

Agreement on Order Processing acc. to Art. 28 GDPR

between

.....

- the Data Controller - hereafter referred to as the Client -

and

Propertybase GmbH, Landwehrstr. 63, 80336 München (Munich), Germany

- the Processor - hereafter referred to as the Contractor -

1. Subject Matter and Duration of the Order

(1) Subject Matter

The subject matter of the order is based on the Master Services Agreement concluded between the Client and the Contractor, to which reference is made here (the Master Services Agreement is hereafter referred to as the "Service Agreement").

(2) Duration

The duration of this order (term) corresponds to the term of the Service Agreement.

2. Concretisation of the Content of the Order

(1) Type and purpose of the intended processing of data

The type and purpose of the processing of personal data by the Contractor for the Client are specifically described in the Service Agreement . In addition to this, the parties hereby state the following: The purposes of the processing are in particular: (i) the processing of personal data in accordance with the Service Agreement for the provision of the services specified therein; (ii) the processing of personal data initiated by the Client or the users authorised by the Client; (iii) the processing of personal data initiated by other documented instructions of the Client, e.g. instructions issued by email.

The Contractor shall provide the Client with a CRM system (Propertybase). This is used by the Client for communication, file management, file storage and for the documentation and backup of documents within the framework of the Client's Client relations. The Contractor takes over the hosting, maintenance and support of the users. Access to personal data of the parties concerned is not excluded in this case.

(2) The contractually agreed data processing is provided partly in a Member State of the European Union or in another state which is party to the Agreement on the European Economic Area, partly in third countries. Processing in third countries is mainly carried out by the subcontractors commissioned by the Contractor (see also Article 6 of this Agreement).

The Client consents to the processing in third countries insofar as this relates to the following processing operations:

- Processing on the technical systems and platforms of the subcontractor **salesforce.com, Inc.** and the companies affiliated with it, as set forth in Article 6 (7) Table 1 of this Agreement. In this respect, the special requirements of Art. 44 ff. of the GDPR are fulfilled. The adequate level of protection in the USA and other third countries
 - is established with regard to processing in the USA by an adequacy decision of the Commission (Art. 45 para. 3 GDPR) and by the self-certification of the subcontractor according to the EU/US Privacy Shield;
 - is established with regard to the processing in the USA and other third countries by binding internal data protection regulations – Binding Corporate Rules (Art. 46 para. 2 section b in conjunction with Art. 47 of the GDPR);
 - is established with regard to the processing in the USA and other third countries by means of standard data protection clauses (Art. 46 para. 2 sections c and d of the GDPR)
- Processing on the technical systems and platforms of **other subcontractors** listed in Article 6 para. 7 Table 2 of this Agreement. In this respect, the special requirements of Art. 44 ff. of the GDPR are fulfilled. The adequate level of protection in the USA and other third countries
 - is established with regard to processing in the USA by an adequacy decision of the Commission (Art. 45 para. 3 GDPR) and by the self-certification of the subcontractor according to the EU/US Privacy Shield.
 - is established with regard to the processing in the USA and other third countries by binding internal data protection regulations – Binding Corporate Rules (Art. 46 para. 2 section b in conjunction with Art. 47 of the GDPR).

(3) Type of data

The subject of the processing of personal data is the following data types/categories (list/description of the data categories)

- Personal master data (first name, surname, title, position, employer, date of birth)
- Account data
- Registration data

- Communication data (e.g. company, telephone, email, postal address)
- Authorisation data (access data, user name, password)
- Contract master data (contractual relationship, interest in a product or contract)
- Client history
- Usage data
- Log files
- Data from social networks
- Analysis data
- Communication and connection data
- ID data of devices
- Localisation data
- Contract billing and payment data
- Planning and control data
- Report data (from third parties such as credit agencies or from public directories)
- Image data
- Text files
- If applicable, further data which is processed by the Client in Propertybase.

(4) Categories of the persons concerned (data subjects)

The categories of the data subjects affected by the processing include:

- All individuals whose data is processed by the Client in Propertybase.

3. Technical and organisational measures

(1) The Contractor must document the implementation of the required technical and organisational measures set out in advance of the award of the contract before the start of processing, in particular with regard to the specific execution of the order, and hand these over to the Client for review. Upon acceptance by the Client, the documented measures shall become the basis of the order. If the Client's review/audit results in a need for adjustment, this shall be implemented by mutual agreement.

