security patching and locked in cabinets. The data centre will only allow approved personnel into the server rooms, who in turn can only access their specified cabinets. As a consequence, only Webcore have physical access to the servers inside the data centre.

Webcore monitors the resources used by the server cluster and the hardware health 24/7 and notify us if there are any reasons for concern. There are firewalls, intrusion protection and secure networking in place.

Backups
Backups are carried out on a 21-day rolling backup cycle.

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 you, by using 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.

Third party services
SiSo does not use any third-party suppliers or services for the purposes of processing the data as part of our service. The only third party we use are Webcore for the provision and maintenance of servers, but they have no access to your data.

Changes to our approach
Should our approach to any aspect covered by this statement change we will make sure, where your data is impacted, we will notify you within a reasonable timeframe.

info@siso.co.uk
+44 (0)1202 777 210
siso.co.uk

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. This will be enough time for you to consider your requirements, under GDPR, for reporting the breach to the ICO and Data Subjects.

We help you to comply with GDPR

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

Furthermore:

- Where required we will provide assistance and functionality to address any requirements that meet your need to respond to any of your Data Subjects' rights
- We will assist you or the Information Commissioner's Office with any query relating to the GDPR compliance of our service

Data protection contact

Any questions, queries or requests for further information regarding our GDPR compliance should be sent to info@siso.co.uk

info@siso.co.uk
+44 (0)1202 777 210
siso.co.uk