Record of Processing Activities

This Record of Processing Activities, in line with Article 12 of the Federal Act on Data Protection (Swiss DPA), offers a compilation of processes where personal data is processes by the controller, alongside the technical and organizational measures in accordance with Article 8 Swiss DPA.

Controller:
Jörg Arnold, Fairpicture AG
Spitalgasse 28
3011 Bern, Switzerland

Date:
December 18, 2024

Index

- **30.5.** Deletion of access information of departing employees
- **30.6.** Use of up-to-date anti-virus software
- **30.7.** Use of software firewall(s)

31. Internal Access Control (permissions for user rights of access to and amendment of data)

- **31.1.** Appropriate authorisation concept
- **31.2.** Regular check of the authorisation concept
- **31.3.** Control of the administrators
- **31.4.** General traceability of data access

32. Transmission Control

- **32.1.** Remote access / remote maintenance via VPN
- **32.2.** Transit encryption of e-mails
- **32.3.** Encrypted transmission of data via websites (TLS)

33. Adherence to Instructions, Purpose Limitation and Separation Control

- **33.1.** Separate documentation of the Processing
- **33.2.** Careful selection of sub-processors and service providers
- **33.3.** Forwarding of instructions to employees and sub-processors
- **33.4.** Verification of compliance with instructions
- **33.5.** Adherence to the deletion periods
- **33.6.** Logical separation of the client's data
- **33.7.** Separation of productive, test and development environment

34. Ensuring the integrity and availability of data as well as the resilience of processing systems

- **34.1.** Use of fail-safe, redundant server systems and services
- **34.2.** Storage of Data with external and reliable hosting providers
- **34.3.** Regular and documented patch management
- **34.4.** Fail-safe power supply of server systems
- **34.5.** Fire protection of the server systems
- **34.6.** Protection of server systems against moisture damage
- **34.7.** Protection of data records against accidental modification or deletion
- **34.8.** Adequate, reliable and controlled backup & recovery

I. Information on the controller

CONTROLLER

_____

Name and Address: Jörg Arnold, Fairpicture AG
Spitalgasse 28
3011 Bern, Switzerland
Email Address: arnold@fairpictureorg

II. General procedural rules and information

1. Preamble

The Records of Processing Activities includes a collection of general information relevant to all the processing processes described below, as well as specific details on individual processing activities, in which personal data (hereinafter also referred to briefly as "data") is processed. This structure aims to maintain clarity and provide precise information. The general information explains fundamental principles and guidelines applicable to all processing activities, such as adherence to data protection principles, the legal bases of data processing, and handling the rights of the individuals concerned. In the specific part of the records, detailed information on individual processing activities is listed, including the purpose of data processing, the categories of data affected, the recipients of the data, and where applicable, the transfer of data to third countries. This record serves as a central document to ensure transparency and traceability of data processing and is an essential element in fulfilling documentation obligations under the General Data Protection Regulation (GDPR).

2. Relevant legal bases

2.1. Relevant legal basis according to the Swiss Data Protection Act

Description:

2.2. Relevant legal basis according to the Swiss Data Protection Act

Description: The controller processes personal data when data subjects are located in Switzerland, based on the Federal Act on Data Protection ("Swiss DPA"). Unlike the GDPR, the Swiss DPA does not generally require that a legal basis for the processing of personal data be named. The processing of personal data is carried out in good faith and is lawful as well as proportionate (Art. 6 para. 1 and 2 of the Swiss DPA). Furthermore, personal data is collected only for a specific purpose that is recognizable to the data subject and processed only in a manner compatible with this purpose (Art. 6 para. 3 of the Swiss DPA).

III. Records of Processing Activities

1. Preamble

Preamble text: With the following privacy policy we would like to inform you which types of your personal data (hereinafter also abbreviated as "data") we process for which purposes and in which scope. The privacy statement applies to all processing of personal data carried out by us, both in the context of providing our services and in particular on our websites, in mobile applications and within external online presences, such as our social media profiles (hereinafter collectively referred to as "online services").
The terms used are not gender-specific.

2. Security Precautions

Description: In accordance with legal requirements and taking into account the state of technology, implementation costs, as well as the nature, scope, circumstances, and purposes of processing alongside the different probabilities of occurrence and the extent of threat to the rights and freedoms of natural persons, the controller implements appropriate technical and organisational measures to ensure a level of protection commensurate with the risk.
These measures specifically include ensuring the confidentiality, integrity, and availability of data by controlling physical and electronic access to data as well as access to it, its input, transfer, securing availability, and its separation.
Furthermore, the controller has established procedures that enable the exercise of data subject rights as well as the deletion of data and responses to threats to data.
In addition, from the outset of developing or selecting hardware, software, and processes, consideration is given by the controller to protect personal data in accordance with the principles of privacy by design and privacy-friendly default settings.

2.1. Securing online connections through TLS/SSL encryption technology (HTTPS)

Description: To protect the data transmitted via the online services of the controller from unauthorised access, the controller employs TLS/SSL encryption technology. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) ensure that information transmitted between the website or app and the user's browser, or between two servers, is encrypted. This protects the data against unauthorised access. TLS, as an advancement of SSL, provides higher security for data transmission and ensures that all transmissions comply with current security standards. The securing of a website with an SSL/TLS certificate is indicated by the presence of HTTPS in the URL, which signals secure and encrypted data transmission.

3. Transmission of Personal Data

Description: In the course of processing personal data by the controller, it may be necessary to transfer this data to other entities such as companies, legally independent organizational units, or individuals, or to disclose it to them. Recipients of this data often include service providers who take on IT tasks, or providers of services and content that are integrated into websites. The controller always ensures compliance with legal data protection regulations and secures data protection at the recipients by concluding appropriate contracts or agreements.

4. International data transfers

4.1. Data Processing in Third Countries

Description: If the controller processes data in a third country (i.e., outside the European Union (EU), the European Economic Area (EEA)) or if the processing occurs within the scope of using third-party services or disclosing/transmitting data to other persons, entities, or companies, this is done only in accordance with legal requirements. If the level of data protection in the third country has been recognised by an adequacy decision (Art. 45 GDPR), this serves as the basis for data transfer. Within the framework of the so-called "Data Privacy Framework" (DPF), the EU Commission has also recognised the level of data protection for certain companies from the USA as secure within its adequacy decision dated 10.07.2023. The list of certified companies and further information on the DPF can be found on the website of the US Department of Commerce at https://www.dataprivacyframework.gov/ (in English). The controller informs data subjects within its privacy notices about which service providers used are certified under the Data Privacy Framework.Furthermore, data transfers only occur if an adequate level of protection is otherwise ensured, particularly through standard contractual clauses (Art. 46 para. 2 lit. c) GDPR), explicit consent or in cases of contractual or legally required transmission (Art. 49 para. 1 GDPR). The controller communicates the bases for third-country transfers for each provider from a third country, with adequacy decisions taking precedence as bases. Information on third-country transfers and existing adequacy decisions can be found in the information provided by the EU Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en?prefLang=de

4.2. Disclosure of Personal Data Abroad

Description: According to the Swiss Data Protection Act (DSG), the controller discloses personal data abroad only if an adequate level of protection for the data subjects is ensured (Art. 16 Swiss DSG). If the Federal Council has not determined an adequate level of protection (list: https://www.bj.admin.ch/bj/en/home/state/data-protection/international/recognition-states.html), the controller adopts alternative security measures. These may include international treaties, specific guarantees, data protection clauses in contracts, standard data protection clauses approved by the Federal Data Protection and Information Commissioner (FDPIC), or internal corporate data protection rules recognized in advance by FDPIC or a competent data protection authority of another country. According to Art. 16 of the Swiss DSG, exceptions for disclosing data abroad can be permitted if certain conditions are met,

including consent from the data subject, contract execution, public interest, protection of life or physical integrity, publicly disclosed data, or data from a legally provided register. These disclosures always comply with legal requirements.Under the so-called "Data Privacy Framework" (DPF), Switzerland has recognized the level of data protection for certain companies from the USA as secure within the framework of an adequacy decision dated 07.06.2024. The list of certified companies and further information on the DPF can be found on the website of the US Department of Commerce at https://www.dataprivacyframework.gov/ (in English). The controller informs data subjects within their privacy notices about which service providers they use are certified under the Data Privacy Framework.

5. General Information on Data Retention and Deletion

Description: Personal data processed by the controller will be deleted in accordance with legal requirements once the underlying consents have been revoked or no further legal bases for processing are present. This applies to cases where the original purpose of processing no longer exists or the data is no longer needed. Exceptions to this rule apply if legal obligations or special interests of the controller necessitate a longer retention or archiving of data.
In particular, data that must be retained for commercial or tax law reasons, or whose retention is necessary for legal action or to protect the rights of other natural or legal persons, should be archived accordingly.
The controller's privacy notices provide additional information on the retention and deletion of data specifically relevant to certain processing processes.
If there are multiple details regarding the retention period or deletion deadlines for a date, the longest period always prevails.
If a period does not explicitly start on a specific date and lasts at least one year, it automatically begins at the end of the calendar year in which the event triggering the period occurred.
Data that can no longer be processed for its originally intended purpose but must be retained due to legal requirements or for other reasons will only be processed by the controller for reasons justifying their retention.

