Data Protection Impact Assessment

This document records Yerado Ltd's Data Protection Impact Assessment (DPIA) for the Lief Care service. It follows the process set out by the Information Commissioner's Office (ICO) DPIA guidance and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs. Yerado Ltd is referred to as Yerado throughout this DPIA and the service is referred to as Lief.

This DPIA is kept under review and was last updated on 3rd October 2026.
The amendments included the addition of the Sub Processor list, more detail about the types of data stored in Lief Care, clarification of Lief's role as a Data Processor, further details about information security arrangements (including the addition of Lief's ISO 27001 certification) and the correction of minor anomalies in the sub-processor information.

Step 1 – Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Lief, developed by Yerado Ltd, is an outsourced service to help Care / Support Providers (typically Children's Homes & Supported Accommodation) to reduce the administrative burden involved in processing and recording care. It helps care providers to efficiently manage homes, improve care provided and excel at compliance.

The following are examples of the types of information that can be recorded, stored and reported upon within Lief.

- Young People Care Records (e.g. Profile, Plans, Sessions, Logs, Reports, documents);
- Staff Records (e.g. Rota, Staff Leave, Task Management, Training, Profile).

Lief provides a fast and easy way for care providers to produce care reports. This part of the service uses Artificial Intelligence (AI) to help a Lief user to summarise a report so that they can add their professional insights without doing everything from scratch. This is also beneficial when preparing for inspections (SCIFF, Ofsted and CQC) to help to ensure that the requisite documentation is compliant.

The AI element of the service saves staff time because the initial summary of the report is pre-compiled, ready for review.

It is important to emphasise that the AI element of the service is not intended to entirely automate this reporting process and that the entire process is validated by suitably trained and qualified care providers. This is referred to as 'human in the loop AI' or HITL. What this means in practice is that a user of the service is able to review and change the outcome of the AI-generated report.

Benefits:

- **The Care Provider** gains valuable time saved on staff efficiency, more consistent and faster reporting and mitigation of staffing issues.
- **The Individuals** in care benefit because all the information that forms their care record is securely stored in one place providing their carers with a 360-degree view of the care that is being delivered to them.

A DPIA is required as the implementation of Lief involves processing data on behalf of the care organisation (as the data controller) of the data types listed in Step 2 (Scope of the Processing). This data includes health/special category data, which is afforded greater protection under UK data protection law.

Step 2 – Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
The Care provider is the source of the data entered about the individuals under their care and is the data controller in this context. Lief is the data processor of the care home residents' data. This data, alongside the carers' personal data, is shared with Lief so that they can provide the outsourced, hosted Lief service. Data is hosted securely on Amazon Web Services (AWS) in an appropriate location (the UK based data centre for UK deployments). The platform was selected to protect this special category data because AWS holds a raft of security certificates and is, importantly, certified as ISO/IEC 27001 compliant. AWS encrypts all data and metadata at rest using an industry-standard AES-256 encryption algorithm. All NFS traffic is encrypted in transit using Transport Layer Security 1.2 (TLS) with an industry-standard AES-256 cipher. TLS is a set of industry-standard cryptographic protocols used for encrypting information that is exchanged over the network. AES-256 is a 256-bit encryption cipher used for data transmission in TLS. Encryption has the following benefits: ● Helps to ensure that if data falls into an attacker's hands, the attacker cannot read the data without also having access to the encryption keys. Even if attackers obtain the storage devices that contain customer data, they won't be able to understand or decrypt it. ● Helps to reduce the surface of attack by cutting out the lower layers of the hardware and software stack. ● Acts as a chokepoint because centrally managed encryption keys create a single place where access to data is enforced and can be audited. ● Helps to reduce the attack surface because instead of having to protect all data, businesses can focus their protection strategies on the encryption keys. ● Provides an important privacy mechanism for Lief's customers. When data is encrypted at rest, it limits the access that systems and engineers have to the data. Regarding deletion of data, data is stored encrypted at rest within AWS, so that on

deletion request, the encryption keys are first deleted, ensuring that data is unreadable (cryptographic erasure), with the physical data later deleted and over time expired from backup systems. Additionally, at end-of-life drives are securely sanitised.

