LIGS LIMITED, LOCKTON COMPANIES LLP, AND LOCKTON RE LLP PRIVACY NOTICE FOR CANDIDATES

I. WHAT IS THE PURPOSE OF THIS DOCUMENT?

This privacy notice describes how we collect and use personal information about you in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the UK enactment of the EU GDPR and other data protection laws, as applicable ("**Data Protection Legislation**").

It applies to all prospective employees and workers ("**Associates**") and contractors ("**Consultants**") (collectively "**Candidates"**) of LIGS Limited, Lockton Companies LLP, and Lockton Re LLP (collectively "**Lockton**"). You are receiving this privacy notice because you are applying for work with us (whether as an Associate or Consultant). It makes you aware of how and why your personal data will be used, namely for the purposes of recruitment, and how long it will usually be retained for.

Lockton is committed to protecting the privacy and security of your personal information.

Lockton is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under applicable Data Protection Legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services.

II. DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for specified, explicit and legitimate purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant and adequate to the purposes we have told you about and limited only to those purposes.
4. Accurate and where necessary kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

III. THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified.

There are "special categories" of more sensitive personal data which require a higher level of protection. These categories are personal data concerning a person's: (1) racial or ethnic origin, (2) political opinions, (3)

philosophical or religious beliefs, (4) trade union membership, (4) genetic data, (5) biometric data, (6) health, (7) sex life and (8) sexual orientation.

We will collect, store, and use the following categories of personal information (which includes certain special categories and criminal offence data) about you:

- The information you have provided to us in your curriculum vitae (CV) and covering letter
- The information you have provided on our application form, including:
    - Name
    - Address
    - Email address
    - Contact number
    - Date of birth
    - Education and qualifications
    - Employment history and information
- Information contained in right to work documentation
- Any information you provide to us during an interview
- Any other information provided as part of the recruitment process, including references
- Gender and gender identity
- Racial or ethnic origin and nationality
- Next of kin and emergency contact information
- Required adjustments (such as for attending interviews) (if any)
- Public official information including that of a partner or family member
- For Candidates in Northern Ireland, religion

IV. HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about Candidates through the application and recruitment process, either directly from candidates, professional networking platforms such as LinkedIn or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, education history, credit reference agencies or other background check agencies.

If you fail to provide personal information

If you fail to provide certain information, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further. We may also be prevented from complying with our legal obligations. We shall inform you if by not providing certain information to us, it prevents us from performing certain activities or requirements required by law or regulation.

Do we need your consent?

We do not need your consent to collect and process your personal information, special category or criminal offence data in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. However, in a very limited number circumstances, we may need to rely on consent where there is no legal obligation or other lawful basis on which we can rely. In those cases, a prominent and concise consent form, which is separate from other terms and conditions and easy to understand will be provided

("**Consent Form**"). The Consent Form shall provide you with relevant information, including: full details of the information that we would like, Lockton as data controller, the name of any third party controllers who will rely on the consent, why Lockton wants the data, what Lockton will do with it, and that individuals can withdraw consent at any time. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us and you should carefully consider whether you wish to consent.

Throughout this notice we had indicated with an asterisk (*) those limited circumstances where reliance on consent is possible, but it does not mean consent is required or that you have a right to ask that your consent be acquired.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your wellbeing and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

What is an "Appropriate Policy Document"?

If we rely upon certain conditions to process special category data or criminal offence data, we are required to have in place an Appropriate Policy Document ("**APD**"), which is provided in template form by the Information Commissioner's Officer ("**ICO**"). This document sets out the specific purposes for which we collect, process and use special category data and criminal offence data in greater detail than the requirements of a privacy notice and ensures the processing is compliant with applicable Data Protection Legislation. For certain conditions that we rely upon, we will not have to 'show' a substantial public interest for use of that condition over and above the creation of the appropriate policy document.

Under your rights as a data subject, you may be entitled to a copy the APD. If you would like to request a copy or know more about your rights, please contact the Data Protection Manager by email to dataprotection@uk.lockton.com.