Responsible for deletion processes: Deletion of customer data, Daniel Caspari (CRM)
Deletion of employee data, Jörg Arnold (HR)
Deletion of other data, Hazem Abdelhafez (IT)

5.1. Data Retention and Deletion

Description: The following general retention and archiving periods apply under Swiss law:

- 10 years - Retention period for books and records, annual financial statements, inventories, management reports, opening balances, accounting vouchers and invoices, as well as all necessary working instructions and other organizational documents (Article 958f of the Swiss Code of Obligations (OR)).
- 10 years - Data necessary to consider potential claims for damages or similar contractual claims and rights, as well as for the processing of related inquiries based on previous business experiences and usual industry practices, will be stored for the statutory limitation period of ten years, unless a shorter period of five years is applicable, which is

relevant in certain cases (Articles 127, 130 OR). Claims for rent, lease, and interest on capital, as well as other periodic services, for the delivery of food, for board and lodging, for innkeeper debts, as well as for craftsmanship, small-scale sales of goods, medical care, professional services by lawyers, legal agents, procurators, and notaries, and from the employment relationship of employees, expire after five years (Article 128 OR).

6. Changes and Updates

Description: The directory of processing activities will be updated as soon as changes in the processing processes require it, or when legal provisions or other compelling reasons make an adjustment necessary. Regardless of such events, a regular review of the directory takes place at least once a year to ensure that the directory always corresponds to the current processing activities and legal requirements.

7. Rights of Data Subjects

_____

7.1. Rights of the Data Subjects under the GDPR

Description: Data subjects are comprehensively informed about their rights in accordance with the GDPR. This information is provided either through a public privacy statement or on a case-by-case basis in a precise, transparent, understandable, and easily accessible manner. Communication is carried out in clear and simple language. The key rights include: a) the right to object, b) the right to withdraw consent, c) the right of access, d) the right to rectification, e) the right to erasure and restriction of processing, f) the right to data portability, and g) the right to lodge a complaint with a supervisory authority.

7.2. Rights of the data subjects under the Swiss DPA

Description: Affected individuals are comprehensively informed about their rights in accordance with the Swiss Federal Act on Data Protection. This information is provided either in a public privacy statement or, on a case-by-case basis, in a precise, transparent, understandable, and easily accessible manner. Communication is carried out in clear and simple language. The key rights include: the right to access, the right to data portability or release, the right to rectification, the right to object, deletion and destruction of data, as well as the right to withdraw consent.

8. Terminology and Definitions

Description: In this section, you will find an overview of the terminology used in this privacy policy. Where the terminology is legally defined, their legal definitions apply. The following explanations, however, are primarily intended to aid understanding.

9. Business services

Description: Data from contractual and business partners, such as customers and prospects (collectively referred to as "contractual partners"), are processed by the controller within the framework of contractual and comparable legal relationships as well as related measures and with regard to communication with the contractual partners (or pre-contractually), for example, to answer inquiries.

These data are used to fulfil the contractual obligations of the controller. This includes in particular the obligations to provide agreed services, any update obligations, and remedies for warranty and other performance disturbances. Furthermore, the data are used to protect the rights of the controller and for purposes related to administrative tasks associated with these obligations, as well as organisational management of the company.

In addition, based on legitimate interests of the controller in proper and economic business management as well as security measures to protect its contractual partners and its business operations from abuse, endangerment of their data, secrets, information, and rights (e.g., involving telecommunication-, transport- and other auxiliary services as well as subcontractors, banks, tax- and legal advisors, payment service providers or financial authorities), data is processed.

Within the scope of applicable law, data from contractual partners is only disclosed to third parties insofar as this is necessary for the aforementioned purposes or for fulfilling legal obligations. Contractual partners are informed about further forms of processing, such as for marketing purposes, within the privacy policy.

Which data are required for the aforementioned purposes will be communicated to the contractual partners before or during data collection e.g., in online forms through special marking (e.g., colours) or symbols (e.g., asterisks) or personally.

The deletion of data occurs after expiry of statutory warranty obligations and similar duties; that is generally after four years unless it is intended that data should be stored in a customer account or so long as they must be retained for legal reasons of archiving (for tax purposes usually ten years). Data disclosed by a contractual partner to the controller within a contract are deleted according to legal requirements and generally after completion of the contract.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category.

Data subjects: Service recipients and clients; Prospective customers; Business and contractual partners; Education and course participants.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations; Communication; Office and organisational procedures; Organisational and Administrative Procedures; Business processes and management procedures.

Data sources: Receipt through transmission or other communication by business partners and clients; Collection from data subjects; Data collection from other sources; Data collection through interfaces to services of other providers; Collection in connection with advertising and marketing campaigns.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Compliance with a legal obligation (Article 6 (1) (c) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

9.1. Agency Services

Description: The controller processes the data of customers for the provision of its contractual services. These services include, among others, conceptual and strategic consulting, campaign planning, software and design development/consulting or maintenance, the implementation of campaigns and processes, handling, server administration, data analysis/consulting services as well as training services.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

9.2. Education and Training Services

Description: The controller processes the data of participants in its education and training offerings (collectively referred to as "trainees"), in order to provide them with its training services. The data processed, as well as the nature, scope, purpose, and necessity of their processing, are determined by the underlying contractual and training relationship. The processing activities also include performance assessment and the evaluation of the services provided by the controller and those of the educators. In the course of its

activities, the controller may also process special categories of data, in particular information on the health of trainees and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. Where necessary, the controller obtains explicit consent from trainees for this. Otherwise, special categories of data are only processed if it is necessary for providing training services, for purposes of preventive or occupational medicine, for social protection measures or for protecting vital interests of trainees.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.
- **Data subjects:** Education and course participants.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

9.3. Consulting

Description: The data of clients, prospective clients, and other contracting parties or partners (collectively referred to as "clients") are processed by the controller in order to provide services to them. The procedures that are part of and for the purposes of consulting include: contacting and communicating with clients, conducting needs and requirements analyses, planning and implementing consulting projects, documenting project progress and results, capturing and managing client-specific information and data, scheduling and organizing appointments, providing consulting resources and materials, billing and payment management, post-processing and follow-up of consulting projects as well as quality assurance and feedback processes. The processed data as well as the type, scope, purpose, and necessity of their processing are determined by the underlying contractual relationship with the client.If necessary for fulfilling the contract by the controller, for protecting vital interests or required by law or if there is consent from the clients, their data will be disclosed or transferred to third parties or agents such as authorities, subcontractors or in the field of IT-, office- or similar services while observing professional legal requirements.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

9.4. Marketing Services

Description: The controller processes the data of its customers and clients (hereinafter uniformly referred to as "customers") in order to offer marketing services such as market research, advertising campaigns, content creation, and social media management. The required information is identified as such during the commissioning process and includes details necessary for service provision and billing, as well as contact information to facilitate any consultations. Insofar as access to information of end customers, employees, or other individuals is granted, it is processed in accordance with legal and contractual requirements.Processes that are necessary within the scope of marketing and advertising measures include creating marketing strategies and campaigns, designing advertising materials and content, selecting advertising channels and platforms, conducting market analyses and target group surveys, as well as measuring and analyzing the success of marketing actions. Furthermore, they involve managing and maintaining customer and prospect data, segmenting target groups, sending newsletters and promotional emails, tracking online marketing activities, as well as collaborating with external service providers in the field of marketing and advertising.These processes aim to develop effective marketing strategies for the controller's customers, design advertising measures tailored to specific target groups, measure and analyze the success of marketing activities, as well as ensure efficient management of customer contacts and information.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.), Payment Data (e.g. bank details, invoices, payment history), Contact data (e.g. postal and email addresses or phone numbers), Contract data (e.g. contract object, duration, customer category.
- **Data subjects:** Service recipients and clients, Prospective

customers, Business and contractual partners.

- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations, Communication, Office and organisational procedures, Organisational and Administrative Procedures.
- **Data sources:** Collection from data subjects, Receipt through transmission or other communication by business partners and clients, Data collection from other sources, Data collection through interfaces to services of other providers, Collection in connection with advertising and marketing campaigns.

