

Global Data Privacy Notice for Workers

1. Introduction

We respect the privacy rights of individuals and are committed to handling personal information responsibly and in accordance with applicable law. **It is important that you read all of this Notice carefully as it sets out how the Wood group of companies ("Wood", "we", "us" or "our") handle your personal information and the rights you have in connection with that information.** If you are in any doubt regarding the applicable standards, or have any comments or questions about this Notice, please contact us using the contact details set out at Section 11 below.

2. Scope

This Notice applies to all of Wood's workers. The term "**worker**" includes those who work on a non-permanent basis, including contingent workers, temporary and contract workers, independent contractors, consultants, professional advisors, secondees and interns. This Privacy Notice is relevant for all Wood workers, however under some local laws there is a legal requirement for a supplementary Data Privacy Notice to be provided. Please see the Appendix for a list of these countries and a link to the relevant Data Privacy Notice.

People working outside of the European Economic Area, United Kingdom (**UK**) and Canada may also have local arrangements which their HR contacts and business managers will inform them about these from time to time. This notice is in compliance with any requirements pursuant to the Californian Consumer Privacy Act 2018 in relation to workers.

3. Types of personal information we collect and process

In the course of your employment at Wood, we may process personal information about you and your dependents, beneficiaries and other individuals whose personal information has been provided to us. As a responsible and trusted employer, we want all our workers to clearly understand the types of information we may process and purposes for doing so.

The types of personal information we may process include, but are not limited to:

- identification data - such as your name, gender, photograph, date of birth, worker IDs;
- contact details - such as home and business address, personal and home telephone numbers, personal email addresses and emergency contact details;
- employment details - such as job title/position, office location, employment contract, performance, talent management and disciplinary records, grievance procedures, or medical /holiday records, details of actual or alleged incidents/violations/breaches of law, policies and procedures;



- background information - such as academic/professional qualifications, education, CV/resumé, criminal records data (for vetting purposes, where permissible and in accordance with applicable law);
- national identifiers - such as national ID/passport, immigration/visa status, social security numbers;
- family details - next of kin and dependents information, emergency contacts, marital status;
- financial information - such as banking details, tax information, withholdings, salary, benefits, expenses, company allowances, stock and equity grants;
- IT information and communications - information required to provide access to company IT systems and networks such as IP addresses, log files and login information, or any personal data which may incidental to our monitoring (as detailed further below in Section 4)
- sensitive information - such as racial or ethnic origin, religious, political or philosophical beliefs, genetic data, biometric data for the purposes of unique identification, trade union membership, sexual orientation or information about your health or sex life.

If you are a contingent worker, the types of personal information we process are limited to that needed to manage your particular work assignment with Wood and our internal business needs.

4. Purposes for processing personal information

Employment or work-related purpose

We collect and process your personal information for the purpose of managing our employment or working relationship with you: for example, your employment records and contract information (so we can manage our employment relationship with you), your bank account and salary details (so we can pay you), your equity grants (for stock and benefits plans administration) and details of your spouse and dependents (for emergency contact and benefits purposes) and your trade union membership (to deduct trade union premiums, register the status of a protected employee and to comply with employment law obligations). Failure to collect personal information for this purpose may impact the benefits that Wood can provide you.

We process your personal information using many different IT systems. This will often involve transferring your personal information internationally to our servers or those of our third-party providers, but in either case, we will be responsible for ensuring that your personal information is adequately protected.

The Wood global directory and other internal systems

We maintain a global directory of our workers, which contains your professional contact details (such as your name, location, photo, job title and contact details). We may also use your professional contact details on our internal platforms and systems such as SharePoint pages and dashboards. This information will be available to everyone in Wood to facilitate global cooperation, communication and teamwork.



Monitoring

We may monitor communications and correspondence in connection with your use of Wood's IT resources, including telephone and computer systems, and any personal use of them, by automated software or otherwise. Any monitoring we undertake, is only carried out to the extent permitted or as required by applicable laws and which we have determined is reasonable, proportionate and justifiable for our relevant purposes.

We take appropriate measures to ensure adequate and sufficient safeguards are in place to ensure your rights to privacy are preserved when we carry out any monitoring, as set out in our Monitoring Standard.

