Data processing agreement according to Art. 28 GDPR

Agreement

between

Controller

Licensee:
<<Lizenznehmer>>

License number:
<<Lizenznummer>>

Contact E-Mail address:
<<Emailadresse>>

and

FastViewer GmbH

Processor

Schwesterhausgasse 11
D-92318 Neumarkt

represented by

Mr. Fürsch / Mr. Hickisch

Director(s)

the following data processing agreement pursuant to Article 28 (3) and other provisions of Regulation 2016/679 EU (EU General Data Protection Regulation – in brief: GDPR) as well as further applicable data protection provisions shall be concluded as follows:

§ 1 Subject and duration of the contract, content of the order

1. Content

The contractor (processor) processes personal data on behalf of the controller. This contract covers all issues with regard to data protection between controller and processor.

2. Subject matter

The subject matter of this order is the performance of the following tasks by the processor:
- Provision of the FastViewer software
- Provision of the FastViewer communication server
- Provision of the FastViewer online portal and the associated functionalities
(e.G FastViewer Online-Log)
- Provision of remote maintenance services and support

3. Duration

The duration of this agreement corresponds to the duration of the master / performance / service level agreement.

4. Nature and purpose of the intended data processing

Detailed description of the subject of the agreement with regard to scope, nature and purpose of processor tasks:
- Provision of the FastViewer software
- Provision of the FastViewer communication server
- Provision of the FastViewer online portal and the associated functionalities
(e.G FastViewer Online-Log)
- Provision of remote maintenance services and support

5. Location of Data processing

The provision of the contractually agreed data processing can take place at the choice of the user exclusively in Germany, alternatively in countries within the European Union or worldwide.
The prerequisite therefore is the adaptation of the setting "Use the following server farm" of the FastViewer customer portal (https://portal.fastviewer.com). Any relocation to a third country requires the prior notification of the client and may only take place if the special requirements of Art. 44 ff. EU-GDPR are met.

6. Type of data

The following data types are subject of the processing of personal data:

- ✓*person-related master data*
- ✓*communication data (e.g. telephone, e-mail)*
- ✓*contract master data (contractual relationship, product interest)*
- ✓*customer history*
- ✓*contract billing and payment data*
- ✓*planning and control data*
- ✓*information from third parties (e.g. credit bureaus, public directories)*

7. Categories of data subjects

The categories of persons affected by processing include:

✓*customers*
✓*prospects*
✓*subscribers*
✓*employees*
✓*suppliers*
✓*sales representatives*
✓*contact persons*

§ 2 Controller's obligations / right to control

1. In the context of the contractual relationship between controller and processor, the controller is solely responsible for assessing the legal admissibility of the processing to be performed by the processor with regard to GDPR provisions and other rules on data protection.

2. The controller has the right to carry out inspections in consultation with the processor or to have them carried out by an examiner to be named on a case-by-case basis. The controller moreover has the right to verify that the processor complies with this agreement in his business. The execution of such random checks shall be announced on reasonable notice. The processor shall ensure that the controller can convince himself of the processor´s compliance with regard to all of the latter´s obligations in accordance with Art. 28 GDPR.

   Upon request, the processor undertakes to provide the controller with all necessary information, what particularly applies to evidence on the implementation of appropriate technical and organizational measures and obligations agreed upon in this agreement by suitable means.

   The demonstration of such measures, which do not only concern the concrete order/agreement, is feasbile in any of the following ways:

   - Compliance with a code 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 statements issued by independent bodies (e.g. privacy or auditors, accountants, data protection officers, IT security department)
   - Appropriate certification through IT-security or privacy audits such as e.g. ISO 27001

   The processor shall be entitled to seek compensation for providing the controller with the opportunity to execute his controls.

   Processing of data in private homes shall be agreed on as admissible. In such cases, the processor has to ensure that any applicable data protection provision is observed.

3. The processor is obliged to inform the controller immediately if the processor finds any errors or irregularities regarding data protection regulations in the context of the examination of order results.

§ 3 Processor's obligations

In addition to compliance with the provisions of this agreement, the contractor has to comply with statutory obligations set forth in Art. 28 to 33 EU-DS-GVO. In particular, the processor has to make sure his compliance with the following issues:

1. Written appointment of a data protection officer (DPO), if required by law.

   The following person has been appointed as processor's data protection officer: Mr. Norbert Rauch, Atarax GmbH, datenschutz@fastviewer.de
   Any changes with regard to the appointment of a DPO and the latter´s contact details must be communicated immediately to the controller.