9.5. Online Courses and Online Training

Description: The controller processes the data of participants in its online courses and training sessions to provide course and training services to the participants. The processed data, including their type, scope, purpose, and the necessity of their processing, are determined by the underlying contractual relationship. These data typically include information about the courses and services utilized, as well as personal preferences and results of the participants if part of the service offering. Processing also encompasses performance assessment and evaluation of the offered services and those of course and training instructors. Depending on the equipment and structure of the respective courses or learning content, additional processing activities may be required. This includes attendance tracking for documenting participation, progress monitoring for measuring and analyzing learning progress through collecting exam and test results, as well as analyzing interactions on learning platforms such as forum posts and assignment submissions.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

9.6. Software and Platform Services

Description: The controller processes the data of users, including registered and any test users (hereinafter collectively referred to as "users"), in order to be able to provide its contractual services to them. Furthermore, processing is based on legitimate interests, especially to ensure the security of the service and to develop it further. The details required within the context of contract, order, or comparable contract conclusion are marked as such and include information necessary for the provision of services and billing, as well as contact information to potentially hold consultations.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

9.7. Film and Television Production

Description: The controller processes the data of its clients and contractors to enable them to plan, produce, and distribute film and television content, as well as related services. The necessary details include information required for project realisation and billing, as well as contact information for necessary coordination. Insofar as the controller gains access to information from end customers, actors, employees or other individuals, these are processed in accordance with legal and contractual requirements.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Compliance with a legal obligation (Article 6 (1) (c) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.), Payment Data (e.g. bank details, invoices, payment history), Contact data (e.g. postal and email addresses or phone numbers), Contract data (e.g. contract object, duration, customer category.
- **Data subjects:** Service recipients and clients, Prospective customers, Business and contractual partners.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations, Communication, Office and organisational procedures, Organisational and Administrative Procedures.

10. Providers and services used in the course of business

Description: In the course of the controller's business activities, additional services, platforms, interfaces, or plug-ins from third parties (hereinafter referred to as "Services") are used in compliance with legal requirements. The use of these Services is based on the controller's interest in proper, lawful, and economical management of its business operations and internal organization.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Contract data (e.g. contract object, duration, customer category.

Data subjects: Service recipients and clients; Prospective customers; Business and contractual partners.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures.

Data sources: Receipt through transmission or other communication by business partners and clients; Collection from data subjects; Data collection through interfaces to services of other providers.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

10.1. Freshdesk

Description: Management of contact requests and communication.

- **Website:** https://www.freshworks.com.
- **Privacy Policy:** https://www.freshworks.com/privacy.
- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.

11. Payment Procedure

Description: In the context of contractual and other legal relationships, due to legal obligations or otherwise based on the legitimate interests of the controller, efficient and secure payment options are offered to the data subjects. For this purpose, in addition to banks and credit institutions, the controller employs additional service providers (collectively referred to as "payment service providers").

The data processed by payment service providers include inventory data, such as names and addresses, bank details, such as account numbers or credit card numbers, passwords, TANs (transaction authentication numbers), and checksums as well as contract-related information including amounts and recipient details. These details are necessary for conducting transactions. However, the entered data is exclusively processed and stored by the payment service providers. This means that the controller does not receive any account- or credit card-related information but only information confirming or denying payment. In some cases, payment service providers may transmit data to credit reporting agencies. This transmission serves identity verification and credit assessment purposes. In this context, reference is made to the general terms and conditions and privacy notices of the payment service providers.

Furthermore, the business terms and privacy notices of the respective payment service providers apply to payment transactions. These are accessible on their websites or transaction applications. The controller also refers to these for further information as well as for exercising rights of withdrawal, access, and other rights of affected persons.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Service recipients and clients; Business and contractual partners; Prospective customers.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations;

Business processes and management procedures.

Data sources: Receipt through transmission or other communication by business partners and clients; Collection from data subjects; Data collection through interfaces to services of other providers.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

11.1. Stripe

Description: Payment-Service-Provider (technical integration of online-payment-methods.

- **Service Provider:** Stripe, Inc., 510 Townsend Street, San Francisco, CA 94103, USA.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.
- **Website:** https://stripe.com/de;
- **Privacy Policy:** https://stripe.com/en-de/privacy;
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.), Payment Data (e.g. bank details, invoices, payment history), Contract data (e.g. contract object, duration, customer category.
- **Data subjects:** Service recipients and clients, Prospective customers.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

12. Provision of online services and web hosting

_____

Description: The data of the users is processed in order to provide them with the online services of the controller. For this purpose, the IP address of the users is also processed, which is necessary to transmit the contents and functions of the controller's online services to the user's browser or device.

Data categories: Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Log data (e.g. log files concerning logins or data retrieval or access times.); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).); Security measures; Content Delivery Network (CDN.

Data sources: Collection from users; Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

12.1. Provision of online offer on rented hosting space

Description: To provide our online services, storage space, computing capacity, and software are used, which are rented or otherwise obtained from a corresponding server provider (also referred to as "web host").

- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Provision of our online services and usability, Information technology infrastructure (Operation and

provision of information systems and technical devices, such as computers, servers, etc.).

12.2. Collection of Access Data and Log Files

Description: Access to the online service provided by the responsible party is logged in the form of so-called "server log files". The server log files can include the address and name of the accessed web pages and files, date and time of access, transferred data volumes, notification of successful retrieval, type of browser along with version, the user's operating system, referrer URL (the previously visited page), and usually IP addresses and the requesting provider. The server log files are used for security purposes, e.g., to prevent server overload (especially in the case of abusive attacks, known as DDoS attacks), and also to ensure the servers' load management and stability.

- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.;
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Security measures, Provision of our online services and usability, Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).

12.3. Content-Delivery-Network

Description: We use a so-called "Content Delivery Network" (CDN). A CDN is a service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet.

- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Processed data types:** Usage data (e.g. page views and

duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

- **Data subjects:** Users (e.g. website visitors, users of online services.

12.4. Cloudflare

Description: Content-Delivery-Network (CDN) - service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster and more securely with the help of regionally distributed servers connected via the Internet.

- **Service Provider:** Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.cloudflare.com;
- **Privacy Policy:** https://www.cloudflare.com/privacypolicy/;
- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.), Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Content Delivery Network (CDN.

12.5. Cyon

Description: Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities.

- **Website:** https://www.cyon.ch.
- **Privacy Policy:** https://www.cyon.ch/legal/datenschutzerklaerung.
- **Service Provider:** cyon GmbH, Brunngässlein 12, CH - 4052 Basel, Switzerland.

13. Use of Cookies

Description: The controller uses cookies in accordance with legal regulations. Accordingly, prior consent is obtained from users unless it is not required by law. Permission is particularly unnecessary when the storage and reading of information – including cookies – are absolutely necessary to provide a telemedia service (i.e., the online offer of the controller) explicitly requested by the users. The revocable consent is clearly communicated to users and contains information on the specific use of cookies.

Regarding the legal basis for data protection: The legal basis for processing personal data of users with the help of cookies by the controller depends on whether consent is obtained. If users give their consent, the processing of their data is based on this declared consent. Otherwise, the processing of data collected through cookies is based on legitimate interests of the controller (e.g., in an economic operation of his online offer and its improvement) or as part of fulfilling contractual obligations of the controller, if the use of cookies is necessary for this purpose.

Retention Period: A distinction is made between the following types of cookies:
Temporary Cookies (also known as session or session cookies): These are deleted at the latest after a user has left an online offer and closed his terminal device (e.g., browser or mobile application).

Permanent Cookies: These remain stored even after closing the terminal device and can be used e.g., to display login status directly upon revisiting a website or to hold preferred content as well as being used for reach measurement. Unless explicit information on the type and storage duration of cookies is provided by the controller (e.g., in obtaining consent), users should assume that these are permanent and may have a storage duration of up to two years.

General notes on revocation and objection (Opt-out): Users can revoke their given consents at any time and also declare an objection against processing their data according to legal provisions.

Within this Records of Processing Activities, files or other storage notes that store information on terminal devices and read it from them are understood as cookies. They can serve e.g., to save login status in a user account or content accessed or functions used in an online offer. In addition, cookies can be used for various purposes such as ensuring functionality, security, comfortability of online offers, as well as creating analyses of visitor flows.

Data Meta, communication and process data (e.g. IP addresses, timestamps,

categories: identification numbers, involved parties.

Data subjects: Users (e.g. website visitors, users of online services.

Data sources: Collection from users; Collection from data subjects.

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR); Consent (Article 6 (1) (a) GDPR.

13.1. Processing Cookie Data on the Basis of Consent

Description: The controller implements a consent management solution, where users' consent for the use of cookies or for the processes and providers mentioned within the scope of the consent management solution is obtained. This process serves to acquire, log, manage, and revoke consents, particularly regarding the use of cookies and similar technologies deployed for storing, reading out, and processing information on users' end devices. Within this process, users' consents for the use of cookies and the associated information processing activities, including those specific processes and providers mentioned in the consent management procedure, are obtained. Users also have the option to manage and revoke their consents. The declarations of consent are stored to avoid repeated queries and to provide proof of consent in accordance with legal requirements. Storage occurs server-side and/or in a cookie (so-called Opt-In-Cookie) or by using comparable technologies to assign the consent to a specific user or their device. In absence of specific details about providers of consent management services, the following general notes apply: The duration of consent storage is up to two years. During this time, a pseudonymous user identifier is created, which is stored along with the time of consent, details on the extent of consent (e.g., relevant categories of cookies and/or service providers), as well as information about the browser, system, and used end device.

