1 Purpose

This policy amounts to a privacy notice for the purposes of the relevant data protection legislation, including, but not limited to, the European Union General Data Protection Regulation (GDPR), and contains all the information Noble is required to provide to individuals under data protection legislation.

2 Scope

This document applies to all Noble personnel, customers, contractors, and third parties on Noble-operated facilities and offshore assets worldwide. This policy is considered superseded where there is a conflict with local laws and/or regulations, unless Nobles policies are stricter than the local law, in which case this policy must apply.

3 Definitions

Data Subject: A person whose personal data is the subject of processing.

Data Subject Access Request: A request made under Article 3 of the General Data Protection Regulation (GDPR) or other applicable law.

Personal Data: Any information about an individual from which that person can be identified. Such data is referred to as personally identifiable information (PII). This can include particularly sensitive data such as race, ethnicity, political opinions, religion, trade union data, genetic or biometric data, health, and sexual orientation. This does not include data where the identity has been removed, i.e., anonymized.

4 Procedures

Noble is committed to protecting and maintaining the accuracy, privacy, confidentiality, and security of its current, former, and prospective employees PII as well as PII of Noble suppliers and customers.

This policy describes how Noble collects and uses personal data and sets out the responsibilities of individuals with respect to any personal data they may handle and use while working for or providing services to Noble. As a Data Controller and a Data Processor, Noble is responsible for deciding how it holds and uses PII about individuals. This policy is issued so individuals are aware of Nobles approach to the management of personal data.

4.1 Core Principles

In accordance with the applicable laws, the information Noble holds about individuals will be

- used lawfully, fairly, and in a transparent way;
- collected and shared only for legitimate business purposes that have been clearly explained to the individual;
- relevant to the purposes for which it was gathered and limited to only those purposes;
- accurate and kept up to date.
- kept only for as long as is necessary for the purposes communicated to the individual; and

- kept securely.

4.2 Security of PII

Noble has put in place measures to protect the security of individuals personal information and, where appropriate, carries out documented risk assessments. These prevent PII from being accidentally lost, used, or accessed in an unauthorized way; altered; or disclosed. In addition, access to personal information is limited to those employees and third parties who have a business need to know.
Employee(s) must take appropriate safeguards to protect PII, such as:

- Securing paper and other hard copies containing PII in a locked location when not in use.
- Securing computers and other access points by logging out or locking when not in use.
- Guarding and not sharing passwords and user identification numbers.
- Using shredders and other approved devices or third-party providers shredder services to destroy documents which are no longer needed for business purposes.
- Not making or distributing unauthorized copies of documents and other tangible media containing PII.
- Storing electronic files containing PII only in company approved Human Resources (HR) or other approved system(s), which have measures of specific access rights to designated employees who handle PII for Noble.
- Home computers are considered unsecure, except if used to access a secure company network via a secure portal.

Third parties will only process PII on the companys instructions and where they have agreed to treat the information confidentially and keep it secure.

4.3 Data Collection and Collection Methods

For the purpose of this policy, PII is information which does or can identify an individual, other than the individuals job title or business contact information, when used or disclosed for the purpose of business communications.
To conduct business globally and comply with applicable laws, the company collects and maintains various types of PII, including but not limited to:

- Contact information such as name, home address, telephone number, e-mail address.
- Identification information such as date of birth, social security number/national identification number, copy of passport, drivers license and/or other official documentation.
- Information about nationality, gender, race, ethnicity, marital status, and military status.

- Next of kin/dependents/beneficiary and emergency contact information.
- Work information such as employee identification number, hire date, job location, work e-mail address, work phone number, job title/position, full time/part time employment status, promotions, registration of work hours, etc.
- Financial information, such as salary and other compensation and benefits, bonus, taxes, bank account number, use of company credit card, travel expenses, etc.
- Information necessary to administer health insurance, pension schemes, and other personal benefits.
- Visas, work, and residency permits and details related to travel, such as frequent flier account details; seat preferences; home airport locations; and travel itineraries.
- Absences from work due to sickness, maternity, paternity, or other types of leave.
- Training, education, required licenses.
- Performance reviews and appraisals, results of personality or other tests.
- Disciplinary actions, performance improvement plans, grievance resolutions.
- Copies of criminal records or other information on criminal offences.
- Photo(s) and potential videos.
- Information about the individuals use of Nobles information and communications systems, usernames, and passwords.

