

Privacy Policy

Preamble

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.

Last Update: 18 September 2026 (version D-1.3)

Table of contents

Preamble
Controller
Overview of processing operations
Relevant legal bases
Security Precautions
Transmission of Personal Data
International data transfers
General Information on Data Retention and Deletion
Rights of Data Subjects
Business services
Business processes and operations
Providers and services used in the course of business
Payment Procedure
Provision of online services and web hosting
Use of Cookies
Registration, Login and User Account
Contact and Inquiry Management
Communication via Messenger
Profiles in Social Networks (Social Media)
Management, Organization and Utilities
Changes and Updates
Terminology and Definitions

Controller

Daniël, Bonnema c/o POSTFLEX PFX-606-638 Emsdettener Straße 10 48268, Greven, Germany

Authorised Representatives: Daniël, Bonnema

E-mail address: info@nutritiongnome.com

Legal Notice: <https://nutritiongnome.com/impressum/>

Overview of processing operations

The following table summarises the types of data processed, the purposes for which they are processed and the concerned data subjects.

Categories of Processed Data

Inventory data.

Payment Data.
Contact data.
Content data.
Contract data.
Usage data.
Meta, communication and process data.
Log data.

Special Categories of Data

Health Data.

Categories of Data Subjects

Service recipients and clients.
Prospective customers.
Communication partner.
Users.
Business and contractual partners.
Third parties.
Customers.

Purposes of Processing

Provision of contractual services and fulfillment of contractual obligations.
Communication.
Security measures.
Office and organisational procedures.
Organisational and Administrative Procedures.
Feedback.
Marketing.
Provision of our online services and usability.
Information technology infrastructure.
Financial and Payment Management.
Public relations.
Sales promotion.
Business processes and management procedures.
Web analytics.

Relevant legal bases

Relevant legal bases according to the GDPR: In the following, you will find an overview of the legal basis of the GDPR on which we base the processing of personal data. Please note that in addition to the provisions of the GDPR, national data protection provisions of your or our country of residence or domicile may apply. If, in addition, more specific legal bases are applicable in individual cases, we will inform you of these in the data protection declaration.

Consent (Article 6 (1) (a) GDPR) - The data subject has given consent to the processing of his or her personal data for one or more specific purposes.

Performance of a contract and prior requests (Article 6 (1) (b) GDPR) - Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Compliance with a legal obligation (Article 6 (1) (c) GDPR) - Processing is necessary for compliance with a legal obligation to which the controller is subject.

Legitimate Interests (Article 6 (1) (f) GDPR) - the processing is necessary for the protection of the legitimate interests of the controller or a third party, provided that the interests, fundamental rights, and freedoms of the data subject, which require the protection of personal data, do not prevail.

Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR) - The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

National data protection regulations in Germany: In addition to the data protection regulations of the GDPR, national regulations apply to data protection in Germany. This includes in particular the Federal Data Protection Act (BDSG). In particular, the BDSG contains special provisions on the right to access, the right to erase, the right to object, the processing of special categories of personal data, processing for other purposes and transmission as well as automated individual decision-making, including profiling. Furthermore, data protection laws of the individual federal states may apply.

Reference to the applicability of the GDPR and the Swiss DPA: This privacy policy is intended to provide information in accordance with both the Swiss Federal Act on Data Protection (FADP) and the General Data Protection Regulation (GDPR). Where references are made to concepts such as the processing of personal data, legitimate interests, or special categories of data, these references are to be understood in accordance with the applicable data protection laws. Within the scope of application of the Swiss FADP, the legal interpretation of these terms is determined exclusively by Swiss law.

Security Precautions

We take appropriate technical and organisational measures in accordance with the legal requirements, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, in order to ensure a level of security appropriate to the risk.

The measures include, in particular, safeguarding the confidentiality, integrity and availability of data by controlling physical and electronic access to the data as well as access to, input, transmission, securing and separation of the data. In addition, we have established procedures to ensure that data subjects' rights are respected, that data is erased, and that we are prepared to respond to data threats rapidly. Furthermore, we take the protection of personal data into account as early as the development or selection of hardware, software and service providers, in accordance with the principle of privacy by design and privacy by default.

Securing online connections through TLS/SSL encryption technology (HTTPS): To protect the data of users transmitted via our online services from unauthorized access, we employ TLS/SSL encryption technology. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the cornerstones of secure data transmission on the internet. These technologies encrypt the information that is transferred between the website or app and the user's browser (or between two servers), thereby safeguarding the data from unauthorized access. TLS, as the more advanced and secure version of SSL, ensures that all data transmissions conform to the highest security standards. When a website is secured with an SSL/TLS certificate, this is indicated by the display of HTTPS in the URL. This serves as an indicator to users that their data is being securely and encryptedly transmitted.

Transmission of Personal Data

In the course of processing personal data, it may happen that this data is transmitted to or disclosed to other entities, companies, legally independent organizational units, or individuals. Recipients of this data may include service providers tasked with IT duties or providers of services and content that are integrated into a website. In such cases, we observe the legal requirements and particularly conclude relevant contracts or agreements that serve to protect your data with the recipients of your data.

International data transfers

Data Processing in Third Countries: If we transfer data to a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)), or if this occurs in the context of using third-party services or the disclosure or transfer of data to other individuals, entities, or companies (which becomes apparent either from the postal address of the respective provider or when explicitly mentioned in the privacy policy regarding data transfer to third countries), this is always done in accordance with legal requirements.

For data transfers to the USA, we primarily rely on the Data Privacy Framework (DPF), which has been recognized as a secure legal framework by the EU Commission's adequacy decision of July 10, 2023. Additionally, we have concluded Standard Contractual Clauses with the respective providers, which comply with the EU Commission's requirements and establish contractual obligations to protect your data.

This dual safeguard ensures comprehensive protection of your data: The DPF serves as the primary level of protection, while the Standard Contractual Clauses act as an additional security measure. Should any changes occur within the DPF framework, the Standard Contractual Clauses will serve as a reliable fallback option. This ensures that your data remains adequately protected even in the event of political or legal changes.

For individual service providers, we will inform you whether they are certified under the DPF and if Standard Contractual Clauses are in place. The list of certified companies and further information about the DPF can be found on the U.S. Department of Commerce's website at <https://www.dataprivacyframework.gov/>.

For data transfers to other third countries, appropriate safeguards apply, particularly Standard Contractual Clauses, explicit consent, or legally required transfers. Information on third-country transfers and applicable 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.

We will inform you which of our service providers are certified under the Data Privacy Framework as part of our data protection notices.

