Data Protection Policy

Wood is committed to compliance with data protection and privacy laws globally. As a responsible organisation we respect the personal data and data protection rights of all individuals. This Policy explains the key principles which you must comply with when handling personal data of clients, contacts, suppliers and colleagues.

Purpose:

A breach of data protection law can have a significant impact on a company's reputation. It could impact its share price or expose it to claims for breach of contract by its counterparties. In addition to reputational damage, organisations that breach data protection laws can be fined for breaches. Levels of fines vary from country to country but can reach as high as 4% of global turnover. Regulatory authorities can also impose sanctions such as prohibitions on processing data, audits and/or monitoring arrangements.

Breaches of this Policy will be taken seriously and may result in disciplinary action.

Scope:

The policy applies to all Wood people across our global organisation and is reviewed regularly. Regardless of business or location, we are all responsible for complying with this Policy. In this Policy, "we" "you" or "our" refers to Wood employees, including short-term workers and consultants working within Wood, officers and directors. We also expect our business partners, such as agents, suppliers, contractors, intermediaries, representatives and joint venture partners, to follow the principles set out in this Policy.

Policy Requirements:

As a global business operating in many markets, Wood applies the following data protection principles:

- We ensure we are legally entitled to process personal information under applicable data protection law ("lawful grounds") and that no personal information is used for unlawful or discriminatory purposes;
- We are transparent with individuals about what personal information we process and why ("transparency");
- We only use personal information for the purpose for which it is collected ("purpose limitation");
- We collect the minimum personal information necessary for the purpose for which it is processed ("minimisation");
- We keep personal information accurate and up-to-date ("accuracy");
- We respect an individual's data subject rights ("data subject rights") and provide access and information about the information we hold about them;
- We keep personal information secure when it is used internally and when it is shared with third parties and take steps to ensure that no damage is caused from the processing of the data ("security");
- We only allow the transfer of or access to personal information outside a country if appropriate data transfer arrangements are in place;
- We build appropriate data protection compliance into any new project, system or way of working that involves personal information processing or new uses of personal information ("data protection by design and default").

Roles and Responsibilities:

Wood has a Privacy Team, sitting within the Ethics and Compliance team and led by the Group Data Protection Officer. The Privacy Team can be contacted on all matters referred to within this Policy at privacy@woodplc.com.

Complying with Data Protection Principles:

Lawful grounds to process personal information

We must only process personal information if permitted under data protection law. The main grounds which permit us to process personal information are the following:

- To comply with a legal obligation (for example, as an employer Wood may be required to process certain information about employees);
- To protect the vital interests of the individual (for example, if there is a medical emergency);
- For performance of a contract with the individual or to perform steps prior to entering into a contract at the request of the data subject;
- For the legitimate interests of Wood or a third party but only if individuals' rights do not outweigh those interests; and/or
- Where the individual has given their consent (although this should only be sought if one or more of the other grounds above do not apply or it is more appropriate under local law).

When deciding whether to collect personal information we should always consider whether the purpose could be equally as well achieved if the personal information was anonymised or pseudonymised.

The laws of many countries have additional special requirements for processing personal information which is regarded as particularly special or sensitive. This includes data about race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for identifying a person), health data and data about sex life or sexual orientation. Special requirements often also apply to criminal records and children's data.

Sensitive data, criminal records or children's data must not be collected unless the collection and processing have been reviewed and approved by the Privacy Team.

Relying on Consent

Whenever relying on consent to process personal information we must make sure that consent is:

- Documented so we demonstrate we have obtained consent lawfully;
- Given affirmatively (such as ticking a box or signing a document) – we cannot rely on 'inaction' as a way of obtaining consent (e.g., no pre-ticked boxes);
- Informed so that the individual who is giving consent has clear information about the personal data processing being agreed to;
- Freely given and retractable at any time – it must be as easy to withdraw as to give consent; and
- Not 'tied' i.e. conditional on accepting services/offers.
- Compliant with applicable country laws.

Transparency, purpose limitation and minimisation

When we collect personal information, we only collect the minimum information necessary for the intended purpose of collection.

Before or as soon as possible after collecting any personal information, Wood must provide the relevant individual a privacy notice. A privacy notice must contain certain information. Wood has privacy notices on its website, our home page, the Privacy Page and in other locations where certain data is used or requested. The Privacy Team administers Wood's privacy notices and should be notified of any change of processing of personal information.

Personal information should only be used for the purpose for which it was collected. If that changes or if you want to use it for another purpose then the applicable privacy notice will need to be amended.

Personal information should only be retained for as long as necessary for the purpose it was collected. Privacy notices describe how long the personal information is kept for the relevant purpose. Further information about how to apply retention and destruction and specific retention periods are set out in the Data Retention Standard.

Accuracy

Personal information must be kept accurate. When personal information is collected, responsibility for caring for it should be allocated to an owner along with a clearly understood process for keeping information updated and accurate. For example, by self-service systems, regular verification exercises or by providing information to individuals so they know who to contact if their details change.