  Such data will only be accessed or monitored if deemed necessary for purposes relating to IT security, safety, physical security, protection against intrusion and viruses; for operational, system optimization, documentation, restoring, control, and audit purposes; or in case of reasonable suspicion of activities contrary to law, contractual obligations, or Noble policies. In the event such access is deemed necessary, access will be granted to a limited number of persons upon proper approval and in accordance with the relevant Noble policies and applicable law.

Nobles use of video surveillance/CCTV is governed by the applicable regulations and policies and the areas where the company has installed video surveillance or CCTV are clearly marked with signs.

Telephone calls will only be monitored if the employee has been notified in advance, unless permitted by law, e.g., in case of reasonable suspicion of criminal activities.

Most of the data types listed above are considered non-sensitive data. However, the processing of social security/national identification number, criminal records, race, ethnicity, gender, passports, and other information may be considered sensitive data

and subject to stricter rules.
Further, in some cases Noble may be required to collect and process other special categories of PII, considered particularly sensitive personal data, as necessary, such as

- health data, e.g., in connection with a work-related injury or due to obligations imposed by law such as the Act of Sickness Benefits; or
- trade union membership, e.g., due to obligations deriving from collective bargaining agreements.

Noble collects information about individuals through the following methods:

- Application, recruitment, and on-boarding process, from both the Data Subject and an agency, if applicable.
- Pre-employment background checks and (where permitted by law) drug testing from third-party providers.
- Health information from occupational health providers and/or as a part of Nobles benefits program(s).
- Other third parties, such as former employers or other references provided by the Data Subject.
- Licensing and certifications from the organizations providing them.
- During job-related activities throughout the period an individual works for Noble.
- Through Nobles IT systems and technical solutions to ensure security of the companys premises and assets and to ensure compliance with law and Noble policies. This relates to collecting data about employees and their actions in regards to IT, internet, software, equipment, documents, electronic messages, websites visited, applications downloaded, documents sent and received (whether via e-mail, Microsoft Teams, or other means), footage on CCTV/video surveillance, access to buildings, networks, and information, etc.).

4.4 Private Personal Data

Noble highlights the importance of using business resources for business purposes only. Employees may from time to time engage in private personal communications or save private personal files within the companys IT infrastructure, and the company respects the privacy of such purely personal records. However, employees should be aware that all e-mails, messages, communication files, and documents stored within the companys IT infrastructure are accessible to and may be accessed by the company to the extent permitted by law.
Employees are highly encouraged to mark private emails as private or personal in the subject line. Even if marked as private, e-mails, messages, communication, files, and documents will only be considered private if they do not contain business related information or any inappropriate or illegal content. Files saved in My Documents will generally be considered business-related.

4.5 Use of PII

Noble will only use collected personal information when the law allows it. Most commonly, personal information will be used in the following circumstances:

- Evaluate job or employment applications;
- Manage all aspects of the employment relationship, including but not limited to, compensation, benefits, qualifications and development, attendance, performance, absence;
- Monitor an individuals use of Nobles information and communications systems, and compliance with all applicable IT policies for the purpose of protecting Noble assets, keeping Noble data and systems secure and to manage and optimize the services provided.
- Equal Opportunity and other Human Resources or DEI monitoring as required;
- Dealing with necessary due diligence in connection with any business transfer;
- Any legal obligation, such as, labor inspections, governmental reporting, e.g., social security, tax and/or work-related accidents.