The following are examples of the types of monitoring Wood carries out;

- Monitoring of swipe card door access systems for staff or office access times, for time recording and client charging purposes;
- CCTV on our premises as provided in the CCTV Monitoring Standard;
- Automated monitoring of our websites, emails and systems such as our computer networks and connections, for security and compliance purposes, to protect business confidential information, to detect unusual activity, including the extraction or transfer of business information from Wood's systems and networks;
- e-mail monitoring and Instant messenger monitoring (for example, MS Teams information) for employment performance or misconduct purposes, or when individuals are on annual leave;
- Monitoring to ensure the protection of confidential business contact or contract information;
- Internet and Intranet monitoring, such as examining logs of websites visited or use of social media accounts and networks (for example, Yammer, Facebook or LinkedIn) for employment purposes, such as ensuring compliance with the Wood's Social Media Policy and to protect reputational interests of Wood.
- Monitoring for investigating and collecting evidence, including use of e-discovery technology, because of regulatory requirements or for legal claims purposes e.g., Subject Access Requests, fraud, Ethics and Compliance investigations, HR investigations.

Further information on the monitoring we undertake in the workplace, including the consequences of monitoring and how we do this is available in our Monitoring Standard, available on the BMS. If you have concerns or questions about any monitoring Wood may undertake, please contact us using the contact details set out at Section 11 below.

Health and safety

As part of our response to the threat of Coronavirus and in the case of any future pandemics, we may need to collect or request on a voluntary disclosure basis where permissible and in accordance with applicable law, personal information, for example your state of health, the health of those you care for and live with and your vaccination status. At all times, Wood seeks to do this proportionately and taking into account your privacy and the public interest in protecting people's health.

Diversity and inclusion and equal opportunity monitoring

We may need to collect, or request on a voluntary disclosure basis where permissible and in accordance with applicable law, some personal information about your racial/ethnic origin, gender or gender identity and sexual orientation for the purposes of equal opportunities monitoring and in order to achieve the aims set out in [Wood's Inclusion and](#)



[Diversity Consent Information and Privacy Notice.](#)

Other legitimate business purposes

We may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for general HR resourcing on a global level, IT security/management, forecasting assessment of performance, accounting purposes, or financial planning. We use your name and selected cv/resume information for certain purposes including (i) to win bids and tenders for contracts with third parties and (ii) to identify people with skills and expertise on systems such as Wood Solutions.

In some circumstances, we may need to collect, or request on a voluntary disclosure basis where permissible and in accordance with applicable law, information about your physical or mental condition to provide work-related accommodations, health and insurance benefits to you and your dependents, or to manage absences from work.

We may also process your personal information to carry out audits and reviews to confirm compliance with our internal policies and procedures, or to investigate any suspected or actual violations of law or breaches of our internal policies and procedures, or in connection with the sale or purchase of business or assets.

We may also process your personal information to investigate violations of law or breaches of our internal policies and procedures or in connection with the sale or purchase of business or assets.

Law-related purposes

We also may use your personal information where we consider it necessary for complying with laws and regulations, including collecting and disclosing worker personal information as required by law (e.g. , for tax, health and safety, anti-discrimination, labour laws), under judicial authorization, or to exercise or defend Wood's legal rights.

5. Who we share your personal information with

We take care to allow access to personal information only to those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it. Whenever we permit a third party to access personal information, we will implement appropriate measures to ensure the information is used in a manner consistent with this Notice and that the security and confidentiality of the information is maintained.

Transfers to other Wood companies

We will share your personal information with other Wood companies around the world to administer human resources, processing compensation and benefits, as well as for other legitimate business purposes such as IT services/security, tax and accounting, and general business management.

Transfers to third party service providers



We may make certain personal information available to third parties who provide services to us. We will only do so on a "need to know basis" and in accordance with applicable data privacy law.

For example, some personal information will be available to the providers of our Global HR system (Oracle), our IT business partners Wissen, our auditors and other outsourced service providers, such as our benefits administrators.

