

Privacy notice for applicants

Introduction

Brit Group Services Limited (“Brit”, “we” or “us”) is committed to protecting the privacy and security of your personal data. References to your “personal data” will include any or all of your personal data, as the context requires, including “special categories of personal data”, which involves more sensitive information about you.

This privacy notice describes how we are or will be processing personal data about you during the hiring process and beyond. “Processing” covers such actions as collecting, using, storing, disclosing, erasing or destroying your personal data.

This notice applies only to those who apply to us for a vacant job or temporary assignment (whether as a temporary or fixed term worker or part time or full-time employee). However, it will not apply once you join us, (or for sponsored migrants, once you have been assigned a Certificate of Sponsorship which is used in a successful application to work for us); in this event you should and you should then refer instead to the Privacy notice for employees, workers and contractors. It does not form part of any contract of employment or other contract to provide services.

Identity and contact details of the data controller and the data protection officer

Brit is a “data controller”. This means that we are responsible for deciding how we hold and use personal data about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

The contact details of Brit are:

The Leadenhall Building
122 Leadenhall Street
London
EC3V 4AB

Main office number: 020 3857 0000

We have appointed a data protection officer (“DPO”) whose contact details are as follows:

Tim Harmer, Group Director of Legal and Compliance, 020 3857 0163, tim.harmer@britinsurance.com.

The DPO is responsible for overseeing compliance with this privacy notice and for handling any data protection queries or issues involving Brit. However, please contact the Head of Recruitment – careers@britinsurance.com, in the first instance.

What type of personal data do we process about you?

We may process the following categories of personal data about you:

- Recruitment information (including any details provided by third party referees over which we have no control (should you have accepted a job offer but then subsequently decline or

have your offer withdrawn due to unsatisfactory references or any other reason) and other information held on CV or passed to us by an employment agency).

- Previous employment history, including education background information.
- Personal contact details such as name, title, address, telephone numbers, and personal email address.
- Your date of birth and gender.
- Your national Insurance number.
- CCTV footage from your visits to Brit.

We may also process the following “special categories” of more sensitive personal data:

- Information contained on our equality and diversity form (which you will be invited to complete) about your race or ethnicity, religious beliefs, sexual orientation, gender, disability, age, parental and caring responsibilities, socio-economic for the purposes of equal opportunities and diversity monitoring and reporting.
- Information about criminal convictions and offences (if you have completed the background verification form and the results came back to Brit) – please see “Information about criminal convictions” below for further information.
- Information relating to your right to work in the UK, including your nationality, immigration status and information from related documents/online checks, such as your passport, Biometric Residence Permit or other identification and immigration information.

How do we collect your personal data?

We will collect personal data about you through the application and recruitment process, either directly from you or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers (in the form of references) digital identity service providers or government authorities (in relation to UK right to work checks).

What are the legal bases and the purposes for which we process your personal data?

We will only use your personal data as permitted by law. We will typically use your personal data in the following circumstances:

1. Where we have your consent to do so.
2. Where we need to perform the contract, we have entered into with you.
3. Where we need to comply with a legal obligation.
4. Where the processing is necessary to perform a task in the public interest
5. 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 are required to specify what the legitimate interests are (see below for further details). The examples given below do not form

an exhaustive list of purposes for which your personal data will be processed, and we reserve the right to add to them at any time.

Consent

If your personal data is sent to us by a recruitment agency, the agency will firstly have obtained your consent to release that information to us. Once we have your personal data, we will process that information in accordance with the lawful bases set out below.

We invite all applicants for work at Brit to complete a Personal Information Request form for the purposes of equality and diversity monitoring and reporting. We rely on your explicit consent to allow us to process the personal data that you provide to us on that form.

Necessary to comply with a legal obligation

The following purposes come under this category:

- Checking that you are legally entitled to work in the UK. – your nationality and immigration status and information from related documents/ online checks such as your passport and other identification and immigration documentation.
- Handling any potential, threatened or actual legal disputes involving you or third parties.
- To prevent fraud.
- For compliance with Home Office legal obligations there are requirements on us to retain information where a migrant whom we sponsor is recruited instead of you. The information we must retain will depend on the applicable process:
 - Where a formal resident labour market test was required in the sponsored migrant's recruitment, we are obliged to retain the following information where a sponsored migrant is recruited instead of you:
 - Your application in the medium in which it was received, for example, emails, CVs, application form, including your details such as name, address, date of birth; and
 - interview notes or other documentation which show the reasons why you were not recruited.
 - Where a formal resident labour market test was not required in the sponsored migrant's recruitment, we may retain the following information where a sponsored migrant is recruited instead of you:
 - interview notes or other documentation which show the reasons why you were not recruited; and / or
 - any other relevant information or evidence which shows the process we used to identify the recruited migrant as the most suitable candidate

Please note that, whereas we normally retain personal data pertaining to unsuccessful applications for work with us for 6 months, we have a statutory duty to keep the above information for longer where a sponsored migrant is recruited instead of you. We have a legal obligation to retain such information for the duration of the sponsored migrant's sponsorship plus one year after their

sponsored has ended, or until a Home Office Compliance officer has approved the paperwork, if sooner.

