Data processing agreement

in accordance with

Article 28 of the GDPR

The controller:	The processor:
[*NN*] [*Address*]	**Roomle GmbH** Peter-Behrens-Platz 2 4020 Linz, Austria
(hereinafter referred to as the client)	(hereinafter referred to as the contractor)

1. SUBJECT MATTER OF THE AGREEMENT

(1) The subject matter of this order is the execution of data processing operations in connection with the Roomle platform. Roomle provides a cloud-based web application for room planning and product configuration. This allows end consumers to save their own plans and products on the client's platform for later use via their email address and a password.

(2) The following data categories are processed:
- *Platform users:* email address, password, name (optional), address (optional), date of birth (optional), telephone number (optional), plan and configuration data, favourites, login country, last access, anonymised IP, order details (delivery address, furniture ordered, email address)
- *Licensees:* contact details, contractual details, invoicing details, communication details

(3) The following categories of data subjects are subject to data processing: licensees, Roomle platform users, suppliers, employees and hosting data

2. DURATION OF THE AGREEMENT

The agreement is concluded for an indefinite period of time and may be cancelled by either party.

3. THE CONTRACTOR'S OBLIGATIONS

(1) The contractor shall undertake to process data and processing results solely within the scope defined by the client's written orders. If the contractor is instructed to surrender the client's data to a government authority they must, if permitted by law, inform the client of this immediately and refer the authority to him or her. Likewise, processing the data for the contractor's own purposes shall require a written order.

(2) The contractor declares in a legally binding manner that all persons assigned to data processing tasks have been bound to confidentiality before commencing work or are bound by suitable legal non-disclosure obligations. In particular, the obligation of the persons assigned to data processing to maintain confidentiality shall continue to apply after they leave the contractor's employ or after termination of their activities.

(3) The contractor declares in a legally binding manner that he or she has undertaken all measures necessary to ensure security of processing pursuant to Article 32 GDPR (details listed in Annex./1).

(4) The contractor shall undertake all technical and organisational measures necessary to allow the client to implement the rights of the affected person defined in Chapter III of the GDPR (the rights to information, communication, rectification, erasure, and data portability, the right to object, and rights related to automated individual decision-making) at any time within the statutory periods and shall provide the client with all the information necessary for this. If an application to this effect is submitted to the contractor and indicates that the person submitting the application has mistakenly assumed that the contractor is the contracting client of the data application in question, the contractor must immediately forward the application on to the client and inform the person submitting the application of this.

(5) The contractor shall assist the client in complying with the obligations specified in Articles 32 to 36 of the GDPR (data security measures, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the affected person, data protection impact assessment, prior consultation).

(6) The contractor is hereby advised that they must create a record of processing activities pursuant to Article 30 of the GDPR for the processing contract in question.

(7) With respect to the processing of data submitted by the client, the client shall be granted the right to inspect and monitor the data processing facilities at any time, or to instruct a third party to do so. The contractor shall undertake to provide the client with any information necessary to monitor compliance with the obligations listed in this agreement.

(8) After termination of this agreement, the contractor is obligated to submit all the results of processing and documents containing data to the client, or to destroy them on his or her behalf. If the contractor processes the data in a specific technical format, they shall undertake to hand over the data either in the same format or, if desired by the client, in the format in which they received the data from the client or in another commonly used format after termination of this agreement.

(9) The contractor shall inform the client immediately if, in his or her opinion, an instruction issued by the client violates the data protection regulations of the EU or EU member states.

4. PLACE OF DATA PROCESSING

All data processing activities are carried out exclusively within the EU or the EAA.

5. SUB-PROCESSORS

The client agrees that the contractor may, in the performance of their contractually agreed services, involve the contractor's associated companies in the performance of these services or subcontract these services out to another company. This applies in particular, but not exclusively, to the maintenance and installation of computer centre infrastructure, telecommunication services, and user services.

If the contractor engages a subcontractor, the contractor shall undertake to assign their obligations arising from this data processing contract to the subcontractor.

[*City*], [*Date*]	Linz, 07.05.2018
On behalf of the client:	*On behalf of the contractor:*
.....	.....
[*Name and role*]	[*Albert Ortig, CEO Roomle GmbH*]

ANNEX./1 – TECHNICAL AND ORGANISATIONAL MEASURES

CONFIDENTIALITY

- Physical access control: internal data processing facilities can only be accessed by administrators with a key.
- Electronic access control: all computers and access points are password - protected. Access to the Google Cloud Services infrastructure has been granted to individual, clearly defined employees. They are tied to our Google Services' authentication system. As soon as a user leaves the company, their account and all other access options are deactivated.
- Internal access control: unauthorised reading, copying, changes or deletions are not possible. Access to the database is password protected. Access to servers is granted only to authorised users via SSH. Both are only accessible via the internal network (password protected VPN if necessary). Assigned access rights are reviewed periodically.
- Pseudonymisation (Article 32(1)a of the GDPR; Article 25(1) of the GDPR): Plans are saved with a PlanID which does not enable access to information about the user. The plan data are stored and made available separately from the user-specific data.

INTEGRITY

- Data transfer control: users cannot view or change their own data until they have logged in. Data are transmitted electronically only in the form of data extracts. This is recorded as a log entry, which can be viewed at any time by our client. It comprises the number of data sets, the date and time of withdrawal, the type of transmission and the intended recipient. All data are transmitted in encrypted form (HTTPS).
- Data entry control: access to our Google data infrastructure via the access console is logged (using logfiles). Records of changes to data sets include the user's IP address and the date of modification.
- Internal systems: can only be accessed by users with administrative functions.

AVAILABILITY AND RESILIENCE

- Availability control:
  - *User data*: automatic database (DB) backups, server monitoring (Dynatrace). Firewall and antivirus protection installed on the application server, load balancer for productive systems. We back the data up onto a parallel system every 15 minutes.
  - *Licensees:* standard processes for changes/switchovers of company-specific data and the licensee's use/licensing of the product when using Roomle platforms and dedicated services (e.g. the order process). Protection from accidental or wilful destruction or loss, e.g. backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS, diesel generator), antivirus protection, firewall, reporting and emergency plans; security checks at the infrastructure and application levels, multi-stage backup strategy in which the backup copies are encrypted and stored in an off-site backup computer centre, standardised processes for changes of employees/employees leaving the company; rapid recoverability;
- Deletion periods:
  - *User data & licensee data*: all data are automatically deleted within 30 days after cancellation of the account/contract.
  - *Logs*: semi-automatic deletion after 90 days.

PROCEDURES FOR REGULAR TESTING, ASSESSMENT AND EVALUATION

- Data protection management: we have commissioned a third-party provider to conduct systemic security tests at irregular intervals. The findings are documented.
- Privacy-enhancing default settings for platform users: all newly created plans are set to private by default (can only be viewed by the creator), users must actively sign up for the newsletter.
- Contract control (platform users): personal data in the Google Cloud: data processing contract. No third-party data processing as defined by Article 28 of the GDPR without corresponding instructions from the client, e.g.: unambiguous phrasing in the contract, formalised order management, strict controls on the selection of the service provider, duty of pre-evaluation, supervisory follow-up checks.