V. HOW WE WILL USE YOUR PERSONAL DATA

We will only use your personal information in accordance with applicable Data Protection Legislation. Most commonly, we will collect and use your personal information:

1. Assess your skills, qualifications, and suitability for the work or role;
2. Carry out background and reference checks, where applicable;
3. Communicate with you about the recruitment process;
4. Keep records related to our hiring processes;
5. Where we need to comply with a legal obligation or regulatory requirements;
6. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests; or
7. Where you provide your explicit consent for us to do so by the Consent Form (see section IV above on consent).

Having received your CV and application information, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to invite you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role or work. If we decide to offer you the role or work, we will then take up references. We may also carry out criminal records and fitness and propriety checks at a later stage of the process before your appointment is confirmed.

We have set out below, in a table format, a description of the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your personal data. Additionally, the reliance on the respective lawful grounds is not equally weighted, therefore reliance on certain bases will be prioritised over others, with consent only being relied on where required and if the data subject completed the Consent Form. Please contact our Data Protection Manager if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Processing Type	**Applicable Lawful Basis**
Making a decision about your recruitment or appointment.	→ For our legitimate business interests (to recruit Candidates and ensure your suitability so we can on-board you).
Determining the terms on which you work for us.	→ For our legitimate business interests (for business management to enable us to manage and run our business).
Checking you are legally entitled to work in the UK.	→ For our legitimate business interests (for business management to enable us to manage and run our business, and to maintain appropriate records for defending legal claims).
Ascertaining your fitness to work (where relevant).	→ Enable us to comply with a legal obligation. → For our legitimate business interests (for business management to enable us to manage and run our business, to plan and manage our workforce, manage your attendance at work, assess your fitness for work, manage health and safety risks, consider, and make reasonable adjustments).
To comply with health and safety obligations.	→ Enable us to comply with a legal obligation. → For our legitimate business interests (for business management to enable us to manage and run our business and manage health and safety risks. This includes next of kin and emergency contact information).
To prevent and detect fraud.	→ Enable us to comply with a legal obligation. → For our legitimate business interests (for business management and planning, including accounting and auditing to enable us to manage and run our business).

Equal opportunities monitoring.	→ Enable us to comply with a legal obligation. → For our legitimate business interests (to ensure our business is a fair place to work).
Public Official information, credit history and criminal records (see section below for more details on the collection of criminal offence data).	→ Enable us to comply with legal obligation (to ensure that business and recruitment and hiring activities are compliant and in line with local law and practice). → For our legitimate business interests (to ensure the company is a safe place to work and had a competent and qualified workforce). → *Consent of data subject if required and data subject has completed Consent Form.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you during the recruitment process and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

VI. HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION (SPECIAL CATEGORY DATA)

”Special categories” of particularly sensitive personal information require higher levels of protection. As mentioned above, data relating to a person’s racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or a person’s sex life or sexual orientation, are defined as ‘special category’ data. We need to have further justification and satisfy an additional lawful basis for collecting, storing, and using this type of personal information with some of those conditions requiring an additional APD (See below for more information).

Generally, we may process special categories of data under applicable Data Protection Legislation as follows:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment, social security and social protection.
3. Where it is needed for a substantial public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme or one of the other 23 specified public interests are met (which are set out in the Data Protection Act 2018, Schedule 1 (paras 6 – 28)).

Less commonly, we may process this type of information under applicable Data Protection Legislation as follows:

1. Where it relates to legal claims or judicial acts;
2. Where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent; or

3. Where you have already made the information public.

Where necessary we have in place an APD, as described above, and safeguards which we are required by applicable Data Protection Legislation to maintain when processing such data. Should we need to process special category for any purpose not listed here, we will check to see if it is compatible with our original purposes. Only where required, if we are unable to rely on any specific exemption(s) under applicable Data Protection Legislation, will we obtain specific consent from you to process any special category information about you. Your consent must be freely given and you are under no obligation or expectation to provide it if you wish not to.