Flow Ref	Flow name/	Going from	Going to	Method of access/ Transfer and control	Specify the security control(s) in place for the flow
01	*Data In*	*Data Controller (Care Home staff enter data).*	*Lief AWS Cloud Infrastructure*	*Sent directly and encrypted in transit.*	*Lief's data is encrypted in transit and uses TLS v1.2*

AI Summary Feature – Pseudonymisation and De-identification Controls

For the AI-assisted report summarisation feature only, Lief applies a pseudonymisation process to report content before it is submitted to the AI provider. The purpose of this process is to reduce the amount of personal data disclosed during AI processing by replacing identifiable information with temporary placeholders where possible.

This obfuscation is essentially pseudonymisation which enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.

Specifically, the GDPR defines pseudonymisation in Article 3, as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymise a data set, the "additional information" must be "kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person."

Lief applies this pseudonymisation process specifically to data used within the AI-assisted report summarisation functionality. Other sub processors may process identifiable personal data where this is necessary to provide authentication, hosting, communications, transcription, support or other core service functions.

Unless otherwise stated, Sub Processors receive only the minimum personal data necessary to provide their contracted services. Pseudonymisation is not applied universally across all Sub Processors because certain service functions, such as authentication, hosting, email

delivery and speech transcription, require access to identifiable information to operate.

Sub-processors
Lief utilises the following sub-processors:

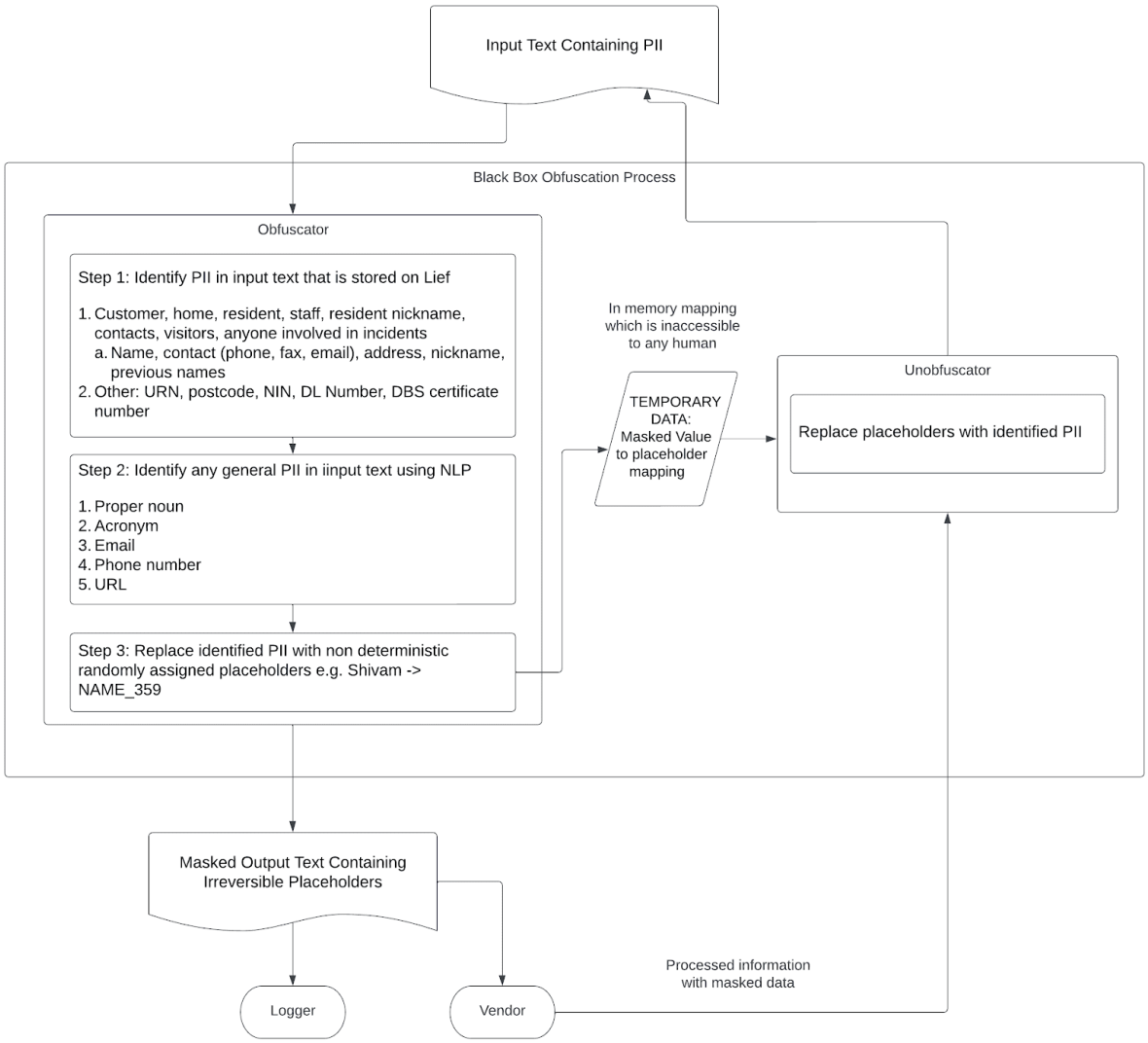
Supplier	Purpose	Data Processed	Location	Transfer mechanism
Auth0	User authentication	Email address and authentication credentials	EU	DPA and SCCs with UK Addendum
AWS	Hosting and storage	All customer data	UK	N/A – data remains in the UK. DPA in place.
Cloudflare	DNS, firewall and traffic routing	Data in transit (transient access only)	US (UK/EU routing)	DPA; UK-US Data Bridge
Google Workspace	Email, document storage and video conferencing	Internal email and documents. Customer (care provider) business and contact data may be included. No resident data.	US	DPA; UK-US Data Bridge
Mailgun	User invitation and system notification emails	User email address and account information	EU	DPA, SCCs and UK Addendum
Microsoft Azure OpenAI	AI-assisted speech-to-text transcription and AI-assisted report and summary generation	Audio submitted for transcription; pseudonymised/de-identified report content submitted through the AI summarisation feature	UK (UK data residency) *	N/A – data remains in the UK. Microsoft DPA.
Mixpanel	User analytics within the Lief product	Usage and behavioural data of authenticated users	US	DPA and SCCs with UK Addendum
Offshore technical support team (India)	Product support, incident resolution and software maintenance	Customer data viewed within the UK-hosted platform only when needed for a specific support issue; no data stored in India	India (access only)	UK IDTA; Transfer Risk Assessment (June 2026, updated October 2026)
Prior	Data Security and	Personal data only where	UK	N/A – UK

