

1 Introduction

Privacy and data protection laws protect the integrity and confidentiality of an individual's personal data. Altera is committed to protecting the privacy rights of those with whom we have business contact. We will only use your personal data fairly and lawfully for specific and valid business purposes, in accordance with applicable law.

Altera processes personal data about individuals employed or engaged by us, working from Altera facilities and within Altera systems, and who are in a recruitment process with us. Separate privacy statements apply to these individuals. This Privacy Statement for External Parties primarily applies to other individuals with whom Altera interacts, including representatives and personnel of suppliers, clients, business partners and authorities; visitors; offshore and project personnel; shareholders and other stakeholders; and individuals whose personal data is processed in connection with compliance, security, safety or corporate activities. This privacy statement does not have contractual effect and does not form any part of any contractual relationship between you, your employer, and/or Altera.

Within Altera, the data controller for personal data collected and processed for the purposes described herein will be **Altera Infrastructure Production AS** (Brattørkaia 17A, 7010 Trondheim, Norway, reg. no. 939 545 832) and/or the specific Altera entity with which you have a business relationship.

The Altera Chief Compliance Officer serves as the Data Protection Officer for the Altera group of companies: **Lesley Coben** (lesley.coben@alterainfra.com).

This Privacy Statement for External Parties is **effective as of the date indicated in document footer**. We may amend it at any time.

2 Details of Processing

We generally obtain personal data directly from you or from the organisation you represent. Depending on the relevant activity, we may also obtain personal data from Altera personnel, clients, suppliers, business partners, public authorities, professional advisers, publicly available sources, screening providers, security systems and other third parties involved in the relevant business process. Altera processes personal data about individuals who are not employed or engaged by Altera for the following purposes.

2.1 Procurement and Supplier Management

Altera relies on a network of reputable suppliers and service providers to support our activities. We conduct supplier selection and onboarding, sourcing, purchasing, and supplier management according to documented supply chain management procedures.

As part of these activities, we process personal data about supplier and contractor personnel and representatives, including names and contact information, roles, company affiliations, correspondence, signatures and invoicing information, to facilitate, for example, communication, contract management, and invoicing, as well as signatures of authorised representatives to ensure contracts are legally enforceable.

The legal basis for this processing is our legitimate interest¹ in ensuring good supply chain management.

2.2 Business Development, Tendering, and Client Contract Management

Altera engages directly with a wide scope of client representatives to pursue business opportunities, prepare tender submissions for potential contracts, manage customer relationships, and to manage contract performance and invoicing.

The personal data processed for this purpose may include the name and contact information of individuals at current and potential clients for the purpose of business communication, signatures of authorised representatives to ensure contracts are legally enforceable, as well as internal administrative tasks such as invoicing and relationship management.

The legal basis for this processing is our legitimate interest in pursuing and securing business opportunities and contracts.

2.3 Integrity Due Diligence and Screening

Altera conducts appropriate and risk-based integrity due diligence and restricted party screenings on third parties with which Altera may establish a business relationship.

The personal data processed for this purpose may include the name and contact information of individuals associated with such third parties (for example as owners, directors, officers, or other key representatives), as well as other personal data which may result from our integrity due diligence queries. In some instances, this information will be provided directly by relevant third parties, and in other instances will result from background screenings we conduct separately.

The legal basis for this processing is our legitimate interests in ensuring we partner with third parties of good reputation, our need to comply with legal obligations², or for the establishment, exercise or defence of legal claims³.

2.4 Integrity Line

Altera maintains a confidential and secure Integrity Line to allow employees, staff, and other stakeholders to report suspected activity in violation of law or the Altera Code of Conduct. More information about the Integrity Line is available on the Altera website.

¹ E.g., EU GDPR Art. 6(1)(f); UK GDPR Art. 6(1)(f); Brazilian LGPD Art. 7(IX) – Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This reference applies to all other mentions of legitimate interests as a legal basis for processing within this Privacy Statement.