General Information on Data Retention and Deletion

We delete personal data that we process in accordance with legal regulations as soon as the underlying consents are revoked or no further legal bases for processing exist. This applies to cases where the original purpose of processing is no longer applicable or the data is no longer needed. Exceptions to this rule exist if statutory obligations or special interests require a longer retention or archiving of the data.

In particular, data that must be retained for commercial or tax law reasons, or whose storage is necessary for legal prosecution or protection of the rights of other natural or legal persons, must be archived accordingly.

Our privacy notices contain additional information on the retention and deletion of data specifically applicable to certain processing processes.

In cases where multiple retention periods or deletion deadlines for a data item are specified, the longest period always prevails.

Data that is no longer stored for its originally intended purpose but due to legal requirements or other reasons are processed exclusively for the reasons justifying their retention.

Data Retention and Deletion: The following general deadlines apply for the retention and archiving according to German law:

10 Years - Fiscal Code/Commercial Code - Retention period for books and records, annual financial statements, inventories, management reports, opening balance sheet as well as the necessary work instructions and other organisational documents (Section 147 Paragraph 1 No. 1 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 1 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).

8 years - Accounting documents, such as invoices, booking and expense receipts (Section 147 Paragraph 1 No. 4 and 4a in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 14b Paragraph 1 of the German VAT Act (UStG), Section 257 Paragraph 1 No. 4 in conjunction with Paragraph 4 of the German Commercial Code (HGB))

6 Years - Other business documents: received commercial or business letters, copies of dispatched commercial or business letters, and other documents to the extent that they are significant for taxation purposes, for example, hourly wage slips, operating accounting sheets, calculation documents, price tags, as well as payroll accounting documents, provided they are not already accounting vouchers and cash register tapes (Section 147 Paragraph 1 No. 2, 3, 5 in conjunction with Paragraph 3 of the German General Tax Code (AO), Section 257 Paragraph 1 No. 2 and 3 in conjunction with Paragraph 4 of the German Commercial Code (HGB)).

3 Years - Data required to consider potential warranty and compensation claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experiences and common industry practices, will be stored for the duration of the regular statutory limitation period of three years. This

period begins at the end of the year in which the relevant contractual transaction took place or the contractual relationship ended in the case of ongoing contracts (Sections 195, 199 of the German Civil Code).

Start of the period at the end of the year: If a period does not expressly 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. In the case of ongoing contractual relationships in the context of which data is stored, the event triggering the deadline is the time at which the termination or other termination of the legal relationship takes effect.

Rights of Data Subjects

Rights of the Data Subjects under the GDPR: As data subject, you are entitled to various rights under the GDPR, which arise in particular from Articles 15 to 21 of the GDPR:

Right to Object: You have the right, on grounds arising from your particular situation, to object at any time to the processing of your personal data which is based on letter (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of the personal data concerning you for the purpose of such marketing, which includes profiling to the extent that it is related to such direct marketing.

Right of withdrawal for consents: You have the right to revoke consents at any time.

Right of access: You have the right to request confirmation as to whether the data in question will be processed and to be informed of this data and to receive further information and a copy of the data in accordance with the provisions of the law.

Right to rectification: You have the right, in accordance with the law, to request the completion of the data concerning you or the rectification of the incorrect data concerning you.

Right to Erasure and Right to Restriction of Processing: In accordance with the statutory provisions, you have the right to demand that the relevant data be erased immediately or, alternatively, to demand that the processing of the data be restricted in accordance with the statutory provisions.

Right to data portability: You have the right to receive data concerning you which you have provided to us in a structured, common and machine-readable format in accordance with the legal requirements, or to request its transmission to another controller.

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a data protection supervisory authority if you consider that the processing of your personal data infringes the GDPR. In particular, you may lodge a complaint with a supervisory authority in the Member State of your habitual residence, place of work or the place of the alleged infringement.

Business services

We process personal data of our contractual and business partners, such as Customers, Clients, Prospective Customers, Suppliers and other cooperation partners (collectively referred to as "Contractual Partners"), for the initiation, execution and settlement of contractual relationships as well as comparable legal relationships. This also includes pre-contractual measures carried out at the request of the parties and communication related to the respective contractual relationship.

Processing serves in particular to fulfil our primary and secondary contractual obligations. This includes providing the agreed services, any update and information obligations, handling warranty claims and other service disruptions, processing revocations, terminations of continuing obligations, reversals, refunds as well as handling other contract-related statements and enquiries. Both one-off contracts and ongoing contractual relationships are covered.

In particular, we process master data such as name, address and where applicable company name; contact details such as email address and telephone number; contract and service data such as subject matter of the contract, duration of the contract, order or transaction number; usage and performance data; payment and billing data; as well as communication content and histories. Where necessary, we also process data disclosed or transmitted to us in connection with carrying out an assignment.

Furthermore, we process the data to safeguard our rights and to comply with legal obligations. This particularly includes commercial law and tax law retention requirements, documentation obligations as well as possible duties

of proof or accountability. Processing may also take place on the basis of our legitimate interests in proper business management, internal administration, risk control and IT security as well as in protecting our business operations and Contractual Partners against misuse or threats to data, secrets or other legal assets. This may include involving external Service Providers such as IT- and telecommunications providers, transport- or logistics companies, payment service providers, banks, tax advisors or legal advisors or other vicarious agents insofar as this is required for executing contracts or fulfilling legal obligations.

Personal data will only be passed on to third parties if this is necessary for fulfilling a contract or conducting pre-contractual measures; safeguarding legitimate interests; or complying with statutory obligations. We will inform you separately within this privacy policy about any further processing activities, particularly those undertaken for marketing purposes.

Which specific data is required in each case will be communicated to Contractual Partners during collection, for example by appropriate labelling in online forms or during personal contact.

Data will be deleted once it is no longer required for these purposes provided there are no statutory retention requirements preventing deletion. Statutory retention periods, particularly under commercial or tax law, may require longer storage periods. Data transmitted in connection with a specific assignment will be deleted after completion of that assignment and expiration of any applicable retention period unless further statutory or contractual storage obligations exist.

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). Health data (e.g. nutritional and biometric data). Content data (e.g. content and communications submitted in the course of the coaching).

Special categories of personal data: Health Data.

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

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

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

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). Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR).