Supplier	Purpose	Data Processed	Location	Transfer mechanism
Analytics Ltd	Protection Consulting, including our appointed Data Protection Officer	needed to provide data protection advice, for example when assessing an incident		based. DPA in place.
Slack	Internal communications	Internal staff communications. Customer (care provider) business and contact data may be included. No resident data.	US	DPA; UK-US Data Bridge
Trainn	Product training services	Name and email address	US	DPA and SCCs with UK Addendum
Zapier	Internal workflow automations	Limited contact and account data passed between integrated services	US	DPA and SCCs with UK Addendum
Zoho	CRM, helpdesk and customer support emails	Contact and account details of customer organisations' staff only. No resident data.	US	DPA with UK IDTA or Addendum

International transfers are protected by Data Processing Agreements and the transfer mechanism shown for each supplier above. Suppliers located in the EU are also covered by the UK's adequacy regulations for the EU.

There is an outsourced Indian team which may view customer data within the UK-hosted platform to provide product support. No customer data is stored in India. This access is covered by a UK International Data Transfer Agreement (IDTA) and a separate Transfer Risk Assessment and DPIA (June 2026, updated October 2026).

* All processing is performed in Microsoft's UK South Azure region (London, United Kingdom). Speech-to-text data is stored and processed only within the region in which the service is deployed, and the AI API service uses a regional (UK South) deployment, meaning requests are processed in the UK rather than routed to Microsoft data centres elsewhere. Data at rest also remains in the UK. Microsoft may replicate data to its paired UK West region (Cardiff) for resilience and disaster recovery purposes; this remains within the United Kingdom. No customer data is transferred to the United States as part of this processing.


Input Text Containing PII
Black Box Obfuscation Process
Obfuscator
Step 1: Identify PII in input text that is stored on Lief
1. Customer, home, resident, staff, resident nickname, contacts, visitors, anyone involved in incidents
a. Name, contact (phone, fax, email), address, nickname, previous names
2. Other: URN, postcode, NIN, DL Number, DBS certificate number
Step 2: Identify any general PII in iinput text using NLP
1. Proper noun
2. Acronym
3. Email
4. Phone number
5. URL
Step 3: Replace identified PII with non deterministic randomly assigned placeholders e.g. Shivam -> NAME_359
In memory mapping which is inaccessible to any human
TEMPORARY DATA: Masked Value to placeholder mapping
Unobfuscator
Replace placeholders with identified PII
Masked Output Text Containing Irreversible Placeholders
Logger
Vendor
Processed information with masked data

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Personal data used:

☒Customer
☒Home
☒Resident
☒Staff
☒Resident nickname
☒Contact
☒Visitor Information
☒Anyone involved in incidents
☒Home Telephone Number
☒Mobile Telephone Number
☒Email address
☒Fax
☒Previous Names
☒URN
☒Address Fields
☒NIN
☒DL Number
☒DBS Certificate Number
☒Other – see below:

Care Records can contain a wealth of personal data because a carer can write 'free text' rather than being governed by a data entry form. Carers are trained to collect the minimal amount of information that they need to be able to offer safe direct care. In this respect, the key data elements that it is anticipated that the service will process are listed below, but they may not be exhaustive.

Additional categories of personal data processed may include:

- Date of birth
- Profile photographs
- Professional experience and education records
- Employment history
- Contact and next-of-kin details
- Daily activity records
- Personal documents uploaded by users
- Facility and care-related records

The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

For direct care purposes, the following **special category data** (all relating to the resident in the care home) is anticipated to be used:

- The Clinician responsible for the individual (where, for example, a child is under the care of a psychiatrist).
- The names of other clinicians who have viewed or modified or been involved in the child's direct care.
- medical diagnoses and treatment options discussed, including results and observations.
- names of parties that are relevant to the ongoing care of the patient, for example, a special needs assessor.

Additional special category data may include ethnicity, religion, physical identification characteristics, health information, mental health information and any special category information entered within care records.

Clinicians and care home staff are provided with Information Governance Training annually as part of their organisation's requirement to submit the DSP Toolkit and are familiar with data minimisation principles. The capture of any special category data listed above (in free form text) will only be to promote the best care for the individual who resides in the care home.

Data subjects in the UK will have their data processed in the UK.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
The carer who enters the details into the Lief service (about the individual under their care) has a direct care relationship with that individual. This has been the way that the system has worked for decades; hence, there are no prior concerns relating to this type of processing, and it is not considered novel data processing. The Lief service simply acts as a 'one stop shop' for the collation of a centralised and securely stored care record. There are concerns about the use of Artificial Intelligence to process personal data. This is why Lief has adopted the 'human in the loop AI' approach described in Section 2. It is important to realise that the Lief service was initially an entirely manual process (prior to the AI and machine learning technology being available). In this respect, should the automation and AI element not be available for some reason, the same service could still be performed by the care professionals without any sort of detriment to the individuals under their care. As the data subjects are in Children's care homes / Supported accommodation, it is inevitable that the majority will be children and belong to vulnerable groups, but the individual care providers operate under stringent regulatory controls – e.g. OFSTED and CQC inspections. In this respect, they all have their own safeguarding procedures and mitigating controls in place to reduce risk to this category of patient.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
It is important that Lief is able to consistently improve the algorithms used within the Lief service, and the beneficial effects of this are considered to outweigh any concerns about the intrusiveness of the processing (using machine learning/AI). Pseudonymised feedback from the annotation and editing of reports will be fed back into Lief's core machine learning platform to iteratively improve the product. The individuals in care benefit because their carers are often overworked, and removing an administrative burden frees up their time to be able to provide better care. This also provides a larger benefit to society, as such saving will ultimately result in a reduction in public expenditure.

Step 3 – Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
The following are typically consulted as relevant stakeholders during the deployment process and will contribute to the identification and assessment of risks: • Information governance representatives; • Care team representatives; • Digital / IT representatives; • Cyber / IT security representatives; Lief never underestimates the importance of data security and always consults with relevant partners to ensure that any personal data is kept in a secure manner. This means consulting with in-house and external consultants to work out the best practical means of receiving, processing and destroying the data in a way that is consistent with current UK data protection legislation.

Step 4 – Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
Lief does not have any direct relationship with the individuals residing in care homes and our sole purpose is to conduct our business as an outsourced provider of the Lief service. Lief is the data processor on behalf of the care home. Therefore, we do not determine the nature and means of the processing of their residents' data as this is their responsibility as data controller. However, given that the purpose of processing is for the delivery of direct care. The legal basis for processing is usually:

- Art.6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Art.9(2)(h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

Residents in homes can include children and other vulnerable groups. As it is special category data, there are many prior concerns over the way the data is processed; therefore, Lief submits Data Security and Protection (DSP) Toolkit to allow us to measure and publish our performance against the National Data Guardian's data security standards. The organisation also maintains Cyber Essentials Plus certification.

Customer organisations remain the Data Controllers and determine the purposes and means of processing. Yerado Limited acts as a Data Processor and processes personal data solely on documented instructions from the customer.

- Individuals should be informed about the best ways to use Lief via communication directly from their Care Home Manager and as part of onboarding and training. This is the responsibility of the data controller.
- Good practice in terms of data quality and minimisation is achieved via training and awareness, and data resides on UK servers.
- The Lief development team are fully versed in the principles of 'privacy by design and default'.

Step 5 – Assess Risks

Risk Assessment Matrix

Score	Likelihood	Severity
1	Rare	Negligible
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost certain	Catastrophic

Likelihood

Risk (Likelihood x Severity)

5	**5**	**10**	**15**	**20**	**25**	**High**	Unacceptable. Requires Mitigation
4	**4**	**8**	**12**	**16**	**20**		
3	**3**	**6**	**9**	**12**	**15**		Unacceptable. Requires Mitigation
2	**2**	**4**	**6**	**8**	**10**	**Medium**	
1	**1**	**2**	**3**	**4**	**5**	**Low**	Acceptable. Consider Mitigation
	1	2	3	4	5		

Severity

Detail sources of potential harm to Data Subjects, nature of potential impact and estimate risk

Risk Category	Source of Risk and nature of potential impact on data subject?	Likelihood	Severity	Risk
Confidentiality of Personal Data (Confidentiality is defined as unauthorised disclosure of, or access to, Personal Data)	Access to a care home resident's personal data by persons other than the data controller (i.e. the authorised User).	Rare	Major	Low
	Access to a Lief service user's Personal data by persons other than the data subject or the Data Controller.	Rare	Moderate	Low
Integrity of Personal Data (Integrity is defined as unauthorised or accidental alteration of Personal Data)	A service user records data on the wrong contact record in Lief.	Unlikely	Major	Medium
Availability of Personal Data (Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data)	Technical issues prevent access to the data for authorised users or the ability to recover a resident's data, or the machine learning/AI element fails.	Rare	Moderate	Low
Information Security / Cyber Security	Data Leak due to a security breach or malicious attack	Unlikely	Major	Medium
GDPR Principles	A Privacy by Design approach has been taken to ensure that Lief conforms to: Lawfulness, fairness and transparency Purpose limitation Data minimisation Accuracy Storage Limitation Integrity and Confidentiality (Security) Accountability	Unlikely	Minor	Low

