GDPR & Data Protection Compliance

Yerado Ltd (trading as Lief Care) | 3 October 2026

1. Overview

Lief Care is a cloud-based care records platform for children's homes, supported accommodation and other care services. Yerado Ltd operates in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and maintains documented data protection, information security and incident management procedures certified to ISO/IEC 27001:2022.

When care providers use Lief, the care provider is the data controller for the records held in the platform and Lief acts as its data processor, under the Data Processing Agreement in clause 7 of our Terms of Service.

2. Certifications and registrations

ISO/IEC 27001:2022	Certified (UKAS-accredited).
Cyber Essentials Plus	Certified. Certificate number 2a036188-b4d0-4916-85b0-74cafba24aee. Certified 1 May 2026; recertification due 1 May 2027.
NHS Data Security and Protection Toolkit	2025-26: Standards Exceeded (organisation code Y7I1D), published 3 June 2026.
ICO registration	ZB482173.
Data Protection Officer	Prior Analytics Ltd, privacy@lief.care.
Senior Information Risk Owner	Shivam Agarwal, CTO.

Copies of certificates are available on request or through our Trust Center.

3. Supporting documentation

Terms of Service (v2.0)	Includes our Data Processing Agreement (clause 7), which meets Article 28 UK GDPR.
Sub-Processor Register	October 2026. Lists every sub-processor with its purpose, location and transfer safeguard.
Data Protection Impact Assessment	Lief's DPIA, updated 3 October 2026. Available on request.
DPIA template for care providers	Pre-filled with information about Lief to help customers complete their own DPIA.
Policies	Data Privacy and Protection Policy (v1.1); Information Security Policy including Acceptable Use Policy (v1.0); Data Management Policy (v1.0); Incident Response Plan (v1.0); Operations Security Policy (v1.0). Available on request.

Privacy Notice	Published on our website.

4. Hosting and data location

All customer data, including care records, is hosted on Amazon Web Services in the UK (London, eu-west-2), across multiple availability zones. Backups are also stored in the UK, and production never fails over to servers outside the UK. Development and testing environments are UK-based and do not use live customer data.

All AI processing uses Microsoft Azure OpenAI with UK data residency (UK South, London, with UK West, Cardiff, for resilience).

A small number of providers process limited data outside the UK, in the EU and US. This is limited to staff users' and customer organisations' contact, account and business details, and never includes care records or other resident data. Each transfer is covered by a Data Processing Agreement and a named transfer safeguard (see section 10).

Offshore technical support: our technical support team in India may need to view customer data within the UK-hosted platform to resolve a specific support issue or incident. No data is stored in India. Access is role-based, just-in-time (no standing production access), limited to the minimum necessary and fully audit-logged, and bulk export is not permitted. This is covered by a UK International Data Transfer Agreement (IDTA) and a Transfer Risk Assessment and DPIA completed in June 2026 and updated in October 2026, which assessed the residual risk as Low.

5. Security controls

Encryption	AES-256 at rest across all databases, file storage and backups. TLS 1.2 or higher for all data in transit, with HSTS enforced.
Access control	Role-based access control with home-level scoping; confidential records can be restricted to named users. Multi-factor authentication via Auth0, enforceable for the whole organisation. Account lock-out, configurable session timeouts and IP/device restrictions.
Audit logging	Tamper-evident logging of logins, user activity, administrative changes and data modifications. Infrastructure logging via AWS CloudTrail and CloudWatch.
Network security	Cloudflare web application firewall with OWASP rule sets and DDoS protection. AWS VPC segmentation with Security Groups and NACLs.
Endpoint protection	All staff devices enrolled in mobile device management, with disk encryption, Microsoft Defender (Windows) or Apple XProtect (macOS) and web filtering. Critical patches applied within 24 hours and high-risk patches within 14 days.
Vulnerability management	Continuous scanning via Vanta and AWS Inspector, weekly external scans and an annual independent penetration test.
Backups and resilience	Encrypted daily backups kept for 35 days in the UK. Documented business continuity and disaster recovery plan, tested at least annually.
People	Background checks, confidentiality obligations and mandatory annual data protection and security training for all staff.

