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 global 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.

For jurisdictions outside of the UK that have different processes, we have detailed this below.

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, address history, references, credit checks, directorship 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, if you are offered a role. These include right to work in the UK, fraud prevention and financial crime risk management and DBS and directorship checks.
- 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.

- Where you have consented to be part of our communities, we will communicate with you regarding job opportunities and L&G news.
- 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 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. Note for the USA background checks are conducted on our behalf by HIRE RIGHT

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. Where applicable, 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.
- Where it is needed in the public interest for preventing unlawful acts, dishonesty, malpractice, or other seriously improper conduct.
- 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.

Your information is stored in our HR system and can only be accessed by dedicated 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.

NOTE: **For Bermuda,** as part of their pre- employment screening process, we collect passport and health information, an attestation on health status is required as part of the local laws. This information will be collected on your spouse/family members as well if they plan on relocating with the applicant. The health result will be shared with the local hospital as mandated by local laws.

NOTE: For the USA, local state laws will apply, California will be subject to CCPA / CPRA

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.

For Bermuda, if an applicant is successful, we will get a police report, and this will be shared with HR, and it will vary depending on where you are coming from.

AI, AUTOMATED DECISION-MAKING & PROFILING

As part of our recruitment and candidate evaluation processes, Legal & General leverages various "Smart Recruiters" technologies, including Artificial Intelligence (AI) functionality, to help us ensure applications are reviewed consistently, fairly, and effectively, against the requirements of each role. In specific circumstances, AI may be used to **assist** with tasks such as identifying role-specific skills and experience or evaluating applications against pre-defined criteria. Non-Generative AI technologies are used in specific circumstances to automatically screen applications for non-negotiable requirements.

Where used, AI is used only as a supportive mechanism to enhance fairness and efficiency. It does **not** make final hiring decisions. AI-assisted outcomes that affect your progression in the recruitment process are reviewed and confirmed by a trained human recruiter. We maintain strict oversight of all AI-enabled tools to ensure they are used in a transparent, fair, and accountable manner. These tools are continuously monitored and evaluated to ensure they operate as intended and remain aligned with our standards for fairness, accuracy, and responsible use.

Legal & General may use certain elements of candidate data, and the outputs of algorithmic processing of candidate data, to help us improve the performance, accuracy, and fairness of our recruitment processes and the AI tools that support them. This may include reviewing outcomes to ensure the service is functioning as expected in a fair and effective way. Participation in this improvement activity is optional, and you may choose to opt out at any time without affecting your application or future opportunities with Legal & General. Opt out by contacting therecruitmentteam@landg.com

For certain roles, minimum requirements may apply, for example: mandatory qualifications such as a degree, or eligibility criteria such as the ability to work in the UK without sponsorship. Where these requirements are essential for the role, applications that do not meet these may be automatically declined. The criteria are set by Legal & General and is applied consistently to all applicants.

We regularly assess the tools we use to ensure they comply with applicable data protection laws and support fair recruitment outcomes. Your personal data is handled securely throughout the process, and you retain all rights provided under relevant privacy legislation.

Some roles that you may apply for may also require you to undertake a psychometric assessment. For future talent roles you will be asked a series of questions with pre-weighted answers that align to behaviours which are linked to success within L&G. These will be marked via automated means to provide a score which will be reviewed by an assessor. Please note that there is a possibility that your application could be rejected if you do not meet the minimum requirements for the role.

If you disagree with the outcome of the automated decision, you are able to contest the decision and have the information reviewed by a human by following the individual rights process detailed below. For executive roles, you may be required to undertake an assessment which will detail your personality traits including your strengths and weaknesses. This information is reviewed by a trained assessor who will then conduct a further interview with you before any decisions are made on your application.

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.

We will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by anyone employed or engaged or potentially employed or engaged by them. If any of these are detected, you could be refused certain services or employment. Details of the personal information that will be processed by Cifas include name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number, and nationality. Where relevant, other data including employment details will also be processed.

Your personal information will also be used to verify your identity. Cifas will hold your personal data for up to six years if you are considered to pose a fraud or relevant Conduct risk

If you are resident outside of the UK, we may transfer your personal information into the UK. If we do, the data protection laws may dictate a different level of protection to your data and impose additional safeguards to transfer the data. As the Data Controller we have taken 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.

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 24 months to consider you for further opportunities where you have consented to be part of our community 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.

For Bermuda, police reports will be kept for one year and deleted after.

YOUR RIGHTS IN RELATION TO PERSONAL DATA

Under certain circumstances and laws, you may have the following rights. For information as to what rights apply in your local country, please see the table below.

- **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 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 GroupHRDP@landg.com in writing.