(2) The Contractor shall provide the security pursuant to Art. 28 para. 3 section c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 of the GDPR. Overall, the measures to be taken are data security measures which are taken to ensure a level of protection that is appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. On this point, the state of the art, the costs of implementation and the nature, scope and purposes of the processing, as well as the varying likelihood of occurrence and severity of the risk for the rights and freedoms of natural persons in the sense of Art. 32 para.1 of the GDPR must be considered [for details see **Appendix 1**].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative appropriate measures. The safety level of the specified measures must be fulfilled. Significant changes are to be documented.

4. Correction, restriction and deletion of data

(1) The Contractor may not rectify, delete or restrict the processing of the data which is processed on behalf of the Client without authorisation, but only in accordance with the documented instructions of the Client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall immediately forward this request to the Client.

(2) Insofar as they are included in the scope of services, the deletion concept, the right to be forgotten, rectification, data portability and information according to the Client's documented instructions are to be ensured by the Contractor directly.

5. Quality assurance and other obligations of the Contractor

In addition to the obligation to comply with the terms set out in this order, the Contractor has statutory obligations under Art. 28 to 33 of the GDPR; in this respect, the Contractor ensures compliance with the following requirements in particular:

- a) Written appointment of a Data Protection Officer who carries out his/her work in accordance with Art. 38 and 39 GDPR. Dr. Michael Karger, Martiusstr. 5, 80802 Munich, tel. +49 (0)89/38367880 has been appointed Data Protection Officer at the Contractor. Any change of Data Protection Officer shall be notified to the Principal without delay.
- b) The maintenance of confidentiality in accordance with Art. 28 para. 3 sentence 2 section b, 29, 32 para. 4 of the GDPR. In carrying out the work, the Contractor shall exclusively use employees who are bound to confidentiality and who have previously been familiarised with the relevant data protection provisions. The Contractor and any person under the Contractor's authority who has access to personal data may only process such data exclusively in accordance with the instructions of the Client, including the powers granted in this Contract, unless they are legally obliged to process it.
- c) The implementation of and compliance with all technical and organisational measures required for this order in accordance with Art. 28 para. 3 sentence 2 section c, 32 of the GDPR [for details see **Appendix 1**].
- d) On request, the Client and the Contractor shall work together with the supervisory authority in the performance of their tasks.
- e) The immediate supply of information from the Client about control procedures and measures taken by the supervisory authority insofar as they relate to this order. This also applies insofar as a competent authority is conducting an investigation within the context of an administrative offence or criminal procedure with regard to the processing of personal data on behalf of the Client.
- f) If the Client is itself subject to an inspection by the supervisory authority, administrative or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the processing of personal data on behalf of the Client by the Contractor, the Contractor shall support the Client to the best of its ability.

- g) The Contractor shall regularly monitor the internal processes and the technical and organisational measures to ensure that the processing within its area of responsibility is carried out in accordance with the requirements of the applicable data protection legislation and that the rights of the data subject are protected.
- h) Verifiability of the technical and organisational measures taken with respect to the Client within the scope of its control powers according to Article 7 of this Agreement.

6. Subcontractor Relationships

(1) As a matter of principle, the commissioning of subcontractors to process the Contractor's data requires either the separate approval of the Contractor in a specific case or general approval (Art. 28 para. 2 GDPR). In any case, the Contractor must ensure that it carefully selects the subcontractor, taking into account in particular the suitability of the technical and organisational measures implemented by the subcontractor within the meaning of Art. 32 GDPR. The relevant documents for selection procedure are to be made available to the Client on request.

(2) A subcontractor relationship requiring approval is deemed to exist if the Contractor commissions further Contractors with the entire or part of the service to be performed under the Service Agreement. Services which are not considered subcontractor relationships within the meaning of this provision are those which the Contractor avails itself of from third parties as an ancillary service in order to obtain support with the execution of the order. These include, for example, telecommunications services, maintenance and user service (if the Client's data cannot be accessed), cleaning staff, inspectors or the disposal of data carriers. However, the integration of waste disposal companies is subject to compulsory notification if the main aspect of the commissioning process includes the disposal of documents/data carriers which contain the Client's data. The Contractor shall, however, also conclude appropriate and legally-compliant contractual agreements in the case of outsourced ancillary services and take the necessary control measures in order to ensure the protection and security of the Client's data.

