

Sirius Business Services Ltd

Data Protection Policy

INTRODUCTION

Sirius Business Services Ltd (SIRIUS) is committed to complying with the requirements of the General Data Protection Regulation (GDPR), protecting the personal, and special category data of all individuals and organisations it works with, or provides services to.

As required by the GDPR, SIRIUS is registered with the Information Commissioner's Office (ICO) as a data controller, registration number Z7604983.

SIRIUS collects and processes data to administrate and award regulated and non regulated qualifications and provide advice and consultancy services. SIRIUS does not pass on, sell, or make available any data to any other person or organisation for any other purpose.

SIRIUS's role is of 'Data Controller' in respect of non-regulated training and some advice and consultancy services and as 'Data Processor' is respect of regulated training and other advice and consultancy services.

TYPES OF DATA STORED

LEARNER DATA

SIRIUS collects, processes and stores personal data, and in certain circumstances special category data, of learners. Special category data is only collected, processed and stored for the application and potential award of a reasonable adjustment for the regulated or non-regulated qualification the learner is undertaking.

SIRIUS works with clients and awarding bodies in collecting, processing and storing learner data.

SIRIUS's role is of 'Data Controller' in respect of non-regulated training, and as 'Data Processor' is respect of regulated training.

SIRIUS collects, processes and stores the following learner personal data:

- Name
- Email address
- Grade/Job description
- Company
- Company Address
- Company Contact
- Date of birth (*regulated qualifications only)
- Personal Postcode (*regulated qualifications only)
- and gender (*regulated qualifications only)

Note : *(only if the learner has requested the achievement to be entered onto their Personal Learning Record)

SIRIUS and the Awarding Bodies collect, process and store the following special category data when provided by a learner:

- Any disability
- Any medical condition
- Any learning need

Legal basis for processing – Processing is required for the performance of a contract. Learners enrol onto a qualification directly with SIRIUS. To enable SIRIUS and the Awarding Body to deliver, administrate and award the qualification, the processing of the learner's personal data, and where required special category data, is required.

How is the data used? – SIRIUS and the Awarding Body only use learner personal and special category data for the purposes of administrating, delivering and awarding the qualification the learner has chosen to undertake. SIRIUS does not pass on, sell or make available learner's personal or special category data to any person or organisation external to the administration and award of the learner's qualification. SIRIUS does not use learner data for any marketing purposes; it is purely used for the administration and award of the relevant qualification.

Is learner's personal or special category data ever shared? – The only situation in which learner data would be shared is in the event of an investigation by the Awarding Body or Regulatory Bodies or by an official legal body such as the police.

How is the information provided to SIRIUS? – Learner's personal and special category data is provided by the learner to SIRIUS and the Awarding Body during qualification enrolment through the completion of official SIRIUS/Awarding Body course paperwork/ documentation.

Where is this data stored? – Data is entered onto SIRIUS's or the Awarding Bodies course paperwork/documentation. Course paperwork/ documentation is stored securely in either hard copy or electronic format. The data is processed and entered onto the Awarding Bodies secure online administration system.

How is data destroyed? – Electronic data is securely deleted from all relevant computer systems when required and all backup copies and archived copies are permanently deleted. Hard copy paperwork/documentation is destroyed through a contract with a certificated disposal company. Paperwork/documentation and computer records held by SIRIUS is stored in compliance with the GDPR, and standards set by the Awarding Bodies and Regulatory Bodies.

How long is data held? – Learner data is held indefinitely to allow SIRIUS and Awarding Bodies to provide the learner with confirmation of their achievements should it be required. Learners have the right to erasure of their data and SIRIUS and the Awarding Bodies will do so in line with their relevant privacy notices.

SIRIUS APPROVED TRAINING CENTRE DATA

SIRIUS collects and stores the (centre and relevant personnel) data required for the operation of a regulated training centre. The data is collected and stored at the time of registration as a centre. The data is updated when requested by the Awarding Organisation. The centre data is also held on the Awarding Bodies secure online administration system

The data is only accessible to approved SIRIUS team members through a unique and secure log in.

SIRIUS and the Awarding Body collects, processes and stores approved Centre data regarding:

- The Centre itself
- The appointed Centre Head
- The Centre's registered Trainer/Assessors
- The Centre's quality assurance staff

Only the following personal data is collected and stored:

- Names of Centre staff
- The Centre's postal address
- Phone numbers
- Email addresses

Legal basis for processing – Processing is required for the performance of a contract.

How is the data used? - SIRIUS and the Awarding Body does not pass on or make available to any person or business, personal data of a Centre or their personnel. The data is only used for administrating, quality assuring and awarding the Awarding Bodies qualifications. Awarding Bodies have a regulatory duty to ensure the approved Centre is operating as per required regulations and to do this are required to process the Centre and Centre staff's data.

How is the information provided to the Awarding Body? – Data is provided to the Awarding Body at the time of Centre registration. Data is collected both electronically, in the format of PDF and image documents, and in hard copy format.

Where is this information stored? – This information is stored electronically on the Awarding Bodies secure online administration system Sand on SIRIUS's secure internal computer server. Access to both systems is available only to approved SIRIUS team members each with a unique user name and password.

How is data destroyed? – Electronic data is securely deleted from SIRIUS's computer systems when required with all backup and archive copies also being permanently deleted. Paper documents are destroyed through a contract with a certificated disposal company.