Why we collect special category data

Lockton is committed to the company's diversity, equality, and inclusion strategies and initiatives and as a result would like to understand the needs of its Candidates more in depth. By collecting special data categories, Lockton gets to know its Candidates better and can cater its services to them to foster an inclusive and welcoming workplace environment.

Situations in which we will use your special category data

We have set out below, in a table format, a description of the special category data we plan to use, and on which legal basis we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your special category data for more than one lawful ground depending on the specific purpose for which we are using your personal data. Again, please contact our Data Protection Manager if you need details about the specific legal ground we are relying on to process your special category data.

Data Category	Applicable Lawful Basis	Additional lawful Basis
Racial or ethnic origin data Religion/Philosophical Beliefs	→ For our legitimate business interest (to ensure the company is a fair place to work and inclusive). In particular, we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting. → Legal Obligation (duty of care to assess fitness and requirements to make reasonable adjustments and ensure that the company is free from bias, harassment, and discrimination, protecting the rights and interests of data subjects etc). In particular, we will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process. In Northern Ireland, we will use information on your religion in order to meet specific local requirements to monitor on the basis of religion issued by the Equality	→ Reasons for substantial public interests (with a basis in law) → Equality of opportunity or treatment

	Commission under its Fair Employment in Northern Ireland Code of Practice.	
Health (includes information about physical or mental health, including any disabilities) Sexual Orientation Sex Life	→ Legal Obligation (duty of care to assess fitness and requirements to make reasonable adjustments and ensure that the company is free from bias, harassment, and discrimination, protecting the rights and interests of data subjects etc) → Legitimate Interest (to manage health and safety risk and support, ensure a fair and inclusive workplace culture/diversity of staff and thought and to ensure meaningful equal opportunity monitoring and reporting) → *Consent of data subject if required and data subject has completed Consent Form	→ Employment, social security and social protection law → Reasons for substantial public interests (with a basis in law) → Equality of opportunity or treatment

VII. INFORMATION ABOUT CRIMINAL OFFENCE DATA

We envisage that we will process criminal offence data. This refers to "personal data relating to criminal convictions and offences or related security measures" and covers a wide range of information about criminal activity, allegations (both proven and unproven), investigations, proceedings, personal data of victims and witnesses of crimes, information relating to the absence of convictions, personal data about penalties, conditions or restrictions placed on an individual as part of the criminal justice process and/or civil measures which may lead to a criminal penalty if not adhered to.

We may only use criminal offence data where the law allows us to do so and where we are required to comply with applicable law and/or regulation. Like special category data, we need to have further justification and satisfy additional lawful bases for collecting, storing criminal offense data. We must meet certain standard and enhanced conditions under applicable Data Protection Legislation to collect criminal offence data and we are required to provide an APD which provides in greater detail the specific purposes in which we collect, process and use criminal offence data.

We process criminal offence data when processing "is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law in connection with employment, social security or social protection."

We may use criminal offence data where it is necessary in relation to legal claims, where it is necessary 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.

However, we will only collect criminal offence data if it is appropriate given the nature of the role and where we are legally able to do so or required as a result of regulatory requirements. Where appropriate, we will collect criminal offence data as part of the recruitment process. In particular, we will collect information about your criminal convictions history if we would like to offer you the work or role (conditional on checks and any other conditions, such as references, being satisfactory) and we are required or entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the work or role.

We will use criminal offence data in the following ways:

Data Use	**Applicable Lawful Basis**	**Additional lawful Basis**
FCA compliance	→ Legal obligation: the processing is necessary for us to comply with the law and regulatory bodies → Legitimate interests: the processing is necessary to ensure workforce maintains integrity and is fit to engage in regulated activities, manage financial instruments, and adhere to company standards → *Consent if required and data subject has completed Consent Form	→ Employment, social security and social protection law → Reasons for substantial public interests (with a basis in law) → Preventing or detecting unlawful acts → Preventing fraud → Suspicion of Terrorist financing or money laundering (can only rely on this to process data relating to disclosure of suspicion)
Fitness and Propriety	→ Legal obligation: the processing is necessary for us to comply with employment law and regulatory bodies → Legitimate interests: the processing is necessary to ensure workforce maintains integrity and is fit to engage in regulated activities, manage financial instruments, and adhere to company standards.	→ Employment, social security and social protection law → Reasons for substantial public interests (with a basis in law) → Preventing fraud
Other roles with regulatory oversight	→ Contract: Performance of our contract with you such as to monitor your qualification and competence for roles	→ Employment, social security and social protection law → Reasons for substantial public interests (with a basis in law)