- **Legal Basis:** Consent (Article 6 (1) (a) GDPR.

14. Special Notes on Applications (Apps)

_____

Description: The data of the application's users are processed by the controller as far as it is necessary for the provision of the application and its functionalities, to monitor its security, and to further develop the application. Furthermore, the controller may contact users in compliance with legal requirements if communication is necessary for purposes of administration or use of the application. Otherwise, with regard to processing user data, reference is made to the Records of Processing Activities.
The processing of data necessary for providing the functionalities of the application is carried out to fulfil contractual obligations of the controller. This also applies when providing functions requires authorisation from users (e.g., permissions for device functionalities). If processing data is not necessary for providing functionalities of the application but serves to secure the application or the commercial interests of the controller (e.g., collecting data for purposes of optimising the application or security reasons), it is based on legitimate interests of the controller. If users explicitly consent to their data being processed, this processing is based on such consent.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations; Security measures; Provision of our online services and usability.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

14.1. Storage of the universally unique identifier (UUID)

Description: For analytical purposes and to store user settings, the application uses a universal and unique identifier, also known as Universally Unique Identifier (UUID). This identifier is generated upon the installation of the application,

remains throughout its use and updates, and is deleted when users uninstall the application from their devices.

14.2. Device authorizations for access to functions and data

Description: The use of the application or its functionalities may require user permissions for accessing certain features of the devices used, or data stored on the devices or accessible with the help of the devices. These permissions must be granted by users by default and can be revoked at any time in the settings of the respective devices. The exact process for controlling app permissions may depend on the device and software being used by the user. If further explanations are needed, users can contact the controller. It is noted that refusing or revoking the relevant permissions may affect the functionality of the application.

15. Purchase of applications via Appstores

Description: The acquisition of the application from the controller is carried out via special online platforms that are operated by other service providers (so-called "Appstores"). In this context, in addition to the Records of processing activities of the controller, the privacy notices of the respective Appstores apply. This is particularly relevant with regard to the processes used on the platforms for reach measurement and interest-based marketing, as well as any potential costs involved.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. postal and email addresses or phone numbers); Contract data (e.g. contract object, duration, customer category); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Service recipients and clients; Users (e.g. website visitors, users of online services.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations; Marketing; Provision of our online services and usability.

Data sources: Collection from users; Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

15.1. Apple App Store

Description: App and software distribution platform.

- **Service Provider:** Apple Inc., Infinite Loop, Cupertino, CA 95014, USA.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.apple.com/app-store/;
- **Privacy Policy:** https://www.apple.com/privacy/privacy-policy/;
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.), Payment Data (e.g. bank details, invoices, payment history), Contact data (e.g. postal and email addresses or phone numbers),

Contract data (e.g. contract object, duration, customer category), Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

- **Data subjects:** Service recipients and clients.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

15.2. Google Play

Description: App and software distribution platform.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://play.google.com/store/apps?hl=en;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Processed data types:** Inventory data (For example, the full name, residential address, contact information, customer number, etc.), Payment Data (e.g. bank details, invoices, payment history), Contact data (e.g. postal and email addresses or phone numbers), Contract data (e.g. contract object, duration, customer category), Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Service recipients and clients.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

16. Registration, Login and User Account

Description: Users can create an account. During the registration process, users are informed of the necessary mandatory information and processed for the purpose of providing the user account on the basis of contractual obligation fulfillment by the controller. The data processed by the controller includes in particular login information (username, password, and an email address).
In the context of using registration and login functions as well as the use of the user account by the user, the controller stores the IP address and time of each user action. The storage is based on legitimate interests of both the controller and users in protection against misuse and other unauthorized use. Generally, this data is not shared with third parties unless it is necessary to pursue claims by the controller or there is a legal obligation to do so.
Users can be informed via email about processes relevant to their user account, such as technical changes. This is documented in the "Records of processing activities" of the controller.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Log data (e.g. log files concerning logins or data retrieval or access times.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations; Security measures; Organisational and Administrative Procedures; Provision of our online services and usability.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion"; Deletion after termination.

Legal bases: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

16.1. Registration with a real name

Description: The controller requests that users, due to the nature of the community, use the service under their real names. This means that the use of pseudonyms is not permitted.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

16.2. Deletion of data after termination

Description: If users have terminated their user account, their data relating to the user account will be deleted, subject to any legal permission, obligation or consent of the users.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

16.3. No obligation to retain data

Description: It is the responsibility of the users to secure their data upon termination before the end of the contract. The controller is authorized to irretrievably delete all data of the user stored during the term of the contract.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

17. Blogs and publication media

Description: Blogs or similar means of online communication and publication (hereinafter referred to as "publication medium") are used. The data of the readers is processed by the controller for the purposes of the publication medium only to the extent necessary for its presentation and the communication between authors and readers or for reasons of security. For further information on the processing of visitors' data in relation to the publication medium, please refer to the Records of Processing Activities.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Feedback (e.g. collecting feedback via online form); Provision of our online services and usability.

Data sources: Collection from users; Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

18. Contact and Inquiry Management

Description: When initiating contact with the responsible party (e.g., by mail, contact form, email, telephone, or via social media) as well as within the scope of existing user and business relationships, the information provided by the inquiring individuals is processed by the responsible party to the extent necessary for responding to contact requests and any requested actions.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Communication partner (Recipients of e-mails, letters, etc.

Purposes/interest: Communication; Organisational and Administrative Procedures; Feedback (e.g. collecting feedback via online form); Provision of our online services and usability.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR); Performance of a contract and prior requests (Article 6 (1) (b) GDPR.

18.1. Contact form

Description: When initiating contact via the contact form, by email, or through other communication channels, the controller processes the personal data transmitted to them for the purpose of responding to and processing the respective request. This typically includes details such as name, contact information, and possibly additional information provided that is necessary for appropriate processing. These data are used exclusively for the stated purpose of making contact and communication.

- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Processed data types:** Contact data (e.g. postal and email addresses or phone numbers), Content data (e.g. textual or

pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.), Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.
- **Purposes of processing:** Communication, Organisational and Administrative Procedures.

18.2. Freshdesk

Description: Management of contact requests and communication.

- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.freshworks.com;
- **Privacy Policy:** https://www.freshworks.com/privacy/;

18.3. Freshdesk

Description: Management of contact requests and communication.

- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.freshworks.com;
- **Privacy Policy:** https://www.freshworks.com/privacy/;

18.4. Freshdesk

Description: Management of contact requests and communication.

- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.freshworks.com;
- **Privacy Policy:** https://www.freshworks.com/privacy/;

18.5. Freshdesk

Description: Management of contact requests and communication.

- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.freshworks.com;
- **Privacy Policy:** https://www.freshworks.com/privacy/;

18.6. Freshdesk

Description: Management of contact requests and communication.

- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.freshworks.com;
- **Privacy Policy:** https://www.freshworks.com/privacy/;

19. Communication via Messenger

Description: For communication purposes, messengers are used, and attention is drawn to the following notes on the functionality of the messengers, encryption, use of communication metadata, and options for objection.
Contact can also be made via alternative means, such as telephone or email. The contact options have either been communicated or are specified within the online service.
In cases of end-to-end encryption of contents (i.e., the content of your message and attachments), it is noted that the communication contents (i.e., the content of the message and attached images) are encrypted from end to end. This means that the contents of messages are not visible, not even to the messenger providers themselves. It is recommended to always use an up-to-date version of the messenger with activated encryption to ensure encryption of message contents.
However, it is additionally noted that while messenger providers cannot see the content, they can ascertain that and when communication partners communicate with the responsible party as well as process technical information about the device used by communication partners and depending on their device settings also location information (so-called metadata).
Revocation, objection and deletion: A given consent can be revoked at any time; likewise, an objection to communication via messenger is possible at any time. In case of communication via messenger, messages are deleted according to the general deletion policies of the responsible party (i.e., as described above, after contractual relationships end or in context with archiving requirements etc.) and otherwise as soon as it can be assumed that any inquiries have been responded to; this also applies if no reference back to a previous conversation is expected and provided no legal retention obligations prevent deletion.
Reservation of referral to other means of communication: To ensure security, there is understanding on part of the responsible party that for certain reasons requests via messenger may not be answerable. This concerns situations where contract details need to be treated with particular confidentiality or a response via messenger does not meet formal requirements. In these cases, it is recommended to resort back to more suitable channels of communication.

