Liaison Group (Website) Privacy Notice

1. Introduction

This Privacy Notice explains how Liaison Financial Services Limited (trading as Liaison Group) collects, uses, stores and protects personal data when individuals interact with our website (liaison-care.co.uk). It applies to website visitors, enquirers, job applicants, prospective customers, and individuals accessing our charity pages. It also applies to personal data collected when you contact us by telephone. It does not apply to users of our SaaS platforms or Liaison National Bank services, which have separate privacy notices.

2. Who We Are

Liaison Financial Services Limited (company no. 06426660) is the data controller for personal data collected through our website. Our registered office is Estate House, Evesham Street, Redditch, Worcestershire, B97 4HP.

3. How to Contact Us

Data Protection Officer
Liaison Group
Market House
61 High Street
Tring
HP23 4AB
Email: infogov@liaisongroup.com
Phone: 0845 603 9000

4. Personal Data We Collect

We collect:

- Identity and contact data
- Enquiry and correspondence data
- Marketing preference data
- Technical and analytics data (including cookies)

- Server logs and security data

- Recruitment and job application data (such as CVs, qualifications, right-to-work information, referee details, and information provided during the recruitment process)

- Equality and diversity monitoring data (collected for reporting only; not used in decision-making; where full anonymisation is not technically possible, access is restricted and data is used only in aggregated form)

This includes information you provide via website forms, email, telephone or other communication channels. For recruitment purposes, this may include information about third parties such as referees. We may also receive data indirectly via recruitment agencies or third-party recruitment platforms.

5. How We Use Your Personal Data

We use personal data to:

- Respond to enquiries and provide requested information

- Manage marketing preferences and communications

- Improve and secure our website

- Process job applications and conduct recruitment activities

- Monitor equality and diversity (not used in recruitment decision-making)

- Maintain records and comply with legal obligations

We do not make automated decisions that have legal or similarly significant effects.

6. Legal Bases for Processing

Our lawful bases include:

- Legitimate interests (e.g., responding to enquiries, improving services, assessing candidate suitability)

- Consent (e.g., non-essential cookies, marketing where required)

- Legal obligation (e.g., right-to-work checks, safeguarding)

- Steps necessary before entering an employment contract

7. Legitimate Interests

We rely on legitimate interests as a lawful basis where the processing is necessary to pursue our organisational interests in a way that is proportionate and does not override your rights or freedoms. These interests include:

• Responding to enquiries and providing requested information.

• Maintaining and improving our website, IT systems and services.

• Managing recruitment, including assessing candidate suitability, contacting referees, conducting proportionate background checks, and retaining talent pool information where requested.

• Operating our business efficiently, including managing customer and partner relationships and promoting our services.

Where we rely on legitimate interests, we have carried out a balancing test to ensure that our interests do not override your rights and freedoms. You have the right to object to processing based on legitimate interests at any time.

8. Recruitment Data

We process personal data submitted during job applications via our website, email, third-party recruitment platforms or recruitment agencies. This may include CVs, qualifications, right-to-work information, referee details, DBS information, occupational health data and equality and diversity monitoring data. This information is used solely for recruitment and pre-employment checks and is not used for automated decision-making.

8.1 Criminal Offence Data and DBS Checks

8.1.1 DBS checks legally required for a role

Where a DBS check is legally required, we rely on:

- Article 6(1)(c) UK GDPR (legal obligation), and
- Article 10 UK GDPR together with Schedule 1, Part 1, Paragraph 1 of the Data Protection Act 2018 (“employment, social security and social protection law”).

This authorises the processing of criminal offence data necessary to meet statutory or regulatory requirements.

8.1.2 DBS checks not legally required (legitimate interests)

Where a DBS check is not legally required, we rely on Article 6(1)(f) UK GDPR (legitimate interests) to ensure the suitability, integrity and safety of our workforce, our services and the individuals we work with.

For any associated criminal offence data, we rely on Article 10 UK GDPR together with the relevant conditions in the Data Protection Act 2018:

- Schedule 1, Part 1, Paragraph 1 (employment-related purposes), and/or
- Schedule 1, Part 2, Paragraph 10 (preventing or detecting unlawful acts).

These provide lawful domestic authorisation for processing criminal offence data for roles where screening is necessary and proportionate.

We have carried out a legitimate interest balancing test, ensure that the processing is necessary and proportionate, and maintain an Appropriate Policy Document (APD) covering this processing.