Some of the above basis for processing will overlap, and there may be several business requirements that justify the companys use of an individuals PII.
An individuals personal information will only be used for the purposes for which it is collected, unless Noble reasonably considers a need to use it for another reason and that reason is compatible with the original purpose. If an individuals PII is necessary for an unrelated purpose, Noble will notify the individual and explain the legal basis that allows the use of the information.
Please note that Noble may process an individuals PII without their knowledge or consent, in compliance with the above rules, where this is required by law.
Particularly sensitive personal information requires higher levels of protection, and require further justification for collecting, storing, and using this type of personal information. Noble may process such particularly sensitive personal information in the following circumstances:

- Where it is needed to assess an individuals working capacity on health grounds, subject to appropriate confidentiality safeguards;
- Where Noble needs to carry out its legal obligations;
- Where the personal information is needed in the public interest, such as for equal opportunities monitoring or in relation to Nobles occupational pension scheme;
- In limited circumstances, with the explicit written consent of the individual.

Less commonly, Noble may process this type of information where it is needed in relation to legal claims or where it is needed to protect the individuals (or someone else's interests) and he or she is not capable of giving consent, or where he or she has already made the information public.
Noble may use an individuals particularly sensitive personal information in the

following ways:

- Information relating to absence, which may include sickness absence or family-related leave, to comply with applicable laws;
- Information related to health, where appropriate, in the context of its provision of private medical coverage;
- Information about an individuals physical or mental health, or disability status, to ensure their health and safety in the workplace and to assess their fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, and to administer benefits;
- Information about an individuals race, nationality, ethnicity, or other information required for equal opportunity monitoring and reporting.

4.6 Updating PII

Employees must properly update PII when it changes so that Noble may maintain accurate data. To do so, employees may access and change most of their PII through available resources or by contacting the HR department. Suppliers and customers should advise their internal Noble contact for updates or questions.

4.7 Failure to Provide PII

If an individual fails to provide certain information when requested, Noble may not be able to perform the contract entered into with that individual (such as paying salary or providing a benefit) or may be prevented from complying with its legal obligations (such as ensuring the health and safety of its workers).
Failure to provide PII necessary for Noble to fulfill its obligations may result in a contract with an individual being terminated.

4.8 Disclosure of PII

Noble may have to share an individuals data with third parties where it is necessary to administer the working relationship with the individual or where it has another legitimate interest in doing so. Noble requires third parties to respect the security of personal data and to treat it in accordance with the law. Noble may transfer an individuals PII to other countries and, if so, the individual can expect a similar degree of protection with respect to their PII.

4.8.1 Within Noble Corporate Structure

Certain corporate functions are shared across Noble, including HR, Finance, IT, Commercial and Legal. Accordingly, some of the collected PII will be disclosed to other Noble entities for the purpose of facilitating such shared functions. The recipients only have access to the PII to the extent necessary to perform their work duties and employment administration. Further to that, Noble will share data with other companies within Nobles organizational structure where it has a legitimate business interest in

doing so. This may be as part of regular reporting activities on company or individual performance, in the context of a business reorganization or group restructuring exercise, or for system maintenance support and hosting of data. The data expected to be transferred includes appraisal and other relevant performance documentation; core identification data, including date of birth and notes of days of absence; and, where necessary, details in relation to any litigation in which Noble may be involved.

4.8.2 Third-Party Service Providers

Collected PII may, to the extent necessary, be made available to third parties providing relevant services under contract with Noble, such as processors of payroll, expenses, and other compensation information; IT hosting and maintenance providers; management and compliance consultants, etc. Such service providers will only process the PII in accordance with Nobles instructions.
Noble may share PII with third parties outside the company, who then process the personal data for their own purposes. For example, we may share data with:

- Clients, in the context of commercial business activities.
- Client subcontractors, in the context of Nobles performance under specific commercial contracts.
- Clients, banks, and lending institutions when completing necessary diligence processes as part of tendering or other business activities.
- Providers of salary and remuneration benchmarking services.
- Pension and Insurance providers, leasing bureaus, financial institutions.
- Travel agencies, if needed for business travel or accommodation arrangements.
- Government bodies, regulators, law enforcement agencies, courts, or other authorities, at their request if necessary for the purpose set out herein, to enforce or defend the rights of the company or its affiliates or any third party, or due to legal requirements.
- External legal counsel, accountants, or other trusted advisors.
- Any successors in title to our business as a result of a sale, merger, consolidation, change of control, transfer of assets or re-organization of the company or any of its affiliates.

