Data Processing Addendum

Updated March 28, 2025

This Data Processing Addendum ("DPA") is incorporated into and forms part of Lime's Terms of Service ("Agreement") entered into by and between the Lime entity and Customer identified in the Agreement. The purpose of this DPA is to reflect the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Applicable Data Protection Law. All capitalized terms not defined herein shall have the meaning set forth in the Agreement or the DPA, as applicable.

In the course of providing the Services to Customer pursuant to the Agreement, Lime may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data. Lime will hereinafter be referred to as "Processor" and the Customer as "Controller", alternatively "party" or collectively as "parties".

This DPA takes precedence over conflicting or incompatible provisions on the Processing of Personal Data in the Terms of Service.

1 Definitions

In addition to the terms defined in the body text of the DPA, the following terms shall have the meanings set out below.

1.1 **Personal Data**: Any type of data relating to an identified or identifiable person (the Data Subject).

1.2 **Data Subject**: An identified or identifiable natural person. An identifiable person is someone who can be identified, either directly or indirectly, particularly through reference to an identification number or to one or more factors specific to the person's physical, physiological, mental, economic, cultural or social identity.

1.3 **Processing (of Personal Data)**: Any measure or series of measures taken in respect of Personal Data, regardless of whether or not this takes place automatically, e.g. collection, registration, organisation, storage, adaptation or modification, search, consultation, use, transfer, dissemination or other supply, compilation or combination, blocking, deletion or destruction.

1.4 **Controller**: A natural or legal person, authority, institution or other body that alone or together with others determines the purposes and means for the Processing of Personal Data.

1.5 **Processor**: A natural or legal person, authority, institution or other body that carries out Processing of Personal Data on behalf of the Controller.

1.6 **Applicable Data Protection Legislation**: The General Data Protection Regulation (GDPR) – i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC – and national laws that implement or supplement the GDPR and apply to the Processing of Personal Data under this DPA.

1.7 **Sensitive Personal data**: Racial or ethnic origin, or political, philosophical or religious beliefs, trade union membership, if a person is suspected or has been prosecuted or convicted of a crime, health, genetic data, biometric data used to uniquely identify a person, a person's sexual life or sexual orientation, or other sensitive Personal Data.

1.8 **Third Country**: A country outside of the EU/EEA.

2 Processing of Personal Data

2.1 The Processor shall carry out Processing of Personal Data only in accordance with this DPA and in accordance with documented instructions issued by the Controller, unless

the Processor is obliged under EU law (including the national laws of its member states) to carry out Processing of the Personal Data.

2.2 The Controller shall issue written instructions to the Processor on how to carry out the Processing.

2.3 The Processor shall carry out Processing of the Personal Data for the entire term stated in the Agreement and for a limited period thereafter (see section 11). **Appendix A** contains information on the Processing of Personal Data including i) categories of Personal Data, ii) categories of Data Subject, iii) nature and purpose of the Processing, iv) site for Processing and v) duration of the Processing.

2.4 This DPA does not apply to Personal Data once transferred from the Service to a Third Party Software (as defined in the Agreement), as the Controller's relevant and separate agreement with that Third Party Software provider will instead govern.

3 The obligations of the Processor

3.1 The Processor shall carry out the Processing only in accordance with the DPA and instructions. For the sake of clarity, the Processor may carry out Processing of Personal Data if such Processing is required in accordance with a relevant law that applies to the Processor. The Processor shall inform the Controller of such requirements if it is not prohibited from disclosing such information due to an important public interest. When Processing Personal Data in accordance with the DPA, the Processor shall comply with Applicable Data Protection Legislation.

3.2 The Processor shall ensure that all natural persons who work under its management and have access to Personal Data comply with the DPA and the Controller's instructions.

3.3 During the Processing, the Processor and its staff shall observe a duty of confidentiality and secrecy regarding the Personal Data they have access to under this DPA. This provision also applies after the DPA is terminated.

3.4 The Processor shall take the security precautions required by Article 32 of the GDPR.

3.5 To the extent possible, the Processor shall help the Controller fulfil its obligations towards the Data Subjects by taking appropriate technical and organisational measures.