Transfers to other third parties

We may also disclose personal information to third parties on other lawful grounds, including:

- to comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process, including, but not limited to, a subpoena, government audit or search warrant; or other forms of request from any judicial, administrative or regulatory body, any government or public or government agency, any instrumentality or authority or any domestic or foreign tax, revenue, fiscal or monetary authority or agency, or in Wood's judgment to comply with applicable law.;
- to receive professional services from our professional advisors (including but not limited to tax, legal or other corporate advisors);
- to receive business services (including but not limited to services from third party suppliers, business partners and sub-contractors for business administration, support, processing, services, or IT purposes);
- in response to lawful requests by other individuals (e.g., other workers raising a data subject access request). We would carry out the balancing test required by law and weigh up your rights and the rights of the other person before deciding whether to do this;
- for the purposes of investigating any actual or suspected criminal activity or other regulatory or legal matters (including but not limited to sharing with our regulators, law enforcement or fraud prevention agencies, as well as the, courts, the police and any other authorised bodies;
- in response to lawful requests by public authorities (including for national security or law enforcement purposes);
- as necessary to establish, exercise or defend against potential, threatened or actual litigation;
- where necessary to protect the vital interests of another person;
- where necessary, to manage and minimise the threat and the risks of Coronavirus or any future pandemic in the workplace, at client sites and in relation to public health safety;
- in connection with the prospective or actual sale, assignment or other transfer of our business or assets (including to professional advisors and prospective or actual seller(s) or buyer(s)); and
- with your consent.

Where the processing of personal data is delegated to a third party, Wood will delegate such processing in writing, will choose a third party that provides sufficient guarantees with respect to technical and organizational



security measures governing the relevant processing and will ensure that the third party acts on our behalf and under our instructions. In addition, Wood will impose in writing appropriate data protection and information security requirements on such third party.

Transfers to clients

In some countries where our employees are located, we may be required to disclose personal information to clients based on other lawful grounds, including:

- to comply with our legal obligations, including where necessary to abide by law, regulation, or contractual obligations;
- To administer our employment relationship with you, including payroll and benefits for costs-based contracts when working on specific client contracts; and
- with your consent.

6. Legal basis for processing personal information

If you are a worker in the European Economic Area ("**EEA**") UK or South Africa our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect, it.

However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you (i.e., to administer an employment or work relationship with us), or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect personal information from you (e.g., comply with health and safety legislation as part of our response to Coronavirus) or may otherwise need the personal information to protect your vital interests or those of another person.

Where we undertake any monitoring of our websites, emails, and systems, we rely upon legitimate interests, except in limited circumstances, where another more appropriate legal basis may apply. Wood has several legitimate interests to undertaken monitoring, for example, to protect security of our systems and preserve confidential information, to ensure our policies are adhered to, for employment purposes and for legal reasons such as defending legal claims or investigations. We document our legal basis for all monitoring, as further explained in our Monitoring Standard available on the intranet.

As a general rule, where we process sensitive information, such as medical or health data, we will do so in order to fulfil our health and safety obligations, for the purposes of carrying out our obligations in our employment contract with you, for the establishment, exercise, or defence of legal claims, for reasons of public interest in the area of public health, such as protecting the cross-border spread of Coronavirus or any other future pandemics, or we will seek your consent.

If you are a worker outside of the EEA, UK or South Africa, in your particular jurisdiction similar rights may apply. If you have questions about or need further information concerning the legal basis on which we collect and use



your personal information, please contact us using the contact details provided at Section 11 below.

7. Transfer of personal information abroad

As we operate in markets around the world, we may need to transfer personal information to countries other than the ones in which the information was originally collected. When we export your personal information to a different country, we will take steps to ensure that such data exports comply with applicable laws. For example, if we transfer personal information from the European Economic Area or United Kingdom to a country outside, such as the United States, we will implement an appropriate data export solution such as entering into European standard contractual clauses or UK approved contractual measures with the data importer and completing appropriate assessments or taking other measures to provide an adequate level of data protection under European and UK law.

8. Data retention periods

Personal information will be stored in accordance with applicable laws and kept as long as needed to carry out the purposes described in this Notice or as otherwise required by applicable law. Data retention periods are set out in our Data Retention Standard. Where it is not specifically set out in the Data Retention Standard and except for the personal information needed to provide you with ongoing pensions or other benefits, your personal information will generally be retained for 7 years after the end of your employment or work relationship with us, to document the proper termination of your employment or work relationship (e.g. to tax authorities), to respond to employment or work-related inquiries, or to deal with any legal matters (e.g. judicial or disciplinary actions).

