



License Conditions (EULA)

1. Application

1.1 These license conditions apply between Snapview GmbH, Munich, Germany (hereinafter referred to as Snapview) and any physical person or legal entity that procures and/or uses the Mikogo software (hereinafter referred to as Software) on a chargeable or non-chargeable basis (hereinafter referred to as Customer).

1.2. In the event that the Software is procured in return for payment, the Customer accepts these license conditions in relation with Snapview or upon conclusion or extension of the lease agreement. Otherwise, the Customer accepts these conditions with the first download of the Software, upon starting to use the Software, or upon registration of a user account. In any event, Snapview does not require the Customer's declaration of acceptance to be received at its premises.

1.3. The continuing applicability of this license agreement is dependent upon the continuation of the underlying lease agreement (except in the event of use for free) and will share its fate insofar as it will cease to be valid on the same date that the latter ceases to be valid (if such is the case) (e.g. upon revocation by the consumer pursuant to section 312 g of the German Civil Code [BGB]).

1.4. The product description of the respective licensed software also forms part of the license conditions.

1.5. Mikogo is a registered trademark of Snapview GmbH, Munich, Germany.

2. Applicable Law, Jurisdiction

2.1. The laws of the Federal Republic of Germany are applicable for this contract, to the exclusion of the United Nations Convention on the International Sale of Goods.

2.2. Munich, Germany shall be stipulated as the exclusive place of jurisdiction for disputes resulting from or relating to this contract insofar as the Customer has a general place of jurisdiction in Germany and is a businessman, corporate entity operating under public law or a public separate-assets firm.

2.3. This place of jurisdiction also applies if the Customer has no general place of jurisdiction (i.e. residence) in Germany and is not a user who falls under the general jurisdiction of the European Union, Norway, Iceland, or Switzerland.

2.4 In principle the place of jurisdiction for obligations arising from this agreement is Munich, Germany. Statutory regulations on jurisdiction are not affected.

3. Functionality

3.1. The Software enables the Customer to send their computer-screen display via the Internet to the computer screens of persons who they select themselves (hereinafter referred to as Participants) and display information on those screens (in what is hereinafter referred to as a Session). Further specifications are to be found in the relevant product description.



3.2. The Software consists of a server software package that is provided by Snapview, a client software package for use on the sending Customer's computer, which has access to the server software, and an executable file for use by the Participants (connection program).

3.3. The point of transfer for server-based services provided to the Customer is the outgoing server of the Snapview system.

4. Licensed Product

4.1. The Customer shall receive authorization for a limited period of time for the joint use of the server software, and for the use of the client software and the executable file (license). If the software is procured in return for payment, the Customer will be sent a license code with which, following registration, they can activate the agreed software functions in accordance with the product description in the user account management.

4.2. Usage rights shall only be granted to one natural person who must be specified by name upon registration of the user account in the user account management and who need not be the Customer him or herself. The product version determines the maximum possible number of receiving Participants for a session and the available features in the software.

4.3. The client software may be installed on up to three (3) Customer computers. Individuals from companies that are affiliated to the Customer's company are not authorized for use.

4.4. The Customer will be provided with access authorization to the server Software with an average annual availability rate of 99%. Should the Customer achieve a higher rate of availability during use, Snapview shall grant this to them for free.

4.5. The Customer is not authorized to transfer or lease usage rights or to relinquish the software or their server access to third parties with the exception of Participant use in accordance with the contractual terms. Companies associated with the Customer concerned are also considered third parties.

4.6. The source code for any Snapview software or its disclosure or installation, Customer or Participant training Sessions, or any warranty of the Software's suitability for the purposes intended by the Customer are not contractual items and are also not the subject of any other kind of obligation of Snapview.

4.7. The Customer is not authorized to edit or reprogram or modify any part of the software, or to rework it or reinstall it in another place.

4.8. Technical information, descriptions and instructions for use are provided to the Customer in electronic form on the Mikogo websites, where the client software and the executable file (both in object code only) are also available for downloading.

5. Use for Free

After setting up a user account (including under a pseudonym) the Customer is permitted to use the software to a reduced extent for free and thus to lead Sessions. For the receiving Participant, use is always for free. Snapview reserves the right to terminate such use for free at any time, or to modify or suspend functionality.



6. LIABILITY FOR DEFECTS

SNAPVIEW IS LIABLE FOR ANY SOFTWARE DEFECTS PURSUANT TO THE LEGAL REGULATIONS, WITH THE RESTRICTION THAT NO-FAULT LIABILITY FOR DAMAGE COMPENSATION FOR DEFECTS EXISTING AT THE TIME OF CONTRACT CONCLUSION PURSUANT TO SECTION 536A OF THE GERMAN CIVIL CODE (BGB) SHALL BE EXCLUDED. OTHER GROUNDS FOR LIABILITY SHALL REMAIN UNAFFECTED.

THE RIGHT TO SUBSTITUTE PERFORMANCE IS EXCLUDED. IN ALL OTHER RESPECTS, THE STATUTORY PROVISIONS SHALL APPLY WITH REGARD TO CLAIMS FOR DEFECTS.

7. LIABILITY FOR DAMAGES

7.1. SNAPVIEW'S LIABILITY FOR INFRINGEMENTS OF CONTRACTUAL OBLIGATIONS AND IN TORT IS LIMITED TO WILLFUL INTENT AND GROSS NEGLIGENCE.

7.2. THIS IS NOT APPLICABLE TO INJURY TO LIFE, LIMB OR HEALTH, CLAIMS DUE TO THE BREACH OF CARDINAL OBLIGATIONS OR COMPENSATION FOR DAMAGES DUE TO DELAY (SECTION 286 OF THE GERMAN CIVIL CODE [BGB]). IN THIS RESPECT, SNAPVIEW IS LIABLE FOR EVERY DEGREE OF FAULT. CARDINAL OBLIGATIONS ARE THOSE FUNDAMENTAL RIGHTS AND OBLIGATIONS THAT RESULT FROM THE NATURE OF THE CONTRACT AND WHOSE DAMNIFICATION WOULD ENDANGER THE PURPOSE OF THE CONTRACT AND ON WHOSE ADHERENCE THE CONTRACTUAL PARTIES MAY REGULARLY RELY ON. LIABILITY FOR BREACH OF CARDINAL OBLIGATIONS ON THE BASIS OF ORDINARY NEGLIGENCE IS LIMITED TO FORESEEABLE AND TYPICALLY ARISING DAMAGE.

7.3. IN ADDITION, IN THE EVENT OF USE OF THE SOFTWARE FOR FREE, SNAPVIEW IS LIABLE FOR DAMAGE ARISING AS A RESULT OF A SOFTWARE DEFECT ONLY IF THE DEFECT IN QUESTION HAS BEEN DELIBERATELY CONCEALED BY SNAPVIEW.

7.4. INSOFAR AS LIABILITY IS NOT EXCLUDED FOR DAMAGES DUE TO SLIGHT NEGLIGENCE THAT DO NOT INVOLVE INJURY TO THE CUSTOMER'S LIFE, LIMB OR HEALTH, OR FOR SLIGHT NEGLIGENCE, OR FOR BREACH OF CARDINAL OBLIGATIONS, SUCH CLAIMS EXPIRE ONE YEAR FROM THE INITIATION OF THE CLAIM.

7.5. INSOFAR AS LIABILITY FOR DAMAGES IS EXCLUDED OR LIMITED FOR SNAPVIEW, THIS APPLIES ALSO IN RESPECT OF PERSONAL LIABILITY FOR DAMAGE COMPENSATION FOR SNAPVIEW EMPLOYEES, REPRESENTATIVES, AND AGENTS.

7.6. LIABILITY ARISING FROM THE GERMAN PRODUCT LIABILITY ACT REMAINS UNAFFECTED IN ALL CASES.

8. Customer Obligations and Contractual Penalties

8.1 For each case of infringement of an agreement as detailed in items 4.2, 4.3 and 4.5, the Customer who is not a consumer is obliged to pay Snapview a contractual penalty sum of EUR 35,000 (in words: thirty-five thousand).

8.2 The Customer must observe legal regulations when using Snapview Software and in particular must refrain from sending unlawful content.

8.3 The Customer holding a lease license is obliged, on receipt of the license code, immediately to perform the installation indicated in the documentation and a functional test, and to set up a user account with their personal details (first name and last name, company name, address, email address), to specify the



authorized persons pursuant to 4.2 (first name and last name) and to choose a new secure password and subsequently change this on a regular basis.

8.4 The Customer must provide the hardware and software environments indicated in the product specifications as well as ensure that the Participant is also equipped with the sufficient requirements.

8.5. When using the Software and after the use of the Software, the Customer intends to carry out timely and adequate back-up and storage of all data under their own responsibility and at their own cost, and where appropriate to ensure that this is also done at the premises of the Participants. Similarly, they must under their own responsibility secure their data against unauthorized access.

8.6 The Customer is obliged to treat the server resources with care and to log out correctly when ending a Session or in the event of long intermissions between data transmission.

8.7 The Customer is obliged to install updates and upgrades provided by Snapview for the client software and the executable file.

8.8 The Customer must inform Snapview in due time of any changes of data that are important for the license agreement.

8.9 The Customer indemnifies Snapview from all third-party claims arising from Software use that is not in accordance with the contract.

8.10 The Customer must delete all Snapview Software entirely from their computers, servers, and storage media upon contract expiration and submit a cancellation deed upon request.

9. Limitation of Claims, Offsetting

9.1. By way of deviation from section 195 of the German Civil Code (BGB), Snapview's claims to payment expire after five (5) years have elapsed. Section 199 of the German Civil Code (BGB) applies with regard to the start of the expiration period.

9.2. Offsetting rights of the Customer apply only if their claims are the subject of a final and conclusive judgment, or are uncontested, or have been acknowledged by Snapview.

10. Reference Listing

Snapview shall be granted the right to identify the Customer who is not a consumer as a reference Customer for the purpose of advertising Snapview software, by providing that Customer's company name, brand or company logo as well as their URL (e.g. identification on website and on printed advertising material). The Customer may revoke his or her consent for the future by providing written notification.

11. Infringement When Using Snapview Software

In the event of strong suspicion that infringements are arising during Customer access to Snapview servers, Snapview reserves the right to suspend its functionality. The Customer shall immediately be informed thereof.

12. Data Protection

Both Snapview and the Customer are obligated to adhere to data privacy regulations. In accordance with the data protection declaration, Customer data will be used exclusively for the purpose of the conclusion



and performance of the contract and for customer information and market analysis and will be treated confidentially. They shall only be potentially passed on to third parties within this framework, who shall also be bound to confidentiality by Snapview.

13. Agents

Snapview is authorized to employ third parties of its choice in order to fulfill its contractual obligations.

14. Written Form

Legally binding declarations or notifications that the Customer must submit to Snapview or a third party must be provided in writing; this shall not apply to the cases envisaged in section 312 g of the German Civil Code (BGB) (consumer revocation).

15. Force Majeure

Neither of the parties is obligated to fulfill contractual obligations in the event of and for the duration of any hindrance due to force majeure. The following circumstances shall be particularly considered as force majeure: technical Internet problems that a party cannot control, explosion/fire/flooding beyond the party's reasonable control, war, mutiny, blockade, embargo, or a labor dispute lasting for more than six (6) weeks and which is not caused by the party. Each contracting party must immediately inform the other of such an occurrence in the event of force majeure in written form, insofar as this is possible.

Date: 2018-05-25



General Terms and Conditions

1. Scope of Application

These General Terms and Conditions apply to all contracts of Snapview GmbH, Munich, Germany (hereinafter referred to as Snapview) and its customer (hereinafter referred to as the Customer) on an exclusive basis. Customer terms that differ from or conflict with these General Terms and Conditions shall not be formally recognized. These Conditions shall also apply if Snapview provides services in the knowledge of contrary or differing Customer General Terms and Conditions. For contracts with Snapview, the Snapview License Conditions (EULA) and Snapview product specifications are also to be regarded as forming part of these General Terms and Conditions.

2. Applicable Law, Jurisdiction

2.1. The laws of the Federal Republic of Germany are applicable for this contract, to the exclusion of the United Nations Convention on the International Sale of Goods.

2.2. Munich, Germany shall be stipulated as the exclusive place of jurisdiction for disputes resulting from or relating to this contract insofar as the Customer has a general place of jurisdiction in Germany and is a businessman, corporate entity operating under public law or a public separate-assets firm.

2.3. This place of jurisdiction also applies if the Customer has no general place of jurisdiction (i.e. residence) in Germany and is not a user who falls under the general jurisdiction of the European Union, Norway, Iceland, or Switzerland.

3. Products of Snapview

The software product Mikogo for online collaboration (hereinafter referred to as Software), is distributed or provided for use exclusively in accordance with the Snapview License Conditions (EULA) and the relevant Snapview product specifications. Mikogo is a registered trademark of Snapview GmbH, Munich, Germany.

4. Place of Execution, General Matters

4.1. In principle, the place of execution and place of payment concerning all direct contractual relationships with Snapview is Munich, Germany. Statutory regulations concerning places of jurisdiction are not affected.

4.2. Information published or issued directly by Snapview does not constitute a contractual offer and is non-binding.

4.3. Snapview reserves all rights (especially proprietary rights, usage rights, and copyrights) to all information, software trials, and software trial accesses remaining from contractual negotiations.

4.4 Legally binding declarations or notifications that the Customer must submit to Snapview or a third party must be provided in writing (except in case of revocation by a consumer).

5. Online Shops

5.1. The online shops at www.mikogo.net.cn, www.mikogo.com.br, www.mikogo.fr, www.mikogo.ru, www.mikogo.it, www.mikogo.es, www.mikogo.jp, www.mikogo.de and www.mikogo.com are operated by Snapview's partner company, cleverbridge AG, Gereonstr. 43-65, 50670 Cologne, Germany, in its own name and on an entirely independent basis. Consequently, transactions with Cleverbridge are subject to the conditions and declarations of Cleverbridge.



5.2. Upon conclusion of a contract with Cleverbridge, the Customer agrees that the Snapview License Conditions (EULA) and the relevant Snapview product specification shall also apply.

6. Direct Procurement from Snapview, Contractual Term, Termination

6.1. Outside the online shops, the Software license can also be procured directly from Snapview after consulting with Snapview. The Customer can procure a lease license.

6.2. Acceptance of contractual offers by Snapview is only by express declaration or by the sending of a license code by email for access to the Software ordered.

6.3. Lease license.

6.3.1. With the lease license, the Customer acquires, for the duration of the lease relationship, a right of use of the software in accordance with the license conditions (EULA) and the relevant product specification.

6.3.2. The rental fee for the stipulated contractual period must be paid in full in advance and is due upon contract conclusion.

6.3.3. The lease will automatically be renewed at the end of the original concluded contractual period (contractual duration) by an additional lease with the same duration and terms, provided that the contract is not terminated in writing through the receipt of one (1) month written notice submitted before the end of the ongoing contractual period.

7. Use for Free

7.1. Snapview allows its customers to use the Software for free, and to this end makes the client Software and executable file available for downloading under the Snapview license conditions (EULA). The download offers represent offers to conclude an agreement according to these General Terms and Conditions and the Snapview license conditions (EULA), which the Customer accepts by activating the download or starting to use the Software. Snapview does not require access to this declaration of acceptance by the Customer.

7.2. Snapview is entitled to terminate the contractual relationship at any time by suspending the functionality of the Software.

8. LIABILITY FOR DEFECTS

SNAPVIEW IS LIABLE FOR ANY SOFTWARE DEFECTS PURSUANT TO THE LEGAL REGULATIONS WITH THE FOLLOWING RESTRICTION: SNAPVIEW'S NO-FAULT LIABILITY FOR DAMAGE COMPENSATION FOR DEFECTS EXISTING AT THE TIME OF CONTRACT CONCLUSION PURSUANT TO SECTION 536A OF THE GERMAN CIVIL CODE (BGB) SHALL BE EXCLUDED. OTHER BASES FOR LIABILITY SHALL REMAIN UNAFFECTED.

THE RIGHT TO SUBSTITUTE PERFORMANCE IS EXCLUDED. IN ALL OTHER RESPECTS, THE STATUTORY PROVISIONS SHALL APPLY WITH REGARD TO CLAIMS FOR DEFECTS.

9. LIABILITY FOR DAMAGE

9.1. SNAPVIEW'S LIABILITY FOR INFRINGEMENTS OF CONTRACTUAL OBLIGATIONS AND IN TORT IS LIMITED TO WILLFUL INTENT AND GROSS NEGLIGENCE.

9.2. THIS IS NOT APPLICABLE TO INJURY TO LIFE, LIMB OR HEALTH, CLAIMS DUE TO THE BREACH OF CARDINAL OBLIGATIONS OR COMPENSATION FOR DAMAGES DUE TO DELAY (SECTION 286 OF THE



GERMAN CIVIL CODE [BGB]). IN THIS RESPECT, SNAPVIEW IS LIABLE FOR EVERY DEGREE OF FAULT. CARDINAL OBLIGATIONS ARE THOSE FUNDAMENTAL RIGHTS AND OBLIGATIONS THAT RESULT FROM THE NATURE OF THE CONTRACT AND WHOSE DAMNIFICATION WOULD ENDANGER THE PURPOSE OF THE CONTRACT AND ON WHOSE ADHERENCE THE CONTRACTUAL PARTIES MAY REGULARLY RELY ON. LIABILITY FOR BREACH OF CARDINAL OBLIGATIONS ON THE BASIS OF ORDINARY NEGLIGENCE IS LIMITED TO FORESEEABLE AND TYPICALLY ARISING DAMAGE.

9.3. IN ADDITION, IN THE EVENT OF USE OF THE SOFTWARE FOR FREE, SNAPVIEW IS LIABLE FOR DAMAGE ARISING AS A RESULT OF A SOFTWARE DEFECT ONLY IF THE DEFECT IN QUESTION HAS BEEN DELIBERATELY CONCEALED BY SNAPVIEW.

9.4. INSOFAR AS LIABILITY IS NOT EXCLUDED FOR DAMAGES DUE TO SLIGHT NEGLIGENCE THAT DO NOT INVOLVE INJURY TO THE CUSTOMER'S LIFE, LIMB OR HEALTH, OR FOR SLIGHT NEGLIGENCE, OR FOR BREACH OF CARDINAL OBLIGATIONS, SUCH CLAIMS EXPIRE ONE YEAR FROM THE INITIATION OF THE CLAIM.

9.5. INSOFAR AS LIABILITY FOR DAMAGES IS EXCLUDED OR LIMITED FOR SNAPVIEW, IT IS ALSO APPLICABLE TO PERSONAL LIABILITY FOR DAMAGE COMPENSATION FOR SNAPVIEW EMPLOYEES, REPRESENTATIVES, AND AGENTS.

9.6. LIABILITY UNDER THE GERMAN PRODUCT LIABILITY ACT SHALL REMAIN UNAFFECTED.

10. Customer Obligations and Contractual Penalties

10.1. The Customer must observe the duties arising from the license conditions (EULA). In some instances, these duties are subject to a contractual penalty (8.1 of the license conditions).

10.2. In addition, the Customer is also under a contractual obligation to observe statutory conditions, and in particular undertakes not to transmit any unlawful content.

11. Fees and Payment Terms

11.1. In principle, advertised and agreed payments are understood as inclusive of VAT at the statutory rate as far as consumers are concerned, and exclusive of VAT at the statutory rate for businesses. For businesses, any customs or other public levies arising are also not included and are to be borne by the business in question.

11.2. Invoices from Snapview must be settled within fourteen (14) days of receipt. Snapview reserves the right to send invoices in electronic form.

12. Overdue Customer Payment

12.1. Should the Customer be late for an invoice payment or should a credit-card or a direct-debit charge fails for reasons for which the Customer is solely responsible (e.g. insufficient funds, incorrect data), Snapview reserves the right to charge punitive damages for processing costs up to an amount of EUR 15. Provision of proof for higher or lower costs shall remain permissible for both sides.

12.2. Should the Customer be over three (3) months overdue in settling an invoice for a contractual period or for an important part thereof, Snapview reserves the right to retain its services unpaid up to that point and to terminate the contract without prior notice after a warning has been issued.



13. Limitation of Snapview Claims

Contrary to section 195 of the German Civil Code (BGB), Snapview's claims to payment expire after five (5) years have elapsed. Section 199 of the German Civil Code (BGB) is applicable from the start of the expiration period.

14. Offsetting

Offsetting rights of the Customer apply only if their claims are the subject of a final and conclusive judgment, or are uncontested, or have been acknowledged by Snapview.

15. Identification of References

Snapview shall be granted the right to identify the Customer who is not a consumer as a reference customer for the purpose of advertising Snapview Software by providing their company name, brand or company logo as well as its URL (e.g. identification on website and on printed advertising material). The Customer may revoke his or her consent for the future by providing written notification.

16. Infringement When Using Snapview Software

In the event of strong suspicion that infringements are arising during Customer access to Snapview servers, Snapview reserves the right to suspend its functionality. The Customer shall immediately be informed thereof.

17. Data Protection

Snapview and the Customer agree on order processing according to Art. 28 GDPR. This order processing agreement is part of these General Terms and Conditions as Annex 1.

18. Agents

Snapview is authorized to employ third parties of its choice in order to fulfill its contractual obligations.

19. Force Majeure

None of the parties is obligated to fulfill contractual obligations in the event of and for the duration of force majeure. The following circumstances shall be particularly considered as force majeure: technical Internet problems that a party cannot control, explosion/fire/flooding beyond the party's reasonable control, war, mutiny, blockade, embargo, or a labor dispute lasting for more than six (6) weeks and which is not caused by the party. Each contracting party must immediately inform the other of such an occurrence in the event of force majeure in written form, insofar as this is possible.

Date: 2018-05-25



Annex 1: Processing in accordance with Article 28 GDPR

Agreement between Customer - the Controller - hereinafter referred to as the Client - and Snapview GmbH - the Processor - hereinafter referred to as the Supplier

1. Subject matter and duration of the Order or Contract

(1) The Subject matter of the Order or Contract results from the Service Agreement if the software is procured in return for payment (Principle Contract), which is referred to here (hereinafter referred to as Service Agreement).

(2) The duration of this Order or Contract corresponds to the duration of the Service Agreement.

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data. Nature and Purpose of Processing of personal data by the Supplier for the Client are precisely defined in the Service Agreement. The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every Transfer of Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

(2) Type of Data. The Subject Matter of the processing of personal data comprises the following data types/categories: Personal Master Data (Key Personal Data), Contact Data (e.g. phone, e-mail address), Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest), Contract Billing and Payments Data (banking and account data), Session Connection Data (session number, session password – if assigned, start date and time, end date and time)

(3) Categories of Data Subjects. The Categories of Data Subjects comprise: Customers, Potential Customers, Subscribers, Employees (staff, applicants, trainees), Suppliers, Authorised Agents, Contact Persons (at customers, potential customers and suppliers)

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. [Details in Appendix 1]

(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

- a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. The Supplier has appointed Mr. Helge Kauert, Lawyer and Managing Director of dataLEGAL Rechtsanwalts-gesellschaft mbH (Address: Oskar-von-Miller-Ring 33 in 80333 München, telephone +49-89-2488268-0, e-mail: DSB.Snapview@datalegal.de) as Data Protection Officer. The Client shall be informed immediately of any change of Data Protection Officer.
- b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.
- c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 1].
- d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.
- e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.
- f) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

- g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
- h) Verifiability of the Technical and Organisational Measures conducted by the Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Supplier shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Name of subcontractor	City of registration/Country	Services
PlusServer GmbH	Cologne, Germany	Server Hosting
filoo GmbH	Gütersloh, Germany	Server Hosting
Cogeco Peer 1 (UK) Ltd.	United Kingdom	Server Hosting
Cogeco Peer 1 (USA) Inc.	USA	Server Hosting
Amazon Web Services Inc.	USA	Server Hosting
Microsoft Inc.	USA	Server Hosting

(3) The outsourcing to subcontractors or the change of the existing subcontractor are permissible, provided that a contractual agreement is based between the contractor and the subcontractor in accordance with Article 28 paragraphs 2-4 GDPR and the contractor notifies the client of such outsourcing to subcontractors in writing or in text form in advance and the client does not object to the planned outsourcing within 14 days in writing or in text form for important reasons. Failure by the client to lodge an objection within the aforementioned period shall be deemed to constitute consent to the assignment of the new subcontractor. The client is aware that the non-assignment of a new subcontractor can lead to a delay or non-performance of the services and increased remuneration. The contractor shall inform the client in writing or in text form of any impairment of the services or increase in remuneration resulting from an objection by the client to the commissioning of the new subcontractor. The client may then either conclude a written amendment to the contract in order to comply with the change or terminate the contract in accordance with the provisions of the contract. Such termination shall not constitute termination for good cause or for breach of contract.

(4) The transfer of personal data from the Client to the subcontractor and the subcontractors' commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.



(5) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(6) Further outsourcing by the subcontractor requires the express consent of the Supplier (at the minimum in text form); all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by compliance with approved Codes of Conduct pursuant to Article 40 GDPR; or by certification according to an approved certification procedure in accordance with Article 42 GDPR; or by current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor); or by a suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

- a) Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
- b) The obligation to report a personal data breach immediately to the Client
- c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
- d) Supporting the Client with its data protection impact assessment
- e) Supporting the Client with regard to prior consultation of the supervisory authority

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.



9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Appendix 1 - Technical and Organisational Measures

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control. No unauthorised access to Data Processing Facilities.
 - Offices and data centres are only accessible to authorized persons and other persons accompanied by them
 - Lockable rooms with a manual locking system where only staff and cleaning staff have a key
 - Key reception on entry and exit from the company will be acknowledged
 - Careful selection of cleaning personnel
- Electronic Access Control. No unauthorised use of the Data Processing and Data Storage Systems.
 - Assignment of user rights
 - Password assignment, authentication with user name and password, confidential handling of passwords
 - Password creation policy for servers
 - Key control
 - Use of anti-virus software
 - Creation of user profiles, use of VPN technology; use of a software firewall
 - Assignment of authorizations and their documentation by the Manager IT Operations in accordance with management instructions
- Internal Access Control (permissions for user rights of access to and amendment of data). No unauthorised Reading, Copying, Changes or Deletions of Data within the system.
 - Authorization concept

- Number of administrators reduced to the bare minimum
- Physical erasure of data carriers before reuse; use of shredders
- Administration of rights by system administrators
- Proper destruction of data carriers
- Isolation Control. The isolated Processing of Data, which is collected for differing purposes.
 - Logically separated storage on separate systems or data carriers
 - Creation of an authorization concept
 - Separation of production and test system
- Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR). The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures.
 - The systems described in the service agreement can be used by the parties with pseudonyms ("Privacy by Default").

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control. No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport.
 - Installation of VPN tunnels (Virtual Private Networks)
 - For physical transport: careful selection of transport personnel and transport vehicles and confirmation of collection and receipt
 - Personal data is only transmitted in encrypted form
- Data Entry Control. Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted.
 - Accesses, especially during the entry, modification and deletion of data, as well as failed login attempts are logged
 - A multi-level authorization concept ensures that different users have different rights to enter, change and delete data
 - Access is via individual user names and passwords

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control. Prevention of accidental or wilful destruction or loss.
 - Regular testing of data recovery
 - Storage of data backups in a secure, outsourced location
 - Creation of a backup & recovery concept
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);
 - Redundant systems
 - Load balancing
 - Continuous backups
 - Ongoing monitoring of the systems with notification of failures

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control. No third-party data processing as per Article 28 GDPR without corresponding instructions from the Client.



- Careful selection of subcontractors (in particular with regard to data security)
- Instructions in writing to the contractor (e.g. by data processing contracts)
- Obligation of the contractor's employees to data secrecy
- Assignment of rights to input
- Formalised order management
- Duty of pre-evaluation
- Supervisory follow-up checks

Date: 2018-05-25