Lift Relations Data Processing Agreement

Version v.110126 · Effective November 1, 2026

This Data Processing Agreement ("DPA") forms part of the agreement between Lift Relations ApS, CVR no. 33356706, Sortedam Dossering 55, 2100 Copenhagen Ø, Denmark ("Lift Relations") and the customer named in the Order Form ("Customer"), consisting of the Lift Relations Terms and Conditions, the Order Form(s) and this DPA (the "Agreement"). It governs Lift Relations' processing of Personal Data on behalf of the Customer, and sets out the limited processing Lift Relations carries out as an independent Controller under section 2.3. The parties are bound by this DPA from the date the Agreement takes effect. In case of conflict between this DPA and the rest of the Agreement regarding the processing of Personal Data, this DPA prevails, and the Standard Contractual Clauses prevail over this DPA.

1. Definitions

Capitalised terms not defined here have the meanings given in the Agreement.

- **"Data Protection Laws"** means all laws applicable to the processing of Personal Data under the Agreement, including the GDPR, the UK GDPR, the Danish Data Protection Act and US Privacy Laws.
- **"GDPR"** means Regulation (EU) 2016/679. The terms "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" have the meanings given in the GDPR. Where US Privacy Laws apply, "Controller" includes "business", "Processor" includes "service provider", and "Personal Data" includes "personal information".
- **"Customer Personal Data"** means Personal Data contained in Customer Data that Lift Relations processes on the Customer's behalf.
- **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and, for the UK, the International Data Transfer Addendum issued by the UK Information Commissioner.
- **"Sub-processor"** means any processor engaged by Lift Relations to process Customer Personal Data.
- **"US Privacy Laws"** means the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA") and other comprehensive US state privacy laws, to the extent applicable.

2. Roles and Instructions

2.1 For Customer Personal Data, the Customer is the Controller and Lift Relations is the Processor, except for the processing described in section 2.3. Where the Customer acts as processor for its own customer, Lift Relations is the Customer's sub-processor.

2.2 Except as set out in section 2.3, Lift Relations will process Customer Personal Data only on the Customer's documented instructions, unless required to do so by EU or Member State law, in which case it will inform the Customer before processing unless the law prohibits this. The Customer's instructions are set out in the Agreement, including Schedule 1, and in the Customer's configuration and use of the Services. Additional instructions require written agreement.

2.3 Aggregated Data and model development. The Customer authorises Lift Relations to (a) aggregate and de-identify Customer Personal Data to create Aggregated Data, and (b) use Customer Personal Data in pseudonymised form to develop, train, test and improve the models and features of the Services, in each case as described in sections 7.2 and 7.3 of the Terms and Conditions. For this processing Lift Relations acts as an independent Controller on the basis of its legitimate interests and is responsible for its own compliance with Data Protection Laws. Once data qualifies as Aggregated Data, it no longer constitutes Personal Data and is not subject to this DPA. The Customer confirms that it may make Customer Personal Data available to Lift Relations for these purposes and will inform Data Subjects of them, including by reference to the Lift Relations Privacy Policy. This authorisation forms part of the Agreement and is not an instruction that the Customer may withdraw or vary under section 2.2.

2.4 Lift Relations will inform the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Laws.

2.5 The Customer is responsible for having a lawful basis for the processing it instructs, for providing any notices to Data Subjects (including survey respondents) required by Data Protection Laws, and for the accuracy of Customer Personal Data. Lift Relations will display a short privacy notice on survey pages identifying Lift Relations as the Customer's processor and, for the processing in section 2.3, as an independent controller, and describing the use of aggregated, de-identified results for benchmarks and of pseudonymised data for model development.

3. Personnel

Lift Relations will ensure that persons authorised to process Customer Personal Data are subject to confidentiality obligations, have received appropriate data protection training, and access Customer Personal Data only to the extent needed to perform the Services.

4. Security

Lift Relations will implement and maintain appropriate technical and organisational measures to protect Customer Personal Data, taking into account the state of the art, implementation costs and the nature, scope, context and purposes of the processing, as required by Article 32 GDPR. The current measures are described in Schedule 3. Lift Relations may update them, provided the overall level of security is not materially decreased during a subscription term.