Data categories: Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.

Data subjects: Communication partner (Recipients of e-mails, letters, etc.

Purposes/interest: Communication.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Consent (Article 6 (1) (a) GDPR); Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

20. Video Conferences, Online Meetings, Webinars and Screen-Sharing

_____

Description: The data controller employs platforms and applications for video and audio conferences, webinars, as well as other types of meetings (hereinafter collectively referred to as "conference"). Data processed by conference platforms: In the context of participating in a conference, the utilised conference platforms process personal data of the participants. The extent of data processing depends on the information required for a specific conference as well as optionally provided data. The processing includes not only conducting the conference itself but may also encompass security measures and service optimisations. The processed data comprise personal information (first name, last name), contact information (email address, phone number), access data (access codes or passwords), profile pictures, professional position/function, IP address of internet access, details on end devices, operating systems, browsers including technical and language settings, contents of communication processes such as chat contributions as well as audio and video data and the use of further features (e.g., polls). Communication content is encrypted within the technically feasible framework provided by the conference providers. For registered users of the conference platforms, additional data can be processed according to agreements with the respective provider.
Logging and recordings: Participants are transparently informed in advance about logging text entries, results from participations (such as survey results), as well as video or audio recordings and consent is obtained where necessary.
Data protection measures by participants: Participants are advised that they should inform themselves about the privacy policies of the utilised conference platforms and select appropriate security and privacy settings. Furthermore, measures should be taken to protect data and personal rights during video conferences (e.g., advising cohabitants, locking doors or using blurring functions for backgrounds). Links to conference rooms and access data should not be shared with unauthorised third parties.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g.

page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Images and/ or video recordings (e.g. photographs or video recordings of a person); Audio recordings; Log data (e.g. log files concerning logins or data retrieval or access times.

Data subjects: Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services); Persons depicted.

Purposes/interest: Provision of contractual services and fulfillment of contractual obligations; Communication; Office and organisational procedures.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

20.1. Google Hangouts / Meet

Description: Conference and communication software.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://hangouts.google.com/;
- **Privacy Policy:** https://policies.google.com/privacy;

20.2. Zoom

Description: Video conferences, online meetings, webinars, screen sharing, optional recording of sessions, chat function, integration with calendars and other apps.

- **Service Provider:** Zoom Video Communications, Inc., 55 Almaden Blvd., Suite 600, San Jose, CA 95113, USA.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://zoom.us;
- **Privacy Policy:** https://explore.zoom.us/en/privacy/;

21. Cloud Services

Description: Software services accessible over the Internet and executed on their providers' servers (known as "Cloud Services", also referred to as "Software as a Service") are used for storing and managing content (e.g., document storage and management, exchanging documents, content, and information with certain recipients or publishing content and information).
Within this context, personal data may be processed and stored on the providers' servers, insofar as they are part of communication processes with the controller or are otherwise processed by the controller, as outlined in the Records of Processing Activities. This data may include, in particular, basic personal data and contact details of users, data related to transactions, contracts, other processes, and their contents. The providers of cloud services further process usage data and metadata for security purposes and service optimization.
If forms or other documents and content are made available for other users or publicly accessible websites through the use of cloud services, the providers may store cookies on the users' devices for web analytics purposes or to save user settings (e.g., in the case of media control).

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Images and/ or video recordings (e.g. photographs or video recordings of a person.

Data subjects: Prospective customers; Communication partner (Recipients of e-mails, letters, etc.); Business and contractual partners; Users (e.g. website visitors, users of online services.

Purposes/interest: Office and organisational procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).); Provision of contractual services and fulfillment of contractual obligations.

Data sources: Collection from data subjects.

Retention and Deletion in accordance with the information provided in the section

deletion: "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

21.1. Adobe Creative Cloud

Description: Cloud storage, cloud infrastructure services, and cloud-based application software, among others for photo editing, video editing, graphic design, web development.

- **Service Provider:** Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.adobe.com/creativecloud.html;
- **Privacy Policy:** https://www.adobe.com/privacy.html;
- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.), Images and/ or video recordings (e.g. photographs or video recordings of a person.
- **Purposes of processing:** Provision of contractual services and fulfillment of contractual obligations.

21.2. Google Workspace

Description: Cloud storage, cloud infrastructure services and cloud-based application software.

- **Service Provider:** Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://workspace.google.com/;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Further Information:** https://cloud.google.com/privacy;
- **Processed data types:** Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.), Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features.
- **Data subjects:** Users (e.g. website visitors, users of online services.

21.3. Freshdesk

Description: Management of contact requests and communication.

- **Website:** https://www.freshworks.com.
- **Privacy Policy:** https://www.freshworks.com/privacy.
- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.

22. Newsletter and Electronic Communications

Description: Newsletters, emails, and other electronic notifications (hereinafter referred to as "newsletters") are sent exclusively with the consent of the recipients or on a legal basis. If the contents of the newsletter are specified at the time of subscription, these contents are decisive for the users' consent. Normally, providing an email address is sufficient for subscribing to the newsletter of the responsible party. However, in order to offer a personalized service, it may be necessary to request the name for personal salutation in the newsletter or further information if required for the purpose of the newsletter.

Email addresses that have been unsubscribed can be stored for up to three years on the basis of legitimate interests of the responsible party before being deleted in order to prove a previously given consent. The processing of this data is limited to the purpose of potentially defending against claims. An individual deletion request is possible at any time, provided that at the same time, former consent is confirmed. In case of obligations to permanently observe objections, the responsible party reserves the right to store email addresses solely for this purpose in a blocklist.

The logging of the registration process is based on legitimate interests of responsible parties to prove its proper execution. Email dispatch services are commissioned based on legitimate interests in an efficient and secure dispatch system by responsible parties.

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features.

Data subjects: Communication partner (Recipients of e-mails, letters, etc.

Purposes/interest: Direct marketing (e.g. by e-mail or postal.

Legal bases: Consent (Article 6 (1) (a) GDPR.

Contents: Information about us, our services, promotions and offers.

22.1. Measurement of opening rates and click rates

Description: The controller uses newsletters that contain a so-called "web beacon." This is a pixel-sized file that is retrieved from the controller's server or from a

dispatch service provider's server, if one is used, when the newsletter is opened. During this retrieval, technical information such as browser details and system information, as well as the IP address and the time of retrieval are collected. This data serves to technically optimise the newsletter based on technical data or audience analyses based on the locations of access (which can be identified through the IP address) or access times. The analysis also includes determining whether and when the newsletters are opened and which links are clicked. The collected information is assigned to individual recipients and stored in their profiles until deletion. These evaluations help to understand users' reading behaviour and adjust our content accordingly or send different content based on users' interests. The measurement of open and click rates, as well as the storage of these measurement results in user profiles, is based on users' consent.

- **Legal Basis:** Consent (Article 6 (1) (a) GDPR.
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.
- **Purposes of processing:** Direct marketing (e.g. by e-mail or postal.

22.2. Freshdesk

Description: Management of contact requests and communication.

- **Website:** https://www.freshworks.com.
- **Privacy Policy:** https://www.freshworks.com/privacy.
- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street, Suite 201, San Mateo, CA 94403, USA.

23. Commercial communication by E-Mail, Postal Mail, Fax or Telephone

---

Description: Personal data is processed by the controller for the purposes of promotional communication, which may take place through various channels such as email, telephone, mail, or fax in accordance with legal requirements. Recipients have the right to withdraw their consent at any time or to object to promotional communication at any time.
Following a withdrawal or objection, the data required to prove previous authorization for contact or dispatch will be stored by the controller for up to three years after the end of the year of withdrawal or objection on the basis of its legitimate interests. The processing of this data is limited to the purpose of potentially defending against claims. Based on the legitimate interest in permanently observing users' withdrawal or objection, the controller also stores the data necessary to prevent further contact (e.g., depending on the communication channel, email address, telephone number, name).

Data categories: Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.

Data subjects: Communication partner (Recipients of e-mails, letters, etc.

Purposes/interest: Direct marketing (e.g. by e-mail or postal); Marketing; Sales promotion.

Data sources: Receipt through transmission or other communication by business partners and clients; Collection from data subjects; Collection in connection with advertising and marketing campaigns; External databases, archives, and data collections.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Consent (Article 6 (1) (a) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

23.1. Freshdesk

Description: Management of contact requests and communication.

- **Website:** https://www.freshworks.com.
- **Privacy Policy:** https://www.freshworks.com/privacy.
- **Service Provider:** Freshworks, Inc., 2950 S.Delaware Street,

Suite 201, San Mateo, CA 94403, USA.

