Agreement on Processing of Commissions pursuant to the General Data Protection Regulation (GDPR)

TeamDrive Systems GmbH
Max-Brauer-Allee 50
22765 Hamburg

(Data Importer)

hereby enters into an obligation vis-à-vis

Customer number:

(the Client)

in accordance with the following provisions:

The Contractor shall process personal data on behalf of the Client within the meaning of Art. 4 no. 8 and Art. 28 of Directive (EU) No. 2016/679 (the General Data Protection Regulation, or GDPR). This agreement governs the rights and obligations of the parties relating to the processing of personal data.

Any references to the term “data processing” or “processing” (of data) in this agreement are based on the definition of “processing” within the meaning of Art. 4 no. 2 GDPR.

§ 1 Subject matter and term of the mandate

The mandate relates to the fulfilment of the contract that was concluded between the parties relating to the use of TeamDrive by the Client based on the general terms and conditions of business (the "Main Contract").

The contractually agreed data processing shall only be provided in a member state of the European Union (EU) or in another signatory state to the Agreement on the European Economic Area. Any outsourcing of this agreed data processing and/or parts thereof to a third country requires the prior consent of the Client and may only take place if the specific criteria under Art. 44ff. GDPR are complied with and this compliance is demonstrated to the Client by the Contractor.

The agreement is concluded for an unlimited term. It shall end at the same time as the Main Contract without needing to be formally terminated. The right to terminate the contract for good cause shall remain unaffected.

This agreement shall not be applied insofar as personal data is processed as part of a free or trial version of TeamDrive in accordance with the provisions of the Main Contract.

Moreover, the parties agree that any previous data processing agreements shall come to an end by mutual consent when this agreement enters into force.

§ 2 Scope, nature and purpose of data processing; types of data and data subjects

The Contractor is obliged to process the personal data made available to them exclusively to provide the contractually agreed service.

The Contractor is entitled to create intermediate, temporary or duplicate files required on procedural or security technology grounds to process or use the personal data in order to provide the service unless doing so would modify its content. The Contractor is not permitted to make copies of the personal data without authorisation.

More details on the scope, nature and purpose of data collection, processing and use are provided in the Main Contract specified in § 1.

The nature of the personal data is defined under letter B in Annex 1

The data subjects are listed under letter C in Annex 1

§ 3 Technical and organisational data security measures

(1) The Contractor is obliged to implement technical and organisational measures that are appropriate in relation to the desired protective purpose. A level of security appropriate to the risk shall be ensured, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. This includes, in particular, the provisions of Art. 32 GDPR. The Contractor shall continuously evaluate the appropriateness and effectiveness of the measures taken by them against the provisions of Art. 32 GDPR and shall document the results of this evaluation.

(2) The status of the technical and organisational measures at the time of conclusion of the agreement is enclosed as Annex 2 to this agreement. The parties agree that the technical and organisational measures may need to be modified in order to adapt to technical and legal circumstances. The Contractor will agree any modifications in advance with the Client that could impair the integrity, confidentiality or availability of the personal data or adversely impact the rights and freedoms of the data subjects. Measures that only result in minor technical or organisational modifications and that do not adversely affect the integrity, confidentiality or availability of the personal data can be implemented by the Contractor without consulting the Client. The Contractor shall amend Annex 2 accordingly and shall notify the Client of any amendment to Annex 2 unless the Client has already given its consent. The latest version of Annex 2 shall be made available on the Contractor's website.

§ 4 Rectification, erasure and blocking of data; rights of data subjects

(1) The Contractor shall rectify, erase or block the data being processed under this agreement in accordance with the Client's instructions.

(2) Should a data subject contact the Contractor directly in order to exercise their rights under Chapter 3 GDPR, the Contractor shall refer them to the Client insofar as they are able to do so. If they are not able to do so and the Client is not under any obligation vis-à-vis the data subject in the capacity of controller in accordance with Chapter 3 GDPR, the Contractor shall inform the data subject that they are working as a processor on behalf of third parties and are unable to disclose the identity of the third party to the data subject. If and insofar as the Contractor is under an obligation vis-à-vis the data subject in the capacity of controller in accordance with Chapter 3 GDPR, responsibility for complying with the relevant obligations lies solely with the Contractor in their capacity as controller.