Necessary for our legitimate interests or those of a third party

Recruitment:

- Personal data provided by you on your CV or by the employment agency if applicable – the legitimate interests are to ascertain your suitability for employment/engagement.
- Personal data provided by you on new starter or temporary new starter forms (if applicable), specifically your gender, mobile phone number, next of kin details – the legitimate interests are for identity and reporting, for emergency contact/disaster recovery.
- Personal data obtained through CCTV – the legitimate interest is the protection of health and safety (including the identification of individuals on premises in the event of a fire or other serious incident) and the prevention and detection of criminal acts.

If employment is offered:

- Personal data obtained through our external background screening providers (which, where relevant, may include address history, employment history, education background, criminal records information (see below for more details), credit history and regulatory references under the Senior Managers and Certification Regime) – the legitimate interests are: for verifying the information provided by you on your CV, to verify the relevant qualifications/requirements for the role, to verify your employee declaration and as necessary for compliance and as required by regulatory bodies, and to ensure that there are no issues with your credit history that could place unnecessary risks on Brit or third parties. If you decide not to take up Brit's offer of employment and provide us with any reasons why you are declining the offer, we will keep a note of the reasons you provide to review and assess our recruitment processes.

How we use special categories of personal data

"Special categories" of personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. Unless you go on to become an employee, it is unlikely that we will process any special categories of personal data other than in the following circumstances:

1. Where it is needed in the public interest.
2. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

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.

We will use your special categories of personal data in the following ways:

- We will use information about your physical or mental health, or disability status, to assess your fitness to work and reasonable adjustments to your job or working environment. We may obtain such information from the employment agency to which you would have provided such information.

- We will use information about your race or nationality or ethnic origin, religious or other beliefs, disability or your sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us and we have a legitimate reason to do so. For some roles there is a regulatory requirement or expectation that criminal record checks will be conducted, and for all roles appropriate checks are considered necessary to protect Brit's business and its systems and to ensure we maintain the trust of clients. Brit's legitimate interests are pursued by ensuring that, as far as practicable, Brit has trustworthy staff who can be relied up on to operate within the law and the checks are necessary to enable Brit to perform or exercise its employment law rights and obligations. In all cases we will ask you to authorise our third party screening provider to obtain a basic criminal record disclosure from the Disclosure and Barring Service (DBS) as part of our background screening checks. For most roles within Brit, any criminal record disclosures will not include information on spent convictions but in instances where they are you will be notified of this separately in advance of the checks being completed.

We may also 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. Further information about how we handle criminal record information is available on request.

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 in the course of you working for us.

With whom might we share your personal data?

We may have to share your data with third parties. See below for further details.

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 data outside the EU via our external background screening provider when it is necessary for them to conduct international checks as part of the process.

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

Why might we share your personal data with third parties?

We may share your personal data with third parties where required by law or where we have another legitimate interest in doing so.

How secure is your information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal data 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 are data controllers in their own right in relation to your personal data. Where they operate as our "data processors" (i.e. they process your personal data on our behalf and acting only on our instructions), we only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about disclosure to other third parties?

We may share your personal data with other third parties, for example in the context of the possible sale or restructuring of Brit. We may also need to share your personal data with a regulator, to external legal or other professional advisers, or to otherwise comply with the law.

How long will we retain your personal data?

We will only retain your personal data 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. Details of retention periods for different aspects of your personal data are available in our Document Retention and Secure Document Disposal Policy which is available on The Hub. This will be accessible to you once you join Brit as an employee or other worker. Please contact our DPO if you want further information on this or if you are unable to access the Hub.

In some circumstances we may anonymise your personal data 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 securely destroy your personal data in accordance with our retention policy.

Your rights in connection with personal data

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

- Request access to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data 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 data. This enables you to ask us to delete or remove personal data only 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 data where you have exercised your right to object to processing (see below).
- Object to processing of your personal data 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.
- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal data to another party.

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

No fee usually required

You will not have to pay a fee to access your personal data (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 data is not disclosed to any person who has no right to receive it.

What are your rights to withdraw consent to processing?

You may withdraw your consent to allow us to continue processing your personal data, but only where consent was sought as a lawful means of processing your personal data.

In the limited circumstances where you may have provided your consent to the processing of your personal data 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 DPO. 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, in which case we will notify you of this in advance.

What are your rights to lodge a complaint about the way in which your personal data are being processed?

Firstly, we would urge you to contact the DPO in writing. If you are not satisfied with the DPO's response, you may contact the Information Commissioner's Office ("ICO") on 0303 123 1113.

You are free to contact the ICO at any time. However, the DPO may be able to answer your concerns or questions more quickly.

Personal data received from someone other than you

If we obtain personal data from someone other than you (such as a referee, or information from a regulator), we will provide you with information as to the source of such personal data and, if applicable, whether it came from publicly available sources.

What data security measures are in place to protect my personal data?

We have put in place measures to protect the security of your information. Details of these measures are available upon request. There are locked cupboards with employee/contractor/candidate personal data held securely within the HR department. Electronic data of this nature is held securely on our systems and any special category data is password protected. You are also referred to the Brit Corporate Information Security Policy which sets out the information security framework in operation at Brit. This will apply to your personal data as well as personal data of third parties.

Third party data processors will only process your personal data 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 data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have

a business need to know. They will only process your personal data 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.

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 data.

If you have any questions about this privacy notice, please contact the DPO.