Data Processing Addendum (DPA)

This Data Processing Addendum supplements the Userlane Master Subscription Agreement / Terms of Service concluded by and between the Customer (referred to as "Customer" or "Controller" hereinafter) and Userlane GmbH, Rosenheimer Str. 143c (10th floor), 81671 Munich, Germany (referred to as "Processor" hereinafter).

Preamble

This Data Processing Addendum (hereinafter: "Agreement" or "DPA") specifies the contractual parties' obligations under data protection law resulting from the Processor´s data processing on behalf of the Customer based on Userlane Master Subscription Agreement / Terms of Service (hereinafter: "Main Contract") concluded between the parties.

Section 1 Object of the DPA; Controller Instructions

(1) The Processor processes the Customer's personal data. Type and purpose of this data processing can be consulted in Schedule 1 of this Agreement and in the Main Contract.

(2) The Customer is authorised to issue instructions to the Processor regarding the data processing. In principle, instructions are to be issued in text form. If, on an exceptional basis, instructions are given verbally, they are to be subsequently documented in writing in text form without delay by the Customer. The Processor and all the Processor´s subordinates with access to personal data may only process the data that are the object of this Agreement further to the Customer's instruction, including the powers granted in this Agreement, unless they are legally obliged to do the processing. The Processor shall inform the Customer without delay if they believe that an instruction violates data protection regulations. The Processor shall be entitled to defer the execution of the instruction in question until such time as it is confirmed or changed by the Customer.

Section 2 Obligations of the Processor

(1) The Processor shall structure in-house organisation in a manner complying with data protection requirements. Processor shall enact technical and organisational measures that meet the requirements of the General Data Protection Regulation (Art. 32 GDPR).

(2) In executing the work, the Processor shall only use employees that have been familiarised with the relevant data protection regulations and properly obligated to maintain secrecy (Art. 28 Para. 3 Clause 2 lit. b and Art. 29 GDRP).
(3) In Schedule 2, the Processor has documented the implementation of the technical and organisational measures needed for the specific performance of this Agreement. The Customer is familiar with these technical and organisational measures and is responsible to evaluate that these measures are offering adequate risk protection for the data to be processed.
(4) The technical and organisational measures are subject to technical progress and development. The Processor is permitted to implement adequate alternative measures assuming that the security level of the measures according to Schedule 2 may not be undercut. Important changes are to be documented.
(5) The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR. This includes responding to data subjects' inquiries concerning either the Controller's information obligation, their right of access, their right of rectification, erasure, restriction of processing, data portability and related communication obligations of the Controller, or the right to object to automated decisions, including profiling, if the data subject asserts any such rights. Furthermore, the Processor will assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Processor.
(6) Where a data subject contacts the Processor with one of his rights under Chapter III GDPR, Processor may only provide information about personal data from the contractual relationship after prior instruction in accordance with Section 1 of this Agreement or upon prior approval by the Controller.
(7) Contact details of the Processor´s data protection officer and the internal representative are mentioned in Schedule 3.

Section 3 Customer and Supervisory Authority Controls

(1) If, on a case-by-case basis, it should become necessary for the Customer to inspect the technical organisational measures, such inspections will be conducted during normal

working hours, without disturbance to operations, further to prior notification and allowing for an appropriate lead time.

(2) The Processor may make inspection contingent upon the signing of a confidentiality agreement regarding the data of other customers, and the technical and organisational measures established, if the Customer does not commission an investigator who is under a secrecy obligation for legal reasons and/or for reasons of professional law.

(3) If the investigator commissioned by the Customer is in competition with the Processor, the Processor shall have veto power.

(4) If a data protection supervisory authority or another of the Customer's sovereign supervisory authorities wants to inspect the data processing, the Processor will support the Customer. The above paragraphs apply accordingly.

