Data Privacy Policy

Last updated: 25 January 2025

Contents

Purpose
Everyone is entitled to privacy and that means handling everyone's personal data in the right way.

UK General Data Protection Regulation (UK GDPR) evolves from the Data Protection Act 1998 (DPA) to protect personal information in the computer age. UK GDPR has a wide scope and places compliance obligations on Data Controllers and strengthens the rights for customers and employees. European Geophysical Services Limited collects, stores and processes personal data about our employees, customers, suppliers and other third parties. We recognise that the correct and lawful treatment of this personal data will maintain confidence in the organisation and will provide for successful business operations.

This Data Privacy Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, suppliers or any other Data Subject.

Scope
Our Company Data Privacy Policy applies to you if you are employed by or carry out work on behalf European Geophysical Services Limited and extends to any employees, contractors, temporary employees and agency workers.

You must read, understand and comply with this Data Privacy Policy when processing Personal Data on our behalf.

You must comply with all Related Policies and Privacy Guidelines issued by the Company.

This Data Privacy Policy does not set terms or conditions of employment or form part of an employment contract.

Any breach of this Data Privacy Policy may result in disciplinary action or termination of agreements.

Aim
Our aim is to ensure that the Personal Data of our customers, suppliers, employees, workers and other third parties, together with other confidential information:

- remains safe and secure;
- is treated correctly and lawfully; and
- is managed in accordance with this Data Privacy Policy.

Our aim is also to ensure that our employees are aware of and understand their privacy responsibilities.

We do this to maintain confidence in our Company and to provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

Policy
What is personal data?
Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession).

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour (for example, employee performance reviews or customer rating).

Special category data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition and sex life or sexual preference.

When special categories of personal data are being processed, additional conditions must be met and typically we must either obtain the explicit consent of the data subject to record, use and store that data or

be required to process such special categories of personal data to comply with our legal obligations or be in the public interest.

Criminal allegations or offences are subject to the same additional conditions as special categories of data.

Lawful Basis for Processing
Under Article 6 of UK GDPR, we are only allowed to process personal data on the basis of one of the following legal grounds:

- Legal obligation – To comply with a legal obligation to which European Geophysical Services Limited is subject;
- Performance of contract - the processing is necessary for entering in to or for the performance of a contract with the data subject;
- Public task - to perform a specific task in the public interest that is set out in law;
- Legitimate interest - for the legitimate interest of European Geophysical Services Limited or the party to whom the personal data is disclosed; or
- Vital interest - for the vital interest of our customers or employees;
- Consent - the data subject's consents to the processing.

When we process personal data, we should adhere to the six key principles of UK GDPR:

- Lawfulness, fairness and transparency - We will process personal data lawfully, fairly and transparently
- Purpose Limitation - We will only use data for specific purposes which individuals have been made aware of
- Data Minimisation - We will only hold the minimum amount of personal data required for our processing purposes
- Data Accuracy - We will keep personal data we hold accurate and up-to-date
- Data Retention - We will not hold personal data we no longer require
- Data Security - We will hold personal data securely and protect it against misuse, loss or damage

The Accountability Principle
In addition, we also ensure that we take responsibility for what we, our Company and contract partners do with personal data by:

- Adopting and implementing data protection policies;
- Taking a 'data protection by design and default' approach as defined by UK GDPR;
- Putting written contracts in place with organisations that process personal data on your behalf;
- Implementing appropriate technical and security measures;
- Recording and, where necessary, reporting personal data breaches;
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;

Our Customers and Employees Rights
- Right of access - You have the right to ask us for copies of your personal information.
- Right to rectification - You have the right to question any information we have about you that you think is wrong or incomplete. Please contact us if you want to do this. If you do, we will take reasonable steps to check its accuracy and correct it.
- Right to erasure - You can request the deletion or removal of personal data where there is no reason for its continued processing. This right is also known as the "Right to be Forgotten".
- Right to be informed - You can ask for details of how we process your personal data, as covered by our Privacy Notice.
- Right to object to processing - You can request that your personal data is not processed for specific purposes such as direct marketing.
- Right to restriction of processing - You can request that no further processing of
- the personal data we have previously collected occurs.

- Your right to data portability - In certain circumstances, you can request that we transfer personal information that you have provided to us to a third party.

Storage Limitation
The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time, unless a law requires such data to be kept for a minimum time.

You must comply with the Company's retention policies and procedures.

Data Subjects should be informed of the period for which data is stored and how that period is determined. If specific retention periods are not available, Data Subjects should be advised of the criteria used to determine that retention period. This information must be included in in any applicable Privacy Notice.

Security Integrity and Confidentiality
Protecting Personal Data
Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are also responsible for protecting the Personal Data we hold and you must follow all procedures we put in place to maintain the security of all Personal Data which includes complying with the Company's Information Security Policy.

We will only transfer Personal Data to third-party service providers who have or agree to put technical, organisational and security measures in place.

Reporting a Personal Data Breach
The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator, which in the UK is the Information Commissioner and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Managing Director. You should preserve all evidence relating to the potential Personal Data Breach.

Transfer Limitation
You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if certain conditions apply, the most relevant of which are:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism; or
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks.

Record Keeping
The GDPR requires us to keep full and accurate records of all our data Processing activities, including records of Data Subjects' Consents and procedures for obtaining Consents. These records should include, at a

minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

Training and Audit
We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws.

You must undergo all mandatory data privacy related training.

We must also test our systems and processes to assess compliance.

Privacy by Design and Data Protection Impact Assessment (DPIA)
We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

We must also conduct DPIAs in respect of high-risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM; and
- large scale Processing of Sensitive Data.

A DPIA must include:

- a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

<u>Automated Processing (including profiling) and Automated Decision-Making</u>
Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless: (i) a Data Subject has Explicitly Consented; (ii) the Processing is authorised by law; or (iii) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (ii) or (iii) will not be allowed, but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed of their right to object when you first communicate with them. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Direct marketing
We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data
You may only share the Personal Data we hold with another employee, agent or representative of our Company (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any cross-border transfer restrictions (if applicable) and an appropriate agreement is in place.

- You may only share the Personal Data we hold with third parties, such as our service providers if:
- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to put appropriate organisational, technical and security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a written contract containing GDPR approved third party clauses is in place.

Our Responsibilities
Our employees' responsibility
We are all responsible for protecting our employee and customer data in our roles. Employees need to consider and implement the commitments made in our Company Data Privacy Policy when performing your work activities and when making decisions.

Our leaders
Our leaders are responsible for making proper arrangements to ensure compliance with this Company Data Privacy Policy.

If you have a question or a concern about this policy or any security matter, you can contact the Managing Director.

Management and Administration
The Managing Director will be responsible for the management of this Policy and has final authority over this Policy.

Any requests for changes to the Policy should be made to the Policy owner. Any changes shall be reviewed and approved in accordance with European Geophysical Services Limited policy review process.

Questions regarding this Policy, or suggestions for new policies or suggested changes to existing policies should be directed to the Managing Director.

James Whitford
Managing Director

Document Details
Owner: Managing Director
Approved By: Managing Director
Date of Approval: January 2025

Version no.	Ref Number	Last Review Date	Next Review Date	Author	Version Update
1.0	008	25/01/2025	31/12/2026	HR	Published