	UK, EEA & Switzerland	Hong Kong	Singapore	Japan	Australia	Bermuda
Access	X	X	X	X	X	X
Correction	X	X	X	X	X	X
Erasure	X			X		X
Object to processing	X					x
Restriction of processing	X					X
Transfer (Portability of data)	X					x
Automated Decision Making	X					
Right to withdraw consent.	X	X	X	X	X	X

Notice to California Residents

Pursuant to the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 ("CCPA"), we are required to provide California employees with a privacy policy that contains a comprehensive description of our online and offline practices regarding our collection, use, sale sharing, and retention of their personal information as well as a description of the rights they have regarding their personal information. This Privacy Policy sub-section provides the information the CCPA requires as well as other useful information regarding our collection and use of personal information.

The CCPA defines "personal information" to mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular California resident or household. Personal information does not include publicly available, deidentified, or aggregated information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this Privacy Policy, we will refer to this information as "Personal Information."

The categories of Personal Information we currently collect and, in the 12 months prior to the Effective Date of this Privacy Policy, have collected from past, current, and potential employees have been listed above.

In addition, this may also include, Characteristics of protected classifications under California or federal law (race; colour; sex/gender (including pregnancy, childbirth, breastfeeding and/or related medical conditions); sexual orientation or sex life; gender identity/expression; age (40 and older); religion (including religious dress and grooming practices); national or ethnic origin; ancestry; union membership; disability (mental and physical, including HIV/AIDS, cancer, and genetic characteristics); citizenship or immigration status; genetic information;

marital status; medical condition (genetic characteristics, cancer or a record or history of cancer); military or veteran status; political affiliations or activities; status as a victim of domestic violence, assault, or stalking; requests for family care leave, for leave for an employee's own serious health condition, or for pregnancy disability leave; and retaliation for reporting patient abuse in tax-supported institutions).
We may also use information for the purpose of Identify you as a veteran.
Please note that the Personal Information we collect depends on your position, relationship to us, what information you choose to provide, and what information we are required to collect. Not all Personal Information listed below is collected from all past, current, and potential employees.
If you are a California employee, you have the following rights with respect to your Personal Information:

1. right to know what Personal Information we have collected about you, including the categories of Personal Information, the categories of sources from which we collected Personal Information, the business or commercial purpose for collecting, selling, or sharing Personal Information (if applicable), the categories of third parties to whom we disclose Personal Information (if applicable), and the specific pieces of Personal Information we collected about you;
2. The right to delete Personal Information that we collected from you, subject to certain exceptions.
3. The right to correct inaccurate Personal Information that we maintain about you.
4. If we sell or share Personal Information, the right to opt-out of the sale or sharing.
5. If we use or disclose sensitive Personal Information for purposes other than those allowed by the CCPA and its regulations, the right to limit our use or disclosure; and
6. The right not to receive discriminatory treatment by us for the exercise of privacy rights conferred by the CCPA.

You may submit a request to grouphrdp@landg.com
We will acknowledge your requested within 10 days and process the request within 45 days unless the shorter period of 15 business days applies. In some cases, and where permissible, we may need to extend to 90 days in total and we will notify within the first 45 days if this is thew case.
We are committed to ensuring this Privacy Policy is accessible to individuals with disabilities. If you wish to access this Privacy Policy in an alternative format, please contact us as described below.
We have not sold or shared Personal Information in the twelve (12) months preceding the Effective Date of this Privacy Policy. We do not knowingly collect, sell, or share the Personal Information of individuals under 16 years of age. We do not collect or process Personal Information for the purpose of inferring characteristics.

Do we use your personal information for marketing?

We do not use your personal information obtained for employment purposes to carry out direct marketing in general, but we may use the information we hold to communicate with you about your employment and to keep you informed about matters concerning L&G and/or the business you work for. This may therefore include special offers, product discounts and other benefits as a result of you being an employee that we wish to make available to you.

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 and all other local supervisory authorities for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

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

Version ID	Version date	Change summary
MyHRv1.0	30 October 2023	This policy was reviewed to update to bring up to date with processing activities that have changed and improve level of detail and transparency.
MyHRv2.0	04 June 2024	Updated to include: • to improve transparency around the checks carried out to for fraud prevention and Financial Crime risk management. • Updated email address for applicants to contact us
MyHRv2.0	15 December 2025	Updated to include: • to include notes for US • Updated Automation of recruitment including 'knock out questions'

Appendix 1 – Legal purposes and bases table - If you would like more information about our purposes or lawful bases please contact GroupHRDP@landg.com

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	x								
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		x		x						
	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	To verify your identity using biometric means	x		x		x				
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	To understand the equality impact of our employment practices	x		x			x	x		
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			x								
	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		x		x				x		

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			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	x			

For Bermuda, all processing activities in relation to applicants will be reliant upon Employment activities and legal obligation as the lawful basis according to their local laws.