24. Web Analysis, Monitoring and Optimization

Description: Web analysis, also referred to as reach measurement, is used by the controller for evaluating visitor flows of the online service and may include behaviour, interests, or demographic information about visitors such as age or gender in the form of pseudonymous values. Through reach analysis, it is possible for the controller to identify when the online service or its functions or contents are most frequently used or invite reuse. Similarly, it can be understood which areas require optimisation.
Furthermore, the controller employs testing processes to test and optimise different versions of the online service or its components.
Unless stated otherwise below, profiles can be created for these purposes and information can be stored and read in a browser or on an end device. The data collected particularly includes visited websites and elements used there as well as technical information like the browser used, computer system, and details on usage times. If users have consented to the collection of their location data by the controller or towards providers of utilised services, processing of location data is also possible.
Moreover, the controller stores users' IP addresses using an IP masking process (i.e., pseudonymisation by shortening the IP address) to protect users. In the context of web analysis, A/B testing and optimisation, clear data from users (such as email addresses or names) are fundamentally not stored but pseudonyms are used instead. This means that neither the controller nor providers of employed software know users' actual identity but only information stored in their profiles for each respective process.
Notes on legal bases: If consent from users is obtained for third-party use, this consent serves as a legal basis for data processing. Otherwise user data processing is based on legitimate interests of the controller (i.e., interest in efficient, economical and recipient-friendly services). In this regard reference is made to cookie use according to "Records of processing activities".

Data categories: Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Web Analytics (e.g. access statistics, recognition of returning visitors);

Profiles with user-related information (Creating user profiles); Provision of our online services and usability.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion"; Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.

Security measures: IP Masking (Pseudonymization of the IP address.

Legal bases: Consent (Article 6 (1) (a) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

24.1. Google Analytics

Description: We use Google Analytics to perform measurement and analysis of the use of our online services by users based on a pseudonymous user identification number. This identification number does not contain any unique data, such as names or email addresses. It is used to assign analysis information to an end device in order to recognize which content users have accessed within one or various usage processes, which search terms they have used, have accessed again or have interacted with our online services. Likewise, the time of use and its duration are stored, as well as the sources of users referring to our online services and technical aspects of their end devices and browsers. In the process, pseudonymous profiles of users are created with information from the use of various devices, and cookies may be used. Google Analytics does not log or store individual IP addresses. Analytics does provide coarse geo-location data by deriving the following metadata from IP addresses: City (and the derived latitude, and longitude of the city), Continent, Country, Region, Subcontinent (and ID-based counterparts). For EU-based traffic, IP-address data is used solely for geo-location data derivation before being immediately discarded. It is not logged, accessible, or used for any additional use cases. When Analytics collects measurement data, all IP lookups are performed on EU-based servers before forwarding traffic to Analytics servers for processing.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR.
- **Website:** https://marketingplatform.google.com/intl/en/about/analytics/;

- **Privacy Policy:** https://policies.google.com/privacy;
- **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff;
- **Further Information:** https://business.safety.google/adsservices/ (Types of processing and data processed);
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors), Provision of our online services and usability.
- **Security measures:** IP Masking (Pseudonymization of the IP address.

24.2. Google Tag Manager

Description: We use Google Tag Manager, a software provided by Google, which enables us to manage so-called website tags centrally via a user interface. Tags are small code elements on our website that serve to record and analyse visitor activities. This technology assists us in improving our website and the content offered on it. Google Tag Manager itself does not create user profiles, store cookies with user profiles, or perform any independent analyses. Its function is limited to simplifying and making the integration and management of tools and services we use on our website more efficient. Nevertheless, when using Google Tag Manager, users' IP addresses are transmitted to Google, which is technically necessary to implement the services we use. Cookies may also be set in this process. However, this data processing only occurs if services are integrated via the Tag Manager. For more detailed information about these services and their data processing, please refer to the further sections of this privacy policy.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

- **Legal Basis:** Consent (Article 6 (1) (a) GDPR.
- **Website:** https://marketingplatform.google.com;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features.

25. Online Marketing

_____

Description: The data controller processes personal data for the purpose of online marketing, which may particularly include the marketing of advertising spaces or the display of advertising and other content based on potential user interests as well as measuring their effectiveness. For these purposes, user profiles are created and stored in a file (the so-called "cookie") or similar processes are used to store relevant information about the user for displaying the mentioned content. This includes, among other things, viewed content, visited websites, used online networks as well as communication partners and technical details such as the browser used, the computer system, and information about usage times and functions used. If users have consented to the collection of their location data, this can also be processed.

Furthermore, the data controller stores IP addresses of users, employing IP masking techniques for pseudonymisation by shortening the IP address to protect users. In the context of online marketing processes, no clear data of users (such as email addresses or names) are stored but pseudonyms are used instead. This means that neither the controller nor providers of online marketing processes know the actual identity of users but only the information stored in their profiles.

The data collected within these profiles is usually stored in cookies or by similar processes. These cookies can later be read and analysed on other websites and supplemented with further data and stored on the server of the provider of online marketing processes.

In exceptional cases, it is possible to assign clear data to profiles, especially when users are members of a social network whose online marketing process is being used and that network connects profiles with corresponding information. The controller points out that users can enter into additional agreements with providers, for example through consent during registration.

The controller generally only has access to aggregated information about the success of his advertisements. However, he can check within so-called conversion measurements which marketing measures have led to a conversion – for example, concluding a contract with him. Conversion measurement is solely aimed at analysing the success of these measures.

Unless otherwise stated it is assumed that employed cookies are stored for

a period of two years.
Regarding legal bases: When consent is sought for using third-party services this consent constitutes the legal basis for processing data. Otherwise processing is based on legitimate interests of the controller (i.e., interest in efficient economic operations beneficial to recipients). The controller refers affected individuals in "Records of processing activities" to information regarding cookie usage.

Data categories: Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Web Analytics (e.g. access statistics, recognition of returning visitors); Targeting (e.g. profiling based on interests and behaviour, use of cookies); Affiliate Tracking; Marketing; Profiles with user-related information (Creating user profiles); Conversion tracking (Measurement of the effectiveness of marketing activities); Provision of our online services and usability.

Data sources: Collection from data subjects; Data collection from other sources.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion"; Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.

Security measures: IP Masking (Pseudonymization of the IP address.

Legal bases: Consent (Article 6 (1) (a) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

25.1. Google Ad Manager

Description: The controller uses the service "Google Ad Manager" to place advertisements within the Google advertising network (e.g., in search results, videos, websites, etc.). The Google Ad Manager is characterized by the real-time display of advertisements based on presumed user interests. This enables the controller to specifically show ads for their online services to users who may potentially be interested in what they offer or have already shown interest, as well as to measure the success of these ads.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://marketingplatform.google.com;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Further Information:** Types of processing and data processed: https://business.safety.google/adsservices/; Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: https://business.safety.google/adscontrollerterms; where Google acts as processor, Data Processing Conditions for Google Advertising Products and standard contractual clauses for data transfers to third countries: https://business.safety.google/adsprocessorterms apply;
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors), Targeting (e.g. profiling based on interests and behaviour, use of cookies), Profiles with user-related information (Creating user profiles), Provision of our online services and usability.

25.2. Google Ads and Conversion Tracking

Description: Online marketing process for purposes of placing content and advertisements within the provider's advertising network (e.g., in search results, in videos, on web pages, etc.) so that they are displayed to users who have a presumed interest in the ads. Furthermore, we measure the conversion of the ads, i.e. whether the users took them as a reason to interact with the ads and make use of the advertised offers (so-called conversion). However, we only receive anonymous information and no personal information about individual users.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR.

- **Website:** https://marketingplatform.google.com;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Further Information:** Types of processing and data processed: https://business.safety.google/adsservices/; Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: https://business.safety.google/adscontrollerterms;
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors), Conversion tracking (Measurement of the effectiveness of marketing activities), Marketing.

25.3. LinkedIn Insight Tag

Description: Code that is loaded when a user visits our online offering and tracks the user's behavior and conversions, as well as stores it in a profile (possible use cases: measuring campaign performance, optimizing ad delivery, building custom and similar target groups).

- **Service Provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland.
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR.
- **Website:** https://www.linkedin.com;
- **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy, cookie policy: https://www.linkedin.com/legal/cookie_policy;
- **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out;

26. Profiles in Social Networks (Social Media)

Description: The controller maintains online presences within social networks and processes user data in this context to communicate with active users or to offer information about themselves.
The data controller informs the individuals concerned in the privacy notices that user data may be processed outside the European Union. This could pose risks to users because, for example, it could make it more difficult to enforce their rights.
Furthermore, the data controller typically processes user data within social networks for market research and advertising purposes. Based on user behavior and resulting interests, usage profiles can be created. These profiles may be used to place advertisements inside and outside of the networks that could match the interests of the users. Consequently, cookies are usually stored on the users' computers, which save their usage behavior and interests. In addition, data may be stored in the usage profiles regardless of the devices used by the users (especially if they are members of the respective platforms and logged in there).
For a detailed description of each processing activity and how to opt-out, the data controller refers to the privacy policies and information provided by the operators of the respective networks.
Regarding requests for information and exercising of subject rights, the data controller advises users that these can most effectively be made directly with the providers. Only these entities have access to user data and can take direct action as well as provide information. Should individuals still require assistance, the data controller is available to help.