² E.g., EU GDPR Art. 6(1)(c); UK GDPR Art. 6(1)(c); Brazilian LGPD Art. 7(II) – Processing is necessary for compliance with a legal obligation to which the controller is subject. This same reference applies to all other mentions of legal obligation as a legal basis for processing within this Privacy Statement.

³ E.g., EU GDPR Art. 6(1)(f); UK GDPR Art. 6(1)(f); Brazilian LGPD Art. 7(VI) – Processing is necessary for the establishment, exercise, or defence of legal claims by the controller. This same reference applies to all other mentions of legal claims as a legal basis for processing within this Privacy Statement.

The personal data processed for this purpose may include the name and contact information of the person making a report to the Integrity Line (if such report is not submitted anonymously), as well as any personal data that may be included in the report (which may include special categories of personal data), and the personal data that is necessary to enable Altera to handle and respond to the report.

The legal basis for this processing is our legitimate interest in providing and administering a confidential misconduct reporting channel, our need to comply with legal obligations, or for the establishment, exercise or defence of legal claims.

2.5 Information Requests under the Norwegian Transparency Act

Altera has a duty of disclosure under the Norwegian Transparency Act (the “Act”) and processes personal data to respond to requests for information made under the Act.

The personal data processed for this purpose may include the name and contact information of the person making the information request, as well as personal data that is necessary to Altera’s response to the request.

We process this personal data on the basis of our legal obligation to comply with the Act, to safeguard our legitimate business interests or potentially to establish, exercise, and defend legal claims.

2.6 Communication

Altera communicates internally and externally with a wide variety of parties across various channels in the normal course of business. This includes direct communication with individuals, as well as communication directed to the general public and targeted groups via email, distribution lists, press releases, company reports, websites, and our social media channels.

The personal data processed for this purpose may include names, contact information of individuals, company affiliation, role, photographs, audio recordings, videos and other communication-related personal data.

We process this personal data on the basis of our legitimate business interests in advertising and sharing information about our business activities, stakeholder engagement, or your consent⁴.

2.7 Recruitment and Engagement

Altera processes personal data as part of our recruitment process to ensure that we recruit qualified candidates, and as necessary to establish contracts with successful candidates.

The personal data processed for this purpose may include names, contact information, recruitment and human resources information (CV, resume, qualifications, reference checks, background

⁴ E.g., EU GDPR Art. 6(1)(a); UK GDPR Art. 6(1)(a); Brazilian LGPD Art. 7(I) – The data subject has given consent to the processing for one or more specific purposes. This same reference applies to all other mentions of consent as a legal basis for processing within this Privacy Statement.

screenings). For roles requiring work offshore or aboard one of our assets, we will also process information necessary to confirm medical fitness for offshore work.

We process this personal data on the basis of our legitimate interest in recruiting qualified candidates, our legal obligation to ensure medical fitness to fulfil role requirements, steps necessary to enter into a contract at the request of successful candidates⁵, and consent to retention of recruitment data following the recruitment process.

Please also see our [Privacy Statement for Recruitment](#), available on our website.

2.8 Security and Access to Altera Assets and Facilities

For reasons of safety and security, and in some cases to comply with regulatory requirements, Altera restricts access to its offshore assets and onshore offices and facilities and collects identification information from those seeking access to these areas.

The personal data processed for this purpose may include names, contact information, company affiliation (for non-Altera personnel), and identity documents of the individuals seeking access.

We process this personal data on the basis of our legitimate interest in ensuring safety and security and to comply with legal requirements in the relevant jurisdiction.

2.9 Safety and Emergency Response

To ensure safety in an emergency, Altera maintains lists of individuals on our offshore assets at any given time (personnel on board). This includes Altera personnel and third-party representatives and individuals who are onboard.

The personal data processed for this purpose may include names, contact information, company affiliation (for non-Altera personnel), identity documents, and onboard accommodation or muster assignment, emergency contact details and other information needed to account for or assist individuals during an emergency.

