CHALLENGE GROUP HOLDINGS LTD

DATA PROCESSING NOTICE

(LEGITIMATE BASIS PROCESSING)

What is the purpose of this document?

This privacy notice applies to Challenge Group Holdings Limited and affiliated companies. A reference to “we”, “us” or “ours" in this notice is a reference to the specific company in the Challenge Group Holdings Limited group which employs or engages you.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation and any other applicable privacy laws (referred to as “GDPR” in this notice).

This notice applies to all employees, workers and contractors engaged or employed or used by us (including permanent salaried colleagues, hourly paid front line operatives, contractors engaged via their own personal services company, and directors).

Challenge Group Holdings Ltd 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 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. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Where can you find a copy of this privacy notice?

THIS NOTICE WILL BE PUBLISHED IN THE FOLLOWING PLACES AND MAY BE UPDATED FROM TIME TO TIME THE PUBLISHED VERSION WILL BE THE CORRECT VERSION

Challenge Group Holdings Limited Website: www.challengetrg.co.uk

A COPY OF THE CURRENT PRIVACY NOTICE IS AVAILABLE ON REQUEST FROM THE DATA PROTECTION OFFICER VIA EMAIL: thedpo@challengetrg.co.uk

Challenge-trg
Recruitment

Data protection principles

We will comply with UK GDPR. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected for valid purposes that we have clearly explained to you, and not used in a way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

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. It does not include data where the identity has been removed or made inaccessible (anonymous data or pseudonymised data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

Specific categories of personal data that we could hold about you.

Depending upon your role with us, we will collect, store, and use some or all of the following categories of personal information about you.

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependents.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Dates of employment (and dates of assignment).
- Location of employment or workplace.
- Copy of driving licence or details of licence, and details of personal vehicles you use for work (including copies of insurance information).
- Copy of passport (subject to compliance with applicable local law) or information from passport such as passport number together with visas or other records of proof of right to work.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Proof of right to work.
- Details of your timesheets and, if you are an hourly paid frontline operative, details of your assignments.
- Employment records (including job titles, work history, working hours, and training records. Qualifications, CVs, job applications, and professional memberships).
- Compensation, commission, expenses and pay history.
- Job or assignment performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipecard records.

- Information about your use of our information, equipment and communications systems, or our vehicles.
- Photographs might be used for Microsoft 365 or ID badges or contact information directories.
- Information connected to compliance with health and safety obligations (such as RIDDOR reports and incident reports).
- Geo location or tracking information connected to performance of your work or assignment.
- IP addresses and device information when you connect to or use our systems or networks.
- Records of (or recordings of) telephone calls, hangouts and meetings.
- Records of drug and alcohol tests.
- Records of competency tests (e.g., language or maths proficiency tests).
- Records of apprenticeship or other training or qualifications undertaken in connection with your employment or engagement via a Challenge-trg Group Holdings Limited company.
- Dietary requirements in the event that you attend a Challenge-trg Group Holdings Limited event.
- Travel booking details.
- Survey responses (such as Candour Surveys which you choose to respond to)
- Social networking posts or messages connected to your job or assignment, or to us.
- Authentication data in connection with our devices or systems.
- Information about you which is connected to claims, legal disputes, legal proceedings or criminal or fraud investigations, or details of IVAs or charging orders (e.g., where a court order requires us to make a deduction from your pay or pay some of your pay to a third party such as a creditor).
- Financial records information such as credit ratings (for example where a credit check is required as part of your job or assignment).

We may also collect, store, and use the following "special categories" of sensitive personal information:

- Vetting information relevant to your role (e.g., vetting required by the Security Industry Authority if you are a security officer, or as required if you are working with vulnerable people)
- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions (for example in respect of our legal obligations such as Gender Pay Gap reporting, or for diversity monitoring programmes).
- Trades union membership, particularly where we are applying deductions through payroll to a union of your choice.
- Information about your health, including any medical condition, health, and sickness records.
- Information about occupational health referrals and outcomes.
- Genetic information and biometric data collected as part of monitoring systems (such as biometric time and attendance systems, biometric security features on company equipment such as laptops).
- Information about criminal convictions and offences to the extent permitted by applicable law (e.g., the Rehabilitation of Offenders Act in the UK).

We will only collect, store, and use personal data or special categories of data where this is required in connection with your job or assignment (e.g., to allow us to ensure your wellbeing at work, or in connection with a customer's requirement for a job or assignment).

How is your personal information collected?

We collect personal information through the application, recruitment and onboarding process, either directly from individuals or from an employment agency or umbrella/payroll company or background check provider or through jobs board. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies such as in connection with Disclosure and Barring Services checks.

We will collect additional personal information in the course of your employment or engagement.

We will collect additional information from your use of any "Contact Us" facility on our websites or via any apps we use to facilitate your employment or engagement with us.

If your employment transfers to us under the Transfer of Undertakings (Protection of Employment Regulations 2006 (as amended) or the Acquired Rights Directive or other similar law (referred to collectively as "TUPE"), we will collect information through the TUPE process.

Challenge-trg
Recruitment

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract, we have entered into with you (this includes offering you work and administering your employment or assignment with us).

2. Where we need to comply with a legal obligation (this includes sharing information with customers and auditors to validate your right to work) for example.

3. 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.

We may also use your personal information in the following situations, although these are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest or for official purposes.