9. Your data privacy rights

You may exercise the rights available to you under applicable data protection laws as follows:

- If you wish to access, correct, update or request deletion of your personal information, you can do so at any time by contacting us using the contact details provided at Section 11 below.
- In addition, if you are a resident of the European Economic Area or UK, you can object to processing of your personal information, ask us to restrict processing of your personal information or request portability of your personal information. Again, you can exercise these rights by contacting us using the contact details provided at Section 11 below. If you are a visitor from outside the EEA or UK, similar rights might apply. If you have questions about or need further information concerning the legal basis on which we collect and use your personal information, please contact us at subjectrights@woodplc.com.
- If we have collected and processed your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.



- You have the right to complain to a data protection authority about our collection and use of your personal information. For more information, please contact your local data protection authority. This information can be found in the appendix below.

We will respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

10. Updates to this notice

This Notice may be updated periodically to reflect any necessary changes in our privacy practices. We will inform you of updates via an announcement in Wood News, and if the updates are material, we will also send a company wide email with an explanation of the changes.

11. Contact details

Please address any questions or requests relating to this Notice to privacy@woodplc.com, or alternatively, with your line manager, local P&O representative or Data Protection Officer for your region. Contact details for Wood's Data Protection Officers are available [here](#).

Name: Shona van Diggelen
Position: Group Data Protection Officer
Date: 11 September 2024



Appendix

Supplementary Data Privacy Notices

Country	Link to Data Privacy Notice
New Zealand	New Zealand Worker Privacy Notice
Thailand	Thailand Worker Privacy Notice
Brazil	Brazil Worker Privacy Notice
South Africa	South Africa Supplementary Privacy Notice

Global List of Data Protection Authorities (DPAs)

Country	DPA Name	Website and Contact Information
Australia	Office of the Australian Information Commissioner Australian Communications and Media Authority	Australian Information Commissioner W: oaic.gov.au E: Form available online Agency Contact Australian Communications and Media Authority W: acma.gov.au E: info@acma.gov.au Agency Contact
Austria	Data Protection Authority	W: dsb.gv.at English Home Page E: dsb@dsb.gv.at Agency Contact
Azerbaijan	The Ministry of Transport, Communication, and High Technologies	W: mincom.gov.az English Home Page E: office@mincom.gov.az Agency Contact
Brazil	National Data Protection Authority	W: gov.br/anpd/pt-br E: anpd@anpd.gov.br Agency Contact
Canada	Office of the Privacy Commissioner of Canada	W: priv.gc.ca E: Form available online
Canada -	Office of the Information and Privacy	W: oipc.ab.ca

Alberta	Commissioner of Alberta	E: generalinfo@oipc.ab.ca Agency Contact
Canada – British Columbia	Office of the Information and Privacy Commissioner of British Columbia	W: oipc.bc.ca E: info@oipc.bc.ca Agency Contact
Canada - Québec	Québec Information Access Commission	W: cai.gouv.qc.ca E: renseignements@cai.gouv.qc.ca Agency Contact
Channel Islands - Guernsey	Office of the Data Protection Authority	W: odpa.gg E: info@odpa.gg
Channel Islands - Jersey	Office of the Information Commissioner	W: jerseyoic.org E: enquiries@jerseyoic.org
Chile	There is no national data protection regulator in Chile. However, Chile's Consumer Protection Agency is the state agency charged with consumer-related data protection law enforcement. The Council for Transparency is an independent corporation of public law, with legal status, that provides guidance on the right to access information, transparency, and personal data protection.	Consumer Protection Agency W: sernac.cl/portal/617/w3-channel.html E: oficinadepartes@sernac.cl The Council for Transparency W: consejotransparencia.cl/proteccion-datos-personales/ E: contacto@consejotransparencia.cl
China	The Cyberspace Administration of China The Ministry of Industry and Information Technology Ministry of Public Security	The Cyberspace Administration of China W: cac.gov.cn The Ministry of Industry and Information Technology W: miit.gov.cn Ministry of Public Security W: mps.gov.cn
Colombia	Superintendence of Industry and Commerce	W: sedeelectronica.sic.gov.co E: contactenos@sic.gov.co
Dubai International Financial Centre (DIFC)	Commissioner of Data Protection	W: difc.ae/business/operating/data-protection/Opens in a new window E: Form available online Opens in a new window Agency Contact Webpage
European Union	European Data Protection Board (EDPB)	W: edpb.europa.eu Agency Contact Webpage
Ireland	Data Protection Commission	W: dataprotection.ie English Home Page Agency Contact Webpage
Israel	Privacy Protection Authority	W: gov.il/he/departments/the_privacy_protection_authority/govil-landing-page English Home Page E: ppa@justice.gov.il Agency Contact Webpage (scroll to the bottom)
Malaysia	Department of Personal Data Protection	W: pdp.gov.my/jpdpv2 English Home Page E: aduan@pdp.gov.my Agency Contact Webpage