Section 4 Correction, Restriction, and Deletion of Data

(1) The Processor may only delete or restrict the processing of the data to be processed under the terms of this Agreement if this is provided for in the Main Contract or in this Agreement or if the Customer issues a corresponding instruction. If a data subject addresses the Processor directly with a wish for deletion, this request shall be transmitted without delay to the Customer by the Processor.

(2) After the end of this DPA, all personal data that are the object of this Agreement shall either be deleted or returned by the Processor, at the Customer's request, to the extent that there are no obligations for storage of the personal data under applicable statutory provisions.

(3) Copies or duplicates of the data will not be issued without the Customer's knowledge. Processor is entitled to create backups, to the extent needed to ensure proper data processing. Processor is also entitled to process data needed to meet statutory retention requirements.

Section 5 Subcontractors

(1) In terms of this provision, sub-contractual relations entail those services that relate directly to provision of the main service. This does not include ancillary services availed of by the Processor, e.g., as telecommunications services, postal/transport services, maintenance and user service, or disposal of data carriers, as well as other measures to

ensure the confidentiality, availability, integrity, and capacity of the hardware and software of the data processing equipment. However, in order to ensure the protection and safety of the Customer's data in outsourced ancillary services as well, the Processor is bound to conclude appropriate and legally compliant contractual agreements and to take control measures.

(2) The Processor may only commission sub-contractors (additional contract processors) with the prior approval of the Customer, or pursuant to information from the Customer that corresponds to the requirements of Art. 28 Para. 2 s.2 GDPR. Consent shall be deemed to have been granted and the new subcontractors shall be deemed to have been approved if the Customer does not object either in writing or by e-mail within one month of receipt of the notice of amendment. The Customer will be particularly informed of this consequence by the Processor as part of the notification of amendment. The Customer hereby approves the subcontractors named in www.userlane.com/subprocessors.

(3) If the Customer objects against any new subcontractor, the Processor is not allowed to include this subcontractor in processing Customer´s data. As a consequence of Customer's objection Parties shall be entitled to terminate the Main Contract with a one-month notice period without Processor being obliged to refund any paid license fees.

Section 6 Remuneration

Remuneration for all of the Processor's activities is not part of this Agreement but is based solely on the Main Contract.

Section 7 Term

This Agreement shall apply in this form upon signature of the Main Contract. This Agreement shall end upon the full implementation of the measures described in Schedule 1, without requiring a notice of termination by one of the parties, or with the end of the Main Contract.

Section 8 Final provisions

(1) Changes and supplements to this DPA require written form or text form. This shall also apply to a waiver of this form requirement.

(2) This Agreement shall also apply if and insofar as authorities or courts deviate mutatis mutandis from a joint responsibility of the contracting parties pursuant to Art. 26 GDPR.

Schedule 1: Subject Matter, Type, and Scope of Data

1. Subject Matter

Userlane provides a Digital Adoption Platform as a Cloud Software as a Service to help users to use Customer Applications by providing in-app assistance. For more details see the Main Contract.

2. Data Subjects

Processor processes personal data of the users of the Software. This can be

- Admin Users (persons who are entitled to manage content and configuration of Userlane) or
- End Users (persons who use the Customer Application together with Userlane's in-app assistance (content edited by Admin users) and who can be e.g. Customer's clients, prospective clients and/or Customer´s employees).

3. Scope, Type, and Purpose of Data Processing

In the context of this DPA, personal data are processed by the Processor within the meaning of Art. 4 no. 2 GDPR. In particular, these are the collection, recording, organization, arranging, storage, adaptation or modification, reading out, querying, use, disclosure by transmission, dissemination, or any other form of provisioning, matching or linking, restriction, deletion or annihilation. Furthermore, type and purpose of processing of personal data by the Processor are described in detail in the Main Contract. Subject matter of the processing of personal data are the following types/categories of data (list/description of data categories)