We process this personal data on the basis of our legitimate interests in ensuring safety in emergency situations and to comply with legal requirements in the relevant jurisdiction.

2.10 Camera and Voice Recording of Operations

Altera uses closed circuit television (“CCTV”) recording devices in key areas of its offshore assets and onshore locations to ensure safety and security. CCTV cameras are only sited in areas where there is a relevant safety or security concern and never in private areas. Signage is posted in areas under CCTV recording. In addition, some of our offshore assets may be equipped with voice recording in key control centres to allow for monitoring and investigation of operational actions on an ongoing basis and in the event of a safety or security incident.

⁵ E.g., EU GDPR Art. 6(1)(b); UK GDPR Art. 6(19)(b); Brazilian LGPD Art. 7(V) - Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This same reference applies to all other mentions of contract performance as a legal basis for processing within this Privacy Statement.

The personal data processed for this purpose may include images, voice, and/or statements of individuals captured on the resulting recordings.

We process this information on the basis of our legitimate interest in maintaining the safety and security of our facilities and in some cases to comply with applicable legal requirements.

2.11 Website and Cookies

Please see our Website and Cookie Privacy Statement on the Altera website.

2.12 Project Mobilisation

Altera processes personal data about external personnel who may work on, travel to, visit or provide services for our projects, offices and offshore assets. This supports mobilisation and demobilisation, travel and accommodation arrangements, immigration and work authorisation requirements, scheduling, training, competence assurance and confirmation that individuals meet applicable role or project requirements.

The personal data processed for these purposes may include name and contact information, company affiliation, role, travel and accommodation details, identification and immigration documents, qualifications, certifications, training and competence records and, where required for offshore or safety-critical work, information concerning medical fitness.

We process this personal data on the basis of our legitimate interests in managing projects and operational activities safely and effectively, taking steps necessary in connection with relevant contractual arrangements, and complying with applicable legal requirements.

2.13 Incident Management, Investigations and Legal Matters

Altera may process personal data to report, assess, investigate and respond to safety, security, environmental, compliance, contractual or other incidents and concerns; conduct audits and internal investigations; manage disputes and insurance matters; obtain legal advice; and establish, exercise or defend legal claims.

The personal data processed will depend on the relevant matter and may include identification and contact information, company affiliation, role, statements, correspondence, access or system records, images or recordings, incident details and other information necessary to assess and respond to the matter. This may include special categories of personal data where relevant and permitted by law.

We process this personal data on the basis of our legitimate interests in protecting Altera and others, complying with legal obligations and contractual requirements, and establishing, exercising or defending legal claims.

3 Handling of Your Personal Data

3.1 Automated Decision Making

We do not take decisions about individuals based solely on automated processing (i.e. without human involvement).

3.2 Access to Personal Data

Altera is a global organisation. Personal data collected as described in this Privacy Statement for External Parties may be accessed and reviewed by people within the Altera group to administer the relevant business processes.

We may also share your personal data with external third parties where necessary for the purposes described in this Privacy Statement, including to support our business activities, manage contractual relationships, provide or receive services, pursue business opportunities, comply with legal or regulatory obligations, or protect the rights, property, safety, or security of Altera and others. Depending on the circumstances, recipients may include customers and clients, suppliers, contractors, business partners, professional advisers, auditors, insurers, financial institutions, software application providers and other service providers supporting Altera's operations.

Where relevant to a tender, project, contract, audit, mobilisation activity, or other legitimate business purpose, we may share information relating to your role, experience, qualifications, certifications, training or competence with customers, clients, business partners, contractors or other authorised third parties. We will limit the information shared to what is necessary and appropriate for the relevant purpose.

Additionally, we may need to disclose your personal information as required by applicable law or to comply with official requests from relevant government authorities, regulators, courts, law enforcement agencies, or other public bodies.

Some of the people and parties who may receive access to your personal data may be located outside of the country in which you reside or in which you primarily interact with Altera. Where personal data is transferred internationally, we comply with applicable data protection requirements and use an appropriate transfer mechanism where required, such as an adequacy decision, approved contractual safeguards or another legally recognised basis. Further information about the safeguards used for relevant transfers may be requested by contacting privacy@alterainfra.com.