Data categories: Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.); Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Communication; Feedback (e.g. collecting feedback via online form); Public relations.

Data sources: Collection from data subjects; Data collection through interfaces to services of other providers.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion".

Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR.

26.1. Instagram

Description: Social network, allows the sharing of photos and videos, commenting on and favouriting posts, messaging, subscribing to profiles and pages.

- **Service Provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.instagram.com;
- **Privacy Policy:** https://privacycenter.instagram.com/policy/;

26.2. Facebook Pages

Description: Profiles within the social network Facebook - The controller, as joint controller with Meta Platforms Ireland Limited, is responsible for the collection (but not the further processing) of data from visitors to the Facebook page (also known as "Fanpage"). This data includes information on the types of content that users view or interact with, or actions they take (see "Things you and others do and provide" in the Facebook Data Policy: https://www.facebook.com/privacy/policy/), as well as information about the devices used by users (e.g., IP addresses, operating system, browser type, language settings, cookie data; see "Device information" in the Facebook Data Policy: https://www.facebook.com/privacy/policy/). According to the Facebook Data Policy, Facebook also collects and uses information to provide analytical services, known as "Page Insights", for page operators so they can gain insights into how people interact with their pages and with content associated with them. A specific agreement has been concluded with Facebook ("Information about Page Insights", https://www.facebook.com/legal/terms/page_controller_addendum), which particularly governs what security measures Facebook must observe and where Facebook has agreed to fulfil the rights of data subjects (i.e., users can direct requests for access or deletion directly to Facebook). The rights of users (especially regarding access, deletion, objection, and complaint to a competent supervisory authority) are not restricted by the agreements with Facebook. Further details can be found in the "Information about Page Insights" (https://www.facebook.com/legal/terms/information_about_page_insights_data). The joint controllership is limited to the collection and transmission of

data to Meta Platforms Ireland Limited, a company based in the EU. The further processing of data is solely under the responsibility of Meta Platforms Ireland Limited, which specifically includes transferring data to its parent company Meta Platforms Inc. in the USA.;

- **Service Provider:** Meta Platforms Ireland Limited, Merrion Road, Dublin 4, D04 X2K5, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.facebook.com;
- **Privacy Policy:** https://www.facebook.com/privacy/policy/;

26.3. LinkedIn

Description: Social network - The controller is jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of data from visitors used to generate "Page Insights" (statistics) of the controller's LinkedIn profiles. This data includes information about the types of content users view or interact with, as well as actions they take. Additionally, the controller collects details about the devices used, such as IP addresses, operating system, browser type, language settings, and cookie data, as well as information from user profiles like job function, country, industry, seniority level, company size and employment status. Privacy information regarding LinkedIn's processing of user data can be found in LinkedIn's privacy policy: https://www.linkedin.com/legal/privacy-policy.The controller has entered into a specific agreement with LinkedIn Ireland ("Page Insights Joint Controller Addendum", https://legal.linkedin.com/pages-joint-controller-addendum), which specifically regulates which security measures LinkedIn must observe and in which LinkedIn has agreed to fulfill the rights of the data subjects (i.e., users can direct requests for access or deletion directly to LinkedIn). The rights of users (in particular the right to access, deletion, objection and complaint to the competent supervisory authority) are not restricted by agreements with LinkedIn. The joint responsibility is limited to the collection and transmission of data to LinkedIn Ireland Unlimited Company, a company based in the EU. The further processing of data is solely incumbent upon LinkedIn Ireland Unlimited Company, particularly concerning the transmission of data to its parent company LinkedIn Corporation in the USA.;

- **Service Provider:** LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://www.linkedin.com;

- **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy;
- **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out;

27. Plugins and embedded functions and content

_____

Description: The controller integrates functional and content elements into the online service, which are obtained from the servers of the respective providers (hereinafter referred to as "third-party providers"). This includes, but is not limited to, graphics, videos, or city maps (hereinafter collectively referred to as "content"). The integration of this content requires that third-party providers process the IP address of users since without it, the transmission of content to the browser is not possible. Thus, the IP address is necessary for the display of these contents or functions. The controller aims to use only content for which the respective providers use the IP address solely for delivering the content. Third-party providers may also use so-called pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. Through these pixel tags, information such as visitor traffic on the pages of the online service can be evaluated. The pseudonymized information can also be stored in cookies on users' devices and linked with technical information about the browser and operating system, referring websites, time of visit, and other data regarding the use of the online service. This information may also be merged with data from other sources.
Regarding legal bases: If consent from users is obtained by the controller for the use of third-party providers, their consent serves as a legal basis for data processing. Otherwise, user data is processed based on legitimate interests of the controller (i.e., interest in efficient, economical services that are friendly to recipients). In this context, within records of processing activities',

Data categories: Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties); Inventory data (For example, the full name, residential address, contact information, customer number, etc.); Contact data (e.g. postal and email addresses or phone numbers); Content data (e.g. textual or pictorial messages and contributions, as well as information pertaining to them, such as details of authorship or the time of creation.

Data subjects: Users (e.g. website visitors, users of online services.

Purposes/interest: Provision of our online services and usability.

Data sources: Collection from data subjects.

Retention and deletion: Deletion in accordance with the information provided in the section "General Information on Data Retention and Deletion"; Storage of cookies for up to 2 years (Unless otherwise stated, cookies and similar storage methods may be stored on users' devices for a period of two years.

Legal bases: Consent (Article 6 (1) (a) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR.

27.1. Google Fonts (from Google Server)

Description: Obtaining fonts (and symbols) for the purpose of a technically secure, maintenance-free and efficient use of fonts and symbols with regard to timeliness and loading times, their uniform presentation and consideration of possible restrictions under licensing law. The provider of the fonts is informed of the user's IP address so that the fonts can be made available in the user's browser. In addition, technical data (language settings, screen resolution, operating system, hardware used) are transmitted which are necessary for the provision of the fonts depending on the devices used and the technical environment. This data may be processed on a server of the provider of the fonts in the USA - When visiting our online services, users' browsers send their browser HTTP requests to the Google Fonts Web API. The Google Fonts Web API provides users with Google Fonts' cascading style sheets (CSS) and then with the fonts specified in the CCS. These HTTP requests include (1) the IP address used by each user to access the Internet, (2) the requested URL on the Google server, and (3) the HTTP headers, including the user agent describing the browser and operating system versions of the website visitors, as well as the referral URL (i.e., the web page where the Google font is to be displayed). IP addresses are not logged or stored on Google servers and they are not analyzed. The Google Fonts Web API logs details of HTTP requests (requested URL, user agent, and referring URL). Access to this data is restricted and strictly controlled. The requested URL identifies the font families for which the user wants to load fonts. This data is logged so that Google can determine how often a particular font family is requested. With the Google Fonts Web API, the user agent must match the font that is generated for the particular browser type. The user agent is logged primarily for debugging purposes and is used to generate aggregate usage statistics that measure the popularity of font families. These aggregate usage statistics are published on Google Fonts' Analytics page. Finally, the referral URL is logged so that the data can be

used for production maintenance and to generate an aggregate report on top integrations based on the number of font requests. Google says it does not use any of the information collected by Google Fonts to profile end users or serve targeted ads.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR.
- **Website:** https://fonts.google.com/;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Further Information:** https://developers.google.com/fonts/faq/privacy?hl=en;
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.
- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Provision of our online services and usability.

27.2. YouTube videos

Description: Video contents.

- **Service Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, , parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR.
- **Website:** https://www.youtube.com;
- **Privacy Policy:** https://policies.google.com/privacy;
- **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://myadcenter.google.com/personalizationoff;
- **Processed data types:** Usage data (e.g. page views and duration of visit, click paths, intensity and frequency of use, types of devices and operating systems used, interactions with content and features), Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties.

- **Data subjects:** Users (e.g. website visitors, users of online services.
- **Purposes of processing:** Web Analytics (e.g. access statistics, recognition of returning visitors), Targeting (e.g. profiling based on interests and behaviour, use of cookies), Affiliate Tracking, Marketing, Provision of our online services and usability.
- **Data sources:** Collection from users.

28. Organisational Measures

Description: Organisational measures have been taken to ensure an adequate level of data protection and its maintenance.

28.1. Data protection management system, or data protection concept

Description: The Processor has implemented an appropriate data protection management system (also referred to as data protection concept) and ensures its implementation.

28.2. Organizational structure for data security and data protection

Description: A suitable organizational structure for data security and data protection is in place and information security is integrated into company-wide processes and procedures.