Function of processed data category	Data categories processed by Processor if data subject is an Admin User	Data categories processed by Processor if data subject is an End User
Identifier	Email address	ID **Optional***: email address
Metadata for secure operation of systems	IP address, URL, browser type and version, time zone and language settings of users.	
Custom attributes	Roles & Permissions, Login information	**Optional***: Attributes that are defined by Customer
Interaction data of User with Userlane	Audit log of changes made to configuration and content elements	Usage of Userlane content elements (e.g. Guide played, Announcement seen, ...)
Interaction data of User with Customer Application		**Optional***: Usage of specifically defined features in Customer Application **Optional***: Interactions (e.g. page visits, clicks) in Customer Application

** Optional features and data fields can be enabled or configured by the Customer.*

4. Place of Processing

The provision of the contractually agreed data processing generally takes place in a Member State of the European Union (EU) or in another Contracting State to the Agreement on the European Economic Area (EEA). The Processor is nonetheless permitted to process personal data outside the EEA in compliance with the provisions of this Agreement if he informs the Controller in advance of the place of data processing and if the requirements of Art. 44 et seq. GDPR are met. Section 5 para 2 applies accordingly.

Schedule 2: Technical and organizational measures

I. Physical Access Controls

Unauthorised persons must be denied physical access to data processing equipment with which personal data are processed or used.

Securing the company premises - demarcation:

The company premises / business premises are demarcated from the public area by:

- Office in larger building complex
- Lockable door

Access control system:

A centrally managed access control system is used in the company.

Access control system - Lockable rooms:

All rooms in the company where access to personal data is possible are lockable.

Access control system - visitor registration:

In the company, the presence of visitors is registered via:

- Visitor passes

Access control system - technical means:

The access control system is based on the following technical means:

- Chip card

Access control system - administration:

The access control system is managed as follows:

- Electronically

II. Logical Access Control

Unauthorised persons shall be denied access to data processing equipment with which personal data are processed or used.

Access to Personal Data in Visitor Areas:

It is ensured that personal data in the company is not freely accessible in visitor areas.

Password Manager:

A password manager is used in the company.
The following password manager is used:

Password Manager - Access Control:

The used password manager offers sufficient access control and encrypted storage.

Portable Terminal Devices - Access Control:

Terminal devices in the company have access control (password, PIN, pattern, etc.).

Single Sign-On Procedure:

A single sign-on procedure is used in the company.

Storage of Sensitive Information:

Employees were instructed to lock personal data up when leaving their workplace in the company (so-called Clean-Desk-Policy).

Two-Factor-Authentication:

Two-factor authentication is used in the company.

Two-factor Authentication for Single Sign-On:

Two-factor authentication is used to log in using single sign-on in the company.

III. Data Access Control

It must be ensured that persons authorised to use a data processing system can only access the data according to designated access permissions.

Allocation of Access Authorisations:

The assignment of access authorisations in the company is based on the functions of the authorised users.

Departing Persons - Withdrawal of Authorisations:

All access authorisations and access rights of a departing person are blocked/deleted promptly.

IV. Data Carriers Control

Data carriers should not be read, copied, changed or removed without authorisation.

Dara Carrier Management - Access Protection:

Data carriers in need of protection and collected for disposal are protected against unauthorised access in the company.

Data Carrier Management - Inventory List:

Inventories for the following data carriers are kept in the company:

- Laptops
- Cell phones
- Tablets

Workplace - Sealable Containers:

There are lockable containers available at every workplace to securely store documents and data carriers in the company.

V. Communication Control

It must be possible to determine and establish where personal data can be transmitted by data transmission equipment.

Connection to the Telecommunications Provider:

The following method is used to connect to the telecommunications provider:

- Regular DSL/fibre optic connection

VI. Transmission Control

It is necessary to prevent unauthorised reading, copying, modification or deletion of data during the transfer of personal data or during the transport of data carriers.

Data Transmission - Data Carriers:

No data carriers with personal data are transmitted.

