

## Policy Statement

SCCS is committed to protecting the privacy and security of data as defined within the General Data Protection Regulations 2018.

This policy, when read in conjunction with (all) Company policies set out how it will identify and control data to achieve compliance with the said regulations.

## Scope

This policy statement applies to:

- All Company business operations for the purpose of the supply, hire, repair, service and calibration of surveying equipment to its customers.
- All Company business operations for the purpose of providing technical support, consultancy and training pertaining to surveying equipment to its customers.

## Definitions

**“Company”** shall mean SCCS Survey Equipment Ltd

**“SCCS”** shall mean SCCS Survey Equipment Ltd

**“Senior Management Team”** shall mean Regional Director, Operations Director and such other personnel deemed appropriate by the Regional Director

**“Data Controller”** shall mean the person or persons within the Company that determine when, why and how to process personal data. They are responsible for establishing practices and policies for the use of data relating to the Company and personal data used by the Company for its own commercial purposes.

**“Data Subject”** is a living, identified or identifiable individual about whom we hold personal data.

**“Personal Data”** is any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes sensitive data but excludes anonymous data or data that has had the identify of an individual permanent removed. Data can be factual or an opinion.

**“Data Breach”** shall mean any act or omission that compromises the security, confidentiality, integrity or availability of data. The loss, or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

**“Processing”** is the act by which Personal Data is used. This includes obtaining, recording, retrieving, using, disclosing, erasing, holding & destroying data.

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

“**Sensitive Personal Data**” is information which reveals racial or ethnic origin, political views, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual orientation, biometric or genetic data and Personal Data relating to criminal offences and convictions.

## Policy Aim & Commitments

### Company Commitment:

The Company is committed to:

- Compliance with all current applicable (relevant) GDPR legislation to meet its legal obligations
- Ensure all its personnel (and any agent acting on its behalf) are suitably trained on the content of this policy.
- Transparency of data use
- Safe handling and use of data in accordance with agreed parameters
- Facilitation of requests to review data held
- Prompt administration & conclusion of requests for data removal

### Employee Commitment:

- To work in accordance with the remit of this policy and as trained.
- To seek guidance, as appropriate, where doubt regarding legal compliance exists.
- To report recognised breaches of data protection to the Company Data Protection Coordinator.
- Not to download onto any external hard drives, memory sticks or similar any data held by the Company unless permission has been granted by the Senior Management Team.
- Where work has been contracted to completed on a third party (management) system no information contained in that system shall be shared, copied, discussed or passed on outside that third party without the permission of the third party.

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

- When making visits (such as customer or supplier or other connected third party) Company personnel will focus only upon the work associated with the scope of the visit and will not work outside that remit (particularly if there is potential to breach the requirements of data protection).
- On leaving a workstation any PC or laptop must be locked so it cannot be viewed by unauthorised personnel.
- Outputs from Company meetings may only be disseminated to those personnel approved and agreed within the said meeting.

## Benefits & Purpose of GDPR Regulations

GDPR legislation provides a set of rules to give Data Subjects more control over their personal data.

The main goal of the legislation is to ensure increased privacy and protection of personal data (including but not limited to name, identification, location data, home and email addresses, logins and passwords)

Data Subjects are provided with a right to know when their data has been hacked.

Data Subjects are able to establish how their personal data is being processed

Data Subjects must be given an easy way to opt out of their personal data being used or stored in any manner they do not desire

Data Subjects have the right to be forgotten (removal of personal data). In some circumstances there may be legitimate grounds for retention. If in doubt refer both to the current legislation and the Hexagon Group Compliance Team.

## GDPR Definitions

Personal data is any information that directly or indirectly relates to an identifiable individual.

Data Subjects is an individual whose personal data is being processed (and have defined legal rights under GDPR legislation).

Typically, a data subject would include (but not be limited to):

- Employees
- Candidates (recruitment)
- Customers
- Suppliers

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

Processing refers to the act of handling personal data. This typically might include collecting, structuring, storing, adapting, using, transmitting and/or erasing personal data.

Controller refers to any entity determining why and how personal data is processed

Processor refers to any entity processing data on behalf of another company (such as a service provider).