Security

Personal information must be kept secure and protected from any unauthorised access, accidental loss, damage or destruction. Each one of us must stay familiar with and follow our security policies and procedures which are designed to protect our IT systems, our premises and the data within them (both confidential information and personal information).

Sharing Data with Third Parties

Before using any third party providers who will hold or have access to personal information on our behalf, due diligence must be carried out to verify that they meet our data protection standards for personal information and are compliant with applicable data protection laws. This is set out in our Supply Chain Code of Conduct.

Personal information should not be shared with anyone or any organisation (including other Wood group companies, joint venture partners and our service providers) unless appropriate contractual arrangements have been put in place or the disclosure is otherwise permitted under applicable data protection laws. A Data Privacy assessment of the Third Party may also be required. This can be checked with your Supply Chain or Clients Contracts' representative or directly to privacy@woodplc.com.

Data transfers

Personal information can only be transferred outside the country in which it was collected under certain conditions and must be done lawfully and appropriately. Where any data is transferred, appropriate arrangements must be in place with any third party who will receive or process the data. Arrangements might include transfers:

- To a country approved by an appropriate regulator as having adequate data protection laws to protect the personal information (an "adequacy decision");
- To an organisation subject to an approved regulatory certification scheme; or
- To an organisation that has entered into a data transfer agreement with Wood (based on approved standard contracts including the Standard Contractual Clauses (EU or UK version).

Data Protection by Design and Default, Records of Processing and Data Protection Impact Assessments

We must maintain records of processing activities involving personal information. In some regions we also need to complete Data Protection Impact Assessments (DPIAs) in relation to new systems, ways of working and amendments to systems and ways of working which process personal information in a way that is regarded as "high risk". This includes where sensitive data is collected or where automated decision making takes place. The Privacy Team operates the OneTrust system for recording personal data processing and carrying out DPIAs.

All governance systems for new projects should include the ability to identify where personal information is being processed, why it is being processed and what should be notified to the privacy@woodplc.com.

Data Subject Rights

Individuals about whom we process personal information are entitled to exercise certain rights and make certain requests with respect to their own personal information. These rights and information about the requests that can be made are explained in the Data Subject Rights Handling Policy.

Training

Business functions must ensure that all Wood employees and agency workers understand the application of data protection in relation to the personal information they work with and undertake data protection training and reminder sessions at appropriate intervals to ensure that knowledge is maintained and all leavers, movers and joiners are kept up-to-speed.

Data Protection Questions and Complaints

For complaints from individuals about Wood's processing of their personal information, please refer the complaint as soon as possible to your local data protection officer, as listed on the Privacy Intranet page, or to privacy@woodplc.com. Where appropriate, complaints will be escalated to Wood's Group Data Protection Officer.

Data Protection Law Breaches and Policy Breaches

A personal data breach is a breach of security leading to the unauthorised/accidental/unlawful loss, destruction, access, alteration or broadcast of or access to personal information transmitted, stored, or otherwise processed. A breach can result from the loss of data internally or externally. For example an email sent to the wrong person or a cyber-attack.

Each one of us is responsible for reporting personal data breaches. IT-related breaches should be reported through the IT service management tool (ServiceNow) and non-IT data breaches should be reported using the Data Privacy Incident Report Form on the Privacy intranet page or by email to privacy@woodplc.com in accordance with the Data Breach Procedure.

Definitions

Term	Definition
Personal information	(also often referred to as "personal data") any information about an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, location date, online identifiers or to one or more factors specific to that person's physical, physiological, genetic, mental, economic, cultural or social identity. Examples of this data in the employment context include but are not limited to: identification data (such as name, address, date and place of birth, photograph); contact details (such as telephone number, email, address); national identifiers (such as ID numbers, tax IDs/social security numbers, driver's licence number, passport number); education and training (educational history, professional qualification and experience, professional organisations, publications); and professional status (such as title, position, location). Examples of this data in a client or candidate context includes name and contact details on our CRM databases, email addresses, IP address, newsletter subscriptions and marketing preferences.
Processing, Process, Processed	any operation or set of operations performed upon personal information, whether or not by automatic means, such as collection, access, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer, remote access or otherwise making available, alignment or combination, blocking, erasure or deletion. Essentially the term "process" covers anything you can do with personal information.

Term	Definition
Sensitive data	personal information that contains information relating to a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for identifying a person), health data and data about sex life or sexual orientation.
Criminal records data	information relating to criminal convictions and offences or related security measures.

References

Document title	Document no.
Code of Conduct	COP-PLD-100008
Data Subject Rights Handling Policy	COP-POL-110003
Information Security Incident Response Policy	GIT-PLD-100009
Data Breach Procedure	COP-PRO-100005
Data Retention Standard	COP-STD-110008
Supply Chain Code of Conduct	SCM-POL-100001

Revision History

Rev no.	Rev date	Summary of changes
0	03-Dec-2024	Issued for Use, replaces COP-PLD-100007; Updates to content and updated references and links for new BMS and intranet.

Name Shona van Diggelen

Position Group Data Protection Officer

Date 03 December 2024