Last reviewed October 2018

EU Privacy Statement

1. Introduction and Scope

Laing O'Rourke is committed to keeping personal information accurate and private. This Privacy Statement, together with any terms of use of our website and systems, sets out what personal information we collect directly from you, through our website or through any other form of communication with us, or which you communicate to our agents or contractors.

This Privacy Statement applies to personal information we handle about our business partners, employees, staff, visitors to our website, individuals who access our sites/premises and other members of the public based in the European Union (EU) only. Personal data collected about non-EU citizens in our offices outside the EU are subject to separate data protection policies in line with the legislative requirements of each location. A copy of our non-EU Privacy Statement can be accessed from our website.

Our Global Code of Conduct is available on our website and sets out the guiding principles and standards we apply across our business to the management of personal information. We expect the same principles and standards from those with whom we do business.

Other Laing O'Rourke policies and protocols relevant to the collection and use of personal information will apply to our employees and staff. Our employees and staff can access the policies and protocols applying to them via our intranet and should direct any queries to their line manager or the Information Security Office.

2. Applicable privacy laws

We are bound by the laws of the countries where we operate which protect the privacy of individuals by regulating the collection and use of personal information. These laws may contain exemptions for the collection and use of some personal information, including employee and staff records. We may also be bound by workplace surveillance legislation in some countries which regulate camera, computer and tracking surveillance of employees and staff.

The relevant data privacy law governing this Privacy Statement is the EU General Data Protection Regulation 2018. To the extent that the relevant data privacy law(s) are amended, substituted or repealed from time to time then this Privacy Statement should be read as referring to those relevant data privacy law(s) as so amended, substituted or repealed.

3. What information does this Privacy Statement apply to?

This Privacy Statement applies to personal data which relates to a living individual who can be identified either directly from data collected, or indirectly from other data within our possession.

This includes, but is not limited to:

Name	Date of Birth	Nationality
Address	Email Address	Telephone Number
National Insurance Number	Passport Information	Driving License Details
Birth Certificate	CCTV	Photographs/Images

Religious Beliefs	Political Opinions	Ethnicity
Sexual Orientation	Drug & Alcohol Test Results	Criminal History
Medical Information	Disabilities	Personal Attributes
Employment Information	Financial Information	Educational History
Biometric Data	Health & Safety Information	Background Checks

A definitive list of personal information collected and reasons why is provided in Section 4 below. This privacy statement covers the management of personal data collected directly as part of recruitment and employee management, as well as indirectly from our websites.

4. What personal information do we collect and why?

The types of personal information we collect and purposes for doing so are described in the following table:

Personal Data Type(s)	Reasons for Processing	Lawful Basis for Processing
Name, address, email address, contact number.	To maintain contact following any queries raised via our websites or in connection with our projects and work sites. As part of our employee recruitment and on-boarding processes. To also control access to our work sites for security and safety related reasons and to assist with time keeping.	To comply with our **legal** and statutory obligations. To fulfil our **contractual** obligations and for the purposes of **legitimate interests**.
Nationality, residency and Immigration Status, visa details.	As part of our employee recruitment and on-boarding processes. To also control access to our work sites for security and safety related reasons and to assist with time keeping.	To comply with our **legal** and statutory obligations e.g. right to work checks. To fulfil our **contractual** obligations and for the purposes of **legitimate interests**.
Identification documents and unique identifiers such as passport, utility bills, national insurance number, date of birth and driving license details.		

Diversity and special category information including gender, marital status, ethnicity, religious beliefs, nationality, sexual orientation and disability information.	To maintain equal opportunities best practice and to identify barriers to workforce equality and diversity. Data is aggregated in a non-identifiable format for statistical reporting and is not mandatory.	Provided with **consent** and to be used for a specific purpose in an anonymised format only
Emergency contact details, next of kin, beneficiaries and dependents.	To maintain health and safety in the workplace and on our other work sites. To also notify next of kin in the event of any incidents.	To comply with our **legal** and statutory obligations and to protect the **vital interests** of the workers, employees, contractors and other individuals that access our sites.
Qualifications, experience and employment history.	As part of our employee recruitment and on-boarding processes.	To comply with our **legal** and statutory obligations. To fulfil our **contractual** obligations and for the purposes of **legitimate interests**.
Courses, programs and training certificates.	As part of our employee recruitment and on-boarding processes and to maintain continuous professional development.	
Other information provided as part of our recruitment and on-boarding processes, including but not limited to, references, criminal records checks, pre-employment verification details, notes from interviews, assessment exercises or other tests.	As part of our employee recruitment and on-boarding processes.	