Situations in which we will use your personal information

Depending upon your role, we need the types of information in the list above to allow us to perform our contract with you and to enable us to comply with our legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment, appointment, or employment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the country in which we have employed or engaged you.
- Paying you and, where appropriate, deducting tax and National Insurance contributions.
- Providing benefits to you.
- Liaising with your pension or benefits provider(s).
- Administering the contract, we have entered into with you.
- Liaising with customers to whom you are assigned from time to time (including the customer's auditors, professional advisers and compliance teams) regarding your assignment and performance.
- In connection with legal or insurance claims/disputes.
- In connection with health and safety reporting or obligations.
- For business management and planning purposes, including accounting, auditing business sales and restructures.
- When conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications and capability for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- In connection with education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness or other absence.
- To conduct data analytics studies (using anonymised or pseudonymised data) to review and better understand employee retention and attrition rates.
- For equal opportunities monitoring.
- To comply with our legal obligations.
- To prevent or investigate fraud, theft or other wrongdoing.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing you with a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

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 usually notify you. The exception to this is where the change is made in respect of one or more categories of employee, worker or contractor (e.g., due to a change in law) in which case such changes will be notified through the publication of a revised privacy notice. We will always endeavour to tell you about these types of changes, and we will explain the legal basis which allows us to undertake this new processing.

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.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection.

We need to have further justification for collecting, storing and using this type of personal information. 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:

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 (for example in connection with your health, safety, wellbeing, or fitness to work).

3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme].

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.

Our obligations as an employer

We may use your particularly sensitive personal information in the following ways:

- We may use absence and healthcare information including occupational health information and referrals in connection with absence management or monitoring (including sickness absence, family-related absence or other absence).
- We will use information about your physical or mental health, or disability status to ensure your health, safety and wellbeing in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, and to administer associated benefits.
- We may 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, or to comply with our legal obligations (such as Gender Pay Gap Reporting).
- We may use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- We may use vetting information relevant to your role (e.g. vetting required by the Security Industry Authority if you are a security officer, or as required if you are working with vulnerable people).
- We may use genetic information and biometric data collected as part of monitoring systems (such as biometric time and attendance systems operated at customer premises, or biometric security features on company equipment such as laptops).

- We will use information about criminal convictions and offences to the extent permitted by applicable law (e.g. the Rehabilitation of Offenders Act in the UK).

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy or to carry out our legal obligations and duties (such as under health & safety legislation) or to exercise specific rights in connection with relevant employment law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. In these limited cases, 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.

Information about criminal convictions

We may only use information relating to criminal convictions where the relevant law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided, we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions 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.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you during you working for us. We will use information about criminal convictions and offences in the following ways:

- by providing information about unspent convictions to customers who request them in connection with the performance of our services for our customers.
- where required for vetting or validation purposes (such as in connection with security officer roles, or temporary assignments at airports or other ports).
- in connection with safeguarding.

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 may use automated job searching through an app or algorithm or, more usually through recruitment jobs boards, which may determine whether your CV is provided in connection with a potential job or application (for example by matching key job titles or phrases against a vacancy).

Except for the job matching referred to above, 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.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the Challenge Group Holdings Limited group.

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 EU.

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, or where it is necessary to administer the working relationship with you, or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes the following types of third-party service providers (including their contractors and designated agents):

1. Customers (where you attend customer premises in connection with your role)
2. Managed services companies or managing agents to whom we provide our services for an end customer.
3. Professional advisers (e.g., lawyers or accountants).
4. Law enforcement or regulatory bodies.
5. The Courts.
6. Insurance companies.
7. Jobs boards and CRM systems (e.g., FileStack, Broadbean, Salesforce, Twilio) used by us or our customers.
8. Benefits providers (e.g., pension's administrators or trustees, Wagestream for advances in pay).
9. CV formatting services providers.
10. Training providers (e.g., in connection with apprenticeships)
11. Payroll or accounting services companies we may use.
12. Auditors (including customer auditors).
13. Providers of apps we use (e.g., Certify for expenses payments, DocuSign for contract signature).
14. Other companies within the Challenge Group Holdings Limited group.
15. Companies that host or provide our IT systems, platforms, or apps (e.g. MyHr, Cezanne, AWS)
16. Document or data archiving companies we use to store records in line with our legal data retention obligations.

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 unless they obtain permission from you directly to do so. 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 system maintenance support and hosting of data, through our shared support functions in order to perform our contract with you, and in order to offer you assignments or work elsewhere in the group.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business, with customers to whom you provide services under a contract with us, to umbrella or payroll companies or to companies providing benefits offered to you as part of your employment or engagement with us. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We use cloud-based service providers to host some of our IT systems and apps (including our email and document management systems), and this means that your data may be held outside the EE in those systems. All cloud-based service providers we use have either agreed to specific protections with relevant data authorities or have agreed to keep personal information in accordance with relevant data protection law.

Data security

We have put in place measures to protect the security of your information.

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

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. We keep security measures under review and update our procedures and processes as necessary. We limit access to your personal information to those employees and other third parties who have a business need to see it. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

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.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. 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 or pseudonymise 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. Once you are no longer an employee, worker or contractor of the company we will retain and where possible securely destroy or delete your personal information in accordance with our data retention policy and applicable law.

Where it is not possible to destroy or delete personal information, we may instead move the data to a location which makes it inaccessible. This would have the effect of stopping any processing.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, and in accordance with applicable GDPR or other 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 Officer in writing (The DPO, Challenge Group Holdings**,** 1 Smithy Court, Smithy Brook Road, Wigan WN3 6PS) or via email thedpo@challengetrg.co.uk.

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, unless prevented by law, 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.

Right to withdraw consent

In those very 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 email thedpo@challengetrg.co.uk, making it clear which consent you are seeking to withdraw. 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.

Data protection officer

We have appointed a data protection officer (DPO) 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 DPO (thedpo@challengetrg.co.uk).

You have the right to make a complaint at any time to the supervisory authority with responsibility for the country in which we have employed or engaged you to work. For further details of the relevant authority, please see this link:

- UK: https://ico.org.uk/

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. We may also notify you in other ways from time to time about the processing of your personal information.
ends