Encryption of Transmission:

Data is encrypted during transmission using the following procedures/protocols:

- SSL/TLS
- WPA2

VII. Input control

It must be ensured that it can be subsequently checked and determined whether and by whom personal data have been entered into data processing systems, changed or removed.

Logging - Processing of Personal Data:

Processing of personal data in the company gets logged.

VIII. User Control

It must be prevented that data processing systems can be used by unauthorised persons using data transmission devices.

Administrators - Consistent Accounts:

Administrator accounts are used at the following level in the company:

- Database
- Application

Administrators - Special Accounts:

Special administrator accounts are used in the company.

Blocking Access to Hardware Interfaces:

The access to hardware interfaces of relevant terminal devices is blocked in the company.

Departing Persons - Reclaiming Company Owned Property:

All company-owned property containing personal data are reclaimed of a departing person.

Employee Training:

The following measures are taken to make employees aware of the importance of data protection and to oblige with them in accordance with the requirements:

- Commitment of employees to rules of conduct
- Obligation of employees to maintain data secrecy

IX. Service Provider Control

It must be ensured that personal data processed under contract can only be processed according to the instructions of the client.

External Service Provider - Remote Maintenance:

No remote maintenance is carried out by the company.

External Service Providers:

The company does not work with external service providers.

X. Storage Control

Unauthorised entry into storage systems as well as unauthorised access to, modification or deletion of stored personal data shall be prevented.

Password Protection - Password List:

No unencrypted password list is kept.

Professional Disposal of Personal Data:

Employees in the company are required to dispose of personal data properly.

XI. Availability control

It must be ensured that personal data are available at all times and are protected against accidental destruction or loss.

Archiving Concept:

An archiving concept is defined that regulates how and for how long documents are archived.

Archiving Concept - Legal Retention Obligation:

There is a legal storage obligation for the archived documents.

XII. Reliability

It must be ensured that personal data is secured against accidental loss or destruction.

Critical Systems - Redundancy:

Critical systems and the infrastructure are designed redundantly.

Penetration Tests:

In order to test the resilience of the IT systems, regular penetration tests on IT-systems that simulate high loads have been carried out in the company.

Penetration Tests - Improvement Measures:

On the basis of penetration tests carried out in the past, recommended improvement measures have been implemented in the company.

Penetration Tests - Regularity:

In order to test the resilience of the IT systems, regular penetration tests on IT-systems are carried out that simulate high loads in the company.

XIII. Data Recovery

It is necessary to ensure that personal data can be quickly restored in the event of a physical or technical incident.

Backups:

Backups in the company are performed by cloud provider

XIV. Separability

It has to be ensured that data collected for different purposes can be processed separately.

IT Security - Particularly Sensitive Personal data:

A dedicated and separated network is used for particularly sensitive categories of personal data.

Segregation of Workplaces:

Workplaces where particularly sensitive personal data is processed are physically separated from other workplaces.

XV. Operating system

Unauthorised individuals must be prevented from gaining access to operating systems.

Operating system - Authorisation Concept for Test and Development Environments:

An authorisation concept in test and development environments has been implemented in the company.

Password Protection - Initial Passwords:

Initial passwords must be changed at the first login in the company.

Password Protection - Password Complexity:

There is a default for password complexity in the company.

Password Protection - Password Length:

There is a default for the password length in the company.
The password has a length of at least 8 characters.

Password Protection - User Account:

Each user account of the operating system in the company is protected by a password.

XVI. Applications

It has to be prevented, that unauthorised persons gain access to any applications.

Software - Separation between Environments:

Productive, test and development environments including the data bases are separated from each other in the company.

Schedule 3: Data Protection Contact Details

Data Protection Coordinator

Name	Marina Hoffmann (Information Security Officer)
Email	dpo@userlane.com

Data Protection Officer

Company	DataCo GmbH represented by the managing director Thomas Regier Dachauer Str. 65 80335 Munich Germany www.dataguard.de
Phone	+49 89 740045840
Email	datenschutz@dataguard.de