Medical history and other health information.	To maintain health and safety in the workplace and on our other work sites. To provide health insurance cover and to help manage absence in the workplace.	To comply with our **legal** and statutory obligations. To fulfil our **contractual** obligations and for the purposes of **legitimate interests**
Drug and alcohol testing data.	To maintain health and safety in the workplace and on our other work sites. To minimise potential safety incidents and to help manage absence in the workplace.	
Biometric data	To help control the workers, employees, contractors and other individuals that access our projects and worksites. To assist with time keeping e.g. clock in and out. To also help ensure health and safety in the workplace and on our work sites e.g. fatigue management.	To comply with our **legal** and statutory obligations. To fulfil our **contractual** obligations and for the purposes of **legitimate interests**
Driving and insurance claims history.	To provide company vehicles to employees and for the management of our vehicle and plant fleets and other operational assets.	To fulfil our **contractual** obligations with insurance providers and employees and for the purposes of **legitimate interests.**
Payroll and wage records such as tax number, bank account details, PAYE records, travel and subsistence and national insurance number.	To pay salaries, wages and other service related invoices. To provide benefits and reimburse expenses. To also satisfy our legal and other tax requirements.	To comply with our **legal** and statutory obligations and to fulfil our **contractual** obligations.
Details of remuneration including salary, benefits and rewards		

Incident and accident related details including, but not limited to, accident records, audio, footage recorded on our project and worksite CCTV systems and other data captured through the use of our IT equipment and communication systems.	To maintain health, safety and security in the workplace and on our other work sites. To minimise potential safety incidents. To also investigate accidents and incidents (including disciplinary and grievance procedures) in the workplace or on our other worksites and to prevent and detect crime and anti-social behaviour or misuse of our IT equipment and communication systems.	To comply with our **legal** and statutory obligations and for the purposes of **legitimate interests**. To fulfil our **contractual** obligations with insurance providers, employees, workers and contractors.
Information gathered on employees involved in the concept, design, development and management of our projects and then used as part our working winning and bid process such as name, qualifications, work experience and project employment history.	To bid for new projects and work.	For the purposes of **legitimate interests.**
Information gathered as part of our supply chain due diligence processes such as Companies House records and other information on directors, shareholders, officers and beneficial owners gathered from publicly available open sources.	To build a strong and ethical supply chain and to comply with all applicable regulations and legislation.	To comply with our **legal** and statutory obligations and for the purposes of **legitimate interests.**

Other information collected from workers, employees, contractors and other individuals that access our projects and worksites such as name, address, email address, contact number, date of birth, driving license details, national insurance number and passport.	To control and manage access to our projects and worksites for security and safety related reasons and to also assist with time keeping e.g. clock in and out.	To comply with our **legal** and statutory obligations. To fulfil our **contractual** obligations and for the purposes of **legitimate interests.**
Other information collected for staff and personnel records, including, but not limited to, annual leave records, annual assessment reports, disciplinary and grievance records, maternity records and other records in relation to working time, death benefit and revocation forms and resignation, termination or	To facilitate, manage and administer the employment relationship with our employees and workforce.	To comply with our **legal** and statutory obligations and to fulfil our **contractual** obligations.
Other information collected from visits to our websites including cookies and website usage.	To collect information from our website about usage.	For the purposes of **legitimate interests.** To enable us to provide a better service via our web channels**.**

5. How and why do we collect your personal information?

We only collect personal information that is necessary for us to manage our business effectively, to develop and promote our services and to assist us with complying with our legal and regulatory obligations.

Generally, we try to collect personal information directly from you but, occasionally, we may collect personal information from publicly available records, third parties and/or other sources. We will only collect personal information about you from publicly available records, third parties and/or other sources if there is a lawful basis or we gain consent from yourselves to do so.

We will only collect sensitive information about you if we have your consent or we are permitted or required by law to collect the information.

The ways we collect personal information include:

- during the recruitment and engagement of employees and staff, including reference checking and agency searches;
- as part of training, induction and on-boarding programs;
- through our dealings with government agencies;
- through our dealings with clients, contractors, subcontractors, suppliers and other service providers;
- during conversations between you and our representatives;
- through access to our website;
- from access control systems and registers for individuals accessing our sites and premises;
- through random drug and alcohol testing on operatives on our sites and premises;
- through monitoring and surveillance systems, including CCTV systems;
- from social media web sites and blogs;
- through third party companies engaged to undertake credit reference and due diligence checks;
- on individuals and organisations with whom we engage in the operation of our business;
- as part of incident and accident investigations;
- if we receive your personal information and we did not request it, then we will determine, within a suitable time after receiving that information, whether it is reasonably necessary for us to retain that information and, in the case of sensitive information, whether you consented to the collection. If not, we will de-identify or destroy the information;
- regardless of how we obtain the information, we will take reasonable steps to ensure that you are aware of the way we are collecting the information, any laws requiring the collection, who we usually disclose it to and any consequences for you if we are not provided with the information.

