Data Privacy and Protection Policy

Document Control

Policy Owners: Director
Approval Date: 11/06/2025
Effective Date: 11/06/2025
Review Date: June 2027

Note: This policy must be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness.

Date	Version	Author	Reason for amendment
11/06/2025	1.0	Claire Robinson	Create formalised Policy
18/05/2026	1.1	Claire Robinson	Annual Review
03/10/2026	1.2	Claire Robinson	Updated to reflect Lief's processor role, ISO 27001 certification, UK hosting, AI safeguards and current transfer mechanisms

1. Purpose

This policy outlines the organisation's commitment to protecting personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It sets out the principles for handling personal data to ensure the privacy and rights of individuals are respected, while safeguarding the organisation from data breaches and other privacy risks.

2. Scope

This policy applies to all employees, contractors and third-party providers who collect, process or manage personal data on behalf of the organisation. It covers all personal data, regardless of the format (electronic, paper or other), related to individuals including employees, clients, customers and suppliers.

It covers personal data for which Lief is the data controller and personal data that Lief processes on behalf of its customers as a data processor. When care providers use the Lief platform, the care provider is the data controller and Lief acts as its processor under the Data Processing Agreement in Lief's Terms of Service.

3. Definitions

- Personal Data: Any information that relates to an identified or identifiable individual (data subject), such as name, contact details, ID numbers, online identifiers or physical characteristics.
- Special Category Data: Personal data that is more sensitive, such as information on racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation or biometric data.
- Data Controller: The organisation that determines the purposes and means of processing personal data.
- Data Processor: A third party that processes personal data on behalf of the Data Controller.
- Processing: Any operation or set of operations performed on personal data, such as collection, recording, organisation, storage, retrieval or deletion.
- Data Subject: An individual whose personal data is being processed.
- Sub-processor: A third party engaged by Lief to process personal data on behalf of Lief's customers.
- Pseudonymisation: Processing personal data so that it can no longer be linked to an individual without additional information that is kept separately and securely.

4. Data Protection Principles

In accordance with the UK GDPR, the organisation adheres to the following principles when processing personal data:

4.1. Lawfulness, Fairness and Transparency

- Personal data must be processed lawfully, fairly and in a transparent manner.
- The organisation must inform data subjects about the purpose and legal basis for collecting their data through clear privacy notices.

4.2. Purpose Limitation

- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.

4.3. Data Minimisation

- Personal data must be adequate, relevant and limited to what is necessary for the intended purpose.

4.4. Accuracy

- Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or erased without delay.

4.5. Storage Limitation

- Personal data shall not be kept for longer than necessary. The organisation must implement data retention schedules to ensure data is disposed of securely once no longer required.

4.6. Integrity and Confidentiality

- Personal data must be processed in a way that ensures appropriate security, including protection against unauthorised access, loss, destruction or damage through technical and organisational measures.

4.7. Accountability

- The organisation is responsible for, and must be able to demonstrate, compliance with all data protection principles.

5. Legal Basis for Processing Personal Data

Lief will only process personal data where it has a lawful basis to do so. The lawful bases include:

- Consent: The data subject has given clear consent for their personal data to be processed for a specific purpose.
- Contract: The processing is necessary for the performance of a contract with the data subject or to take steps at the request of the data subject before entering into a contract.
- Legal Obligation: The processing is necessary for compliance with a legal obligation to which the organisation is subject.
- Legitimate Interests: The processing is necessary for the legitimate interests of the organisation or a third party, provided these interests are not overridden by the data subject's rights and interests.
- Vital Interests: The processing is necessary to protect someone's life.
- Public Task: The processing is necessary to perform a task carried out in the public interest or in the exercise of official authority.

Where Lief processes special category data or criminal offence data as a controller, it will also identify a condition under Article 9 or Article 10 of the UK GDPR and, where required, Schedule 1 of the Data Protection Act 2018.

Where Lief acts as a processor, the customer is responsible for determining the lawful basis for processing, and Lief processes the personal data only on the customer's documented instructions.

6. Data Subject Rights

Individuals (data subjects) have the following rights under the UK GDPR, and the organisation must ensure these rights are respected:

6.1. Right to be Informed

Data subjects have the right to be informed about how their personal data is being processed. The organisation must provide transparent and clear privacy notices.

6.2. Right of Access

Data subjects can request access to their personal data and obtain a copy, along with an explanation of how it is being used. Requests must be responded to within one month.

6.3. Right to Rectification

Data subjects have the right to request corrections to their personal data if it is inaccurate or incomplete.

6.4. Right to Erasure ("Right to be Forgotten")

Data subjects can request the deletion of their personal data in certain circumstances, such as when the data is no longer necessary for the purpose it was collected.

