

Last updated August 2022

## UK and EU Privacy Statement

### 1. Introduction and Scope

Laing O'Rourke and its group of companies are committed to keeping personal information accurate and private. This Privacy Statement, together with any terms of use of our website, platforms, individual applications or "Apps" and systems, sets out what personal information we collect directly from you, through our website, platforms, Apps 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, platforms and Apps individuals who access our sites/premises and other members of the public based in the United Kingdom (UK) and the European Union (EU) only. Personal data collected about non-UK or EU citizens in our offices outside the UK and EU are subject to separate data protection policies in line with the legislative requirements of each location. A copy of our non-UK/EU Privacy Statement can be accessed on 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 data 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 applicable data privacy laws governing this Privacy Statement include the UK and EU General Data Protection Regulation 2018 and local implementing and supplementary laws. To the extent that the relevant data privacy law(s) are amended, supplemented, substituted or repealed from time to time then this Privacy Statement should be read as referring to those relevant data privacy law(s) as so amended, substituted or repealed.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. Data controller

We are the data controller of the personal information that we process, i.e. the organisation which determines, alone or jointly with another party, how personal

information is processed and for what purposes. This means that we are legally responsible for ensuring our systems, processes, suppliers and people comply with data protection laws in relation to the personal information that we handle.

Where we transfer personal data to third parties, in certain circumstances those third parties may also be data controllers. More information about this is provided in this Privacy Statement.

#### 4. 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
Third party organisation affiliation such as suppliers	Your role	Your relationship with us

A more detailed list of personal information collected, and reasons why is provided in Section 5 below.

This Privacy Statement covers the management of personal data collected directly as part of recruitment and employee management, supplier due diligence, engagement and management, as well as indirectly from our websites, platforms and Apps.

We may aggregate the data described above such that it no longer relates to any individual person, in which case the data will no longer qualify as personal data.

#### 5. 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 (Contact Information).	<ul style="list-style-type: none"> <li>• To maintain contact following any queries raised via our websites, platforms and Apps or in connection with our projects, services, engagements and work sites.</li> <li>• As part of our employee recruitment and on-boarding processes.</li> <li>• To control access to our work sites for security and safety related reasons and to assist with time keeping.</li> <li>• To facilitate, manage and administer the employment relationship with our employees and workforce.</li> </ul>	To comply with our <b>legal</b> and statutory obligations. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests</b> . Where required by data privacy laws, we rely on <b>consent</b> .
Nationality, residency and Immigration Status, visa details	<ul style="list-style-type: none"> <li>• As part of our employee recruitment and on-boarding processes.</li> <li>• To control access to our work sites for security and safety related reasons and to assist with time keeping.</li> </ul>	To comply with our <b>legal</b> and statutory obligations e.g. right to work checks. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests</b> .
Identification documents and unique identifiers such as passport, utility bills, national insurance number, date of birth and driving license details.	<ul style="list-style-type: none"> <li>• To facilitate, manage and administer the employment relationship with our employees and workforce.</li> </ul>	

Personal Data Type(s)	Reasons for Processing	Lawful Basis for Processing
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 <b>consent</b> and to be used for a specific purpose in an anonymised format only.
Emergency contact details, next of kin, beneficiaries and dependents.	<ul style="list-style-type: none"> <li>• To maintain health and safety in the workplace and on our other work sites.</li> <li>• To notify next of kin in the event of any incidents.</li> <li>• To facilitate, manage and administer the employment relationship with our employees and workforce.</li> </ul>	To comply with our <b>legal</b> and statutory obligations and to protect the <b>vital interests</b> of the workers, employees, contractors and other individuals that access our sites, and for the purposes of <b>legitimate interests</b> .
Qualifications, experience and employment history.	As part of our employee recruitment and on-boarding processes.	To comply with our <b>legal</b> and statutory obligations. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests</b> .
Courses, programs and training certificates.	<ul style="list-style-type: none"> <li>• As part of our employee recruitment and on-boarding processes.</li> <li>• To maintain continuous professional development.</li> <li>• To facilitate, manage and administer the employment relationship with our employees and workforce.</li> </ul>	To comply with our <b>legal</b> and statutory obligations. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests</b> .