Further information on processing methods, procedures and services used:

Coaching: We process the data of our clients as well as prospects and other contractors or business partners (collectively referred to as "clients") in order to provide them with our services. The processes carried out within the framework and for the purposes of coaching include: initiating contact and communication with clients, needs analysis to determine suitable coaching measures, planning and conducting coaching sessions, documenting coaching progress, capturing and managing client-specific information and data, scheduling and organising appointments, providing coaching materials and resources, invoicing and payment management, post-processing and follow-up of coaching sessions, quality assurance and feedback processes. We deliver our coaching services largely asynchronously: clients submit their data and check-ins, we review them and respond with video reviews and written feedback. The processed data, its nature, scope, purpose, and the necessity of its processing are determined by the underlying contractual relationship with the client. Insofar as it is necessary for fulfilling our contract, protecting vital interests or legally required, or if there is consent from the clients, we disclose or transfer the clients' data in compliance with professional legal requirements to third parties or agents such as authorities, billing centers as well as in the field of IT, office or comparable services;

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

Nutritional Counseling: We process the data of our clients to provide them with our consulting services in the field of nutrition and to bill them. The processed data, the type, scope, purpose, and necessity of its processing are determined by the underlying contract relationship and are communicated to the clients in a timely manner. In the course of our activity, we process health information of our clients as special categories of personal data;

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), Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR).

Business processes and operations

Personal data of service recipients and clients - including customers, clients, or in specific cases, mandates, patients, or business partners as well as other third parties - are processed within the framework of contractual and comparable legal relationships and pre-contractual measures such as the initiation of business relations. This data processing supports and facilitates business processes in areas such as customer management, sales, payment transactions, accounting, and project management.

The collected data is used to fulfil contractual obligations and make business processes efficient. This includes the execution of business transactions, the management of customer relationships, the optimisation of sales strategies, and ensuring internal invoicing and financial processes. Additionally, the data supports the protection of the rights of the controller and promotes administrative tasks as well as the organisation of the company.

Personal data may be transferred to third parties if necessary for fulfilling the mentioned purposes or legal obligations. After legal retention periods expire or when the purpose of processing no longer applies, the data will be deleted. This also includes data that must be stored for longer periods due to tax law and legal obligations to provide evidence.

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); 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); Log data (e.g. log files concerning logins or data retrieval or access times.); 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). Health data (e.g. weight developments, within testimonials only with consent).

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

Purposes of processing and legitimate interests: Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures; Business processes and management procedures; Communication; Marketing; Sales promotion; Public relations; Financial and Payment Management. Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.)).

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

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR). Compliance with a legal obligation (Article 6 (1) (c) GDPR). Consent (Article 6 (1) (a) GDPR). Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR).

Further information on processing methods, procedures and services used:

Customer Management and Customer Relationship Management (CRM): Processes required in the context of customer management and Customer Relationship Management (CRM) include customer acquisition in compliance with data protection regulations, measures to promote customer retention and loyalty, effective customer communication, complaint management and customer service with consideration of data protection, data management and analysis to support the customer relationship, management of CRM systems, secure account management, customer segmentation and targeting; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Contact management and contact maintenance: Processes required in the context of organizing, maintaining, and securing contact information (e.g., setting up and maintaining a central contact database, regular updates of contact information, monitoring data integrity, implementing data protection measures, ensuring access controls, conducting backups and restorations of contact data, training employees in effective use of contact management software, regular review of communication history and adjustment of contact

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

General Payment Transactions: Procedures required for carrying out payment transactions, monitoring bank accounts, and controlling payment flows (e.g., creation and verification of transfers, processing of direct debit transactions, checking of account statements, monitoring of incoming and outgoing payments, management of chargebacks, account reconciliation, cash management); **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Accounting, accounts payable, accounts receivable: Procedures required for the collection, processing, and control of business transactions in the area of accounts payable and receivable accounting (e.g., creation and verification of incoming and outgoing invoices, monitoring and management of outstanding items, execution of payment transactions, handling of dunning processes, account reconciliation within the scope of receivables and payables, accounts payable accounting, and accounts receivable accounting); **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).

Financial Accounting and Taxes: Procedures required for the collection, management, and control of finance-related business transactions as well as for the calculation, reporting, and payment of taxes (e.g., accounting and posting of business transactions, preparation of quarterly and annual financial statements, execution of payment transactions, handling of dunning processes, account reconciliation, tax consulting, preparation and submission of tax returns, management of tax affairs); **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).

Marketing, advertising, and sales promotion: Processes required in the context of marketing, advertising, and sales promotion (e.g., market analysis and audience targeting, development of marketing strategies, planning and execution of advertising campaigns, design and production of advertising materials, online marketing including SEO and social media campaigns, event marketing and trade show participation, customer loyalty programs, sales promotion measures, performance measurement and optimisation of marketing activities, budget management and cost control); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Public Relations: Processes required in the context of public relations and public relations activities (e.g., development and implementation of communication strategies, planning and execution of PR campaigns, creation and distribution of press releases, maintenance of media contacts, monitoring and analysis of media response, organisation of press conferences and public events, crisis communication, creation of content for social media and corporate websites, management of corporate branding); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Testimonials and success stories: With the express consent of the clients concerned, we publish testimonials and success stories, for instance on our website and in our social media presences. What is published is determined solely by the consent granted in the individual case: from a purely textual statement without a name through to name, photo and weight development. Where health data (e.g. a weight development graph or information about the nutrition coaching) is published, this is done exclusively on the basis of explicit consent. Consent is voluntary, has no effect on the coaching services and can be withdrawn at any time with effect for the future; after a withdrawal we remove the content concerned from the channels under our control; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR).

Providers and services used in the course of business

As part of our business activities, we use additional services, platforms, interfaces or plug-ins from third-party providers (in short, "services") in compliance with legal requirements. Their use is based on our interests in the proper, legal and economic management of our business operations and internal organization.

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); 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); Health data (e.g. nutritional and biometric data). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties).

Data subjects: Service recipients and clients; Prospective customers; Business and contractual partners. Users (e.g. website visitors, users of online services).

Purposes of processing and legitimate interests: Provision of contractual services and fulfillment of contractual obligations; Office and organisational procedures. Business processes and management procedures.

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

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR). Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR).