All third parties are required to take appropriate security measures to protect individuals personal information in line with Noble policies. Noble only permits third-party service providers to process an individuals relevant personal data for specified purposes and in accordance with the

companys instructions a third party is not permitted to use an individuals personal data for its own purposes.

4.9 Moving Data Across Borders

Noble will transfer the collected PII among countries if it has a legitimate business reason to do so.
To ensure that PII receives an adequate level of protection, Noble has put in place contracts containing model contractual clauses as an appropriate measure to ensure that collected personal information is treated in a way that is consistent with and respects, the applicable laws on data protection. In cases, where PII is required to be transferred to a country without adequate levels of data protection, the transfer must adhere to this policy.
If further information about this protective measure is required, it can be requested from privacy@noblecorp.com.

4.10 Notification and Consent

Privacy laws do not generally require the company to obtain employee consent for the collection, use or disclosure of PII for the purpose of establishing, managing, or terminating the employment relationship. In addition, the company may collect, use, or disclose PII without employee knowledge or consent, where permitted or required to do so by applicable law or regulation.
To the extent that consent is required, the company will assume, unless otherwise advised, that each employee has agreed to the companys collection, use, and disclosure of PII for permissible purposes.

4.11 Retention of PII

Noble will only retain an individuals PII for as long as it is strictly necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements. The company will on a continuous basis assess whether it is necessary to keep an employees personal data.
As a rule, PII will be kept for the least amount of time required following the effective date of termination of employment. Retention lengths are based on Nobles Retention Policy as well as the relevant jurisdiction.
In determining the length of time the PII are to be kept (if longer than the retention period set forth for personal data in the Retention Policy) Noble considers the amount, nature, and sensitivity of the personal data; the potential risk of harm from unauthorized use or disclosure of the personal data; the purposes for which personal data is processed and whether Noble can achieve those purposes through other means, and the applicable legal requirements.
In some circumstances Noble may anonymize an individuals PII, so it can no longer be associated with that individual, in which case such information may be used without further notice to the individual. Once a person is no longer an employee, worker, or contractor of the company, Noble will retain, and at the appropriate time securely destroy, collected PII in accordance with the terms of the foregoing

paragraph.
For additional guidance, please reference Nobles Records Retention Policy.

4.12 Data Breach Incident

As a Data Controller, Noble is required to notify the relevant authorities in the event of the loss or unauthorized access, disclosure, or acquisition of the personal information it holds.
If an individual knows or suspects a data breach has occurred, they should not attempt to investigate the matter. Please contact the Data Privacy Committee at privacy@noblecorp.com or Corporate Compliance at compliance@noblecorp.com immediately and follow their instructions, and preserve all evidence relating to the potential data breach.

4.13 Miscellaneous

This policy does not confer any rights or impose any obligations outside of or in addition to any rights conferred or obligations imposed by the privacy laws applicable to each employees PII.
Violation of this policy may result in disciplinary action, up to and including immediate termination of employment.

4.14 The Individuals Rights and Responsibilities regarding Personal Data

4.14.1 Access, Correction, or Erasure

Under certain circumstances, by law, individuals have the right to:

- Request access to their personal information (commonly known as a data subject access request). This enables the individual to receive a copy of the PII which Noble holds about them and to check that it is being lawfully processed.
- Request correction of the PII that Noble holds about them. This enables individuals to have any incomplete or inaccurate information corrected.
- Request erasure of their PII. This enables individuals to ask Noble to delete or remove PII where there is no reason for Noble to continue to process it. Individuals also have the right to ask Noble to delete or remove their PII where they have exercised their right to object to processing (see below).
- Object to the processing of their PII where Noble is relying on a legitimate interest (or a legitimate interest of a third party) and there is something about their particular situation that makes them want to object to processing on this ground.
- Request the restriction of processing of their personal information. This enables individuals to ask Noble to suspend the processing of PII

about them; for example, if the individual wants Noble to establish the informations accuracy or the reason for processing it.