In all other respects, the Contractor shall, to the best of their abilities, help the Client to comply with its obligations under Chapter 3 GDPR with suitable technical and organisational measures if and insofar as the Contractor's cooperation is expedient for this purpose. To this end, the Client shall notify the Contractor in text form of the support measures that it requires and shall, in this respect, disclose to the Contractor the data required to fulfil its request (particularly data for establishing the identity of the data subject and what support measures are desired). If the Contractor needs more information from the Client in order to be able to fulfil its request, they shall make this known to the Contractor in text form without delay. Otherwise, the Contractor shall perform the services required of them within an appropriate period of time.

The Contractor shall be entitled to reasonable remuneration for the services to be performed, which shall be based on the time required. The Contractor shall not make the provision of the services due from them contingent on the Client agreeing to a particular level of remuneration and/or paying it in advance.

§ 5 Obligations of the Contractor and controls to be performed

To implement the agreement, the Contractor shall only use employees or other auxiliary agents who have undertaken to maintain confidentiality and who have been familiarised with data protection requirements in a suitable manner. The Contractor shall take steps to ensure that any natural person acting under their authority who has access to personal data does not process it except on instructions from the Contractor, unless he or she is required to do so by EU law or the law of an EU member state.

Taking account of the nature of processing and the information available to the Contractor, the Contractor shall also, on request, help the Client to comply with its obligations in accordance with Art. 32–36 GDPR, particularly in relation to the security of personal data (security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject) as well as any necessary data protection impact assessment and prior consultations.

Moreover, the Contractor is obliged to comply with the relevant provisions governing the designation of a data protection officer.

The Contractor shall provide the Client on request with their log of procedures covering data processing on behalf of the Client when the Contractor starts work and subsequently every time a change is made.

By means of suitable controls, the Contractor shall ensure that the data to be processed on the Client's behalf shall only be processed in accordance with its instructions, that the outsourced data processing shall be carried out on a mandate-specific basis, separate from other data processing mandates, and that the data processed is kept strictly separate from other data pools.

The Contractor shall be subject to any control measures by the competent statutory data protection supervisory authority and shall notify the Client without delay of such control measures and their outcome insofar as they affect personal data of the Client.

§ 6 Subcontracting

(1) The Contractor is entitled to task the subcontractors listed in Annex 3 to this agreement with the processing of data. Subcontractors may be switched and additional subcontractors commissioned in accordance with the criteria stipulated in paragraph 2.

(2) The Contractor shall select subcontractors carefully and, prior to commissioning them, shall check that they are able to comply with the agreements entered into between the Contractor and the Client. In particular, the Contractor shall monitor – in advance and regularly during the term of this agreement – whether subcontractors have implemented the technical and organisational measures for protecting personal data that are required under the provisions of this agreement and Art. 32 GDPR. If they are planning to switch subcontractors or planning to commission a new subcontractor, the Contractor shall notify the Client in text form in good time, but at least four weeks before the switch of subcontractor or commissioning of the new subcontractor (the "Notification"). The Client shall be entitled to object to the switch of subcontractor or commissioning of the new subcontractor – giving its reasons where possible – in text form within three weeks of receiving the Notification. The Client can withdraw its objection in text form at any time. If an objection is raised, the Contractor can terminate their contractual relationship with the Client, observing a notice period of at least 14 days as at the end of a calendar month, insofar as the switch of subcontractor or commissioning of the new subcontractor was unacceptable to the Client. A switch of subcontractor or commissioning of a new subcontractor could be deemed unacceptable if the Client had reason to fear being disadvantaged and, in particular, if it would no longer be ensured that the provisions of this agreement and the GDPR would continue to be complied with if the action were taken. The Contractor shall take reasonable account of the Client's interests in determining the notice period. If the Client does not raise an objection within three weeks of receiving the Notification, it shall be deemed to have given its consent to the switch of subcontractor or commissioning of the new subcontractor.

(3) The Contractor shall be obliged to obtain confirmation from the subcontractor that it has designated a company data protection officer in accordance with Art. 37 GDPR insofar as the subcontractor is legally obliged to designate a data protection officer.

(4) The Contractor shall ensure that the regulations agreed in this agreement and any supplementary instructions from the Client also apply to the subcontractor.

(5) The Contractor shall conclude a data processing agreement with the subcontractor that complies with the requirements of Art. 28 GDPR. Furthermore, the Contractor shall impose on the subcontractor the same obligations for protecting personal data as have been agreed between the Contractor and the Client. The Client is to be provided with a copy of the data processing agreement on request.