Further information on processing methods, procedures and services used:

Google Workspace: Cloud-based application software (e.g. word processing and spreadsheets, calendar and contact management), cloud storage, and cloud infrastructure services. We also store our clients' documents created in the course of nutrition coaching in Google Workspace, which may contain health data (e.g. nutritional and biometric data), as well as the information prospective clients submit via our intake form; when the intake form is submitted, a folder and spreadsheets are created for that person, holding this information and later the coaching documents. We process these special categories of personal data on the basis of the explicit consent of the clients and prospective clients. These documents also include photos uploaded by clients; the video reviews created in the course of the coaching are stored with our video service provider (see the Bunny Stream entry). Coaching documents are stored until the end of the coaching contract; clients can download their documents until 90 days after the end of the contract, after which they are deleted unless statutory retention obligations require otherwise. Answers to the pre-call form for a booked consultation are deleted 90 days after the consultation call unless a coaching contract is concluded within that time. In addition, we store invoices and payment records in Google Workspace, including the customer identifier, mandate reference and payment status transmitted by the payment service provider, for the duration of the statutory retention periods. Service provider: Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; Legal bases: Performance of a contract and pre-contractual enquiries (Art. 6(1)(b) GDPR), Legitimate interests (Art. 6(1)(f) GDPR), Consent to the processing of special categories of personal data (Art. 9(2)(a) GDPR); Data processing agreement: <https://cloud.google.com/terms/data-processing-addendum>; Basis for third-country transfers: Data Privacy Framework (DPF), Standard Contractual Clauses (<https://cloud.google.com/terms/eu-model-contract-clause>). Further information: <https://cloud.google.com/privacy>; **Service provider:** Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Ireland; **Website:** <https://workspace.google.com/>. **Privacy Policy:** <https://business.safety.google/privacy/>.

Tally: Creation and evaluation of online forms, surveys, feedback forms, etc. Via Tally we collect, among other things, the information from our intake form ("Getting to know you"), which prospective clients complete before booking an intro call, and from our check-in forms; both may contain health data (e.g. details on allergies, weight, height, nutrition). We also collect via Tally the photos uploaded by clients within the scope of the photo consent. For booked consultations we collect via Tally a pre-call form (including height, weight, sex and health limitations), whose answers serve to check suitability and to prepare the call, and a scheduling form (name, e-mail address, phone number and order number). We process these special categories of personal data on the basis of the data subjects' explicit consent, which is given in the respective form. The intake form is only loaded on our website after users click the corresponding button; only with this click does the browser establish a connection to Tally's servers, transmitting the IP address and technical details about the browser. The embedded form does not set cookies. When the intake form is submitted, a folder and spreadsheets in Google Workspace and a record in our application are created for that person (see the Google Workspace and Clever Cloud entries); we store the information submitted via the forms in Google Workspace. We delete the information of prospective clients with whom no coaching contract is concluded no later than six months after the intake form was submitted; answers to the pre-call form for a consultation are deleted 90 days after the consultation call unless a coaching contract is concluded within that time. Legal bases: Performance of a contract and pre-contractual enquiries (Art. 6(1)(b) GDPR), Legitimate interests (Art. 6(1)(f) GDPR), Consent to the processing of special categories of personal data (Art. 9(2)(a) GDPR); Data processing agreement: A data processing agreement has been concluded (<https://tally.so/help/data-processing-agreement>); **Service provider:** Tally, Muidepoort 19A, 9000 Gent, Belgium; **Website:** <https://tally.so/>. **Privacy Policy:** <https://tally.so/help/privacy-policy>.

Cronometer: A nutrition and biometric tracking service that lets users record and analyse their food intake, nutrient levels, weight, activity, and other biometric values. We use a Cronometer Pro licence to access and manage our clients' data within the scope of our nutrition coaching (for example, viewing food diaries, leaving comments, adjusting target values). This requires clients to maintain their own Cronometer account and to accept our invitation as their coach; the clients' accounts and our Pro account remain separate.

For the data we access on this basis and manage within the coaching, Cronometer acts as our processor; a data processing agreement (DPA) has been concluded for this purpose. To the extent that Cronometer operates the platform for its own purposes (in particular providing, securing, analysing, and improving the service) and handles its own direct contractual relationship with clients as account holders, Cronometer is an independent controller in that respect; Cronometer's own privacy policy applies to this.

In the course of this use, we process health data (e.g. weight, nutritional and biometric information) as a special category of personal data on the basis of the clients' explicit consent. Where agreed in the individual coaching, we export the clients' tracking and biometric data from Cronometer into our own systems with this explicit consent (e.g. to create nutrition plans); the further processing in our systems is governed by the sections on our consulting and coaching services.

Legal bases: Performance of a contract and pre-contractual enquiries (Art. 6(1)(b) GDPR), Legitimate interests (Art. 6(1)(f) GDPR), Consent to the processing of special categories of personal data (Art. 9(2)(a) GDPR); Data processing agreement: A data processing agreement has been concluded (not publicly available); Basis for third-country transfers: Adequacy decision (Canada); storage on servers in the USA is additionally safeguarded by the data processing agreement (including standard contractual clauses for sub-processors engaged); **Service provider:** Cronometer Software Inc., PO Box 3270, Revelstoke, BC V0E 2S0, Canada; **Website:** <https://cronometer.com>. **Privacy Policy:** <https://cronometer.com/privacy/>.

Payment Procedure

Within the framework of contractual and other legal relationships, due to legal obligations or otherwise on the basis of our legitimate interests, we offer data subjects efficient and secure payment options and use other service providers for this purpose in addition to banks and credit institutions (collectively referred to as "payment service providers"). Payment transactions are carried out exclusively via encrypted connections in accordance with the state of the art, ensuring that the data entered is protected from unauthorized access during transmission.

The data processed by the payment service providers includes inventory data, such as the name and address, bank data, such as account numbers or credit card numbers, passwords, TANs and checksums, as well as the contract, total and recipient-related information. The information is required to carry out the transactions. However, the data entered is only processed by the payment service providers and stored with them. I.e. we do not receive full credit card data, but the confirmation or rejection of the payment, the references named in the Mollie entry and, with SEPA direct debit, the payer details held in the mandate (name, IBAN, BIC). Under certain circumstances, the data may be transmitted by the payment service providers to credit agencies. The purpose of this transmission is to check identity and creditworthiness. Please refer to the terms and conditions and data protection information of the payment service providers.

The terms and conditions and data protection information of the respective payment service providers apply to the payment transactions and can be accessed within the respective websites or transaction applications. We also refer to these for further information and the assertion of revocation, information and other data subject rights.

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). Contact data (e.g. postal and email addresses or phone numbers).

Data subjects: Service recipients and clients. Business and contractual partners.

Purposes of processing and legitimate interests: Provision of contractual services and fulfillment of contractual obligations. Business processes and management procedures.

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

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

Further information on processing methods, procedures and services used:

Apple Pay: Payment services provider; **Service provider:** Apple Inc., Infinite Loop, Cupertino, CA 95014, USA; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** <https://www.apple.com/apple-pay/>. **Privacy Policy:** <https://www.apple.com/legal/privacy/en-ww/>.