(3) In cases where subcontractors are commissioned, the Contractor must contractually ensure that the arrangements agreed between itself and the Client also apply to subcontractors.

(4) The Contractor shall be liable to the Client for ensuring that the subcontractor complies with the data protection obligations which have been imposed upon it by the Contractor in accordance with the present section of the contract.

(5) The Client hereby grants general permission to the effect that the Contractor may avail itself of the services of additional or other subcontractors. However, the Contractor shall inform the Client of any intended change with regard to the involvement or replacement of a subcontractor, either by informing the named contact person of the Client or by publishing a list of all subcontractors which are used, no longer used and newly added. The Client may object to such changes within a period of seven days. If there is an important reason pursuant to data protection law for the objection and the parties do not reach an amicable solution on how to proceed, the Contractor shall endeavour to offer the Client a change in performance

or to recommend an economically reasonable change to the configuration or the use of the services in order to avoid the processing of personal data by the rejected subcontractor without placing a disproportionate burden on the Client. If the Contractor is unable to make a corresponding replacement available within a reasonable time (at the latest within 30 days) or the Client rejects the offered change in performance, each of the parties shall be entitled to terminate the services concerned with regard to those services which cannot be provided by the Contractor without the use of the rejected subcontractor. Termination shall require a written declaration to the Contractor. In this case, the Contractor shall reimburse the Client for remuneration paid in advance for the remaining term of the contract concerned on a pro rata basis with regard to the discontinued services.

(6) The subcontractors specified in Article 6 (7) Table 1 and Table 2 of this contract are already engaged in the processing of data on behalf of the Contractor to the extent specified therein at the time of the conclusion of this contract. With respect to such subcontractors, the Contractor shall provide proof upon request that the stated conditions for the commissioning of these subcontractors as set out in this Article 6 have been complied with. The Client hereby declares its agreement to the Contractor that it accepts the commissioning of the subcontractors named in Table 1 and Table 2.

(7) The Client agrees to the assignment of the following subcontractors on condition of a contractual agreement in accordance with Art. 28 para. 2-4 and Art. 44 et seq. of the GDPR:

Table 1: Subcontractor salesforce.com Inc. and its affiliates		
Subcontractor's Firm	Address/Country	Service
salesforce.com, Inc.	Salesforce.com, Inc., The Landmark @ One Market St., Suite 300 San Francisco, California 94105 USA	Core Data Store of Propertybase Clients, Platform, OEM Services
salesforce.com EMEA Limited	England and Wales	If applicable, integrated into the services of salesforce.com Inc.
Kabushi Kaisa Salesforce.com	Japan	If applicable, integrated into the services of salesforce.com Inc.
Salesforce.com Singapore Pte Ltd.	Singapore	If applicable, integrated into the services of salesforce.com Inc.
Salesforce.com Canada Corporation	Canada	If applicable, integrated into the services of salesforce.com Inc.
SFDC Australia Pty Ltd	New South Wales, Australia	If applicable, integrated into the services of salesforce.com Inc.
Demandware, LLC	USA	E-Commerce Platform and Online Shop
Krux Digital LLC	USA	Data Management Platform

Heroku, Inc.	USA	Email Processing, PDF Processing, Portal Publishing
--------------	-----	---

Table 2: Additional subcontractors		
Subcontractor's firm (others)	Address/Country	Service
Amazon.com, Inc.	Amazon.com, Inc. 2021 Seventh Ave Seattle, Washington 98121 USA	Amazon Web Services, Image Store
Basecamp, LLC	Basecamp, LLC 30 N. Racine Ave, Suite 200 Chicago, Illinois 60607, USA	Project Management
Bugsnag, Inc.	Bugsnag, Inc. 939 Harrison St, San Francisco, CA 94107, USA	Automated Crash Detection Platform
CampaignMonitor	Level 38, 201 Elizabeth Street, Sydney, NSW 2000, Australia	Mass Email Service
Digital Ocean, LLC	Digital Ocean, LLC 101 Avenue of the Americas New York, New York 10013, USA	Image Processing
GitHub, Inc.	GitHub, Inc. 88 Colin P Kelly Jr Street San Francisco, California 94107, USA	File Hosting for Software Development
Mailgun	535 Mission St. – 14th Floor San Francisco, CA 94105 USA	Mass Email service
Mandrill	The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000	Mass Email service