3.6 At the request of the Controller, the Processor shall assist the Controller in ensuring that the obligations under Articles 32–36 of the GDPR are met, taking into account the type of Processing and the information available to the Processor.

3.7 The Processor shall notify the Controller immediately if the Processor considers the Controller's instructions to be unclear or in any way contrary to Applicable Data

Protection Legislation. The Processor shall not carry out such an instruction until the Controller has confirmed that the instruction is lawful.

4 The obligations of the Controller

4.1 When using the services provided by the Processor in accordance with the Agreement, the Controller shall carry out Processing of Personal Data in accordance with Applicable Data Protection Legislation. The Controller is responsible for ensuring that there is a lawful basis for the Processing at all times and for formulating correct instructions so that the Processor (and its subprocessors) can fulfil its commitments and obligations under this DPA and, if applicable, the Agreement.

4.2 The Controller is authorised to carry out Processing of and disclose the Personal Data covered by the Agreement to the Processor (including to any subprocessors it may have).

4.3 The Controller is solely responsible for the accuracy, integrity, content, reliability and legality of the Personal Data disclosed to the Processor. The Processor does not bear any responsibility for any consequences of the Personal Data it receives being found to be incorrect.

4.4 The Controller has fulfilled its obligations to provide mandatory information to the Data Subjects about Processing of Personal Data and the transfer of Personal Data to the Processor and the Processor's Processing of Personal Data in accordance with Applicable Data Protection Legislation.

4.5 When using the Services provided by the Processor in accordance with the Agreement, the Controller may not disclose any Sensitive Personal Data to the Processor unless expressly agreed and specified between the parties in writing.

4.6 The Controller shall notify the Processor without delay of any changes to its contact person or contact information.

5 Security precautions

The Processor shall implement appropriate technical and organizational security measures to protect the Personal Data in accordance with Applicable Data Protection Law (including Article 32 of the GDPR) to protect confidentiality, integrity and access to Personal Data, as further described in **Appendix B**. The Processor shall continuously review its technical and organizational security measures and update them where necessary in accordance with Applicable Data Protection Legislation.

6 Audits and inspections

6.1 The Processor shall provide the Controller with access to all the information required to demonstrate that the obligations arising from the DPA have been fulfilled and to

enable and contribute to audits, including inspections, carried out by the Controller or a third party appointed by the Controller.

6.2 The Controller may audit the Processor's compliance with the DPA a maximum of one (1) time a year. If required by Applicable Data Protection Legislation, the Controller may require more frequent reviews.

6.3 To request an audit, the Controller shall submit a detailed audit plan to the Processor at least four weeks before the proposed audit. The plan must include the scope, duration and proposed start date of the audit. If the audit is to be carried out by a third party, as a general rule this must be agreed between the Controller and the Processor. If the Processing takes place in an environment with Personal Data deriving from other Controllers or similar, the Processor may, at its own discretion, decide for security reasons that the audit shall be performed by a generally highly regarded audit company chosen by the Processor.

6.4 If the requested audit has already been performed and described in a report in accordance with ISAE 3402, ISO or similar by a qualified third-party auditor within the last 12 months, and the Processor confirms that the audited controls have not changed materially, the Controller must accept these results instead of requesting an audit of the controls covered by the report.

6.5 The audit shall be carried out during the facility's normal business hours in accordance with the Processor's policies and may not cause unreasonable disruption to the Processor's operations.

6.6 The Controller is responsible for all costs arising in connection with an audit requested by the Controller and the Processor's assistance in this regard.

6.7 The Processor shall give the supervisory authority, or another authority that is legally entitled to it, the opportunity to carry out supervision in accordance with the applicable legislation at any time. The Processor and its staff shall, upon request, co-operate with the supervisory authority as it performs its duties.

7 Support for the Controller

7.1 Taking into account the nature of the Processing and as far as possible, the Processor shall assist the Controller with appropriate technical and organisational measures so that the Controller can fulfil its obligation to respond to requests for Data Subjects to exercise their rights.