A data processor agreement is any agreement made between a Controller and Processor.

## Identified Data

The Company has identified the use of the following types of data in the course of its operations (the list is not exhaustive):

- Employee HR records including, but not limited to name, date of birth, emergency contact information, contractual arrangements, sickness records, medical information, job performance information and other general HR data which might be reasonably required.
- Customer data including, but not limited to, name, telephone numbers, email addresses, purchase orders, pricing arrangements, card payment information (which is immediately deleted after payment is processed) site documentation and other general communications.
- Supplier data including, but not limited to, key contact names, telephone numbers, email addresses, pricing arrangements, supplier audit information, and other general communications.
- Visitor data including, but not limited to, names, telephone numbers, email addresses, other general communications.

## Consent, transparency, and processing

Personal Data may only be used:

- On the basis of one or more of the lawful basis's set out under GDPR legislation.
- Must be used with consent

A Data Subject consents to the processing of their Personal Data if they indicate agreement clearly either by a statement or positive action. Silence cannot be construed as consent to use (Processing).

Data may only be Processed in accordance with the terms of the consent granted.

Data Subjects must be able to easily withdraw consent to Processing at any time and any such request must be promptly honoured.

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

Further consent must be obtained when there is an intention to process Personal Data for a different and incompatible purpose which was not disclosed to the Data Subject when consent was granted.

Only explicit consent is acceptable for Processing or Sensitive Personal Data. Such consent must be captured (recorded) so that the Company can demonstrate compliance with consent requirements.

All GDPR notices must be concise, transparent, intelligible, easy to access and in clear plain language (so that the Data Subject can easily understand them).

Whenever Personal Data is collected/processed in accordance with this policy the Company must provide the Data Subject with all necessary GDPR information including the identify of the Data Controller, how and why we will use, process, disclose, protect and retain that data.

When Personal Data is collected indirectly the Data Controller must provide the Data Subject, as soon as practicable, all the information referred to in 2.8 above.

## Limitation of use and minimisation

- Personal Data must only be collected (and processed) for specified and legitimate purposes and in a manner which is compliant with GDPR legislation.
- You may not store Personal Data for new, different or incompatible purposes from that which was disclosed to the Data Subject without fresh informed consent.
- Personal Data must be relevant and limited to only that which is necessary in relation to the purposes of its use.
- Employees are required to only use data in a manner consistent with their job role and the remit of this policy.
- Once data is no longer required for the specified purpose it will be deleted or anonymised and/or secured from the potential for incorrect use without consent.

## Data Accuracy

- Personal Data must be accurate and, where necessary, kept up to date.
- Whenever data is found to be inaccurate it must be corrected or deleted without delay.
- Where data is held it should be checked for accuracy at regular interval.

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

## Retention of records

The Company will retain data for as long as necessary to fulfil the purpose it was collected for (or as may be required for compliance with relevant applicable legislation).

The Company backs up its systems to an off-site location (in Switzerland) at Hexagon (its Parent Company) where it is securely held.

Data is retained for periods set out within individual Company policies but more specifically:

- Records relating to employee occupational health for a period of not less than 40 years (or indefinitely).
- Records relating to drug tests (where result was negative) for a period of not less than 10 years
- Records relating to drug tests (where the result was positive) indefinitely

The Company will take all reasonable steps to destroy or erase from its systems all Personal Data after a reasonable time from the point of collection for the purpose it was required.

No person in the Company shall retain Personal Data which permits the identification of a Data Subject for longer than needed for a legitimate Company business purpose and for the purpose for which it was originally collected for processing.

## Privacy Officer (Structure Overview)

The Group have appointed a "Group Privacy Officer" to oversee data protection matters.

The "Group Privacy Officer" oversees a Core (Compliance) Team.

The Core (Compliance) Team contains Privacy Leads.

Each legal entity in the Group shall contact at least a Data Protection Coordinator

The identify of the SCCS Data Protection Coordinators is:

- SCCS HR Business Partner and
- Digital Marketing Manager

## GDPR access, amendment, objection & erasure rights

A Data Subject has a right to make a Data Subject Access Request. This entitles the subject to receive a copy of information held about the Data Subject to check that the Company are lawfully processing it.