2. Confidentiality pursuant to Art. 28 para. 2 lit. b, 29, 32 IV GDPR is guaranteed. The processor will only employ and use staff that has been made aware of all relevant data protection regulations; Moreover, the processor confirms that any staff has been obliged to maintain confidentiality in written. Such obligation shall be designed to outlast the termination of the agreement.

3. The processor undertakes to implement and comply with all technical and organizational measures required for this order in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [see Appendix 1 for details].

4. Converning the performance of their duties under applicable data protection regulations, controller and processor will cooperate upon request of the supervisory authority.

5. The processor undertakes to control his internal processes as well as the technical and organizational measures on a regular basis in order to ensure that any processing within his responsibility is performed according to the requirements of the applicable rules on data protection and ensure that the protection of the rights of data subjects is guaranteed at any time.

6. Unless the processor is obliged to data processing by European Union law or by local laws to which the processor is subject (e.g. investigations by law enforcement units or authorities), the processor will only processes controller's personal data in accordance with contractually specified conditions and controller‘s specific individual instructions. In such a case, the processor shall inform the controller of these legal requirements prior to processing, unless the law prohibits such communication because of an important public interest or further legal reason the processor is obliged to comply with. The processor shall not process data for any other purposes and is not entitled to forward them to third parties.

   The processor shall immediately inform the controller if he considers an instruction as violating applicable law. The processor may suspend the execution of the instruction only until it has been confirmed or changed by controllor‘s authorized personnel / representatives where the controller shall bear any risk and cost from the execution of any such instruction turning out to be illegal.

7. The processor is obliged to provide the controller with information at any time as far as controller's data and documents are concerned.

8. The processor keeps records of processing activities in accordance with Art. 30 para. 2 GDPR and makes them available upon controller‘s request. The controller provides the pocessor with necessary information required for this purpose.

The processor moreover supports the controller in preparing the necessary data processing record required under Art. 30 para. 1 GDPR.

9. The processor shall assist the controller in complying with any obligation set forth in Art. 32 to 36 GDPR.

10. The processor may seek compensation for any supportive action he performs in favor of the controller if such action is not part of the contractual duties of the processor and when such action does not have to be performed as consequence of any misbehavior of the processor in regard of this conract.

11. The processor must inform the controller immediately about any actions and measures of supervisory authorities, as far as such relate to this order. This also applies in case that a competent authority initiates any administrative or criminal proceedings against the processor in regard of any data processing activities carried out by the processor.

    In the event that the controller is subject to an inspection by the supervisory authority, an administrative offense or criminal procedure, claims of data subjects or third parties or any other claims in the context of data processing activities in cooperation with the processor, the processor shall support the controller to the best of his ability.

    Any additional costs arising at the processor´s as consequence of the aforementioned actions shall be borne by the controller.

§ 4 Return and deletion

Copies or duplicates of data must not be created without controller‘s knowledge. This does not include backup copies, to the extent necessary to ensure proper data processing, and copies required to comply with legal retention periods.

Upon termination of the contractually agreed services or earlier if requested so by the controller and latest upon termination of the agreement, the processor must either hand out to the controller all documents and processing (utilization) results as well as data sets related to this data processing agreement in his own or subcontractor possession or, provided that the controller´s prior consent is given, delete these data in accordance with data protection requirements. The same applies to test and scrap material.

The processor must keep documentation that provides relevant evidence of orderly and proper data processing in accordance with respective retention periods even beyond the end of this agreement. In order to discharge himself, the processor may hand over such documents to the controller upon termination of this agreement.

§ 5 Subcontractual relations

1. The processor may only employ subcontractors (other processors) provided the controller´s prior consent is given.

   Without written consent, the contractor can perform contract execution while maintaining its duty to monitor orders related companies in the sense of §§15ff. AktG and, in individual cases, other subcontractors with due diligence. In particular, FastViewer Software Development GmbH, Sinagasse 33, AT-1220 Vienna, is considered an approved subcontractor.

2. Prior to employing further or replacing existing subcontractors listed in this agreement, the processor shall inform the controller in due time, either in writing or in text form.

3. The controller may - for important data protection reasons - object to such changes within a reasonable period of time (no longer than two weeks) and appeal to the address/body the processor specified. If there is no objection within the deadline, acceptance of change is considered given. It shall be understood and agreed that any limitation of the service owed from this contract that results from any unfounded objection shall not be part of the responsibility of the processor.

   In exceptional cases an agreement in the aftermath shall be possible. The processor then shall immediately inform the controller about the exchange of a subprocessor.

4. If the subcontractor provides agreed service(s) outside the EU / EEA, controller and processor shall ensure admissability and compliance in terms of data protection by taking appropriate measures.

5. Any further outsourcing by the subcontractor requires explicit controller consent (at least text form); Any contractual provisions with regard to data protection within the ‚contractual chain' must also be imposed on the further subcontractor to ensure data protection requirements are met.

6. Subcontracting in the sense of this agreement always refers to services that directly relate to the provision of the main service. This does not include other (ancillery) services provided by the processor, such as the disposal of data carriers and other measures with the aim to ensure confidentiality, availability, integrity and resilience of hard- and software of data processing systems. However, the processor shall be obliged to hold appropriate and legally compliant contractual agreements and control measures for outsourced ancillary services in order to guaranteeing data protection and data security of of controller's data.

§ 6 Instructions

Data processing is carried out exclusively within the framework of the agreements made and according to controller instructions. The controller shall generally issue all instructions and orders in writing or in a documented electronic format. Within the framework of the order description made in this agreement, the controller reserves a wide-ranging right to instructions regarding type, scope and procedure of data processing, which may be substantiated by means of individual/detailed instructions. Changes to the subject matter of this agreement as well as procedural changes must be jointly agreed and documented in written or electronic form. The controller has to confirm verbal instructions immediately in writing or in a documented electronic format.

§ 7 Rights of data subjects

1. The processor may not correct, delete or restrict the processing of the data processed on behalf of the controller unless a corresponding and documented instruction has been issued by the controller. In the event that a data subject directly addresses the processor in this regard, the processor must immediately forward such request to the controller.

2. The processor shall be entitled to compensation for any additional cost arising from his contribution to measures as under section 7, No. 1.

§ 8 Technical and organizational measures

1. The technical and organizational measures described in Appendix 1 shall be defined as binding.

   The processor must ensure security according to Art. 28 para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 para. 1, 2 GDPR. In general, the actions to be taken consist of data security measures and measures that shall guarantee a level of protection commensurate with the risk as regards confidentiality, integrity, availability and resilience of systems. In this regard, state-of-the-art technology, implementation costs and the nature, scope and purpose of the processing as well as the varying likelihood and severity of risk for rights and freedoms of individuals within the meaning of Art. 32 para. 1 GDPR shall be considered.

2. Technical and organizational measures are subject to technical progress and further development. In that regard, the processor shall be allowed to implement alternative adequate measures. In doing so, the safety level shall be equivalent to specified measures. Significant changes shall be documented.

3. As far as the security measures taken by the processor do not meet controller’s requirments, he shall inform the controller immediately. The same shall apply to any disturbance, violation commited by the processor or his staff if such violation is a breach of applicable rules on data protection or of the contractual obligations. Such information shall also be issued in any case of suspicion of a data breach or irregularity concerning

§ 9 Liability

Liabilty for violations of rules on data protection or this agreement shall be handled in accordance with the applicable provisions of data protection law if not the contractual agreements applying on the underlying services do not include a special provision on liability.

§ 10 Miscellaneous

1. Changes and amendments to this agreement and all of its components - including potential assurance provided by the processor - shall be made either in writing or in an electronic format (text form), including an explicit note on the fact that an amendment or addition is intended. This also applies to the waiver of this form requirement.

2. The controller’s ststutory seat shall be the place of jurisdiction for both parties.

3. Should individual parts of this agreement be ineffective, this does not affect the validity of the agreement as such. The parties shall replace the ineffective provision by a valid provison of the content closest possible to the initial economic intent of the parties.

Appendix 1

General technical and organizational measures

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

a) Entry control

Unauthorized access to data processing systems must be prevented.

(Examples: access control system, ID card readers, magnetic and chip cards, keys including key assignment, plant and door security (electric door openers, etc.), alarm systems, gatekeepers or video monitoring)

Entrance control is ensured by a documented and supervised handover of keys. The server room of FastViewer can only be accessed by persons authorized to enter the server room. The lock on the door to this room prevents unauthorized access by external or third parties.

b) Access control

Unauthorized system use has to be prevented.