Personal Data Type(s)	Reasons for Processing	Lawful Basis for Processing
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.	<ul style="list-style-type: none"> <li>• To maintain health and safety in the workplace and on our other work sites.</li> <li>• To provide health insurance cover and to help manage absence in the workplace.</li> <li>• 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.</li> </ul>	To comply with our <b>legal</b> and statutory obligations. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests</b>
Drug and alcohol testing data.		
Biometric data	<ul style="list-style-type: none"> <li>• To help control the workers, employees, contractors and other individuals that access our projects and worksites.</li> <li>• To assist with time keeping e.g. clock in and out.</li> <li>• To help ensure health and safety in the workplace and on our work sites e.g. fatigue management.</li> </ul>	To comply with our <b>legal</b> and statutory obligations. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests</b>

Personal Data Type(s)	Reasons for Processing	Lawful Basis for Processing
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 <b>contractual</b> obligations with insurance providers and employees and for the purposes of <b>legitimate interests</b> .
Payroll and wage records such as tax number, bank account details, PAYE records, travel and subsistence and national insurance number.	<ul style="list-style-type: none"> <li>• To pay salaries, wages and other service related invoices.</li> <li>• To provide benefits and reimburse expenses.</li> <li>• To satisfy our legal and other tax requirements.</li> <li>• To facilitate, manage and administer the employment relationship with our employees and workforce.</li> </ul>	To comply with our <b>legal</b> and statutory obligations and to fulfil our <b>contractual</b> 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.	<ul style="list-style-type: none"> <li>• To maintain health, safety and security in the workplace and on our other work sites.</li> <li>• To minimise potential safety incidents.</li> <li>• To 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.</li> </ul>	To comply with our <b>legal</b> and statutory obligations and for the purposes of <b>legitimate interests</b> . To fulfil our <b>contractual</b> obligations with insurance providers, employees, workers and contractors.

Personal Data Type(s)	Reasons for Processing	Lawful Basis for Processing
<p>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.</p>	<p>To bid for new projects and work.</p>	<p>For the purposes of <b>legitimate interests.</b></p>
<p>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.</p>	<ul style="list-style-type: none"> <li>• To build a strong and ethical supply chain.</li> <li>• To comply with all applicable regulations and legislation.</li> </ul>	<p>To comply with our <b>legal</b> and statutory obligations and for the purposes of <b>legitimate interests.</b></p>
<p>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.</p>	<ul style="list-style-type: none"> <li>• To control and manage access to our projects and worksites for security and safety related reasons</li> <li>• To assist with time keeping e.g. clock in and out.</li> </ul>	<p>To comply with our <b>legal</b> and statutory obligations. To fulfil our <b>contractual</b> obligations and for the purposes of <b>legitimate interests.</b></p>

Personal Data Type(s)	Reasons for Processing	Lawful Basis for Processing
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 <b>legal</b> and statutory obligations and to fulfil our <b>contractual</b> obligations.
Other information collected from visits to our websites including cookies and website, platform and App usage.	To collect information from our website about usage.	Where required by applicable data privacy laws, we rely on <b>consent</b> . For the purposes of <b>legitimate interests</b> . To enable us to provide a better service via our web channels.
Contact Information, key staff, hours worked, digital signatures, training requests and schedules, task information, claims, shareholder positions, national insurance details and home address.	<ul style="list-style-type: none"> <li>• For verification purposes.</li> <li>• For contracting.</li> <li>• For preparation of HSE reports and comments</li> <li>• To plan delivery schedules and locations.</li> <li>• As part of our sub-contractor on-boarding processes.</li> <li>• To respond to queries regarding project issues and status.</li> </ul>	For the purposes of <b>legitimate interests</b> .

## 6. Cookies technology

'Cookies' are small text files placed on your computer or browsing device by a web page server which may later be retrieved. A cookie enables the setting party to



recognise your computer or device without the need for a fresh request for you to register.

Our website, platforms and Apps may also use cookies and other related technologies (for convenience all technologies are referred to as "cookies") for various functional, operational and analytical purposes. Cookies can also be placed by third parties we have engaged or whose apps we have integrated into our own websites or apps.

As you navigate through our website, platforms or Apps or otherwise use our equipment, systems and technology, we may collect information about your computer or browsing device, including, where available, your IP address, operating system and browser type, for system administration.

## **7. Links to third parties**

Our website, platforms and Apps may contain links or plug-ins to and from third party websites and applications including those of our partner networks and other affiliates. If you follow a link to any of these websites, applications or platforms, or use them on your device, please note that these websites, applications and platforms have their own privacy and cookies policies which we cannot control. Please check these policies before you submit any personal information or allows the setting of any cookies.