28.3. Observation of the state of the art and necessary implementation

Description: The development of the state of the art as well as developments, threats and security measures are continuously monitored and derived in a suitable manner to the own security concept.

28.4. Careful selection of service providers/freelancers and, if necessary, obligation to confidentiality

Description: Service providers who are engaged to perform ancillary tasks (maintenance, security, transport and cleaning services, freelancers, etc.) are carefully selected and it is ensured that they respect the protection of personal data. If the service providers are given access to the Data processed for the Customer in the course of their activities or if there is any other risk of access to the personal data, they have to be specifically bound to secrecy and confidentiality.

28.5. Data protection by design

Description: The protection of personal data shall be taken into account, taking into account the state of the art, implementation costs and the nature, scope, context and purposes of the Processing, as well as the varying likelihood and severity of risks for rights and freedoms of natural persons posed by the Processing, already at the stage of development or selection of hardware, software and procedures, in accordance with the principle of data protection by design and by using privacy friendly presets.

28.6. Current status of hardware and software

Description: Software and hardware used shall always be kept up to date and software updates shall be carried out without delay within a reasonable period of time in consideration of the degree of risk and any need for review. No software and hardware is used which is no longer updated by their providers or makers with regard to data protection and data security issues (e.g. expired operating systems).

28.7. Purchase of standard software and updates from trustworthy sources

Description: Standard software and corresponding updates are only obtained from trusted sources.

28.8. Paperless office

Description: A "paperless office" is being maintained, which means that documents are generally only stored digitally and only in exceptional cases in paper form.

28.9. Appropriate disposal, erasure and deletion concept

Description: A erasure, deletion and disposal concept corresponding to the data protection requirements of the Processing and the state of the art is in place. The physical destruction of documents and data carriers is carried out in compliance with data protection regulations and in accordance with legal requirements, industry standards and state-of-the-art industry norms (e.g. DIN 66399). Employees have been informed about legal requirements, deletion periods and, where applicable, about specifications for data deletion or equipment destruction by appropriate service providers.

29. Data Protection at Employee Level

Introduction Data protection at employee level: Measures have been taken to ensure that employees involved in the processing of personal data have the necessary expertise and reliability required by data protection law.

29.1. Employee commitment to data protection confidentiality

Description: Employees are bound to confidentiality and secrecy with regard to data protection.

29.2. Training and awareness raising of employees

Description: Employees are made aware of and informed about data protection in accordance with the requirements of their function. The training and awareness raising is repeated at appropriate intervals or as and when required by circumstances.

29.3. Withdrawal of access and entry authorisations of departing employees

Description: The keys, access cards or codes issued to employees, as well as authorisations granted with regard to the processing of the Data, shall be collected or revoked after they leave the services of the Processor or after the change of their responsibilities.

29.4. Clean Desk Policy

Description: Employees are obliged to leave their working environment tidy and thus in particular to prevent access to documents or data carriers containing personal data (Clean Desk Policy).

30. Electronic Access Control

Introduction Electronic Access control: Electronic access control measures have been put in place to ensure that access (i.e. already the possibility of exploitation, use or observation) by unauthorised persons to systems, data processing equipment or procedures is being prevented.

30.1. Password concept according to the state of the art

Description: A password concept specifies that passwords must have a minimum length and complexity in line with the state of the art and security requirements.

30.2. Password protection of all data processing systems

Description: All data processing systems are password protected.

30.3. Passwords are not stored or transmitted in plain text

Description: Passwords are generally not stored in plain text and are only transmitted hashed or encrypted.

30.4. Using Password Management Software

Description: A password management software is used.

30.5. Deletion of access information of departing employees

Description: Access credentials are deleted or deactivated when their users have left the company or organization of the Processor.

30.6. Use of up-to-date anti-virus software

Description: Up-to-date anti-virus software is used.

30.7. Use of software firewall(s)

Description: Use of software firewall(s).

31. Internal Access Control (permissions for user rights of access to and amendment of data)

Introduction internal Access, input, change and deletion control: Internal access control measures have been put in place to ensure that persons authorised to use a data processing system can only access the Data covered by their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during the Processing. Furthermore, input control measures have been taken to ensure that it is possible to subsequently check and establish whether and by whom the Data have been input, modified, removed or otherwise processed in data processing systems.

31.1. Appropriate authorisation concept

Description: A rights and roles concept (authorisation concept) ensures that access to personal data is only possible for a group of people selected according to necessity and only to the extent necessary.

31.2. Regular check of the authorisation concept

Description: The rights and roles concept (authorisation concept) is evaluated regularly, within a reasonable time frequency and when required by an occasion (e.g. violations of access restrictions), and updated as necessary.

31.3. Control of the administrators

Description: The activities of the administrators are appropriately monitored and recorded to the extent permitted by law and to the extent technically feasible.

31.4. General traceability of data access

Description: It is ensured that it is traceable which employees or agents had access to which Data and when (e.g. by logging software usage or drawing conclusions from access times and the authorization concept).

32. Transmission Control

Introduction Transmission control: Measures have been taken to control the transmission of the Data to ensure that the Data cannot be read, copied, modified or deleted by unauthorised persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

32.1. Remote access / remote maintenance via VPN

Description: When accessing internal systems from outside (e.g. for remote maintenance), encrypted transmission technologies are used (e.g. VPN).

32.2. Transit encryption of e-mails

Description: E-mails are encrypted during transmission. E-mails are encrypted during transit, which means that the emails are protected against being read by someone with access to the networks through which the email is travelling, on its way from the sender to the destination.

32.3. Encrypted transmission of data via websites (TLS)

Description: The transmission and processing of the client's personal data via online offers (websites, apps, etc.) is protected by TLS or equivalent secure encryption.

33. Adherence to Instructions, Purpose Limitation and Separation Control

Introduction Adherence to Instructions, Purpose Limitation and Separation control: Measures have been taken to ensure that Data processed on behalf of the Customer are only processed in accordance with the instructions of the Customer. The measures ensure that the Data collected for different purposes are processed separately and that there is no merging, combining or other combined processing of the Data contrary to the instructions.

33.1. Separate documentation of the Processing

Description: The processing operations carried out on behalf of the Customer shall be separately documented to an appropriate extent in a record of processing activities.

33.2. Careful selection of sub-processors and service providers

Description: Careful selection of sub-processors and other service providers.

33.3. Forwarding of instructions to employees and sub-processors

Description: Employees and agents are informed in a clear and comprehensible manner about the instructions of the Customer and the permitted processing framework and are trained accordingly. Separate information and training is not required if compliance with the instructions can be reasonably expected in any event, e.g. due to other agreements or internal practice.

33.4. Verification of compliance with instructions

Description: Compliance with instructions of the Customer and the permissible scope of processing of personal data by employees and contractors of the Processor is reviewed at appropriate intervals.

33.5. Adherence to the deletion periods

Description: The deletion terms which apply to the Processing of the Customer's Data shall if necessary be separately documented within the deletion policy of the Processor.

33.6. Logical separation of the client's data

Description: The Data of the Customer shall be processed logically separated from data of other processing operations of the Processor and protected against unauthorised access or connection or combination or mixing with other data (e.g. by storage in different databases or by appropriate attributes).

33.7. Separation of productive, test and development environment

Description: Production and test data are stored strictly separately from each other in different systems. The productive systems are operated separately and independently of the development and test systems.

34. Ensuring the integrity and availability of data as well as the resilience of processing systems

_____

Description: Measures have been taken to ensure that personal data are protected against accidental destruction or loss and can be quickly restored in an emergency.

34.1. Use of fail-safe, redundant server systems and services

Description: Fail-safe server systems and services are used, which are designed as redundant dual or multiple systems.

34.2. Storage of Data with external and reliable hosting providers

Description: The Data is stored with external hosting providers. The hosting providers are carefully selected and comply with the state of the art in terms of protection against damage caused by fire, moisture, power failures, disasters, unauthorized access, data backup and patch management as well as facility security.

34.3. Regular and documented patch management

Description: The Processing of Data is carried out on data processing systems which are subject to regular and documented patch management, i.e. in particular regularly updated.

34.4. Fail-safe power supply of server systems

Description: The server systems used for processing have an uninterruptible power supply (UPS), which is adequately secured against failures and ensures a controlled shutdown in emergencies without data loss.

34.5. Fire protection of the server systems

Description: The server systems used for processing have adequate fire protection (fire and smoke detection systems and appropriate fire extinguishing devices or fire extinguishing equipment).

34.6. Protection of server systems against moisture damage

Description: Server systems are used that have protection against moisture damage (e.g. moisture detectors).

34.7. Protection of data records against accidental modification or deletion

Description: The Customer's data records are protected by the system against inadvertent modification or deletion (e.g. by access restrictions, security checks and backups).

34.8. Adequate, reliable and controlled backup & recovery

Description: Server systems and services are used which have an appropriate, reliable and controlled backup & recovery concept.