8.1.3 Right to object (Article 21 UK GDPR)

Individuals have the right to object to processing conducted on the basis of legitimate interests. Each objection is considered carefully, balancing the individual's rights and interests against the risks, responsibilities and safeguarding requirements of the role.

Where we determine that a role cannot be safely or appropriately performed without screening, we may need to continue processing the data or may be unable to progress the application further.

8.2 Special Category Data

We may process special category data as part of recruitment, including occupational health information and equality and diversity monitoring data. This processing is undertaken only where necessary, proportionate, and supported by the relevant conditions under UK GDPR and the Data Protection Act 2018.

8.2.1 Occupational health data

We process occupational health information where necessary to assess a candidate's or employee's working capacity, to meet our legal obligations regarding health and safety, and to consider reasonable adjustments under the Equality Act 2010.

This processing is carried out under:

- Article 6(1)(c) UK GDPR – processing is necessary to comply with legal obligations relating to employment, health and safety, and reasonable adjustments;
- Article 9(2)(h) UK GDPR – processing is necessary for the assessment of the working capacity of an employee or prospective employee;
- Schedule 1, Part 1, Paragraph 1 DPA 2018 – processing is necessary for employment, social security and social protection law purposes.

Processing is limited to what is necessary for determining fitness for work or meeting our statutory duties as an employer.

8.2.2 Equality and diversity monitoring data

We may process equality and diversity monitoring information for the purposes of monitoring equality of opportunity and treatment, informing our ED&I reporting, and supporting fair and inclusive recruitment practices. This information is kept separate from recruitment decision-making and is anonymised or accessed only in aggregated form wherever possible.

This processing is carried out under:

- Article 6(1)(f) UK GDPR – our legitimate interests in promoting equality, monitoring representation, and ensuring fairness in recruitment and workforce development;
- Article 9(2)(g) UK GDPR – processing is necessary for reasons of substantial public interest;
- Schedule 1, Part 2, Paragraph 8 DPA 2018 – promoting equality of opportunity or treatment.

Providing this information is voluntary, and choosing not to do so does not affect the recruitment process.

8.3 Financial probity checks

For certain roles involving financial responsibilities, fraud-prevention duties, procurement functions or access to sensitive financial systems, we may conduct financial integrity checks such as searches for County Court Judgments (CCJs) or bankruptcy information. These checks are carried out under Article 6(1)(f) UK GDPR (legitimate interests), as they are necessary to ensure the trustworthiness, integrity and suitability of individuals in positions with financial risk exposure. Such checks are limited to roles where they are relevant and proportionate, and they are not used for automated decision-making.

9. Data Sharing

We share data with:

- CRM and marketing providers
- ATS and recruitment processors
- Cloud and IT hosting providers

- Screening and occupational health partners

We use only processors in ICO-approved adequate jurisdictions. Sub-processors must meet equivalent safeguards.

Our processors are not permitted to use your data for their own purposes.

10. International Transfers

We do not intentionally appoint processors based in non-adequate jurisdictions. Where sub-processors operate internationally, we ensure appropriate safeguards (IDTA/SCCs) apply.

11. Cookies and Tracking

Our website uses a cookie banner allowing users to accept, reject or manage non-essential cookies in categories such as analytics and advertising. Full details are available in our Cookie Policy.

Analytics tools are configured to use anonymised or pseudonymised data wherever possible.

12. External Links

Our website may contain links to third-party websites, platforms or resources, including social media pages, video-hosting platforms, charity or partner sites, and external articles or reports (such as NHS or government publications). These third-party websites operate their own privacy notices and cookie practices, and we are not responsible for their content, security or data processing activities.

If you choose to follow a link to a third-party website, that provider may collect information about you, including through cookies or tracking technologies. We recommend reviewing the privacy policy and cookie information of any third-party site before interacting with their services.

13. Retention

We retain:
• Enquiry data: up to 24 months
• Marketing records: until opt-out
• Server logs: 30–90 days
• Recruitment Application Tracking System data: 6 months post campaign
• Unsuccessful Candidate CVs up to 12 months (legitimate interests)
• Successful applicants: retained under employee privacy notice and is provided to all new employees.

14. Your Rights

You have the right to access, correct, erase, restrict or object to processing, withdraw consent for non-essential cookies, and lodge a complaint with the ICO.

15. Updates to This Notice

This notice may be updated periodically. Significant changes will be posted on this page.