Google Pay: Payment services provider; **Service provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** https://pay.google.com/intl/en_uk/about/. **Privacy Policy:** <https://business.safety.google/privacy/>.

Mastercard: Payment-Service-Provider (technical integration of online-payment-methods); **Service provider:** Mastercard Europe SA, Chaussée de Tervuren 198A, B-1410 Waterloo, Belgium; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** <https://www.mastercard.co.uk>. **Privacy Policy:** <https://www.mastercard.co.uk/en-gb/vision/terms-of-use/commitment-to-privacy/privacy.html>.

Mollie: Payment-Service-Provider (technical integration of online-payment-methods). We use Mollie to process our clients' payments; the checkout currently offers card payment (Visa, Mastercard), Apple Pay, Google Pay, SEPA credit transfer, SEPA direct debit and Pay by Bank. Payment is made on Mollie's pages, either via a payment link we send or, when a consultation is ordered through our website, from that order process; payment details are never entered on our website. For recurring payments, a mandate (e.g. a SEPA direct debit mandate) may be set up during checkout and stored by Mollie. We store the customer identifier assigned by Mollie, the mandate reference and the payment status in our business records; for orders placed through our website, our application stores the payment reference assigned by Mollie and the payment status with the respective order (see the Clever Cloud entry). Invoices and payment records are kept in Google Workspace. Mollie processes the payment data as an independent controller, in particular to execute the payment, to prevent fraud and to fulfil its own legal obligations; Mollie's privacy policy applies in this respect. Apple Pay, Google Pay and cards of the Visa and Mastercard schemes are integrated via Mollie; the respective providers process the payment data on their own responsibility under their own privacy notices, and we ourselves do not transmit any data to these providers; Legal basis: Performance of a contract and pre-contractual enquiries (Art. 6(1)(b) GDPR); **Service provider:** Mollie B.V., Keizersgracht 126, 1015 CW Amsterdam, Netherlands; **Website:** <https://www.mollie.com/>. **Privacy Policy:** <https://www.mollie.com/gb/legal/privacy>.

Visa: Payment-Service-Provider (technical integration of online-payment-methods); **Service provider:** Visa Europe Services Inc., Zweigniederlassung London, 1 Sheldon Square, London W2 6TT, UK; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR); **Website:** <https://www.visa.de>. **Privacy Policy:** <https://www.visa.com/en-us/legal/global-privacy-notice>.

Provision of online services and web hosting

We process user data in order to be able to provide them with our online services. For this purpose, we process the IP address of the user, which is necessary to transmit the content and functions of our online services to the user's browser or terminal device.

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, playback data of the video reviews); 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.); Inventory data (e.g. name, customer number, account data of the client area); Contact data (e.g. e-mail addresses); Contract data (e.g. consultation orders, withdrawal requests, contract register with offer number, status, term and prices); Payment data (e.g. payment reference and payment status of orders placed through our website); Content data (e.g. messages exchanged via the Telegram bot, feedback in the client area, summaries of the video reviews). Health data (temporarily, for display in the client area, where shared by clients via the Telegram bot, and in the summaries of the video reviews).

Data subjects: Users (e.g. website visitors, users of online services). Prospective customers. Service recipients and clients. Communication partner (Recipients of e-mails, letters, etc.).

Purposes of processing and legitimate interests: 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. Provision of contractual services and fulfillment of contractual obligations. Web analytics (e.g. access statistics, testing different wordings of a page).

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

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR); Consent to the processing of special categories of personal data (Article 9 (2) (a) GDPR) for the health data displayed in the client area, shared via the Telegram bot and contained in the video review summaries.

Further information on processing methods, procedures and services used:

Provision of online offer on rented hosting space: For the provision of our online services, we use storage space, computing capacity and software that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Collection of Access Data and Log Files: Access to our online service is logged in the form of so-called "server log files". Server log files may include the address and name of the accessed web pages and files, date and time of access, transferred data volumes, notification of successful retrieval, browser type along with version, the user's operating system, referrer URL (the previously visited page), and typically IP addresses and the requesting provider. The server log files can be used for security purposes, e.g., to prevent server overload (especially in the case of abusive attacks, known as DDoS attacks), and to ensure server 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.

Cookie-free reach measurement (self-operated): We measure the use of our online services with a self-operated, server-side method that works without cookies and without third-party scripts; no information is stored on or read from the device. We record the pages accessed, the referring website, the page-to-page course of a visit and the campaign parameters contained in the link address (utm parameters); if the link address carries a click identifier of an advertising network, we only note that the visit came from there, the identifier itself is not stored, and no data is transmitted to advertising networks. Clicks on the booking, WhatsApp contact and order buttons are reported to us by the browser through a small script of our own, transmitting only the kind of button. To test different wordings of a page, the same method determines for the duration of one day which version a visitor sees; we record the version shown and the clicks named above. IP address and User-Agent are used solely to form a daily-changing, pseudonymous visitor identifier and are not stored; the key used to form it is renewed daily and removed once the individual page views are deleted, so that recognition across several days is excluded and subsequent attribution to a person becomes impossible for us as well, at the latest when the individual page views are deleted. Signed-in users, visitors with an active Do Not Track or Global Privacy Control signal and detected automated access are excluded from the measurement. Individual page views are deleted after seven days at the latest and are retained only as aggregated statistics without personal reference. Processing takes place exclusively on the servers of our hosting provider; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); the legitimate interest lies in the statistical analysis and improvement of our online services in a form that requires no tracking techniques and no consent prompts.

Sentry: Monitoring system stability and identifying code errors - Information about the device or error time are collected pseudonymously and are deleted afterwards; **Service provider:** Functional Software Inc., Sentry, 132 Hawthorne Street, San Francisco, California 94107, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** <https://sentry.io>; **Security measures:** IP Masking (Pseudonymization of the IP address); **Privacy Policy:** <https://sentry.io/privacy>; **Data Processing Agreement:** <https://sentry.io/legal/dpa/>. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (<https://sentry.io/legal/dpa/>). We have configured Sentry so that no IP addresses, e-mail addresses, cookies, request contents or local program variables are transmitted; what is captured is essentially error messages, stack traces and the accessed URL path. No health data of our clients (e.g. nutritional or biometric data) reaches Sentry this way. Our account is set to the EU data region; storage takes place in a data centre in Frankfurt am Main.