Mexico	National Institute for Transparency, Access to Information and Protection of Personal Data	W: home.inai.org.mx E: atencion@inai.org.mx Agency Contact Webpage
New Zealand	Office of the Privacy Commissioner	W: privacy.org.nz E: Via form here Agency Contact Webpage
Oman	Ministry of Transport, Communications and Information Technology	W: mtcit.gov.om/ITAPortal_AR/ITA English Home Page E: info@mtcit.gov.om Agency Contact Webpage
The Philippines	National Privacy Commission	W: privacy.gov.ph E: info@privacy.gov.ph Agency Contact Webpage
Qatar	National Cyber Governance and Assurance Affairs in the National Cyber Security Agency (NCSA)	W: assurance.ncsa.gov.qa/ar English Home Page E: assurance@ncsa.gov.qa Agency Contact Webpage
Qatar Financial Centre	Qatar Financial Centre (QFC) Data Protection Office (DPO)	W: qfc.qa/ar/operating-with-qfc/data-protection English Home Page E: info@qfc.qa ; dataprotection@qfc.qa Agency Contact Webpage
Saudi Arabia	Saudi Data and Artificial Intelligence Authority	W: sdaia.gov.sa English Home Page E: Suggestions@sdaia.gov.sa Agency Contact
Singapore	Personal Data Protection Commission (PDPC)	W: pdpc.gov.sg E: Form available here Agency Contact
South Africa	The Information Regulator	W: infoeregulator.org.za E: enquiries@infoeregulator.org.za Agency Contact
South Korea	Personal Information Protection Commission (PIPC) Financial Services Commission (FSC)	Personal Information Protection Commission W: pipc.go.kr/n English Home Agency Contact (scroll to the bottom) Financial Services Commission W: fsc.go.kr/indexOpens in a new window English Home E: fsc.ifd@korea.kr Agency Contact
Thailand	Personal Data Protection Committee (PDPC)	W: mdes.go.th/mission/82 E: saraban@pdpc.or.th Agency Contact (in Thai)
United Arab Emirates (UAE)	Telecommunications and Digital Government Regulatory Authority For information on the DIFC's regulator, see the Dubai International Financial Centre entry.	W: tra.gov.ae/ar English Home page E: Info@tdra.gov.ae Agency Contact
United Kingdom (England & Wales)	Information Commissioner's Office (ICO)	W: ico.org.uk Agency Contact

Wales)		
United States	<p>No national data protection authority.</p> <p>Federal Trade Commission (FTC)</p> <p>Department of Health and Human Services (HHS)</p> <p>Office of Civil Rights (OCR)</p> <p>California Attorney General</p> <p>California Privacy Protection Agency</p>	<p>Federal Trade Commission</p> <p>W: ftc.gov</p> <p>Agency Contact</p> <p>HHS Office of Civil Rights</p> <p>W: hhs.gov/ocr/index.html</p> <p>E: OCRPrivacy@hhs.gov</p> <p>Agency Contact</p> <p>California Attorney General</p> <p>W: oag.ca.gov/privacy/ccpa</p> <p>Agency Contact</p> <p>California Privacy Protection Agency</p> <p>W: cppa.ca.gov/</p> <p>E: info@cppa.ca.gov</p> <p>Agency Contact</p>