	Atlanta, GA 30308 USA	
Mixpanel, Inc.	Mixpanel, Inc. 405 Howard St., Flr 2, San Francisco, CA 94105, USA	Business Analytics Service
Papertrail	7171 Southwest Parkway Bldg 400 Austin, Texas 78735 USA	Logging Management
Propertybase AUS	167 Macquarie Street, Level 13 NSW, Sydney	Customer Service
Propertybase, Inc.	Propertybase Inc., 2560 28th Street, #202, Boulder, CO 80301, USA	Customer Service
Sendgrid	SendGrid, Inc. 1801 California Street, Suite 500 Denver, Colorado 80202, USA	Email Transmission
Slack Technologies, Inc.	Slack Technologies, Inc. 500 Howard Street San Francisco, California 94105, USA	Online Workplace Productivity Tools and Platform
Tableau Software, Inc.	Tableau Software, Inc. Tableau Software 837 N. 34th St. Ste. 200, Seattle, WA, USA	Visualization of Data, Reporting
Zendesk, Inc.	Zendesk, Inc. 1019 Market Street, 6th Floor San Francisco, California 94103, USA	Help Center, Support
Zoom.us	San Jose Office 55 Almaden Boulevard, 6th Floor, San Jose, CA 95113	Screensharing for clients and prospects

7. Control Rights of the Client

(1) The Client has the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors, who are to be appointed in individual cases. The Client has the right to conduct random checks for which, as a rule, notification is to be provided in good time in order to ensure compliance with this Agreement by the Contractor in its business operations.

(2) The Contractor shall ensure that the Client can assure itself of the Contractor's compliance with the obligations pursuant to Art. 28 GDPR. The Contractor undertakes to furnish the necessary information to the Client on request and to provide proof in particular of the implementation of the technical and organisational measures.

(3) Proof of such measures which not only relate to the specific order can be provided at the discretion of the Contractor, in particular by

- compliance with approved rules of conduct in accordance with Art. 40 GDPR;
- certification according to an approved certification procedure in accordance with Art. 42 GDPR;
- current certificates, reports or report extracts from independent bodies (e.g. auditors, auditing departments, data protection officer, IT security department, data protection auditors, quality auditors);
- appropriate certification by means of an IT security or data protection audit (e.g. pursuant to BSI basic protection – "BSI-Grundschutz").

(4) The Contractor can assert a claim for remuneration for enabling the Client to carry out inspections.

8. Notification in the Event of Breaches by the Contractor

(1) The Contractor shall support the Client in complying with the obligations referred to in Articles 32 to 36 of the GDPR concerning the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, among other things,

- a) ensuring an appropriate level of protection by means of technical and organisational measures that take into account the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a possible legal infringement due to security vulnerabilities and make an immediate identification of relevant violations possible;
- b) the obligation to report violations of personal data to the Client without delay;
- c) the obligation to support the Client within the context of its duty to inform the data subject and to make all relevant information available to the Client in this connection without delay;
- d) supporting the Client with its data protection impact assessment;
- e) supporting the Client as part of prior consultations with the supervisory authority.

(2) The Contractor may claim compensation for support services which are not included in the Service Agreement or not attributable to misconduct on the part of the Contractor.

9. Client's Authority to Issue Directives

(1) The Client shall confirm verbal instructions without delay (at least in text form).

(2) The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the Client.

10. Deletion and Return of Personal Data

(1) Copies or duplicates of the data shall not be made without the knowledge of the Client. This shall not apply to backups if these are necessary to ensure proper data processing, as well as data that is required in order to comply with legal retention obligations.

(2) After the completion of the contractually agreed work or earlier at the request of the Client – at the latest upon the termination of the Service Agreement – the Contractor shall hand over to the Client all documents, processing and usage results created and data stocks in its possession that are associated with the contractual relationship or destroy them in accordance with data protection regulations after prior consent. The above also applies to test and rejected material. The deletion log shall be presented upon request.