## **8. How 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 to do so.

We will only collect sensitive information about you if we have your consent or we are otherwise 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, platforms and Apps;
- 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 or whether we have an alternative lawful ground. 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.

## **9. 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 – including the administration and fulfillment of our contracts and services;
- 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.

## **10. How we use your personal information?**

We will only ever use your personal information for the purposes set out in this 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.

Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party)
- Where we need to comply with a legal obligation.

A **legitimate interest** includes when we have a business or commercial reason to use your personal information, so long as this is not overridden by your own rights and interests or would not be reasonably be expected given our relationship. We conduct a balance test of our respective rights to ensure there are no surprises or unexpected uses of personal information.

Generally, we do not rely on consent as a legal basis for processing your personal data.

## **11. How we use particularly sensitive information**

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.
- Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

## **12. How long do we hold onto your personal information?**

We will not ask for more information than we need for the purposes we are collecting it. 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, outdated, inaccurate or expired is securely deleted in line with our legal and regulatory requirements. In essence, we will only keep personal information for the minimum periods of time that are necessary. Our data retention periods vary depending on the nature and context of the personal information that we have in our care, and are calculated taking into account the following factors:

- how long we need to keep the data to fulfil the original purpose for which it was collected;
- potential claims, complaints or litigation;
- guidance from official bodies;
- the nature and sensitivity of personal information; and
- legal and regulatory obligations to which we are subject.

In general, we delete personal information when: the purpose for its processing has been fulfilled or the contractual relationship with you, or your organisation has ended; all mutual duties and claims have been fulfilled; and there are no other legal obligations to retain the personal information nor legal bases for further processing.

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).

### **13. 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, professional advisers, clients and service providers for the purpose of our business operations;
- individuals or organisations to whom we have commercial relationships, including individuals or organisations engaged in providing us with professional, business, technology, IT, 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;
- potential successors if we choose to acquire, restructure, generate investment, sell, transfer, or merge parts of our business, or any assets of the Laing O'Rourke Group.

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

#### 14. Is my personal information processed overseas?

The Laing O'Rourke Group is made up of companies which are incorporated and operate in different countries including Australia, Canada, Hong Kong, the United Arab Emirates and the UK.

Some of the information we collect is stored or hosted on cloud-hosted systems which may be outside the country in which we collect the information.

The data privacy laws in other countries may not be exactly the same as your home location. We will only ever share your data outside of the UK or EU, if one or more of the following apply:

- the third country location is found by a competent authority subject to provide a proportionate and essentially equivalent level of data protection law as the country in which personal information was collected;
- we are permitted or required to do so by law in certain exceptional circumstances by the home territory (for example in connection with legal claims);
- if we have put in place Model Clauses approved by a competent authority for international transfers with the recipient of the data (together with associated supplementary measures following risk assessments); and
- in all cases above, we have taken reasonable steps to ensure that the recipient of the information will not breach the relevant data privacy laws or the approved transfer measures and safeguards of the country in which we collect the information.

Please contact us if you would like more information on the Model Clauses, which can also be accessed from the websites of the EU Commission and the Information Commissioner's Office ("ICO").

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

#### 15. Summary of your individual rights

Right	Description
<b>To be informed</b>	<p>A right to be informed about the personal data we hold about you including via this Privacy Statement and supplementary information provided from time to time at the point of data collection including in forms, via signage or within Apps.</p> <p>If any information is legally or otherwise necessary or essential, we will confirm so at the point of collection alongside any consequences of failing to provide the requisite information.</p>
<b>Of access</b>	<p>A right to access the personal data we hold about you.</p>