Clever Cloud: A cloud platform for running web applications, databases and object storage (storing files in an online storage system). The provider's servers hold the content of the applications operated on them, including the personal data processed there, such as inventory data, contact data and usage data of the people using the application. In our case this concerns our online services including the client area, the associated database and

the Telegram reminder bot. Stored in the database are: the account data described in the registration, login and user account section, including the records of prospective clients who have submitted our intake form (name, e-mail address, the identifier of the form response and the identifiers of the folder and spreadsheets created for that person in Google Workspace); the Telegram user identifier and the messages exchanged via the Telegram bot; the feedback submitted by clients in the client area; sign-ups to our Field Notes via the form in the footer (e-mail address and details of the sign-up process; see the privacy notice for that form); consultation orders placed through our website (name, e-mail address, the service ordered and its price, the payment reference assigned by Mollie and the payment status, and the declarations confirmed during the order process with their timestamps) and withdrawal requests submitted through our website; a contract register for our coaching offers (offer number, customer number, e-mail address, contract status, offer, start and end dates, prices, the versions of the underlying documents and a checksum of the offer document; name, address and the document itself are not stored there); and, for the coaching video reviews, the date, the video identifier at our video service provider, a written summary, which may contain health-related information, and the playback data described in the registration, login and user account section. The coaching data retrieved for display in the client area is processed there only temporarily and is not stored in the database. The contract register is retained after the deletion of a user account for the duration of the statutory retention periods; summaries and playback data of the video reviews are deleted 90 days after the end of the coaching contract. When the application is accessed, technical connection data is processed, in particular IP address, date and time of the request, the resource requested, browser type and operating system. This data is recorded in server log files (automatically generated protocol files) and serves the provision of the service, operational security and error analysis; the provider retains it for seven days. Transmission is encrypted via TLS (Transport Layer Security, an encryption protocol for data transfers over the internet). In addition, metrics and logs for operational monitoring as well as automatic database backups are created; the backups are kept on a rolling seven-day basis and then overwritten. Operations take place in data centres in France; we use the Paris region only. The data processing agreement forms part of the provider's contractual terms and also covers the database services; Legal bases: Legitimate Interests (Article 6 (1) (f) GDPR); Performance of a contract and pre-contractual enquiries (Article 6 (1) (b) GDPR) with regard to order, contract and coaching data; with regard to health-related information in the video review summaries, the explicit consent given within the coaching relationship (Article 9 (2) (a) GDPR); Data Processing Agreement: <https://www.clever.cloud/general-terms-and-conditions-of-use/clever-cloud-data-processing-agreement/>; **Service provider:** Clever Cloud SAS, 4 rue Voltaire, 44000 Nantes, France; **Website:** <https://www.clever.cloud/>. **Privacy Policy:** <https://www.clever.cloud/privacy-policy/>.

Use of Cookies

The term "cookies" refers to functions that store information on users' devices and read it from them. Cookies can also be used for different purposes, such as ensuring the functionality, security, and convenience of online services, as well as analyzing visitor traffic. We use cookies in accordance with legal regulations. If necessary, we obtain users' consent in advance. If consent is not required, we rely on our legitimate interests. This applies when storing and reading information is essential to provide explicitly requested content and functions. This includes, for example, saving settings and ensuring the functionality and security of our online services. Consent can be withdrawn at any time. We clearly inform users about the scope of the consent and which cookies are used.

Information on legal data protection bases: Whether we process personal data using cookies depends on users' consent. If consent is given, it serves as the legal basis. Without consent, we rely on our legitimate interests, as outlined in this section and in the context of the respective services and procedures.

Storage duration: The following types of cookies are distinguished based on their storage duration:

Temporary cookies (also: session cookies): Temporary cookies are deleted at the latest after a user leaves an online service and closes their device (e.g., browser or mobile application).

Permanent cookies: Permanent cookies remain stored even after the device is closed. For example, the login status can be saved, and preferred content can be displayed directly when the user revisits a website. Additionally, the user data collected with cookies may be used for audience measurement. Unless we provide explicit information to users about the type and storage duration of cookies (e.g., when obtaining consent), users should assume that these are permanent and may have a storage duration of up to two years.

General information on withdrawal and objection (opt-out): Users can withdraw their consent at any time and also object to the processing according to legal regulations, including through the privacy settings of their browser.

Processed data types: 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).

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

Local storage: Our online services also store two purely functional settings in your browser's local storage: the chosen display mode (light or dark) and, in the client area, a table view setting. This information remains on your device, is not transmitted to us or to third parties, and can be deleted at any time via your browser settings. Beyond this, our online services set only technically necessary cookies: a CSRF protection cookie (stored for up to one year), a session cookie for the signed-in client area (stored for 14 days), a temporary notice cookie deleted when the browser is closed, and a language cookie (django_language, value de or en, stored for one year), which is set only when you choose a language via the language switch and serves to show you the chosen language version.

Registration, Login and User Account

A user account is available to our coaching clients and to prospective clients who have submitted our intake form; open registration is not possible. Signing in takes place exclusively via an existing Google account (single sign-on); no separate password is created or stored with us. Upon sign-in we receive from Google the details required to maintain the account, in particular name, e-mail address and Google account identifier as well as, where provided, profile picture URL and language setting. Google access tokens are not stored by us. Sign-in attempts from Google accounts not assigned to a person registered with us are rejected without a user account being created. When Google sign-in is used, Google processes the sign-in data under its own responsibility; Google's privacy policy additionally applies (<https://policies.google.com/privacy>).

Within the use of the client area, we store the time of sign-ins and, per day, the number of times the dashboard is opened. For the video reviews we additionally store, per review, whether and when it was first played and whether the end was reached, the furthest point reached and, per ten-second segment, the number of plays. Beyond that, we do not record which content, entries or sections were viewed; no IP addresses or browser details are stored for this purpose. This information serves the coaching support (for instance, recognising whether a client is using their dashboard or has watched a review) and the security of the client area. Sign-in and access data is deleted when the coaching relationship ends, at the latest after three years; the playback data of the video reviews is deleted 90 days after the end of the coaching contract. This data will not be passed on to third parties unless it is necessary to pursue our claims or there is a legal obligation to do so.

Users may be informed by e-mail of information relevant to their user account, such as technical changes.

Processed data types: Inventory data (e.g. name); Contact data (e.g. e-mail address); Usage data (times of sign-ins, number of dashboard opens per day and playback data of the video reviews). Log data (e.g. log files concerning logins).

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

Purposes of processing and legitimate interests: Provision of contractual services and fulfillment of contractual obligations; Security measures; Organisational and Administrative Procedures. Provision of our online services and usability.