(6) In particular, the Contractor shall be obliged to ensure by means of contractual regulations that the powers of control (§ 7 of this agreement) held by the Client and supervisory authorities also apply vis-à-vis the subcontractor and that

corresponding control rights of the Client and supervisory authorities are agreed. The requirement for the subcontractor to tolerate these control measures and any on-site monitoring must also be contractually agreed.

(7) Services that the Contractor obtains from third parties as a purely ancillary service in order to carry out their business activities are not considered subcontracting within the meaning of paragraphs 1–6. These include cleaning services, pure telecommunications services without a specific link to services that the Contractor performs on behalf of the Client, postage and courier services, transport services and security and surveillance services. However, the Contractor is also obliged to ensure in the case of ancillary services provided by third parties that appropriate precautions and technical and organisational measures have been taken to ensure the protection of personal data. Maintaining and updating IT systems or applications shall be deemed to be subcontracting requiring approval and data processing within the meaning of Art. 28 GDPR if this maintenance and updating affects IT systems that are also used in conjunction with providing services on behalf of the Client and if personal data that is being processed on behalf of the Client can be accessed during such maintenance.

§ 7 Control rights of the Client and cooperation obligations of the Contractor

(1) The Client shall have the right to monitor compliance with the statutory data protection obligations and/or compliance with the contractual regulations agreed between the parties and/or compliance with the Client's instructions in the requisite scope.

(2) The Contractor shall be obliged to provide the Client with information insofar as this is required in order to carry out monitoring within the meaning of paragraph 1.

(3) After giving a reasonable amount of advance warning, the Client may carry out monitoring within the meaning of paragraph 1 on the Contractor's business premises during usual business hours. The Client shall ensure that such monitoring is only carried out to the extent required so that the monitoring does not cause undue disruption to the Contractor's business operations. The parties assume that monitoring is required no more than once a year. Further checks must be justified by the Client, stating its grounds. In the event of on-site monitoring, the Client shall reimburse the Contractor for the costs incurred up to a reasonable level, including staff costs for supervising and accompanying monitors on the premises. The Contractor shall submit the basis for cost calculation to the Client before the monitoring is carried out.

(4) Instead of through on-site monitoring, the Contractor may choose to demonstrate compliance with technical and organisational measures by submitting a suitable up-to-date attestation, reports or excerpts of reports from independent bodies (e.g. accountants, auditors, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certificate, if the audit report enables the Client to assure itself in an appropriate way of compliance with the technical and organisational measures in accordance with Annex 3 to this agreement. If the Client has justified doubts over the suitability of the audit document within the meaning of sentence 1, it may carry out on-site monitoring. The Client is aware that on-site monitoring in data centres is not possible or only possible in justified exceptional cases. In this respect, we reiterate that all data received by TeamDrive is encrypted and is always stored in encrypted form.

(5) If the supervisory authority takes action against the Client within the meaning of Art. 58 GDPR, particularly in respect of notification and control obligations, the Contractor shall be obliged to provide the requisite information to the Client and allow the relevant competent supervisory authority to carry out on-site monitoring. The Contractor must notify the Client of any such planned measures.

§ 8 Breaches by the Contractor requiring notification

1. The Contractor is obliged to notify the Client of any breach of data protection law, of the agreements entered into and/or of the instructions issued without delay. The corresponding notification must contain at least:
a) A description of the nature of the breach including, where possible, the nature and quantity of the data affected and the categories of the data subjects;
b) The name and contact details of the data protection officer or other contact point where more information can be obtained;
c) A description of the likely consequences of the personal data breach;
d) A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

2. The Contractor shall bear sole responsibility for submitting any and all notifications required to a supervisory authority and for informing data subjects. The Client shall cooperate with these efforts to the extent required.

§ 9 Obligations of the Client

The Client shall bear sole responsibility for complying with the statutory data protection provisions, particularly for the lawfulness of data processing by the Contractor, and is thus the controller within the meaning of Art. 4 no. 7 GDPR.

If action is taken against the Client by a data subject in respect of any claims under Art. 82 GDPR, the Contractor shall undertake to help the Client to defend itself against such claims to the best of their abilities.

The Client shall provide the Contractor with details of the contact person for data protection issues arising within the scope of the agreement.

§ 10 Scope of powers to issue instructions

The Client shall be responsible for complying with data protection provisions and for the lawfulness of the transfer of data to the Contractor.

The Contractor shall only process the personal data in order to fulfil the Main Contract or follow additional instructions from the Client unless obliged to do so by EU law or the law of EU member states to which the Client is subject; in such a case, the Contractor shall notify the Client of that legal requirement before processing unless that law prohibits such notification on important grounds of public interest.