7.2 As far as practically possible and lawful, the Processor shall notify the Controller of i) requests received from Data Subjects to disclose Personal Data, except when the Controller has authorised the Processor to respond to such a request, and ii) requests from authorities to disclose Personal Data, except where the Controller has authorised the Processor to respond to such a request.

7.3 The Processor may, however, be prevented from notifying the Controller due to investigation secrecy during a law enforcement investigation. The Processor shall not disclose information about this DPA to authorities with regard to Personal Data, unless it is required to do so by law or the request is supported by a court decision, search warrant or similar.

7.4 Taking into account the nature of the Processing and the information available to the Processor, the Processor shall assist the Controller in ensuring that the obligations under Applicable Data Protection Legislation are fulfilled, including (if applicable) the Controller's obligation to i) take appropriate technical and organisational measures, ii) report data breaches to the supervisory authority, iii) notify Data Subjects of data breaches, iv) carry out impact assessments regarding data protection and v) consult the supervisory authority prior to Processing.

7.5 The Processor shall notify the Controller in writing without undue delay if the Processor has become aware of a data breach. The Processor shall provide the Controller with a description of the data breach. In the event that the Processor does not have all of the relevant information regarding the data breach when it first informs the Controller that a data breach has taken place, the Processor may provide such information in batches.

7.6 The Processor is entitled to charge the Controller for work carried out and reasonable costs that have arisen in connection with the Processor's support as described above and in accordance with Applicable Data Protection Legislation, notwithstanding the fulfilment of obligations pursuant to Section 7.5 above (provided that the Personal Data Breach is not attributable to the Controller). This includes e.g. work and costs that have arisen from Data Subjects having requested register extracts regarding the Processing of their Personal Data, the erasure of Personal Data, the transfer of Personal Data (portability) or the disclosure of mandatory information to Data Subjects.

8 Use of subprocessors

8.1 As part of the service delivery provided by the Processor to the Controller in accordance with the Agreement, the Processor is hereby given general written prior authorisation to use subprocessors for the Processing of Personal Data on behalf of the Controller.

8.2 The Processor shall ensure that all subprocessors are bound by written agreements which ensure that the subprocessor is subject to obligations regarding the Processing of Personal Data that, as a minimum, correspond to the obligations set out in this DPA.

8.3 If the subprocessor does not fulfil its obligations in accordance with Applicable Data Protection Legislation, the Processor shall be fully responsible to the Controller for carrying out the subprocessor's obligations.

8.4 The Processor shall make available an updated and current list of subprocessors that are used to carry out the services provided by the Processor under the Agreement. The list shall contain information about the identity of the subprocessors, the contact person for the subprocessor, where the Personal Data is processed and a general description of the type of service provided by each subprocessor. The list of subprocessors is available at Lime's website https://www.lime-technologies.com/subprocessors/. By signing this DPA, the Controller is approving the Processor's use of the listed subprocessors.

8.5 The Processor shall notify the Controller of any plans to hire a new subprocessor or replace an existing one. The Controller may object to such changes. If no objection is made within ten (10) days of receipt of the notification, it is assumed that the Controller has not made any objection.

8.6 The Processor is entitled to take appropriate corrective measures in the event of such an objection. If the Controller finds that no corrective measures have been taken or the objection has not been remedied within thirty (30) days, the parties are entitled to terminate the DPA and, if the DPA is necessary for the parties to fulfil their obligations under the Agreement, terminate the Agreement through written notification.

9 Transfer of personal data to a Third Country

9.1 The Processor and its subprocessors may transfer Personal Data to a Third Country to the extent that it is necessary in order to perform the services provided by the Processor in accordance with the Agreement and provided that the transfer takes place in accordance with Chapter V of the GDPR.

9.2 When using standard contractual clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or decisions and standard contractual clauses that replace these clauses), the Processor or subprocessor is entitled at its own discretion to decide which version and which modules of the standard contractual clauses apply in an individual case.