How long is data held? – SIRIUS and the Awarding Body hold Centre and Centre personnel data indefinitely for archiving and record keeping purposes allowing SIRIUS and the Awarding Body to respond to enquiries/complaints and requests for information from the Regulatory Bodies.

CLIENT DATA

SIRIUS collects, stores and processes data required for the provision of advice and consultancy services to its customers. SIRIUS collects, processes and stores personal data, and in certain circumstances special category data, of client's staff, customers or members of the public they come into contact with. Special category data is only collected, processed and stored for the purposes of investigating or advising on safeguarding, security, fire, accidents, incidents and other health and safety matters.

The data is collected and stored at the time a new client is gained and can be added to or updated when required by SIRIUS or the client.

The data is only accessible to approved SIRIUS team members through a unique and secure log in.

SIRIUS collects, processes and stores the following general client data.

- The Clients name
- The approved contact point
- The names of the clients key staff

Only the following personal data is collected and stored:

- Names of key staff
- Their work postal address
- Phone numbers
- Email addresses
- Names of staff, customers or members of the public
- Address of staff, customers or members of the public

SIRIUS (where necessary) collects, process and stores the following special category data when provided by a client in relation to staff, customers or members of the public:

- Any disability
- Any medical condition
- Any learning need
- Injury sustained
- Treatment given
- Where treatment was given

- Criminal records and convictions

Legal basis for processing – Processing is required for the performance of a contract or for meeting a legal obligation.

How is the data used? - SIRIUS uses the data for the purposes of providing advice. SIRIUS does not pass on or make available to any person or business, personal data of a Client or their personnel. Regulators etc.

How is the information provided to SIRIUS? – Data is provided by the client, the clients staff, customers or members of the public on a when required basis. Data is collected electronically, in the format of PDF and documents, and in hard copy format.

Is clients' personal or special category data ever shared? – The only situation in which data would be shared is in the event of an investigation by and Enforcing Authority, Regulatory Body or by an official legal body such as the police

Where is this information stored? – This information is stored in hardcopy or electronically on the SIRIUS's secure internal computer server. Access to SIRIUS's system is available only to approved SIRIUS team members each with a unique user name and password.

How is data destroyed? – Electronic data is securely deleted from SIRIUS's computer systems when required with all backup and archive copies also being permanently deleted. Paper documents are destroyed through a contract with a certificated disposal company.

How long is data held? – SIRIUS only holds data as long as required to undertake a specific task, or to perform a contracted service, or to respond to enquiries/complaints and requests for information from clients or Regulatory Bodies.

SIRIUS INTERNAL BUSINESS ACTIVITIES

SIRIUS collects and stores the personal data of employees and other contracted team members. Data includes names, addresses, contact phone numbers, email addresses, qualifications, DBS status and bank details. SIRIUS employee data is purely used for the purposes of their employment. SIRIUS engages staff either on the basis of direct employment or on a freelance basis.

Legal basis for processing – Legal obligation.

How is the data used? - SIRIUS has a legal obligation to store and process employee's data. Employee data is never passed on to any business or person external to SIRIUS and is only used in respect of fulfilling SIRIUS's duty as an employer.

How is the information provided to SIRIUS? – This information is provided to SIRIUS by the employee at the time of employment.

Where is this information stored? – This information is stored on SIRIUS's secure computer server.

How is data destroyed? – Any paper documents are destroyed through a contract with a certificated disposal company. Employee data is held indefinitely to allow reference should any legal requirement require it.

TRANSFERRING PERSONAL DATA

When transferring personal, and special category data externally, SIRIUS will ensure that all data is both encrypted and password protected. SIRIUS uses the SendSafely product for sending either encrypted attachments, or fully encrypted emails this provides end-to-end encryption utilising the OpenPGP message format with a 256-bit symmetric AES encryption key. The files are can only de decrypted by use of a Password Key there are various ways that these keys can be sent, including completely separately through SMS messages.

STORAGE OF PERSONAL DATA

The SIRIUS IT server is secured using various means of Software and Physical security. The server has mirrored hard drives to ensure availability of data in the event of the failure of one of the hard drives. Protection includes monitoring software to detect attempts to breach the systems security. All personal data and special category data is stored on separate enhanced secure area of the SIRIUS IT server and is secured using FIPS 140-2 Validated 256 bit AES encryption.

BACKUP OF PERSONAL AND OTHER DATA

All data held by SIRIUS on our IT server (including personal data and special category data) is backed up to an offsite company who fully meet appropriate security and GDPR standards. This backup facility uses the AES-256 encryption algorithm to encrypt data before it leaves the SIRIUS IT server, so that the only SIRIUS staff are able to access the contents of data backup once it has been restored and de encrypted. We have immediate access to these backups (24/7) to ensure business continuity and recovery of lost data at any time.

EXTERNAL LINKS FROM SIRIUS WEBSITES AND RESOURCES

SIRIUS websites and resources may include links to other external websites. We recommend that you review the Privacy Policy of the website before input of any personal data. The Internet is not a secure medium and SIRIUS cannot guarantee the security of information transmitted via the internet.

POLICY REVIEW

SIRIUS will review this policy on a regular basis to ensure its effectiveness and taking into account any feedback. Should you have any feedback regarding this policy then please contact SIRIUS as below.



Gary Hepburn
Managing Director

10 May 2018