

Privacy Notice for Applicants for Jobs at Legal & General

WHAT IS THE PURPOSE OF THIS DOCUMENT

Legal & General is committed to protecting the privacy and security of your personal information, also known as personal data

This privacy notice describes how we collect and use personal information about you when you apply for a job at Legal & General, in accordance with our obligations under data protection legislation including the UK GDPR and UK Data Protection Act 2018.

WHO DOES IT APPLY TO

It applies to all applicants for UK job vacancies advertised to recruit employees, workers, agency workers, contractors, secondees and non-executive directors of Legal & General Resources Limited, Legal & General Group Plc or Legal & General Investment Management (Holdings) Limited ("LGIM(H)"). It also applies to all applicants for UK job vacancies advertised to recruit employees, workers, agency workers, contractors, secondees and non-executive directors of companies in the Legal & General group which are wholly owned by Legal & General, in so far as their data is processed by Legal & General Group Plc, Legal & General Resources Limited or LGIM(H). It also applies to candidates globally to the extent that it relates to the processing of data in the new My HR system.

Legal & General (Legal & General Resources Limited, Legal & General Group Plc or LGIM(H)) 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.

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.

When you provide Legal & General with personal data relating to third parties, such as connected persons who are immediate family or partners sharing the same household or who are dependent on you, please advise them that we will process their data in accordance with this privacy policy and they have the same rights.

If you are offered a role with Legal & General in the UK, your data will be further processed in accordance with our Privacy Notice for Employees, Workers, Agency Workers, Contractors, Secondees and Non-Executive Directors, which supersedes the processing described in this notice.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you (please note this list is not exhaustive):

- The information you have provided to us in your curriculum vitae (CV) and covering letter.
- The information you have provided on our application form and equal opportunities form, including name, title, marital status, address, telephone number, personal email address, date of birth,

gender, employment history, qualifications and your bank or building society details (Where an offer is made).

- Any information you provide to us during an interview.
- Any CCTV Footage and visitor information where a face-to-face interview is conducted.
- Any information gathered during any psychometric testing or assessment process undertaken.
- If we decide to offer you a role:
 - details of your future role including future salary and working hours; and
 - any information collected whilst carrying out pre-employment screening. This includes copies of right to work documentation, references, credit checks and criminal conviction data.

We may also collect, store and use more sensitive personal information some of which is "special category" personal data:

- Information about your race or ethnicity, religion or religious beliefs, sexual orientation and gender identity.
- Information about your health, including any medical condition or disability.
- Information about criminal convictions and offences.
- Biometric data used to verify your identity in the Pre-employment screening.
- Information about your socio economic status.
- Information about any caring responsibilities you may have.

HOW WE COLLECT AND USE INFORMATION ABOUT YOU

How is your personal information collected?

We collect personal information about candidates through the application and recruitment process, either directly from the candidate, recruitment agencies, apprenticeship providers, our background check provider, credit reference agencies, the Disclosure and Barring Service, your named referees, and data from publicly accessible sources such as LinkedIn.

How we will use information about you

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- To communicate with you regarding potential opportunities.
- Comply with legal or regulatory requirements.
- Monitor and develop action plans to address areas of under-representation to improve diversity and equal opportunities through our recruitment process and throughout employment.

It is in our legitimate interests to decide whether to appoint you to the role. We also need to process your personal information to decide whether to enter into a contract of employment with you.

The information provided in your CV and covering letter or your application form and the results from any testing undertaken will be processed 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 call you for an interview, we will use the information previously provided and the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references and carry out any other necessary checks (including right to work checks, credit checks and criminal record checks if appropriate) before confirming your appointment.

How we use special categories of personal data

“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 will use your special categories of more sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- Where it is needed in the public interest for diversity, inclusion and equal opportunities monitoring, we will use information about your race or national or ethnic origin, religious beliefs, sexual orientation and gender identity, disability or long-term health condition, social economic status and caring responsibilities to ensure meaningful diversity monitoring and reporting.
- We may process your biometric data to be able to verify your identity for pre-employment screening purposes. We obtain your explicit consent for this purpose during the pre-employment screening process.
- We may also be aware of your sexual orientation, even if you don't specifically provide this, if you provide us with details of your marital status or your partner's details in conversation.

Your information is stored in our HR system and can only be accessed by a small number of people in our HR team.

If you fail to provide personal information

If you fail to provide information when requested, 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.

INFORMATION ABOUT CRIMINAL CONVICTIONS

As part of our pre-employment screening process, we undertake a criminal record check on all applicants who receive an offer of employment to satisfy ourselves (and in some instances, our regulator) that there is nothing in your criminal convictions history which makes you unsuitable for the role offered. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing criminal conviction data.

AUTOMATED DECISION-MAKING

In some instances, we may make decisions that are automated based on information provided during the recruitment process. For example, we may automatically reject applications which do not meet

certain minimum criteria. We will do this where it is necessary in order to make a short list of possible candidates. If your application is rejected based on an automated decision, we will notify you of this fact.

DATA SHARING

Why might you share my personal information with third parties?

We may share your data with third parties, including other companies within the Legal & General Group and third-party service providers (including contractors and designated agents) where required by law, where it is necessary to process your application or where we have another legitimate interest in doing so.