9.3 In accordance with the requirements set out in Applicable Data Protection Legislation regarding transfers based on appropriate security precautions being taken, the Processor shall carry out a risk assessment in each individual case to ensure that legislation in the Third Country in question does not adversely affect the effectiveness of the appropriate safeguards and to ensure that there are effective remedies for Data Subjects. If necessary, the Processor shall identify and implement supplementary measures, such as technical, organisational or contractual measures, to ensure that the level of protection in the Third Country in question is substantially equivalent to the level of protection within the EU/EEA.

9.4 At the reasonable request of the Controller, the Processor shall report the information on which the risk assessment is based. The Controller is entitled to object in writing to the Processor's risk assessments if they are changed after the DPA comes into force and the Controller deems that the new risk assessments do not fulfil the requirements for the Controller's Processing of Personal Data in accordance with Applicable Data Protection Legislation. The Controller is entitled to request that the Processor take appropriate corrective measures. If the parties do not agree on the risk assessment and/or appropriate corrective measures within thirty (30) days, the parties are entitled to terminate the DPA and, if the DPA is necessary for the parties to fulfil their obligations under the Agreement, entitled to terminate the Agreement through written notification.

9.5 In the event that the European Court of Justice, European Commission or any other competent EU institution or national court or authority finds the transfer mechanism used for the transfer to a Third Country to be invalid or illegal, the Processor shall ensure that all Processing of Personal Data in a Third Country is based on another (valid) transfer mechanism.

10 Term of DPA

10.1 This DPA is valid for as long as the Processor carries out Processing of Personal Data on behalf of the Controller in accordance with the Agreement.

10.2 This DPA automatically ceases to apply when the Agreement is terminated.

11 Measures upon termination of the DPA

11.1 Upon termination of this DPA, the Processor shall, depending on what the Controller instructs the Processor in writing, erase or return all Personal Data being Processed on behalf of the Controller in accordance with the DPA, as well as all copies of the data, unless storage of the Personal Data is required in accordance with Applicable Data Protection Legislation.

11.2 If the Controller has not provided any instructions or responded to the Processor's request for instruction, the Processor may, after thirty (30) days from termination of the DPA, choose to return to the Controller and/or erase all Personal Data.

12 Confidentiality

The Processor shall not, during the term of the DPA or thereafter, disclose information about the Processing of Personal Data in accordance with this DPA to a third party or otherwise reveal information received as a result of this DPA. The confidentiality obligation does not apply to information that the Processor is obliged to disclose to authorities. In addition to this section (12), the confidentiality obligations in the Agreement shall also apply.

13 Amendments and additions

13.1 Amendments to this DPA may occur due to changes in legislation, security requirements or other practical circumstances. In the event of an amendment that affects the Processing of Personal Data in accordance with this DPA, the other party shall be notified by means of an e-mail sent to its contact person stated above. Such notification of an amendment shall be deemed to have been accepted by the other party, provided that the other party has not made reasonable objections in writing within thirty (30) days of the date of the notification.

13.2 Should a competent court, authority or arbitration board find that any provision in this DPA is unenforceable or invalid, the other provisions shall not be affected. In that regard, the parties shall replace the unenforceable or invalid provision with a lawful provision that reflects the purpose of the unenforceable or invalid provision.

14 Liability

14.1 Upon compensation for damages in connection with Processing that, according to a final judgement or settlement, shall be paid to the Data Subject because of a breach of a provision in this DPA, instructions and/or any applicable provision in Applicable Data Protection Legislation, article 82 in GDPR shall be applied.

14.2 Administrative fines according to article 83 in GDPR, or chapter 6, paragraph 2 law (2018:218) with supplementary provisions to the European Union's General Data Protection Regulation, shall be borne by the party that has been imposed such administrative fine.

14.3 Without degrading obligations under 14.1 and 14.2, contractual limitation of liability stated in the Agreement shall also apply to this DPA.

14.4 If any of the parties become aware of any circumstance that may cause the other party damages, that party shall immediately inform the other party about that circumstance and shall actively cooperate with the other party to prevent and minimize such damage.