(3) Documentation that serves as proof that data processing is carried out in compliance with the order and in a proper manner shall be stored by the Contractor beyond the end of the Agreement in accordance with the respective retention periods. The contractor can hand such documentation over to the Client for the purposes of discharge at the end of the Agreement.

11. Other Provisions

(1) The provisions of the Service Agreement for limiting the Contractor's liability shall also apply to this Agreement.

(2) Insofar as the Client's data stored by the Contractor is at the risk of being seized or confiscated, placed at risk by insolvency or composition proceedings or by other measures, the Contractor shall inform the Client thereof immediately. The Contractor shall immediately inform all parties responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the "data controller" within the meaning of the General Data Protection Regulation.

(3) Amendments and supplements to this Agreement and all its components must be in the form of a written agreement, which can also be made in electronic format (text form), and the express indication that this is a change to or supplementation of these conditions. This also applies to the waiver of the written form requirement.

(4) In the event of any contradictions, the provisions of this Agreement on data protection shall take precedence over the provisions of the Service Agreement on data protection. Insofar as individual parts of this Agreement are invalid, this shall not affect the validity of the remaining parts of this Agreement.

(5) German law shall apply exclusively to this Agreement and all questions and disputes associated with it, to the exclusion of all legal norms that refer to a different legal system.

Munich - October 25, 2018

.....
Place/date

DocuSigned by:
Max-Michael Mayer
.....56BAAE8C0160412.....
Max-Michael Mayer (Managing Director)

.....
Name/Position (in block letters)

DocuSigned by:
Michael Wenglein
.....774D2B47B47D4DD.....
Michael Wenglein (Managing Director)

.....
Signature on behalf of the Client

Appendix 1 – Technical and Organisational Measures

Salesforce und Heroku: https://help.salesforce.com/articleView?id=Salesforce-Services-Trust-and-Compliance-Documentation&type=1&language=en_US

1. Pseudonymisation and encryption (Art. 32 para. 1 (a) GDPR)

- Pseudonymisation (Art. 32 para. 1 section a GDPR; Art. 25 para.1 GDPR)
As the contract processor, the Contractor shall not take any pseudonymisation measures in addition to measures which are carried out on the basis of the respective service descriptions of the products / services or which are taken by the person responsible within the framework of the commissioning.
- Encryption
- secure password management in the encrypted password manager, encryption of data carriers and computers, access exclusively via SSL-encrypted connections

2. Confidentiality (Art. 32 para. 1(b) BDSG)

- Physical access control
No unauthorised access to offices: Key, electric door opener, defined process for key management
- Computer access control
No unauthorised system use, (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers and computers, secure password management in the encrypted password manager
- Data access control
No unauthorised reading, copying, modifying or removal within the system, authorisation concept and needs-based access rights, logging of accesses;
- Separation control
Separate processing of data collected for different purposes: multi-client capable, sandboxing

3. Integrity (Art. 32 para. 1 section b GDPR)

- Transfer monitoring
No unauthorised reading, copying, modification or removal during electronic transmission or transport, access exclusively via SSL-encrypted connections
- Input control
Determining if and by whom personal data in data processing systems has been entered, modified or removed. Logging and document management.

4. Availability and resilience (Art. 32 para. 1 section b GDPR)

- Availability control
All data is processed exclusively in highly available cloud services, so that the Contractor is not dependent on any specific hardware or locations.
- Regular checks of the system security of the clients by means of internal audits by software and supervisor.

5. Recoverability (Art. 32 para. 1 section c GDPR)

- Real-time replication of the data in the cloud
- Docker technology for the fastest server recoverability

6. Procedure for regular reviews, assessment and evaluation (Art. 32 para. 1 section d of the GDPR; Art. 25 para. 1 GDPR)

- Data privacy management;
- Incident response management;
- Data protection-friendly pre-settings (Art. 25 para. 2 GDPR);
- Order controls
No data processing on behalf of Client within the meaning of Art. 28 GDPR without corresponding instructions of the Client, e.g.: clear contract design, formalised order management, strict selection of the service provider, prior conviction obligation, follow-up checks.