<b>To rectification</b>	A right to require us to rectify any inaccurate personal data we hold about you.
<b>To erasure</b>	<p>A right to ask us to delete the personal data we hold about you. This right will only apply where (for example):</p> <ul style="list-style-type: none"> <li>• we no longer need to use the personal data to achieve the purpose we collected it for;</li> <li>• where you withdraw your consent if we are using your personal data based on your consent; or</li> <li>• where you object to the way we process your data (in line with Right 6 below).</li> </ul>
<b>To restrict processing</b>	<p>In certain circumstances, a right to restrict our processing of the personal data we hold about you. This right will only apply where (for example):</p> <ul style="list-style-type: none"> <li>• you dispute the accuracy of the personal data held by us;</li> <li>• where you would have the right to ask us to delete the personal data but would prefer that our processing is restricted instead; or</li> <li>• where we no longer need to use the personal data to achieve the purpose we collected it for, but you need the data for the purposes of establishing, exercising or defending legal claims.</li> </ul>
<b>To data portability</b>	In certain circumstances, a right to receive the personal data you have given us, in a structured, commonly used and machine readable format. You also have the right to require us to transfer this personal data to another organisation, at your request.
<b>To object to processing</b>	A right to object to our processing of the personal data we hold about you where our lawful basis is for the purpose of our legitimate interests, unless we are able to demonstrate, on balance, legitimate grounds for continuing to process the personal data which override your rights or which are for the establishment, exercise or defence of legal claims.
<b>In relation to automated decision</b>	A right for you not to be subject to a decision based solely on an automated process, including profiling, which produces legal effects concerning you or similarly significantly affect you.

<b>making and profiling</b>	We do not undertake any automated decision making (or individual profiling) at the date of this Privacy Statement.
<b>To withdraw consent</b>	A right to withdraw your consent, where we are relying on it to use your personal data (for example, the setting of cookies). This does not undermine the processing based on consent prior to the withdrawal.

We will respond to requests without undue delay and within a month where reasonably possible, and will give you access in the manner you request usually by securely mailing or emailing it to you (provided it is reasonably practicable to do so). If we consider we need more time to respond based on the nature of the request, we will let you know and in certain cases we can extend the timescale to respond by a further two months. We will confirm the timescales and keep you updated throughout.

## **16. Access to your personal information and accuracy in more detail**

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. This is not an absolute right however and there are exceptions permitted under data privacy laws where we may be unable to comply with some or all of such requests, 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 have reasonable doubts as to your identity or the request itself;
- where we are prevented by a law or court order; and
- where the request is manifestly unfounded disproportionate or you have requested the same information within a short timeframe.

We reserve the right to require you to verify your identity including if the request is made by a third party on your behalf (so that we process access requests responsibly and to avoid your data being disclosed inappropriately).

We also reserve the right to charge a reasonable administration fee for the costs of retrieval and supply of any requested information where requests are deemed excessive or if you request multiple copies.

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 and we will discuss the delivery concerns with you.

If we can only give you limited or no access to your personal information, we will set out written reasons and grounds under data privacy laws 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 that you become aware of and we will take appropriate steps to update or correct such information in our possession or control.

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 for any reason 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.

## **17. Security of personal information**

Please note any information that is transmitted over the internet is not always 100% secure. We are committed to safeguarding the privacy of all your information, to ensure it is secure at all times and treated in the strictest of confidence.

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.

We will never sell your personal information for financial gain or be irresponsible with personal information collected. The processes we implement for data security consider various factors including the current state and cost of technology or other physical measures, organisational controls and staff training, in light of the risks to your privacy rights and freedoms.

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 or from our systems and servers or those of our suppliers acting on our behalf;
- 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 and providing authorised personnel with appropriate training;



- conducting due diligence on suppliers that process personal data and agreeing contractual terms in respect of data privacy compliance by the supplier/recipient;
- using access control and security measures for our sites, premises, assets and business systems;
- maintaining our infrastructure to prevent and monitor compromise of systems or application containing personal data;
- business continuity planning and running incident testing exercises; and
- procedures to identify and deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so including where the incident would result in relevant risks.

## **18. How to contact us or complain about a breach**

You can contact us for example if you:

- have any questions about this Privacy Statement;
- wish to exercise any of your individuals rights,
- 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](mailto:infosec@laingorourke.com) or write to our Head Office: Bridge Place 1 & 2, Anchor Boulevard, Crossways, Dartford, Kent, DA2 6SN.

### **Whistle-blowing hotline**

You can also 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.

Although you can exercise your individual rights orally using the phone number above, we also 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](http://www.safecall.co.uk/report)
- Email: [LOR@safecall.co.uk](mailto: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 ICO if your concern is in the UK. If you are based in another EU state, another supervisory authority will be able to lead on your complaint and we can confirm the relevant authority on request.

The UK's ICO can be contacted using the following details:

- First Contact Team, ICO, Wycliffe House, Water Lane, Wilmslow, SK9 5AF.
- <https://ico.org.uk/make-a-complaint/>

## **19. 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.

## **20. 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. We will notify you of material changes to our processing where required by applicable data privacy laws.