15 Choice of law and legal forum

15.1 This DPA shall be interpreted and applied in accordance with the provisions on choice of law in the Agreement.

15.2 Any disputes that arise in connection with this DPA shall ultimately be settled in accordance with the provisions on dispute resolution in the Agreement.

Appendix A – Instructions for Processing Personal Data

Categories of Personal Data	The Controller may input Personal Data into the service provided by the Processor in accordance with the Agreement. The Personal Data input into the service is entirely up to the Controller and may e.g. include the following categories of Personal Data: - Name. - Phone number. - E-mail address. - Customer history.
Categories of Data Subject	The Controller may input Personal Data into the service provided by the Processor in accordance with the Agreement. The Personal Data input into the service is entirely up to the Controller and may e.g. include Personal Data concerning the following categories of Data Subject: - The Controller's employees, customers, suppliers and consultants. - Employees of the Controller's potential customers.
Nature and purpose of the Processing	The Processing of Personal Data in order to provide the services provided by the Processor in accordance with the Agreement and the Controller's instructions.
Site for Processing	- The Processor carries out Processing of Personal Data within the EU/EEA. - See the list of subprocessors for details about the subprocessors' Processing.
Duration of the Processing	Processing of Personal Data will take place during the period of validity of the Agreement and for a limited period thereafter in accordance with the DPA. The Processor shall co-operate with the Controller to determine how long the Personal Data shall be stored at the Controller.

Appendix B – Technical Security Measures

Lime shall implement and maintain the following security measures:

Information Security Management System (ISMS)	Lime maintains an ISMS aligned with ISO 27001, covering key areas of its operations. Security policies and procedures—including risk management, incident response, business continuity, and supplier security—are reviewed regularly and subject to internal and external audits.
Organizational Security and Governance	Lime has a designated Security Officer and established governance structure to oversee security operations. Employees are required to complete mandatory security training upon onboarding and on an annual basis.
Access Controls	Access to systems and data is granted based on least privilege and job role requirements. Access requests must be approved by system owners, and regular access reviews are conducted. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) are enforced across key systems.
Password Management	Lime enforces a minimum password length of eight (8) characters with defined complexity requirements. Passwords must not be reused or stored in readable format. Sharing of credentials is prohibited.
System Monitoring and Logging	Lime logs access and system activity across key services. Alerts and automated triggers are configured to detect deviations or suspicious behaviour, supporting incident detection and analysis.
Incident Management	Lime has a documented and tested Incident Response Plan. All incidents are classified by severity and handled by relevant teams. Customers are notified without undue delay of detection if an incident impacts their data.
Backups, Business Continuity and Disaster Recovery	Lime maintains Business Continuity and Disaster Recovery Plans for critical systems. Daily immutable backups are retained for up to 90 days (extendable to maximum 365 days).
Device and Endpoint Security	Company devices are centrally managed and configured with encryption, anti-malware software, and firewalls. Only compliant devices may access Lime's services.
Supplier Security	Lime assesses suppliers during onboarding and on a recurring basis. Suppliers with access to Lime's data or systems must meet defined security and compliance requirements.
Cloud Security and Data Hosting	Lime CRM (SaaS) is hosted on Amazon Web Services (AWS), which maintains industry-leading physical and environmental controls and holds multiple security

	certifications. Data is encrypted in transit using TLS 1.2/1.3 and at rest using AES-256 encryption.
Secure Development Practices	Lime follows a secure software development lifecycle (SDLC) that includes risk assessments, code reviews, vulnerability scanning, and separation of development, testing, and production environments. Developers are trained in secure coding practices, including OWASP Top 10 awareness.
Penetration Testing	Lime cloud services undergo annual penetration testing by independent third parties.
Logging and Audit Trails	Key activities in Lime cloud services and supporting infrastructure are logged, including access and data changes. Customers may request log excerpts for investigations.
Identity and Access Management	Authentication to Lime CRM supports Single Sign-On (SSO) via Microsoft Entra ID or other OIDC providers, with support for MFA when configured via external identity systems.
Product Security and Patch Management	Lime regularly updates its cloud services with security patches and improvements. Automated tooling is used to manage dependencies and identify known vulnerabilities.