3.3 Retention of Personal Data

We retain personal data only for as long as necessary for the purposes for which it was collected and while we have a lawful basis to retain it. In determining the appropriate retention period, we consider the nature and sensitivity of the personal data, the relevant business or contractual relationship, applicable legal and regulatory requirements, limitation periods, safety and security needs and the need to establish, exercise or defend legal claims. Personal data is then deleted, anonymised or securely archived in accordance with our retention requirements.

3.4 Protecting Your Personal Data

In proportion to the sensitivity of the personal data collected, we maintain a variety of technical and organisational measures to protect personal data from loss, misuse or unauthorised access,

disclosure, alteration, or destruction. These measures include appropriate use and business conduct policies, cybersecurity training, risk assessments, system access controls, and a variety of network and endpoint technical security technologies and practices.

If we become aware of a security incident affecting your personal data, we will investigate and comply with all applicable reporting obligations.

4 Your Rights

We are committed to complying with all applicable legal requirements regarding the protection of personal data. These requirements may vary from country to country.

Subject to applicable law, you may have the right to request access to and a copy of the personal data we process about you, to request that we correct your personal data if it is inaccurate, incomplete, or out of date, to object to how we process and use your personal data, to request that we restrict how we process and use your personal data, to request that we delete your personal data if we no longer have a lawful basis to process it, to request that we transfer your personal data to another controller, and to withdraw your consent to the future processing of your personal data. These rights may be subject to legal conditions and exceptions. To exercise these rights, please contact us at privacy@alterainfra.com.

Depending on applicable law, you may also have the right to make a complaint to the relevant data protection authority.

5 Questions and Contact Information

If you have a question regarding this Privacy Statement for External Parties or the handling of your personal data, please contact us at privacy@alterainfra.com.

You also have a right to complain to the relevant Data Protection Authority if you believe that we have not complied with applicable data protection law. The names and contact details of the Data Protection Authorities in our areas of operation are listed below. We encourage you to contact us at privacy@alterainfra.com prior to filing such a complaint, but you are not required to do so.

BRAZIL

Authority:	Autoridade Nacional de Proteção de Dados (ANPD)
Address:	North Commercial Sector - SCN, Block 6, Complex "A", Venâncio Building 3000, Block "A", 9th floor, Zip Code 70.716-900 - Brasília – DF (Setor Comercial Norte - SCN, Quadra 6, Conjunto "A", Edifício Venâncio 3000, Bloco "A", 9º andar, CEP 70.716-900 - Brasília – DF)
Telephone:	+55 (61) 2017-3338 and 2017-3339
Website:	https://www.gov.br/anpd/pt-br

CÔTE D'IVOIRE

Authority:	l'Autorité de Régulation des Télécommunications (ARTCI)
------------	---

Address: Marcory Anoumabo, 18 BP 2203 Abidjan 18 – Côte d'Ivoire
Telephone: +225 27 20 34 43 73
Website: <https://www.autoritedeprotection.ci/>

NORWAY

Authority: Datatilsynet (Norwegian Data Protection Authority)
Address: P.O. Box 458 Sentrum, NO-0105, Oslo, Norway
Telephone: +47 22 39 69 64
Website: In Norwegian - <https://www.datatilsynet.no/>
In English - <https://www.datatilsynet.no/en/>

THE PHILIPPINES

Authority: National Privacy Commission
Address: 5th-27th Floors, The Upper Class Tower, Quezon Ave. Corner Scout Reyes Street, Quezon City, Philippines
Telephone: +63 970 818 0555 (Smart); +63 905 506 1478 (Globe)
Website: <https://privacy.gov.ph/>

THE UK

Authority: Information Commissioner's Office (ICO)
Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK
Telephone: +44 (0) 303 123 1113
Website: <https://www.ico.org.uk>