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

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

Further information on processing methods, procedures and services used:

Users' profiles are not public: The users' profiles are not publicly visible or accessible.

Contact and Inquiry Management

When contacting us (e.g. via mail, e-mail, telephone or via social media) as well as in the context of existing user and business relationships, the information of the inquiring persons is processed to the extent necessary to respond

to the contact requests and any requested measures.

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.).

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

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

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

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

Communication via Messenger

We use messenger services for communication purposes and therefore ask you to observe the following information regarding the functionality of the messenger services, encryption, use of the metadata of the communication and your objection options.

You can also contact us by alternative means, e.g. telephone or e-mail. Please use the contact options provided to you or use the contact options provided within our online services.

In the case of encryption of content (i.e. the content of your message and attachments), we point out that the communication content (i.e. the content of the message and attachments) is encrypted end-to-end. This means that the content of the messages is not visible, not even by the messenger service providers themselves. You should always use a current version of the messenger service with activated encryption, so that the encryption of the message contents is guaranteed.

However, we would like to point out to our communication partners that although messenger service providers do not see the content where it is end-to-end encrypted, they can find out that and when communication partners communicate with us and process technical information on the communication partner's device used and, depending on the settings of their device, also location information (so-called metadata).

Information on Legal basis: If we ask communication partners for permission before communicating with them via messenger services, the legal basis of our processing of their data is their consent. Otherwise, if we do not request consent and you contact us, for example, voluntarily, we use messenger services in our dealings with our contractual partners and as part of the contract initiation process as a contractual measure and in the case of other interested parties and communication partners on the basis of our legitimate interests in fast and efficient communication and meeting the needs of our communication partners for communication via messenger services. We would also like to point out that we do not transmit the contact data provided to us to the messenger service providers for the first time without your consent.

Withdrawal, objection and deletion: You can withdraw your consent or object to communication with us via messenger services at any time. In the case of communication via messenger services, we delete the messages in accordance with our general data retention policy (i.e. as described above after the end of contractual relationships, archiving requirements, etc.) and otherwise as soon as we can assume that we have answered any information provided by the communication partners, if no reference to a previous conversation is to be expected and there are no legal obligations to store the messages to prevent their deletion.

Reservation of reference to other means of communication: For your security, we kindly ask for your understanding that we may not respond to enquiries via messenger for specific reasons. This applies in situations where contract details require heightened confidentiality or a response via messenger does not meet formal requirements. In such cases, we recommend using more appropriate communication channels.

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.). Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers, involved parties). Health data (where volunteered by clients).

Data subjects: Communication partner (Recipients of e-mails, letters, etc.); Service recipients and clients. Prospective customers.

Purposes of processing and legitimate interests: Communication. Provision of contractual services and fulfillment of contractual obligations.

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

Legal Basis: 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). Consent to processing of special categories of personal data (Article 9 (2)(a) GDPR).

Further information on processing methods, procedures and services used:

Telegram: A cloud-based messaging service that enables the sending and receiving of text messages, voice messages, images, videos, files, and voice calls. Telegram stores chats, media, and contacts encrypted on servers to allow cross-platform access. Individual chats can optionally be protected by end-to-end encryption; chats with bots such as ours are not end-to-end encrypted. We operate a Telegram bot through which clients receive reminders (e.g. for check-ins and appointments) and can send us messages. The bot is intended exclusively for existing clients and is linked to the coaching account by starting the bot via the invitation link we provide; in doing so, clients consent to receiving the reminders and can end them at any time. The data processed are the Telegram user identifier, the time and content of the messages exchanged via the bot, and the reminder times. The bot runs in our own application with our hosting provider Clever Cloud; the messages are stored there and deleted in accordance with our general deletion rules. In addition, our application uses the same bot to send us notices of new or changed coaching offers in a chat used only by us; these notices contain the customer number, the offer number and the status, but neither names nor prices nor documents. Telegram can process the messages and metadata (e.g. user identifier, timestamps, device information) for its own purposes, over which we have no influence; in this respect Telegram is an independent controller. The provider is Telegram Messenger Inc., established outside the EEA; according to its own statements, Telegram stores the data of users from the EEA in data centres in the Netherlands. Insofar as this involves a transfer to a third country, it is based on the explicit consent of the clients, who start the bot themselves with knowledge of this information. We do not request health data via the bot and ask that health-related information be sent by e-mail or through the channels agreed in the coaching; e-mail is always available as an alternative channel. If clients nevertheless share health-related information via the bot on their own initiative, this is covered by the explicit consent given within the coaching relationship (Art. 9(2)(a) GDPR). We do not reply via the bot to messages from persons who are not our clients, and we delete them. Legal bases: Performance of a contract and pre-contractual enquiries (Art. 6(1)(b) GDPR) for clients; Legitimate interests (Art. 6(1)(f) GDPR) for other communication partners and with regard to the notices sent to ourselves; with regard to health-related information shared on their own initiative, the explicit consent given within the coaching relationship (Art. 9(2)(a) GDPR); **Service provider:** Representative in the European Union: European Data Protection Office (EDPO), Avenue Huart Hamoir 71, 1030 Brussels, Belgium; **Website:** <https://telegram.org/>. **Privacy Policy:** <https://telegram.org/privacy>.

WhatsApp: A communication service that enables the sending and receiving of text messages, voice messages, images, videos, documents, as well as voice and video calls over the internet. We use a WhatsApp Business account for organisational and administrative communication with clients and prospective clients (e.g. scheduling appointments, questions before a contract is concluded and brief queries). For this purpose our website and the client area offer a button that opens a chat with our number. This is a plain link: before the click, no scripts or cookies from WhatsApp or Meta are loaded, and the address of the page you were on is not passed to WhatsApp when you click; only once you start the chat does WhatsApp process your phone number and your messages. We never request health data via WhatsApp; however, clients may, on their own initiative, share health-related information (e.g. progress updates) through this channel. This is covered by the general consent to the processing of health data that clients provide as part of the coaching relationship (Article 9 (2)(a) GDPR); email is always available as an alternative channel. Communication is conducted through end-to-end encryption, ensuring that content is accessible only to the involved communication partners. We delete chat histories with clients after the end of the coaching relationship in accordance with our general deletion rules; health-related content is deleted at that point in any case. Consents given in the chat (e.g. to the use of photos or testimonials) are kept as proof for as long as the content concerned is in use. Chats with prospective clients with whom no contract is concluded are deleted no later than six months after the last message. To provide the service, the platform processes metadata (e.g. phone numbers, timestamps, device information) and may use this data for its own purposes such as functionality enhancement, security, and service optimisation, on which

we have no influence; in this respect WhatsApp Ireland Limited acts as an independent controller. Service provider: WhatsApp Ireland Limited, Merrion Road 4, D04 X2K5 Dublin, Ireland; Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR) for clients; Legitimate Interests (Article 6 (1) (f) GDPR) for prospective clients; with regard to any health-related information shared by clients on their own initiative, the explicit consent given within the coaching relationship (Article 9 (2)(a) GDPR); **Service provider:** WhatsApp Ireland Limited, Merrion Road 4, D04 X2K5 Dublin, Ireland; **Website:** <https://www.whatsapp.com/>. **Privacy Policy:** <https://www.whatsapp.com/legal/privacy-policy-eea>.