5. Sub-processors

5.1 The Customer gives Lift Relations general authorisation to engage Sub-processors. The Sub-processors authorised at the effective date are listed in Schedule 2, and the current list is made available at lft.ai/legal or on request.

5.2 Lift Relations will notify the Customer by email, or by updating the list at lft.ai/legal, at least twenty (20) days before adding or replacing a Sub-processor. The Customer may object in writing on reasonable data protection grounds within ten (10) days of the notice. The parties will then discuss a solution in good faith, which may include Lift Relations offering an alternative configuration of the Services. If no solution is found within thirty (30) days, Lift Relations may either proceed without using the new Sub-processor for the Customer or terminate the affected Services and refund the prepaid fees for the remainder of the term attributable to them. If the Customer does not object within the objection period, the Sub-processor is deemed authorised.

5.3 Lift Relations will engage each Sub-processor under a written agreement imposing data protection obligations that are substantially equivalent to those in this DPA, and remains responsible to the Customer for each Sub-processor's performance, subject to section 13.

6. Data Subject Rights

Taking into account the nature of the processing, Lift Relations will assist the Customer by appropriate technical and organisational measures, insofar as possible, in responding to requests from Data Subjects to exercise their rights. Lift Relations will promptly forward to the Customer any request it receives directly that relates to Customer Personal Data and will not respond except on the Customer's instructions or as required by law. Requests relating to the processing described in section 2.3 are handled by Lift Relations as Controller in accordance with the Lift Relations Privacy Policy.

7. Personal Data Breach

7.1 Lift Relations will notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 The notice will describe, as far as then known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Information not available at the time will be provided in phases without undue delay.

7.3 Lift Relations will take reasonable steps to contain, investigate and remediate the breach, and cooperate with the Customer to meet its notification obligations. Notification is not an acknowledgement of fault or liability.

8. Assistance

Lift Relations will provide reasonable assistance to the Customer with data protection impact assessments and prior consultations with Supervisory Authorities relating to the Services, taking into account the nature of the processing and the information available to Lift Relations.

9. Deletion and Return

The Customer may export Customer Personal Data at any time during the subscription term through the Services. On expiry or termination of the Agreement, Lift Relations will, at the Customer's choice, return Customer Personal Data by providing a one-off export in CSV or another commonly used format on written request received within thirty (30) days, and will then delete it from the Platform within thirty (30) days and from backups in accordance with its standard backup retention cycle, unless EU or Member State law requires retention or the Customer requests in writing, before deletion, that Lift Relations retain Customer Personal Data for a specified period of up to twelve (12) months. Lift Relations will confirm deletion in writing on request. This clause does not apply to Aggregated Data, Usage Data, models trained in accordance with the Terms and Conditions, or Customer Personal Data held in pseudonymised form by Lift Relations as Controller under section 2.3.

10. Audits

10.1 Lift Relations will make available to the Customer the information reasonably necessary to demonstrate compliance with this DPA, such as completed security questionnaires and a summary of its security policies. Lift Relations is not required to complete more than one security questionnaire in any twelve (12) month period unless required by a Supervisory Authority or following a Personal Data Breach.

10.2 If that information is not sufficient to demonstrate compliance, or a Supervisory Authority requires it, the Customer (or an independent auditor bound by confidentiality and not a competitor of Lift Relations) may conduct an audit no more than once in any twelve (12) month period, on at least thirty (30) days' written notice, during normal business hours and with minimal disruption. The parties will agree the scope, timing and duration in advance, and the audit is limited to records and systems relevant to the Customer Personal Data. The Customer bears all costs of the audit, including the auditor's costs and Lift Relations' reasonable internal costs of supporting it. Audit results are Confidential Information.

11. International Transfers

11.1 Lift Relations hosts and stores Customer Personal Data in the European Economic Area. Customer Personal Data may be accessed by or transferred to Sub-processors outside the EEA as listed in Schedule 2. Any such transfer will comply with Chapter V GDPR, through an adequacy decision (including the EU-US Data Privacy Framework for certified recipients) or the SCCs.