We may also share your data with other third parties for the purpose of responding to external requests for information on the diversity of our business and in respect of our approach to equal opportunities. In this situation we will, so far as possible, share anonymised data only.

We may also share your data with third parties to enable you to complete any psychometric and video based job assessments. This information is used to assess your suitability for the role.

We may also share details on your future role (for example future salary and working hours) to parties where explicitly requested by you, for example for the purposes of mortgage applications or to letting agents. We require third parties to respect the security of your data and to treat it in accordance with the law. All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information.

We may transfer your personal information outside the UK. If we do, the level of protection in those countries may not be the same level as in the UK but we as Data Controller take steps to impose the mechanisms and appropriate safeguards, such as contractual obligations, as we are required to do so by law to ensure personal data is protected.

The personal information we have collected from you will be shared with Cifas (a not-for-profit fraud prevention membership organisation) who will use it to prevent fraud, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct. If any of these are detected you could be refused certain services or employment. Your personal information will also be used to verify your identity. Further details of how your information will be used by us and Cifas can be provided on request. Please email GroupHRDP@landg.com if you want to receive a copy of this policy.

DATA SECURITY

We have put in place measures to protect your information, including appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Details of these measures are available on request. In addition, we limit access to your personal information to those individuals, agents, contractors and other third parties who have a business need to know.

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?

If you are not appointed, we will retain your personal information for a period of 12 months after we have communicated to you our decision about whether to appoint you to the 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.

In addition, we will retain your personal information for 12 months to consider you for further opportunities where you have consented to be part of the talent pool. . After this period, we will securely destroy your personal information in accordance with our data retention policy.

Any CCTV footage that you may appear in at our offices is retained for 30 days and any visitor information relating to visiting the office location is held for 4 years. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have dealt with any injuries and logged them accordingly in our accident book in line with the health and safety regulation. After this period your data will be overwritten or securely destroyed in accordance with our data retention policy.

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 are appointed to the role, we will retain your personal information in accordance with our Employee Privacy notice which can be found on our internal intranet.

YOUR RIGHTS IN RELATION TO PERSONAL DATA

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 (Rectification)** 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 (known as portability).
- **Challenge automated decision making** or request human intervention, if we are carrying out solely automated decision-making that has legal or similarly significant effects on you.
- **Right to withdraw consent.** We will not normally rely on consent to process your data. 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.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, request that we transfer a copy of your personal information to another party, or withdraw your consent for processing your data please contact the HR Governance team GroupHRDP@landg.com in writing.

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 Legal & General's DPO, Liz Bradley, Data.Protection@landg.com, 1 Coleman Street, London, EC2R 5AA. 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.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time.



Category of Personal data	Examples of PII used	Purpose of processing			Legal bases for processing				Conditions for processing Special Category Data						
					Legitimate Interests	Performance of a contract	Legal Obligation	Consent	Explicit Consent	Substantial Public Interest	Legal Obligations under employment and social security law	Defence of legal claims	Occupational Health		
Basic Personal Contact Information	Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses.	To contact you regarding the recruitment and selection process		For defence against potential legal claims											
Identity Information	Your date of birth, gender, marital status and NI number	To manage our employment or working relationship with you		For defence against potential legal claims											
	A copy of your passport or similar photographic identification and / or right to work documentation	To assess the immigration status of an employee and right to work in the UK		For defence against potential legal claims											
Diversity, Inclusion and Equal opportunities	Gender identity; age; ethnic origin; socio-economic data; religious belief; disability or long-term health condition; sexual orientation	To comply with the requirement to make reasonable adjustments		To monitor our compliance with equal opportunities legislation											
Recruitment and selection data	CVs, application forms, covering letter, interview records; employment history; . Evidence of qualifications and references.	To assess applicants' suitability for work and to determine to whom to offer employment													
	Criminal records data (including results of record checks); outcome of credit referencing checks;	To assess an applicants' suitability for work and to determine to whom to offer employment		Compliance with FCA/PRA regulatory requirements											

Category of Personal data	Examples of PII used	Purpose of processing		Legal bases for processing				Conditions for processing Special Category Data						
				Legitimate interests	Performance of a contract	Legal Obligation	Consent	Explicit Consent	Substantial Public Interest	Legal Obligations under employment and social security law	Defence of legal claims	Occupational Health		
	Details of any disabilities disclosed and reasonable adjustments; equal opportunities monitoring data	To comply with the duty to make reasonable adjustments	To monitor our compliance with equal opportunities legislation			x		x			x	x		
	Offer letters and contracts of employment, including written statement of terms and conditions	To maintain a record of employees' contractual and statutory rights	To manage our employment or working relationship with you	For defence against potential legal claims			x	x						
Security and Facilities Management Information	Your photograph and images on CCTV; your name; office attendance;	Issue security passes to provide access to office locations for your interview	To operate security arrangements			x		x						
	Information about your use of our information and communications systems	To protect L&G IT systems and infrastructure.	To operate security arrangements			x								
Regulatory Information	For regulated roles: Personal identity information; outcome of background screening checks;	Compliance with FCA/PRA regulatory requirements	To manage our employment or working relationship with you			x		x						
	Name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality Criminal records data (including results of record checks); outcome of credit referencing checks;	Fraud prevention	Financial crime risk management			x		x	x					