6. Purposes for which we collect personal information

We may collect your personal information to enable us to properly operate, manage and administer our business including:

- the management of our employees and staff and workforce in all of our business operations, including management planning and forecasting;
- maintaining effective access, safety and security controls for our sites and premises;
- in order to investigate any allegation or complaint about our practices or conduct;
- to comply with our legal and regulatory requirements, policies and contractual obligations or in cooperation with any governmental authority of any country;
- management of claims, disputes and litigation proceedings arising out of our business operations;
- engaging the services of external consultants, agents, temporary and casual workers and other operatives;
- obtaining credit references and conducting due diligence on individuals or representatives of corporate entities;
- processing and responding to enquiries, allegations or complaints from members of the public
- maintaining supplier and contractor databases;
- compilation of and access to business contact databases;
- to conduct business processing functions including providing personal information to our related companies, contractors, service providers or other third parties;
- investigation/prevention/detection/prosecution of unlawful or inappropriate activities;
- establishment and operation of our corporate banking accounts and systems;

- provision of health practitioner, health monitoring and emergency medical assistance services;
- monitoring use of our website.

7. Passive information collection

As you navigate through our website or otherwise use our equipment, systems and technology, we may collect information about your computer, including, where available, your IP address, operating system and browser type, for system administration. This is statistical data about our users' browsing actions and patterns, and does not identify any individual.

We use 'cookies' which are small text files placed on your computer by a web page server which may
later be retrieved. A cookie enables us to recognise your computer without the need for a fresh request for you to register.

The cookies do not allow us to collect personally identifiable information about you.

8. How we use your personal information

We will only ever use your personal information for the purposes set out in our privacy statement. This allows us to conduct business in accordance with our legal and regulatory requirements, and to ensure the health and safety of our staff.

We may additionally use your personal information for the following purposes, subject to your explicit consent:

- as part of tenders, bids and proposals we submit to clients and potential clients for the provision of works and services;
- to inform you of existing and proposed services which we provide and commercial opportunities which we offer from time to time;
- for personal information that is sensitive information, we will only collect, use or disclose that information where it is reasonably necessary in the operation of our business and we have received your consent to do or it is permitted or required by law.
- as part of our safety and security commitment to our employees and staff, clients and members of the public, we conduct camera, computer and tracking surveillance of our sites, premises, assets and business systems. If we intend to conduct surveillance activities which might affect you, we will give you notice of those activities as we are required under applicable law(s). Any surveillance activity will only be conducted by appropriate individuals and any resulting personal information collected will be held in accordance with this Privacy Statement.
- we may also use your personal information for purposes related to those described above which would reasonably be expected by you or to which you have consented.

9. How long do we hold onto your personal information?

Personal information is only retained for as long as is necessary to fulfil the purposes for which it was collected. We apply a granular retention policy to ensure personal data that is no longer required, out dated, inaccurate or expired is deleted in line with our legal and regulatory requirements.

Where requested by you, we will delete your personal information if we do not have any other legal or regulatory basis for which to retain it (to make requests for deletion please see "how to contact us" below).

10. Sharing your personal information

We may disclose your personal information in certain circumstances, such as where we are required or permitted by law, where you have consented to us doing so or for any of the purposes for which the information was collected.

The persons to whom we typically may disclose your personal information include:

- specified persons in accordance with a request made by you (for example other employers, banks or property agents);
- our related companies, business partners, contractors, subcontractors, suppliers, consultants, clients and service providers for the purpose of our business operations (only when consented by you);
- individuals or organisations to whom we have commercial relationships, including individuals or organisations engaged in providing us with professional, business, technology, corporate and administrative services which are reasonably required for the effective operation of our business;
- Government agencies (including local tax authorities) and regulators as required or permitted by Law.

Where appropriate, we will only release personal information if we have an appropriate commitment from the recipient to use the information in a lawful, secure and responsible manner and only for the purpose(s) for which it is released.

We will never share your personal information with any unauthorised third parties for any unlawful basis. We will never sell your personal information for financial gain or be irresponsible with personal information collected.

11. Is my personal information processed overseas?

We are a part of the Laing O'Rourke group of companies, which are incorporated and operate in different countries including Australia, Canada, Hong Kong, New Zealand, the United Arab Emirates and the United Kingdom.