11.2 Where the Customer is established outside the EEA and the transfer of Customer Personal Data from Lift Relations to the Customer is a restricted transfer, Module 4 (processor to controller) of the SCCs is incorporated by reference, with Lift Relations as data exporter and the Customer as data importer. Where a transfer from the Customer to Lift Relations requires a transfer mechanism, Module 2 (controller to processor) or, where the Customer is a processor, Module 3 (processor to processor) is incorporated by reference, with the Customer as data exporter and Lift Relations as data importer.

11.3 For the SCCs: clause 7 (docking clause) applies; under clause 9, option 2 (general written authorisation) applies with the notice period in section 5.2; the optional wording in clause 11 does not apply; clauses 17 and 18 are governed by the laws of, and disputes resolved by the courts of, Denmark; and Annexes I and II are completed by Schedules 1 and 3. For UK transfers, the UK International Data Transfer Addendum applies, completed with the same information.

12. US Privacy Laws

Where US Privacy Laws apply to Customer Personal Data, Lift Relations acts as a service provider or processor and will:

1. not sell or share Customer Personal Data, as those terms are defined in the CCPA;
2. not retain, use or disclose Customer Personal Data for any purpose other than the business purposes specified in the Agreement, including outside the direct business relationship between the parties, except as permitted by US Privacy Laws, including to build or improve the quality of the Services and to create deidentified or aggregated information;

3. not combine Customer Personal Data with personal information it receives from other sources, except as permitted by US Privacy Laws;
4. comply with applicable US Privacy Laws and provide the same level of privacy protection they require, and notify the Customer if it can no longer meet its obligations; and
5. allow the Customer to take reasonable and appropriate steps to stop and remediate unauthorised use of Customer Personal Data.

Lift Relations certifies that it understands and will comply with these restrictions.

13. Liability

Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability in the Agreement, except where such limitation is not permitted by Data Protection Laws or the SCCs.

14. Term and Governing Law

This DPA remains in force for as long as Lift Relations processes Customer Personal Data under the Agreement. It is governed by the laws of Denmark, and disputes are resolved as set out in the Agreement, except where the SCCs require otherwise. Notices and questions about the processing of Personal Data can be sent to legal@lft.ai.

Schedule 1 – Details of Processing

Item	Description
Parties	Data exporter / Controller: the Customer named in the Order Form. Data importer / Processor: Lift Relations ApS, Denmark. Contact: legal@lft.ai. For the processing described in section 2.3, Lift Relations acts as an independent Controller (see Purposes).
Subject matter	Provision of the Lift Relations client relationship intelligence platform under the Agreement
Nature of processing	Collection, storage, organisation, analysis, scoring and profiling of relationships and feedback, translation, reporting, pseudonymisation, retrieval, transmission and deletion
Purposes	Providing, securing, supporting and maintaining the Services, including surveys, scoring, alerts, reports, insights, risk and opportunity indicators and recommended actions about the Customer's client relationships, its clients and the individuals involved. Creating Aggregated Data and developing, training and improving models with pseudonymised data is carried out by Lift Relations as an independent Controller under section 2.3 and is not processing on the Customer's behalf.
Categories of Data Subjects	The Customer's employees and contractors who use the Services or respond to team surveys; employees of the Customer's clients who are invited to respond to client surveys
Categories of Personal Data	First and last name; job title; business email address; company and office; username; IP address and login data; survey responses, scores and free-text comments; any other Personal Data the Customer chooses to submit
Special categories	None intended. The Customer shall not submit special categories of Personal Data. Free-text comments may incidentally contain such data; they are protected by the measures in Schedule 3
Frequency	Continuous, for the duration of the Agreement
Retention	For the term of the Agreement, then deleted as set out in section 9
Location of storage	Microsoft Azure data centres in the European Union (Netherlands and Ireland)

Item	Description
Transfers to Sub-processors	As set out in Schedule 2
Competent Supervisory Authority	The Danish Data Protection Agency (Datatilsynet)