The Contractor shall be entitled at any time to issue supplementary instructions concerning the nature, scope and procedure for processing personal data. Instructions can be given verbally or in text form. Verbal instructions must be confirmed and documented for the Contractor in text form without delay.

The Contractor shall notify the Client in text form without delay if they believe that an instruction issued by the Client violates statutory provisions. The Contractor is entitled to hold off following the instruction in question until it is confirmed or modified by the Client. Insofar as the instruction breaches the provisions of the GDPR with which the Contractor is obliged to comply, the Contractor shall be entitled to refuse to follow the instruction.

§ 11 Erasure of data after the end of the mandate

The Contractor shall be obliged to erase the personal data in full in line with data protection provisions (including copies required on procedural or security technology grounds) or return it to the Client when the agreement comes to an end or on the instruction of the Client. The same applies to test and waste material, which must be kept under lock and key in accordance with data protection provisions until it is erased or returned. The erasure log must be presented on request.

§ 12 Compensation

No additional compensation for data processing shall be paid unless otherwise agreed above. This is covered by the remuneration paid for the use of TeamDrive.

,

Hamburg,

TeamDrive Systems GmbH
Max-Brauer-Allee 50
22765 Hamburg

*

- Client -

CEO/Managing Director
Detlef Schmuck

- Contractor -

* Waiver of Physical Signature selected.

Annex 1:
A. Information supplementing § 2, scope, nature and purpose of data processing
B. Nature of data in accordance with § 2
C. Data subjects in accordance with § 2

Annex 2: Data security concept
Measures for monitoring data protection in accordance with Art. 32 GDPR

Annex 3:
Designation of subcontractors, "Approved subcontractors" in accordance with Art. 9 no. 3 GDPR

Annex 1

A. Nature and purpose of the processing

(as defined in Art. 4 no. 2 GDPR):

☑ Hosting of cloud services (SaaS) and support services.

B. Re. § 2, nature of personal data

(as defined in Art. 4 no. 1, 13, 14 and 15 GDPR)

☑ Name
☑ Email
☑ IP address
☑ Usage data
☑ User account
☑ Other categories of personal data: Usage data from the TeamDrive application.

C. Re. § 2, data subjects

(as defined in Art. 4 no. 1 GDPR):

☑ Employees
☑ Freelancers
☑ Customers
☑ Business partners

Annex 2: Data security concept

Measures for monitoring data protection in accordance with Art. 32 GDPR

This document serves to ensure compliance with statutory requirements and is designed to provide a general description that enables a provisional assessment to be made as to whether the data security measures taken are appropriate for the aspects addressed below. This data security concept must be adapted and updated continuously in line with the prevailing circumstances relating to execution of the mandate. All amendments and modifications to the procedures for implementing the agreement must be documented in writing. This document forms an integral part of the agreement and must be shown to the Client in the event of material changes.

Please direct any information security questions about TeamDrive and its services to the data protection officer and, in their absence, to the head of the IT/EDP department:

TeamDrive Systems GmbH
Data Protection Officer
Max-Brauer-Allee 50
D-22765 Hamburg
Tel.: +49 (0)40 60 77 09 300
datenschutz@teamdrive.com

Data protection measures

The data protection measures implemented at TeamDrive are geared towards ensuring data availability, confidentiality, integrity and transparency of all measures for auditability.

Measures for encrypting and pseudonymising personal data are implemented that ensure the current level of security. All server systems, services and technical measures are designed to be subjected to a permanent load in respect of the associated data processing. We thus ensure that the availability of the personal data is restored reliably and swiftly after a physical or technical incident. We also employ measures and technical processes for permanent monitoring and assessment in order to ensure security of processing.

In addition, TeamDrive's business processes are based on the provisions of Art. 32 of the European General Data Protection Regulation (GDPR).

Specific details of individual measures to prevent unauthorised persons from obtaining personal data

a. Physical access control

   Measures to prevent unauthorised persons from accessing data processing facilities used to process or use personal data:

   - Key/key assignment, combination of "having" and "knowing"
   - Door locks (electric door openers etc.) with code lock and token access only after registration with visitor services, accompaniment and briefing
   - CCTV surveillance of all data centre access areas and rooms, alarm system for protection inside (motion sensors) and outside (doors, window opening contacts, lock contacts, glass-break sensors) as well as fire
   - Alarm system connected to an alarm centre

b. System access control

   Measures to prevent unauthorised persons from using data processing systems:

   - Password procedure
   - Automatic blocking

- Individual user accounts for authorised users (not superusers)

c. Data access control

Measures ensuring that the persons authorised to use a data processing system can only access the data that they are entitled to access and that personal data cannot be read, copied, modified or removed without authorisation during processing and use and after storage:

- Devising an authorisation concept and access rights in line with requirements, monitoring them and keeping a record of them.
- Only assigning and logging jobs in writing using a ticket system
- Automatically generating log files where this is technically feasible and makes logical sense, and analysing these in the event of suspicion; cyclical automatic erasure by means of rotation.

d. Transfer controls

Measures ensuring that personal data cannot be read, copied, modified or removed without authorisation during its electronic transfer or its transport or storage on data carriers and that it is possible to verify and establish to which bodies the transfer of personal data by data communication equipment is envisaged:

- Separating networks, particularly between the Internet (outside world) and the service network.
- Implementing multi-tier architectures with tiered security zones and protection mechanisms (e.g. firewalls, intrusion detection systems and similar)
- Encryptions and tunnelling (SSL, VPN, OTPs)
- Keeping a record of logins
- Secure transport

e. Input control

Measures ensuring that a retrospective check can be made of whether and by whom personal data in data processing systems was entered, modified or removed:

- Logging database changes requested
- Evidence of assignment and successful completion in the ticket system

f. Mandate controls

Measures ensuring that personal data being processed on behalf of a client can only be processed in accordance with that client's instructions:

- Concluding a data processing agreement when tasking subcontractors with data processing; transferring the Contractor's obligations to the subcontractor; requiring employees to observe data confidentiality in accordance
- with Section 5 of the German Federal Data Protection Act (BDSG)
- Monitoring data protection precautions and providing written evidence
- Ensuring that data is destroyed after the end of the mandate

g. Availability control

Measures ensuring that personal data is protected against accidental destruction or loss:

- Avoiding a single point of failure as the basic concept underlying all the infrastructure in the data centre, i.e. ensuring availability by having redundant systems and components
- Redundant power supply (main supply, transformer, uninterruptible power supply via online UPS, diesel-powered emergency generators located outside) Data backup, including shared backup; data backup media kept in separate rooms (data safes)

- Using firewalls and load balancers for access and content filtering and horizontal load distribution; can also be ordered for shared services
- Air conditioning
- Server and storage clusters for shared web services, managed root server and NFS.
- Redundant network connection to the data centre backbone and external IP connection (Internet);
- monitoring all infrastructure and supply systems
- 24/7 expert-level support (on-call service) mandatory for infrastructure and supply (shared services) and available as an option (recommended) for housing customer systems in connection with the on-call services.

h. Separation rule

Measures ensuring that data collected for different purposes can be processed separately.

The processing of development, test and production data is kept separate as part of the data processing effected via TeamDrive. The systems operated on behalf of the customer are processed separately in terms of data technology. The separation is supplemented by extensive encryption mechanisms to prevent the data from being amalgamated unlawfully.

- Logical separation of clients
- Authorisation concept defining access rights

i. Review, analysis and evaluation measures

TeamDrive undergoes regular audits by external experts in order to obtain the EuroPriSe seal of quality for data protection. These are supplemented by ongoing monitoring of the processes certified.

The expert and audit reports can be viewed on the TeamDrive website.

Regular in-house tests, exercises and checks supplement these measures.

Supplementary measures for hosting

The Contractor uses 1&1 IONOS SE, Elgendorfer Str. 57, D-56410 Montabaur, to host personal data. The technical and organisational measures taken by this company in this regard can be viewed at https://www.ionos.de/terms-gtc/terms-enterprise-cloud/datenschutzpaket.

Annex 3

Designation of subcontractors, "Approved subcontractors"

1&1 IONOS SE, Elgendorfer Str. 57, D-56410 Montabaur
Hosting all TeamDrive data and operating the servers on which TeamDrive runs as well as backing up data and sending emails whose sending was instigated by the customer (e.g. inviting users)

MailJet GmbH, Rankestr. 21, D-10789 Berlin
Sending emails whose sending was instigated by the customer (e.g. inviting users)
https://www.mailjet.de/sicherheit-datenschutz/

The following subcontractors are exclusively to be used for storing backup data on servers in the EU in encrypted and pseudonymised form.

Microsoft Cloud Deutschland, Hahnstr. 43, D-60528 Frankfurt am Main

Amazon Web Services EMEA Sàrl, 38 Avenue John F. Kennedy, L-1855 Luxembourg

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland