FITOGRAM

Data Processing Agreement pursuant to Art. 28 GDPR

The controller (responsible for the processing) and the processor (Fitogram GmbH) conclude the following data processing agreement pursuant to Art. 28 of the European General Data Protection Regulation (GDPR). On the basis of the contractual relationship existing between the parties (main contract as well as the supplementary conditions of the contract) the processor processes personal data for the controller. The resulting data protection rights and obligations of the parties are specified by this data processing agreement. The appendices to this agreement are part of the agreement. The provisions made apply to all services rendered by the processor for the controller and all associated activities that result in and may result in the processing of personal data.

§ 1 Subject and duration of processing

a) The subject matter of the contract is the processing of personal data (hereinafter referred to as "data") by the processor for the controller on the controllers behalf and in accordance with the controllers instructions. The processor shall undertake the processing of personal data in order to enable the employees and staff of the controller to use the Software provided by the processor. Essentially, this involves the processing of online bookings for courses and course management, including payment and the necessary support by the processor.

b) The controller may terminate this agreement as well as the main agreement at any time without notice in the event of a serious breach by the processor of the provisions of this agreement, such a serious breach shall be deemed to exist in particular if the processor uses the controller 's data for purposes other than those determined in accordance with this agreement or breaches a material obligation under this agreement.

c) Even in the absence of the aforementioned conditions, the controller is entitled to terminate this agreement and the main contract without notice if the processor repeatedly violates this agreement. Prior written notice or a notice in text form on the part of the controller is a prerequisite for this.

§ 2 Scope, nature and purpose of processing

As part of its services, the processor collects and stores personal information about clients of the controller, in particular also information about intended orders by customers. In particular, the Processor shall carry out the following processing operations on behalf of the controller:

- The provision, installation and maintenance of the platform provided by the processor;
- Order fulfillment; billing between controller and processor and customer and processor;

- Customer service of the processor towards controller and controller towards customers.

§ 3 Type of personal data

The processor will have access to the following personal data (as a result of the controller providing it with the data or allowing it access to the data):

> **First name, last name, email, address, IP address for booking(s), account holder, studio name, payment method, account holder & IBAN & BIC, price, contract duration, contract name, SEPA mandate number, SEPA signature date, time of booking(s), booked and cancelled bookings, usage data.**

§ 4 Circle of data subjects

The affected data subjects for the above listed data are:

- Employees, staff and other personnel of the client

§ 5 Rights and Obligations of the controller

a) The controller alone is responsible for the evaluation of the admissibility of the data processing as well as for the protection of the rights of data subjects and thus is the responsible data controller within the meaning of Art. 4 (7) GDPR.

b) The controller gives instructions to the processor regarding the type and extent of processing of the personal data.

c) Prior to the start of the commissioning and the associated data processing and subsequently regularly, the controller is entitled, after timely prior notification (of at least 2 weeks), during normal business hours, to ensure compliance with the processor's technical and organizational data security measures. The controller can also have this check carried out by a third party.

d) The processor agrees that the controller is entitled after prior notification to verify compliance with the provisions on data protection and the contractual agreements to the extent necessary, or to have this done by third parties, in particular by obtaining information and viewing the stored data and the systems as well as through other on-site inspections.

e) The processor must comply with any possible inspection measures of the data protection supervisory authority pursuant to Art. 58 GDPR and § 40 BDSG-new. The processor shall inform the controller immediately after notification or knowledge about the execution of the inspection measures as well as in case of other inquiries, investigations or inquiries of the data protection supervisory authority, in particular also if this occurs in a prior consultation pursuant to Art. 36 GDPR, to the extent that the measures or inquiries may concern data processing that the processor provides for the controller.

f) At the request of the controller, the processor shall prove compliance with the technical and organizational measures taken. Proof can be provided by presenting a current attestation or report (e.g. by an auditor, external data protection officer, inspector or an external data protection auditor) and, if applicable, a suitable certification (e.g. BSI Basic Protection, ISO27001 or according to an approved certification procedure pursuant to Art. 42 GDPR) or adherence to approved rules of conduct pursuant to Art. 40 GDPR. The inspection rights of the controller remain unaffected.

§ 6 Obligations of the processor

a) The processor is obliged to process personal data only in accordance with the instructions and in accordance with the provisions of this agreement.

b) In granting the rights of data subjects pursuant to Art. 15 et seq. GDPR (correction, limitation of processing, deletion, notification and provision of information), the processor shall support the controller upon first request within its means. The processor shall take appropriate technical and organizational measures. The processor shall, upon instruction, correct, delete or restrict the processing of the personal data processed on behalf of the controller.

c) Should the data collected on behalf of the controller be the subject of a request for data portability pursuant to Art. 20 GDPR, the processor shall immediately make the relevant data set available to the controller in a structured, standard and machine-readable format upon request.

d) If a data subject turns directly to the processor to exercise their rights as a data subject, the processor must immediately forward this request to the controller.

e) The processor shall inform the controller immediately if he believes that a given instruction violates legal regulations. The execution of the corresponding instruction may be suspended until it has been confirmed or changed by the controller.

f) After termination of the main contract, the processor is obliged to hand over to the controller all personal data connected with the contractual relationship, which has come into the processor’s possession, and to delete the data in compliance with data protection and data security regulations and in accordance with controller's instructions. This also applies to any data backups at the processor. The data-protection and data-security compliant deletion must be documented in writing and confirmed to the controller in writing.

g) The processor shall ensure that the employees involved in the processing of the data of the controller and other persons working for the processor are prohibited from processing the data outside the instructions. Furthermore, the processor shall guarantee that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to appropriate legal confidentiality. The obligation to confidentiality/secrecy persists even after the commission is completed. Insofar as the processor participates in the provision of commercial telecommunications services in connection with the services rendered for the controller, the processor is required to oblige the employees involved therein in writing to confidentiality regarding telecommunications in accordance with the Telecommunications Act (Telekommunikationsgesetz).

h) The processor shall ensure that in the event of a personal data breach, the processor immediately informs the controller and supports the controller in its obligations pursuant to Art. 33 - 36 GDPR.

i) The processor confirms that he has appointed a data protection officer in accordance with Art. 37 GDPR and monitors compliance with data protection and data security regulations via the data protection officer. The data protection officer for the processor is:

Fresh Compliance GmbH
RA Philipp Heindorff
Schlesische Str. 26
10997 Berlin
dsb@freshcompliance.de

§ 7 Place of performance

a) The processing and use of the data takes place exclusively in the territory of the Federal Republic of Germany, in a member state of the European Union or in another Contracting State of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the controller and may take place only if the special conditions of Art. 44 et seq. GDPR are fulfilled.

b) If the processing of personal data takes place outside the EU, the processor warrants that the requirements applicable under the respective applicable data protection regulations for the occurrence of a permissible circumstance for the processing of personal data outside the EU are met ("justification under data protection law"). This is the case, on the one hand, if and to the extent that the EU Commission has certified an adequate level of protection for the data controller. Furthermore, if the processing is carried out by the processor on the basis of appropriate guarantees within the meaning of Art 46(1)(c) GDPR (EU standard contractual clauses) with further security precautions. Finally, if the processing of personal data outside the EU takes place exclusively within the framework of a program that has been certified by the EU Commission as offering an adequate level of protection and the further processor fulfills the formal and substantive requirements necessary for participation in the program, has qualified for it and remains qualified for the program without interruption during the term of the order.

§ 8 Subcontracting

a) The controller agrees that the processor may involve subcontractors. Before contracting or replacing subcontractors, the processor shall inform the controller in individual cases.

b) The controller may object to the change – within an appropriate period of time – for good cause – vis-à-vis the entity designated by the controller. If no objection is made within the deadline, the consent to the change shall be deemed granted. If there is good cause related to data protection, and if a mutual solution between the parties is not possible, the controller is granted a special right of termination.

c) The processor is liable for subcontractors as well as for its own vicarious agents.

d) The processor must ensure that all obligations under this agreement also apply to the subcontractors and their employees; this applies in particular to the duty to confidentiality and the obligation to privacy.

e) The processor is currently working on the fulfillment of the contract with the following other commissioned data processors, with whose commissioning the controller agrees (Appendix 1).

§ 9 Technical and organizational measures

a) The processor is obliged to comply with the principles of proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. The processor shall take all necessary measures to secure the data or the security of the processing, in particular taking into account the state of the art, as well as to mitigate possible adverse consequences for data subjects. In particular, the measures to be taken shall include measures to ensure adequate pseudonymization and encryption, as well as measures to protect the confidentiality, integrity, availability and resilience of systems and measures ensuring the continuity of post-incident processing.

b) The technical and organizational measures taken by the processor are described in detail in the appendix to this agreement and are part of the agreement.

§ 10 Liability

a) The processor is liable to the controller in accordance with the statutory provisions for all damages occurring in the provision of the contractual service, through culpable violations of this agreement as well as of legal data protection regulations to which it is subject, which are caused by the processor, its employees or those contracted by it for execution of the contract.

b) The controller or the processor is responsible to the data subject pursuant to Art. 82 GDPR for compensation for damages, which a data subject asserts due to inadmissible or incorrect data processing within the scope of the contractual relationship according to the GDPR or the BDSG-new or other regulations regarding data protection. The processor shall indemnify the controller internally from all claims for damages which are asserted against the controller due to a culpable breach of the obligations arising from this agreement by the processor.

§ 11 Deletion and return of personal data

a) The Processor shall not make copies or duplicates of the Data without the knowledge and consent of the Controller, except for the purpose of data backup or making technical copies for the following purposes:

- To carry out the processing activities under this DPA;
- to provide evidence of proper data processing; or
- for the fulfillment of legal obligations to retain data.

b) Upon termination of the contractual commissioned processing or upon the client's request earlier, but no later than upon termination of the contract, the processor shall return to the Controller all documents, processing and usage results and data records, insofar as they relate to this contract, or - after consent has been granted - delete or destroy them in a manner compatible with data protection law. The same applies to all related test, committee, redundant and discarded materials. The log of the deletion or destruction shall be made available upon request.

c) Any documentation serving as evidence of proper data processing in accordance with this DPA may be stored by the Processor beyond the term of the contract in accordance with the applicable retention periods. At the end of the term of the contract, the Processor may hand over such documentation to the Controller so that it is thereby released from this contractual obligation.

§ 12. Final provisions

a) In the event of any inconsistency between the terms of this agreement and the terms of the main contract, the terms of this agreement prevail.

b) Amendments and supplements to this agreement must be made in writing and it must be explicitly stated that the present provisions are thereby amended and/or supplemented. This also applies to a waiver of this formal requirement.

c) Should any provision of this agreement be or become invalid or unenforceable, the remaining provisions of this agreement remain unaffected. The invalid or unenforceable provision shall be replaced by a valid and enforceable provision which comes closest to the purpose of the provision to be replaced.

d) This agreement is subject to German law.

e) If access to the data is endangered by measures of third parties (e.g. measures of an insolvency administrator, seizure by tax authorities, etc.), the processor must inform the controller immediately about this.

____________________________	Cologne, 5.03.2021
Place, Date	Place, Date
	Francois Casanova CEO Fitogram
____________________________	____________________________
Controller	Processor

Appendix 1 _ List of subcontractors

Recipients	**Categories of Personal Data we share.**	**Status of recipient**	**Why we share it**	**Location(s)**
Service Providers (e.g., our hosting provider, CRM and marketing tool providers, our accounting and financial service providers)	-Identity Data -Contact Data -Technical Data -Behavioral Data -Marketing and Communications Data	Our Processors	Our service providers provide us with IT, software, content, applications and solutions management, hosting, system administration, management, project-related, marketing, customer feedback, and other services.	Both within and outside Europe.
Consultants and advisers	-Identity Data -Contact Data -Marketing and Communications Data -Behavioral Data -Technical Data	Our Processors	Our attorneys, bankers, accountants, auditors, insurers, consultants and other advisors who provide us with their respective services may need to receive certain elements of your Personal Data to do so.	Europe.

APPENDIX 2 _ Technical and Organizational Measures (Art. 32 DSGVO)

Fitogram GmbH
Probsteigasse 15-17
50670 Köln
Deutschland
Telefon: 0221 37050023
E-Mail: support@fitogram.pro

Internal Data Protection Officer

Fresh Compliance GmbH
RA Philipp Heindorff
Schlesische Str. 26
10997 Berlin
dsb@freshcompliance.de

Technical and organizational measures

Taking into account the state of the art, the costs of implementation and the nature, scope, circumstances and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, where relevant, the following:

- Ensuring confidentiality
- Access control
- Measures suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used.
- Measures:
- Alarm system
- Office is subject to exclusive use
- Chip cards / transponder systems
- Building is purely an office building
- Bell system with camera
- Manual locking system
- Key control with a list
- Careful selection of cleaning staff

Access control

Measures suitable to prevent data processing systems (computers) from being used by unauthorised persons.

- Anti-virus software
- Automatic desktop lock
- Application of 2-factor authentication
- BIOS protection (separate password)
- Creation of user profiles
- Firewall
- Login with user name and password
- Login with biometric data
- Encryption of notebooks / tablet
- Managing user permissions
- Assignment of user rights
- Database is managed externally at AWS
- Separation of company and guest wifi with separate passwords in each case

Access control

Measures that ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.
Measures:

- Differentiated authorisations (applications)
- Lockable cabinets for backup data carriers
- Document shredder various levels
- Differentiated authorisations (operating system)
- Differentiated authorisations (data)
- Use of programme-based authorisation concepts
- Physical deletion of data carriers
- Logging of the output of data media
- Administration of user rights by administrators
- Separate authentication for critical areas before login (admin tool)

Segregation control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of data.

- Setting database rights
- Data records are provided with purpose attributes
- Control via an authorisation concept
- Separation of productive and test environment

Ensuring integrity

Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

- Documentation of the data recipients
- Provision via encrypted connections such as sftp, https
- Documentation of deletion periods
- Use of VPN technology
- Email encryption
- Confirmation of receipt
- Overview of regular retrieval and transmission processes
- Transmission in anonymised or pseudonymised form
- Clear identification of data carriers and file folders
- Data transfer via Google Drive is subject to a rights system

Input control

Measures that ensure that it can be subsequently verified and determined whether and by whom personal data have been entered into, modified or removed from data processing systems.

- Clear responsibilities for the deletion of data
- Traceability of data processing through individual user names

- Technical logging of changes to data
- Technical logging of data entry
- Technical logging of the deletion of data
- Overview of the use of programmes for processing data
- Assignment of rights for editing data
- Connections to our servers for direct commands are authenticated by private pageant keys.

Pseudonymisation and encryption

Pseudonymisation

Measures that ensure pseudonymisation of data.

- Separation of attribution data
- Encryption
- Measures that ensure encryption of data.
- Measures:
- Encryption of the transport of e-mails

Ensuring availability, resilience and recoverability Availability (of data)

Measures to ensure that personal data is protected against accidental destruction or loss

Ensuring the availability of data.
Measures:

- Backup & recovery concept
- Data backup concept in place
- Daily backups
- Control of the backup process
- SLA with hosting service provider
- Physical data is also stored digitally for double protection.

Resilience (of systems)

Measures to ensure that personal data is protected against accidental destruction or loss - Ensure resilience of systems.

- Use of hardware firewalls
- Use of intrusion detection systems
- Use of software firewalls
- Installation of security updates on all developer systems
- Installation of current security updates on all application servers

Recoverability (of data / systems).

Measures to ensure that personal data is protected against accidental destruction or loss - Ensure recoverability of data and systems.

- Backup and security measures are the responsibility of the respective cloud service providers.

Procedures for regular review, assessment and evaluation - Order control

Measures to ensure that personal data processed on behalf of a client can only be processed in accordance with the client's instructions.

- Conclusion of the necessary commissioned data agreements
- Conclusion of the necessary standard contractual clauses
- Selection of the contractor under due diligence aspects
- Agreement on effective control rights vis-à-vis the contractor
- Obligation to appoint a data protection officer (in case of obligation to appoint)

Data protection management

Measures that ensure that methods have been evaluated to systematically plan, organise, manage and control the legal and operational requirements of data protection.
Measures:

- Appointment of an internal data protection officer
- Documentation of all data protection procedures and regulations
- Carrying out data protection impact assessments (if required)
- Compliance with the information obligations pursuant to Art. 13 DSGVO
- Compliance with the information obligations pursuant to Art. 14 DSGVO
- Regular sensitisation of employees to data protection
- Training of employees on data protection
- Commitment of employees to data secrecy
- Review of the effectiveness of the TOMs (carried out at least annually)

Incident response management

Measures that ensure that security incidents can be prevented or, in the case of security incidents that have already occurred, that data and systems can be protected and that rapid analysis and remediation of the security incident can be carried out.

Measures:

- Documentation of security incidents
- Involvement of data protection officers in security incidents
- Use of an intrusion prevention system (IDS)
- Use of firewalls and their regular updating
- Use of virus scanners and their regular updating

Data protection-friendly default settings

Measures that ensure that a certain level of data protection already exists in advance through the appropriate technical design (privacy by design) and factory settings (privacy by default) of a software.

Measures:

- Ensure easy exercise of a data subject's right of withdrawal.
- Personal data is only collected for the purpose for which it is required