6.5. Right to Restrict Processing

Data subjects can request the restriction of processing of their personal data if they contest its accuracy, or if the processing is unlawful and they oppose erasure.

6.6. Right to Data Portability

Data subjects have the right to obtain and reuse their personal data across different services in a structured, commonly used and machine-readable format.

6.7. Right to Object

Data subjects can object to the processing of their personal data in certain circumstances, such as for direct marketing or when processing is based on legitimate interests.

6.8. Rights Related to Automated Decision-Making

Data subjects have rights concerning decisions made solely by automated means, including profiling, that have legal or significant effects on them.

6.9. Requests About Customer Data

Requests relating to personal data that Lief processes on behalf of a customer are forwarded to that customer without delay. Lief assists the customer in responding, in line with the Data Processing Agreement.

7. Data Security

7.1. Technical and Organisational Measures

Lief will implement appropriate technical and organisational measures to protect personal data from unauthorised access, loss or damage, including:

- Encryption: AES-256 encryption at rest and TLS 1.2 or higher in transit for all personal data.

- Access Control: Role-based access restricted to authorised personnel, protected by multi-factor authentication and audit logging.
- Data Backups: Encrypted daily backups stored in the UK and kept for 35 days.
- Training: Providing data protection training to employees to ensure awareness of their responsibilities.
- Hosting: All customer data is hosted on Amazon Web Services in the UK (London).
- Certification: Lief is certified to ISO/IEC 27001:2022 and Cyber Essentials Plus and achieved Standards Exceeded in the NHS Data Security and Protection Toolkit 2025-26.

7.2. Data Breaches

In the event of a data breach, the organisation will act promptly to:

- Contain the breach and minimise damage.
- Report the breach to the Information Commissioner's Office (ICO) within 72 hours if the breach poses a risk to the rights and freedoms of individuals.
- Where Lief acts as a processor, notify the affected customer without undue delay and within 24 hours of discovery.
- Notify affected data subjects if the breach is likely to result in a high risk to their privacy rights.
- Conduct a post-breach review to prevent recurrence.
- Follow Lief's Incident Response Plan and Data Breach Procedures.

8. Data Transfers

8.1. Transfers Outside the UK

Personal data will not be transferred outside the UK unless adequate protection is provided for the data, such as:

- The recipient country is covered by UK adequacy regulations (for example, countries in the EU).
- The recipient is certified under the UK-US Data Bridge.
- The organisation has put in place the ICO's International Data Transfer Agreement or Standard Contractual Clauses with the ICO's UK Addendum, supported by a transfer risk assessment where required.
- The transfer is covered by a specific exception under the UK GDPR.

Lief's technical support team in India may view customer data within the UK-hosted platform when this is needed to resolve a specific support issue. No data is stored in India, and this access is covered by a UK International Data Transfer Agreement and a

transfer risk assessment. The transfer safeguard for each sub-processor is recorded in Lief's Sub-Processor Register.

8.2. Third-Party Processors

Where personal data is shared with third-party processors or sub-processors, the organisation will put in place Data Processing Agreements that meet Article 28 of the UK GDPR, carry out security due diligence before engagement and annually thereafter and record each one in the Sub-Processor Register.

8.3. Artificial Intelligence

Lief's AI features use Microsoft Azure OpenAI with UK data residency. Report content is pseudonymised before it is sent for summarisation. AI output is always reviewed by a member of staff, and no decisions about individuals are made solely by automated means.

Lief uses pseudonymised feedback from how staff edit AI drafts to improve its product. For this purpose Lief acts as a controller and relies on its legitimate interests, as recorded in its legitimate interests assessment.

9. Training and Awareness

All employees must receive data protection training upon joining the organisation and annual refresher training thereafter. Employees involved in the handling of personal data are responsible for ensuring that they are familiar with and adhere to this policy.

10. Monitoring and Compliance

Lief will monitor compliance with this policy through regular audits and reviews of data processing activities. Any non-compliance will be reported to senior management, and corrective actions will be taken as necessary.

Lief's Data Protection Officer, Prior Analytics Ltd, oversees compliance with this policy, maintains Lief's records of processing activities and data protection impact assessments and reports to the leadership team monthly. Lief carries out a data protection impact assessment before any new processing that is likely to result in a high risk to individuals.

11. Policy Review

This policy will be reviewed annually or when there are significant changes in data protection laws or Lief's data processing practices. Amendments will be communicated to all staff and relevant stakeholders.

12. Contact

Questions about this policy should be sent to Lief's Data Protection Officer at privacy@lief.care. Yerado Ltd is registered with the Information Commissioner's Office under registration number ZB482173.