Some of the information we collect is stored on cloud-hosted systems which may be outside the country in which we collect the information. However, we will only ever share your data outside of the European Union (EU), if one or more of the following apply:

- the third country location is subject to a proportionate level of data protection Law as the country in which personal information was collected;
- we are permitted or required to do so by law;
- we have taken reasonable steps to ensure that the recipient of the information will not breach the relevant privacy laws of the country in which we collect the information;

You may contact us to obtain a list of countries in which likely overseas recipients of your personal information are located (see "How to contact us" below).

12. Access to your personal information

You may request access to any of the personal information we hold about you by contacting us (see
"How to contact us").

We are required to provide you with that access although there are exceptions such as:

- where we cannot gain sufficient assurance that the requestor is authorised to receive data relating to that individual i.e. if you cannot authenticate yourself to us through identification;
- where we are prevented by a Law or court order;
- where the request is disproportionate or you have requested the same information within a short timeframe.

We reserve the right to require you to verify your identity (so that we process access requests responsibly) and to charge a reasonable fee for the costs of retrieval and supply of any requested information where requests are deemed excessive. In some cases, such as where you have requested copies of the personal information that we hold about you (rather than access to that information), we require you to make your request in writing.

We will respond to access requests within a month where reasonably possible, and will give you access in the manner you request usually by mailing or emailing it to you (provided it is reasonably practicable to do so). If we cannot give you access to all the personal information we hold, or if we can't give you access in the manner you requested, we will take steps to give you alternative access that meets our respective needs.

If we can only give you limited or no access to your personal information, we will set out written reasons why this is the case and you may contact us to complain about that refusal (see "How to contact us" below).

We will take reasonable steps to ensure that the personal information we collect, use or disclose is accurate, complete and up to date, relevant and not misleading. Please notify us of any errors or changes to your personal information and we will take appropriate steps to update or correct such information in our possession.

Where we have corrected your personal information we will take reasonable steps to communicate that correction to any third party with whom we've shared the information (unless it is impracticable or unlawful to do so). If we refuse to correct your personal information following a request by you to do so, we will:

- set out written reasons why this is the case and you may contact us to complain about that refusal (see "How to contact us" below);
- at your request (and where we are able to do so), associate with that personal information a statement that it is inaccurate, out-of date, incomplete, irrelevant or misleading in such a way that the statement is apparent to users of the information.
- at your request delete or remove such information if there are no legal requirements for us to retain it.

13. Security of personal information

We store personal information in different ways including in electronic or hard copy form. We will take reasonable precautions in the circumstances to safeguard your information from loss, misuse, interference, unauthorised access, modification, disclosure or destruction.

Some of the measures we take include:

- applying technical and organisational controls in response to identified risk. This may include encryption of data at rest and in transit on our systems;
- insisting on confidentiality from our employees, staff and business partners in their use of personal information we provide to them and/or directing them to the principles we apply regarding personal information as identified in our Global Code of Conduct;
- implementing document management controls;
- Using access control and security measures for our sites, premises, assets and business systems;
- maintaining our infrastructure to prevent compromise of systems or application containing personal data;
- business continuity planning.

14. How to contact us or complain about a breach

If you have any questions about this Privacy Statement, are concerned that we have breached relevant data privacy law(s) or have a complaint about our information management practices, please contact our InfoSec Team at infosec@laingorourke.com or use our dedicated whistle-blowing hotline provided by SafeCall (which is independently run with trained operators available 24/7 and is also completely confidential) so that we can investigate your concerns.

We request that complaints about breaches of privacy be made in writing so that we can be sure about the details of the complaint.

Details of the whistle blowing hotline provided by SafeCall are as follows:
Telephone Number: (+44)0800 915 1571
Website: www.safecall.co.uk/report
Email: LOR@safecall.co.uk

If you feel that we have not adequately dealt with any privacy complaint you have made to us, you may wish to contact the appropriate data privacy authority relevant to your complaint. This is likely to be the Information Commissioner's Office if your concern is in the UK.

15. Anonymity and pseudonyms

You may submit information to us anonymously or by using a pseudonym unless we are required by law to insist that you identify yourself or it is impractical for us to deal with the information unless you have identified yourself.

Where you provide information through our SafeCall line, you may provide personal information on an anonymous basis. However, where you do not provide us with your name

and contact details, we may be limited in our ability to investigate and deal with your complaint and under certain laws (such as the *Public Disclosure Act 1998*) you may not be eligible for the legal protection provided to you by those laws to the extent your complaint relates to a breach of those laws.

16. Changes to this Privacy Statement

Our Privacy Statement may change from time to time as updated on our website. Before providing us with personal information, please check our website for changes.