- Request the transfer of their PII to another Data Controller.

If an individual (i.e. former employee, supplier, or customer) wants to access, verify, correct, or request erasure of their PII; object to or restrict the processing of their PII; or request that Noble transfer a copy of their PII to another party, please contact the Privacy Committee privacy@noblecorp.com. Current employees should initiate a ticket in the Connect system.

Individuals will not have to pay a fee to access their PII (or to exercise any of the other rights); however, Noble may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, Noble may refuse to comply with the request in such circumstances.

Further to this, the above rights are not absolute and are subject to certain legal restrictions.
Noble may need to request specific information from the individual to help confirm identity and ensure the individuals right to access the information (or to exercise any of their other rights). This is another appropriate security measure to ensure that PII is not disclosed to any person who has no right to receive it.

Note Please refer to the section titled Failure to Provide PII

4.14.2 Withdraw Consent

In the limited circumstances where individuals may have provided consent to the collection, processing, and transfer of PII for a specific purpose, they have the right to withdraw consent for that specific processing at any time. To withdraw consent, please contact the Privacy Committee via email at Privacy@noblecorp.com. Once Noble has received notification that consent has been withdrawn, it will no longer process PII for the purpose or purposes originally agreed to, unless it has another legitimate basis in law for doing so.

4.14.3 Individual Responsibilities

The individual is responsible for helping the organization keep their personal data up to date. Individuals should let the HR Department know if PII previously provided to the organization changes, for example, due to a move or change of name.
Individuals may have access to the PII of other individuals, customers, and clients during their working relationship with Noble. In such cases, Noble relies on those individuals to help meet the companys data protection obligations to employees, customers, and clients.

In particular, if an individual has access to the PII of others, they are required

- to only access PII they have authority to access, and only for authorized purposes;
- to only disclose PII to individuals (whether inside or outside the organization) who have appropriate authorization;
- to keep such PII secure (for example, by complying with rules on access to premises; computer access, including password protection; and secure file storage and destruction);
- not to remove PII, or any devices that contain or that can be used to access data, from Noble Corporations premises without adopting appropriate security measures (such as encryption or password protection) to secure the information and the device; and
- not to store PII on local drives or on personal devices used for work purposes.

In addition, individuals must

- ask the Privacy Committee or their manager if they are unsure about this policy or any aspects of data management;
- advise the Privacy Committee at privacy@noblecorp.com, if they become aware of any act or omission that risks compromising the security, confidentiality, or integrity of personal data;
- consult the Privacy Committee if they are involved in or become aware of involvement in any major change of process or system that involves the processing of personal data, as this may require carrying out a data protection impact assessment;
- consult the Privacy Committee if they make use of automated processing or decision taking, unless that has been previously approved;
- complete all mandatory data protection training; and
- make sure they do not hold personal data other than in accordance with this policy and all applicable rules and regulations provided by Noble and comply with all instructions given regarding the deletion of data.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Nobles disciplinary procedure.
To the extent that the GDPR or equivalent legislation permits an individual who does not fall within the scope of this policy to make a Data Subject Access Request, that individual will have the rights and responsibilities relative to such a Request, which are set out in this Clause 5.

5 Responsibilities

Data Controller: Determines, either alone or jointly with others, the purposes and means of the processing of personal data, i.e., the individuals direct employer.

Data *Processor*: Performs or causes to be performed any set of operations on personal data, including, but not limited to, collection, recordings, organization, storage, or retrieval.

Privacy Committee. Noble corporate committee with responsibilities for determining privacy policy and making determinations on individuals privacy-related data requests. Reached through privacy@noblecorp.com.

6 References

Records Retention Policy
General Data Protection Regulation (EU GDPR)