(Examples: secure passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers, creation of a user master record per user)

Access to the premises of the data processing equipment is protected, and all equipment and IT systems are provided with constantly changing passwords.
All computer systems are set up by the IT staff in a manner that allows only authorized users the opportunity to work with them. Consequently, a personal login with a user ID and password is mandatory. The password must then be changed by the respective user with a password consisting of lowercase and uppercase letters as well as digits. The assignment of user IDs for working on IT systems generally occurs on a personal basis. Working under the credentials of another person is not permitted. The user is prohibited from passing on user IDs and passwords to third parties. The respective passwords are changed regularly every 30 days.
If a user does not change his or her password, the system will force the user to do so.

c) User control

No unauthorized reading, copying, modification or removal of data within systems.

(Examples: authorization concepts, need-based access rights, access logging and evaluation, modification and deletion)

Personal data can only be changed on the basis of the authorizations granted according to the "need to know" principle. For this a documented authorization concept is established. Employees cannot edit or copy personal data stored in the system or manipulate this data in any other unauthorized manner. Employees are divided into groups that have different access authorizations for the data records. This is guaranteed by a Windows server structure in conjunction with the "Active Directory".

d) Separation control

Separate processing of data collected for different purposes.

(Examples: multi-client capability / purpose limitation, sandboxing, separation of functions, separation of live / production / test)

Our system guarantees that data collected for different purposes can also be processed separately.

e) Pseudonymization (Art. 32 para. 1 lit. a GDPR, Art. 25 para. 1 GDPR)

The processing of personal data shall take place in such a way that the data can no longer be assigned to a specific person without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures.

All backups (Veeam) are provided with 256-bit AES encryption.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

a) Transfer control

During electronic transmission or transport, no unauthorized reading, copying, alteration or removal may be possible.

(Examples: encryption, virtual private networks, electronic signatures, transport security)

Personal data from the IT system is protected against unauthorized copying to data media. Basically, with FastViewer, no data is played on data media and used outside the company. If an employee works in the field over a VPN connection, access is protected by a firewall and appropriate antivirus, spyware removal and antihacker software. Protection is provided from both the server and the user computers by installing the corresponding software.

b) Input control / memory control / data media control

Determine if and by whom personal information has been entered, altered or removed from data processing systems.

(Examples: logging, document management)

The FastViewer IT system stores any changes, deletions or changes to data and records, as long as the system allows it. In this case it is possible to track which user has made what change and when, etc., at any time.

3. Availability and resilience / recoverability (Art. 32 para. 1 lit. b GDPR)

Protection against accidental or willful destruction or loss.

(Examples: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), disk mirroring, e.g. RAID, separate storage, firewalls, reporting channels and emergency plans; quick recoverability, Art. 32 para. 1 lit. c GDPR)

Scalable server systems based on Microsoft Hyper-V are used, which can be adapted to the load. The servers are backed up fully on a daily basis. All servers have mirrored hard drives in RAID systems and are equipped with redundant components.
The equipment used can be remotely serviced and administered at any time via the FastViewer software solution. The communication servers used for this purpose are located in highly secure data centers.

For the connections themselves, one of the highest quality encryption methods is used to ensure an appropriate security standard (256 bit AES).

All critical systems are subject to permanent monitoring through the monitoring software of the manufacturer Paessler. If critical values regarding the availability or performance of the networks or used devices are reached, the supervising administrators are notified immediately by email/SMS.
The targeted monitoring of system components and processes helps prevent system bottlenecks, congestion and failures. Due to the comprehensive functionality of the monitoring systems by Paessler, it is possible to monitor and document the overall status of the network as well as the individual devices 24 hours a day. The monitoring report is regularly evaluated by an authorized administrator.

4. Procedures for periodic review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR, Art. 25 para. 1 GDPR)

Order control

No order processing in the sense and meaninf of Art. 28 GDPR without corresponding controller instructions

(Examples: clear contract design, formalized order management, strict selection of service providers and subcontractors, follow-up-checks, etc.)

There are written contracts between the Principal and Agents.
The Principal issues directives to the Agent in writing. The Agent has sufficient in-house instructions on the basis of the commission and the related directives of the Principal. Adequate measures to ensure data protection by any potential subagent can also be reviewed by the Principal. A data protection management system will be established, respecting the principles of the PDCA cycle and written deposition.

Further questions?

If required, you can also contact our Data Protection Officer, who will be glad to answer your questions.

Appointed external Data Protection Officer

Mr. Norbert Rauch
atarax GmbH & Co. KG
Dr.-Dassler-Straße 57
91074 Herzogenaurach, Germany

Data Protection Coordinator at FastViewer

Mr. Christoph Meier
Tel: +49 9181 509 56-15
E-mail: datenschutz@fastviewer.com