Schedule 2 – Authorised Sub-processors

Sub-processor	Service	Location of processing	Transfer mechanism
Microsoft Ireland Operations Ltd (Microsoft Azure and Microsoft 365)	Cloud hosting, databases, storage, backups and monitoring; AI-assisted text and sentiment analysis; secure storage of reports and support files	EU (Netherlands, Ireland)	Not applicable (EEA)
IBM (IBM Cloud, Watson Natural Language Understanding)	Sentiment and text analysis of survey comments	EU	Not applicable (EEA)
DeepL SE	Translation of survey content and comments	Germany	Not applicable (EEA)
Anthropic, PBC (Claude)	AI-assisted analysis of survey content, including sentiment and text analysis, summaries and recommended actions	United States	SCCs
Google (Cloud Translation API)	Translation of survey content and comments	United States	EU-US Data Privacy Framework / SCCs
Twilio Inc. (SendGrid)	Delivery of survey invitations and service emails	United States	EU-US Data Privacy Framework / SCCs
Microsoft Corporation (Microsoft Clarity)	Product usage analytics for the Platform	United States	EU-US Data Privacy Framework / SCCs
Intercom (Intercom R&D Unlimited Company and affiliates)	In-app support chat and help centre	United States	EU-US Data Privacy Framework / SCCs
Atlassian (Jira, Confluence)	Support ticket and issue tracking	United States	EU-US Data Privacy Framework / SCCs
SolarWinds Worldwide, LLC	Application performance monitoring and logging	United States	SCCs

Schedule 3 – Technical and Organisational Measures

Governance. Information security is owned by executive management under a written Information Security Policy that is reviewed regularly. A named member of management is responsible for security and data protection.

Hosting and segregation. The Platform is hosted entirely on Microsoft Azure in the EU, whose infrastructure is certified to ISO/IEC 27001 and attested under SOC 2. Lift Relations operates no on-premises servers. Customer data is logically separated by tenant identifiers; every application query is scoped to the authenticated tenant.

Encryption. Data is encrypted in transit with TLS 1.2 or higher, and at rest, including backups, with AES-256.

Access control. Access to production systems and Customer Data is limited to named personnel who need it for their role, under least privilege and role-based access control. Each person uses an individual account; shared accounts are not used for access to production systems or Customer Data. Access to production is reviewed quarterly and other access at least annually, and access is removed within five (5) business days when personnel leave or change roles. Internal accounts not used for ninety (90) days are disabled.

Customer access controls. The Services support role-based permissions and session timeouts for Users. User accounts that have not been used for one hundred and eighty (180) days may be deactivated after notice to the Customer's administrator, who can reactivate them.

Logging and monitoring. Administrative actions, authentication events and system events are logged in Azure monitoring services in the EU and retained in line with Lift Relations' logging policy. Alerts notify the technical team of anomalous activity.

Secure development. Code changes are reviewed before release, tested in non-production environments and deployed through controlled pipelines with rollback capability. Dependencies are checked for known vulnerabilities, and critical vulnerabilities are prioritised for remediation. Production Personal Data is not used in non-production environments unless it has first been masked or pseudonymised.

Vulnerability management. Azure platform patches are applied automatically. Lift Relations performs regular vulnerability scanning of the Platform and its application dependencies, applies critical security patches promptly, and carries out periodic security testing as part of its information security program. Where an independent security test has been completed, Lift Relations will share a high-level summary on request, subject to confidentiality.

Availability and recovery. Databases are backed up daily with point-in-time recovery in Azure EU regions, and backups are retained for thirty (30) days. Restoration procedures are tested periodically.

Incident response. A documented incident response procedure covers detection, containment, eradication, recovery, notification and post-incident review. All incidents are logged.

Endpoint security. Company devices use disk encryption, anti-malware protection and automatic screen locking. Access to company systems from mobile devices requires authentication.

Personnel. All personnel and contractors are bound by written confidentiality obligations and receive security and data protection guidance on joining and periodically thereafter.

Vendor management. Sub-processors are assessed for security and data protection before engagement, bound by written data processing terms, and reviewed periodically.

AI and data minimisation. Survey content sent to AI and text-analysis providers is limited to what the feature requires, names and direct identifiers are removed where feasible, and providers are contractually prohibited from using Customer Data to train their own models.

Deletion. Customer Data is deleted in accordance with section 9 of this DPA. No physical media containing Customer Data is used.