A Data Subject has the right to request the correction of data held by the Company where that data is incomplete or inaccurate.

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

A Data Subject may make a request to delete or remove personal information where they exercise their right to object to processing of data.

A Data Subject may object to the processing of data.

A Data Subject may request to restrict the processing of data whilst, for example, the accuracy of said data is checked.

A Data Subject may request the transfer of its Personal Data to another party.

The Data Subject will not have to pay a fee to access their Personal Data (or to exercise their rights), however, the Company may charge a reasonable fee if the request is clearly unfounded or excessive. Alternatively, the Company may refuse to comply with the request in those circumstances.

To assist the Company with any request set out in this section the Company will need to confirm the Data Subject's identity to ensure they have the right of access to information.

Any employee receiving a request from a Data Subject must immediately escalate the request to the appointed personnel set out in this policy to ensure said personnel can meet with Group target response rates for handling of access requests.

## Handling subject access requests (SAR) and requests to erase data (ED)

**All SAR and ED requests must be immediately referred to Hexagon Compliance team.**

Email: [privacy.geo@hexagon.com](mailto:privacy.geo@hexagon.com)

Within the subject line of your email communication address it as follows:

- GDPR: Subject Access Request, or
- GDPR: Data Subject request to Erase Data
- Once the email has been sent, a copy should be forwarded to the SCCS Data Protection Coordinators.

The identity of the SCCS Data Protection Coordinators is:

- SCCS HR Business Partner
- Digital Marketing Manager

## Handling potential breaches of GDPR Regulations

**There are very strict time scales for handling breaches of GDPR Regulations. As soon as you suspect a breach you must act immediately.**

Do **NOT** contact the parties to a breach (communications are handled directly by Group Compliance) as this could have liability implications. The only exception to this rule is set out below.

# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

If a party has wrongfully received data (pertaining to another Data Subject) please contact that receiving party to request deletion of the data that they have “received in error”. Also request confirmation of the deletion in writing. Do not state in writing that a breach of GDPR has occurred.

Any personnel suspecting a potential breach of GDPR Regulations must immediately refer details of the suspected breach to the Hexagon Compliance Team.

Two options are available for reporting the suspected breach.

1. If you have access, the breach can be reported using the following online form:  
<https://hexagongeosystems.service-now.com/sp>
  - When completing your report to Group Compliance you should provide as much detail as possible including:
    - Date of suspected breach
    - Details of parties to the breach including contact details for the parties
    - How the breach occurred (example: email communication)
2. Email: [privacy.geo@hexagon.com](mailto:privacy.geo@hexagon.com); Within the subject line of your email communication address it as follows:
  - GDPR: Suspected breach of GDPR within SCCS
  - Within the body of the email include information as referred to above.
  - Once the email has been sent, a copy should be forwarded to the SCCS Data Protection Coordinators.

The identity of the SCCS Data Protection Coordinators is:

- SCCS HR Business Partner
- Digital Marketing Manager



# GDPR POLICY

Policy Reference:	011.4.2021.PL
Revision No:	5
Date of Revision:	29.08.2024
Reviewed by:	Roz Wankling
Approved by:	Kevin Smith

## Compliance and Review

The Senior Management Team will be responsible for managing the compliance of all its personnel with the remit of this policy and all its working practices and procedures.

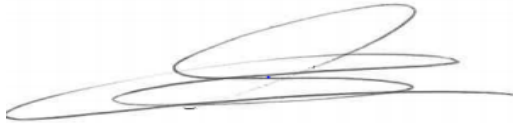
This policy will be reviewed at least annually, or as other circumstances dictate (such as changes in legislation).

The Senior Management Team will be responsible, in conjunction with the Company Data Protection Coordinators, for reviewing all data held for the purpose of carrying out its business operations (business management systems).

The Senior Management Team are responsible for the appropriate review of the remit of this policy.

All Company personnel are responsible for working as trained, in accordance with this and all other Company policies and procedures.

**Signed:**



**Print name:**

Kevin Smith

**Position:**

Regional Director

**Date:**

29<sup>th</sup> August 2024

**Revision**

5

**Next review:**

28<sup>th</sup> August 2025