Step 6: Identify measures to reduce risk				
Identify measures to reduce or eliminate risks, and estimate residual risk post implementation				
Risk Category	**Description of Risk Control Measures**	**Likelihood**	**Severity**	**Risk**
Confidentiality of Personal Data (Confidentiality is defined as unauthorised disclosure of, or access to, Personal Data)	Access to data is limited to only Authorised Users, and they require strict security and authentication when logging-in. Any Personal Data stored by Lief (Resident or User) is encrypted, and access to it is limited.	1	4	4
Integrity of Personal Data (Integrity is defined as unauthorised or accidental alteration of Personal Data)	As above, additionally,y users receive training when onboarding to Lief.	1	4	4
Availability of Personal Data (Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data)	Data is stored in data centres with ISO 27001 certification. The Lief service can operate without the machine learning and AI elements.	1	3	3
Information Security / Cyber Security	Lief is certified to ISO/IEC 27001:2022 (UKAS-accredited certification), holds Cyber Essentials Plus certification and submits the DSP Toolkit annually in June each year (2025-26: Standards Exceeded).	2	2	4
GDPR Principles	A Privacy by Design approach has been taken to ensure that Lief conforms to: Lawfulness, fairness and transparency Purpose limitation Data minimisation Accuracy Storage limitation Integrity and confidentiality (security) Accountability	2	2	4
Any residual risks scoring above 6 after the measures above have been applied will need to be reviewed by the organisation's Leadership Team. All residual risks in this assessment score 4 or below (Low), so no Leadership Team review is required.				

Step 7: Sign off and record outcomes		
Item	Name/position/date	Notes
Measures approved by:	Shivam Agarwal, SIRO 3rd October 2026	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	n/a	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	DPO advises that processing can proceed.	DPO should advise on compliance, risk mitigations and whether processing can proceed
DPO advice accepted or overruled by:	n/a	If overruled, there must be an explanation for reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will be kept under review by:	Shivam Agarwal, SIRO	The DPO should also review ongoing compliance with DPIA

APPENDIX A – MOBILE APPLICATION (PWA) ASSESSMENT

Document Date: December 2025, reviewed 3 October 2026

Related DPIA: Lief (by Yerado Limited)

Background

Yerado Limited has developed mobile applications for iOS and Android to provide customers with access to the existing Lief platform through Apple App Store and Google Play Store distribution.

The mobile applications are implemented as Progressive Web Applications (PWAs). The applications provide an alternative method of accessing the existing Lief service and do not introduce a separate platform, database, hosting environment or processing activity.

Description of Processing

The mobile applications connect to the existing Lief platform using the same authentication, security controls, APIs and backend infrastructure as the web application.

All personal data continues to be processed and stored within the existing AWS-hosted environment described within this DPIA.

The categories of personal data, special category data, data subjects, purposes of processing, retention periods, international transfers, subprocessors and lawful bases for processing remain unchanged.

Assessment of Privacy Impact

The introduction of the mobile applications does not result in:

- New categories of personal data being collected.
- New categories of special category data being processed.
- New categories of data subjects.
- New purposes of processing.
- Automated decision making or profiling.
- New data sharing arrangements.
- New international transfers.
- Material changes to existing security controls.

The applications act solely as a client interface to the existing Lief platform.

Additional Risks Considered

The introduction of mobile access introduces the potential for:

- Loss or theft of a mobile device.
- Unauthorised access to information displayed on a mobile device.
- Interception of data during transmission.

Existing Controls

The following controls apply:

- All communications between the application and backend services are encrypted using TLS.
- User authentication continues to be managed through Auth0.
- Access controls remain governed by the existing role-based permissions within Lief.
- Session management controls remain consistent with those used by the web application.
- Customer administrators retain the ability to manage and revoke user access.
- Data processing and storage continue to take place within the existing AWS-hosted infrastructure.
- Mobile operating system security controls such as device passcodes, biometric authentication, device encryption and remote wipe functionality may be utilised by customers.

Outcome

Following assessment, Yerado Limited has determined that the introduction of the iOS and Android mobile applications does not materially alter the processing activities assessed within the existing DPIA.

The mobile applications provide an additional access method to the existing Lief platform and do not introduce any substantial change to the nature, scope, context or purposes of processing.

The residual privacy risk remains unchanged and is considered acceptable subject to the continued operation of the technical and organisational measures already identified within this DPIA.

Approval

Assessment completed by: Data Protection Officer

Date: December 2025, reviewed 3 October 2026

Decision: Existing DPIA remains valid. No further DPIA assessment required at this time. Reviewed as part of the DPIA update on 3 October 2026; the mobile applications remain covered by this DPIA.