Secure development	OWASP-aligned development lifecycle, peer-reviewed code and controlled CI/CD pipelines with dependency vulnerability scanning. Separate production, staging and development environments.

6. AI features

Lief includes AI-assisted report generation, summaries and speech-to-text, powered by Microsoft Azure OpenAI with UK data residency.

- Report content is pseudonymised before it is sent for summarisation: names, contact details, addresses and reference numbers are replaced with random placeholders, and the real details are only restored inside Lief.
- Microsoft does not use the data to train its models. Under Microsoft's standard terms, prompts and outputs may be retained for up to 30 days solely for abuse monitoring and are then deleted.
- AI output is always a draft that a trained member of staff reviews and edits before it is saved. The AI does not make decisions about individuals.
- AI features are subject to the same access controls and audit logging as the rest of the platform.
- Lief uses pseudonymised feedback from how staff edit AI drafts to improve its product, as set out in clause 7.6 of our Terms of Service.

7. Data subject rights and DPIAs

Lief assists customers in responding to requests from individuals to exercise their data protection rights, and provides reasonable assistance with customers' DPIAs, including our own DPIA and a pre-filled DPIA template for care providers.

8. Data retention and deletion

Lief retains customer data for the duration of the customer's contract. Customers, as controllers, decide how long records are kept within the platform in line with their own retention obligations.

On termination, customer data is returned and/or deleted at the customer's choice. Deletion is carried out by cryptographic erasure, and backup copies expire within 35 days. Written confirmation of deletion is available on request.

9. Incident management and breach reporting

Lief maintains a documented Incident Response Plan, reviewed and tested at least annually. Any personal data breach affecting customer data is notified to the customer within 24 hours of discovery, so that the customer can meet its own 72-hour obligation to the ICO where required.

Data Protection Officer	Claire Robinson, Prior Analytics Ltd – privacy@lief.care
Chief Technology Officer and SIRO	Shivam Agarwal – shivam.agarwal@lief.care
Chief Executive Officer	Pavan Mallikarjun – pavan.mallikarjun@lief.care

10. Sub-processors

All sub-processors are bound by Data Processing Agreements and are subject to security due diligence before engagement and annually thereafter. Our full Sub-Processor Register (October 2026) is available on request or through our Trust Center.

Platform sub-processors

Provider	Purpose	Location	Transfer safeguard
Amazon Web Services	Hosting and storage of all customer data	UK	Not applicable (UK)
Auth0 (Okta)	User authentication	EU	SCCs with UK Addendum
Cloudflare	DNS, firewall and traffic routing	US (UK/EU routing)	UK-US Data Bridge
Google Workspace	Internal email and documents	US	UK-US Data Bridge
Mailgun (Sinch)	Invitation and notification emails	EU	SCCs with UK Addendum
Microsoft Azure OpenAI	AI speech-to-text, report and summary generation	UK (UK data residency)	Not applicable (UK)
Mixpanel	Product usage analytics	US	SCCs with UK Addendum
Slack	Internal staff communications	US	UK-US Data Bridge
Trainn	Product training	US	SCCs with UK Addendum
Zapier	Internal workflow automation	US	SCCs with UK Addendum
Zoho	CRM and helpdesk	US	UK IDTA or Addendum
Offshore technical support team	Product support and incident resolution (access only)	India	UK IDTA with Transfer Risk Assessment

Other suppliers used to run our business

Provider	Purpose	Location	Transfer safeguard
AK Patel & Co. (Chartac Practice Ltd)	Accounting and payroll	UK	Not applicable (UK)
Atlassian	Engineering project management	US / EU	SCCs with UK Addendum
Hostinger	Marketing website hosting	US	Standard Contractual Clauses
Prior Analytics Ltd	Data protection consultancy and DPO	UK	Not applicable (UK)
Stripe	Payment processing and billing	US	SCCs with UK Addendum
Vanta	Compliance and security monitoring	US	SCCs with UK Addendum

Questions about this statement: privacy@lief.care.