	→ Legal obligation: the processing is necessary for us to comply with employment law and regulatory bodies	→ Equality of opportunity and treatment → Preventing fraud

We have in place an ADP and safeguards which we are required by law to maintain when processing such data.

VIII. AUTOMATED DECISION-MAKING

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

IX. DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities in the group for the purposes of processing your application.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?
We will share your personal information with third parties where required by law, where it is necessary to process your application or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?
”Third parties” includes third-party service providers (including recruitment consultancies, background check providers, credit reference agencies, and other contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers in the context of the

recruitment process: assistance with the recruitment process, background checks, credit reference checks and fitness and propriety checks.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

How secure is my information with third-party service providers and other entities in our group?
All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?
We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for preparing budgets, for system maintenance support and hosting of data.

Transferring information outside the UK
We may transfer the personal information we collect about you to the following countries outside the UK in order to perform our contract with you. Those transfers would always be made in compliance with applicable data protection legislation. If you would like further details of how your personal data would be protected if transferred outside the UK, please contact our Data Protection Manager by email to dataprotection@uk.lockton.com.

X. DATA AND INFORMATION SECURITY

We have put in place technical and organisational measures to protect the security of your information. We take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for your rights and freedoms. Details of these measures are available upon request.

We have an information security policy and take steps to make sure the policy is implemented and where necessary, we have additional policies and ensure that controls are in place to enforce them. From time to time, we review our information security policies and measures and, where necessary, improve them.

Third parties will only process your personal information on our instructions and where they have sufficient guarantees about their security measures and agreed to treat the information confidentially and to undertake the same security measures that we would have to take if we were doing the processing ourself. We require any third-party processor to make available all information necessary to demonstrate compliance with our security measures.

We have put in place appropriate security measures to prevent your personal information, special category data, and criminal offence data from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. These include both physical measures like high quality doors and locks with access control measures, alarms, security lighting, and CCTV and technical measures such as network and system security and device security. We also from time to time perform vulnerability tests, and assess and evaluate the effectiveness of any measures we put in place. In addition, we limit access to your personal information, special category data, and criminal offence data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information, special category data and criminal offence data on

our instructions, and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Cyber Security Analyst at dataprotection@uk.lockton.com.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

XI. DATA RETENTION

How long will you use my information for?

We will only retain your personal information, special category data, and criminal offence data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, regulatory or reporting requirements. However, we retain your data for 2 years, after we have communicated to you our decision about whether to appoint you to a role. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. We will also retain your personal information with view to contact you about other relevant job opportunities that may become available at Lockton from time to time. After this period, we will securely destroy your personal information in accordance with our data retention policy and applicable laws and regulations. We periodically review your personal information, special category data and criminal offence data and delete anything we do no longer need to retain.

Details of retention periods for different aspects of your personal information, special category data and criminal offence data are available in our retention policy which is available from the Data Protection Manager. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

If you do not wish for us to retain your information after the application process has closed, please contact us to let us know dataprotection@uk.lockton.com

XII. RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your rights in connection with personal information

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

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to

processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct, or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Manager in writing.

No fee usually required
You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive.

Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you
We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

XIII. RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

XIV. DATA PROTECTION MANAGER

We have appointed a data protection manager to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the data protection manager. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

XV. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. This version is dated 19/07/2022 and historic versions can be obtained by contacting our Data Protection Manager. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Data Protection Manager by email to dataprotection@uk.lockton.com