Profiles in Social Networks (Social Media)

We maintain online presences within social networks and process user data in this context in order to communicate with the users active there or to offer information about us.

We would like to point out that user data may be processed outside the European Union. This may entail risks for users, e.g. by making it more difficult to enforce users' rights.

In addition, user data is usually processed within social networks for market research and advertising purposes. For example, user profiles can be created on the basis of user behaviour and the associated interests of users. The user profiles can then be used, for example, to place advertisements within and outside the networks which are presumed to correspond to the interests of the users. For these purposes, cookies are usually stored on the user's computer, in which the user's usage behaviour and interests are stored. Furthermore, data can be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective networks or will become members later on).

For a detailed description of the respective processing operations and the opt-out options, please refer to the respective data protection declarations and information provided by the providers of the respective networks.

Also in the case of requests for information and the exercise of rights of data subjects, we point out that these can be most effectively pursued with the providers. Only the providers have access to the data of the users and can directly take appropriate measures and provide information. If you still need help, please do not hesitate to contact us.

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).

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

Purposes of processing and legitimate interests: Communication; Feedback (e.g. collecting feedback via online form). Public relations.

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

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

Further information on processing methods, procedures and services used:

Instagram: 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/>. **Basis for third-country transfers:** Data Privacy Framework (DPF).

Facebook Pages: Profiles within the social network Facebook - The controller is jointly responsible with Meta Platforms Ireland Limited for the collection and transmission of data from visitors to our Facebook page ("Fanpage"). This includes, in particular, information about user behaviour (e.g., viewed or interacted content, actions taken) as well as device information (e.g., IP address, operating system, browser type, language settings, cookie data). Further details can be found in the Facebook Data Policy: <https://www.facebook.com/privacy/policy/>. Facebook also uses this data to provide us with statistical evaluations through the "Page Insights" service that give insights into how people interact with our page and its content. The basis for this is an agreement with Facebook ("Information about Page Insights": https://www.facebook.com/legal/terms/page_controller_addendum), which regulates security measures and

the exercise of data subjects' rights. Further information can be found here:

https://www.facebook.com/legal/terms/information_about_page_insights_data. Users can therefore direct requests for information or deletion directly to Facebook. The rights of users (particularly access, deletion, objection, complaint to a supervisory authority) remain unaffected by this. The joint responsibility is limited exclusively to the collection of data by Meta Platforms Ireland Limited (EU). Meta Platforms Ireland Limited alone is responsible for further processing, including any possible transmission to 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/>. **Basis for third-country transfers:** Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.facebook.com/legal/EU_data_transfer_addendum).

Management, Organization and Utilities

We use services, platforms and software from other providers (hereinafter referred to as "third-party providers") for the purposes of organizing, administering, planning and providing our services. When selecting third-party providers and their services, we comply with the legal requirements.

Within this context, personal data may be processed and stored on the servers of third-party providers. This may include various data that we process in accordance with this privacy policy. This data may include in particular master data and contact data of users, data on processes, contracts, other processes and their contents.

If users are referred to the third-party providers or their software or platforms in the context of communication, business or other relationships with us, the third-party provider processing may process usage data and metadata that can be processed by them for security purposes, service optimisation or marketing purposes. We therefore ask you to read the data protection notices of the respective third party providers.

Processed data types: Content data (e.g. video reviews); Usage data (e.g. playback of the video reviews); Meta, communication and process data (e.g. IP addresses, timestamps, identification numbers). Health data (where contained in the video reviews).

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

Purposes of processing and legitimate interests: Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.

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

Legal Basis: Performance of a contract and prior requests (Article 6 (1) (b) GDPR); Legitimate Interests (Article 6 (1) (f) GDPR); Consent to the processing of special categories of personal data (Article 9 (2) (a) GDPR) for the health data contained in the video reviews.

Further information on processing methods, procedures and services used:

Bunny Stream: Video hosting and video streaming. Via Bunny Stream we store and stream the video reviews created in the course of the coaching, which may contain clients' health data (e.g. details on nutrition, weight and progress); we process these special categories of personal data on the basis of the explicit consent given within the coaching relationship. The videos are stored exclusively in a storage region in the EU (Frankfurt) and are not replicated outside it. Playback takes place in the signed-in client area via the provider's embedded player; when a video is played, the browser establishes a connection to Bunny's servers, transmitting the IP address and technical details about the browser. Playback addresses are signed and valid for a limited time only; downloading the videos is not provided for. The player stores no information on the device, and the provider's playback statistics are switched off; the playback data we record ourselves is described in the registration, login and user account section. The videos are deleted at the provider 90 days after the end of the coaching contract; when a user account is deleted, the associated videos are deleted as well. Legal bases: Performance of a contract and pre-contractual enquiries (Art. 6(1)(b) GDPR); Consent to the processing of special categories of personal data (Art. 9(2)(a) GDPR); Data processing agreement: A data processing agreement has been concluded; **Service provider:** BUNNYWAY d.o.o., Dunajska cesta 165, 1000 Ljubljana, Slovenia; **Website:** <https://bunny.net>. **Privacy Policy:** <https://bunny.net/privacy/>.

Changes and Updates

We kindly ask you to inform yourself regularly about the contents of our data protection declaration. We will adjust the privacy policy as changes in our data processing practices make this necessary. We will inform you as soon as the changes require your cooperation (e.g. consent) or other individual notification.

If we provide addresses and contact information of companies and organizations in this privacy policy, we ask you to note that addresses may change over time and to verify the information before contacting us.

Terminology and Definitions

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.

Contact data: Contact details are essential information that enables communication with individuals or organizations. They include, among others, phone numbers, postal addresses, and email addresses, as well as means of communication like social media handles and instant messaging identifiers.

Content data: Content data comprise information generated in the process of creating, editing, and publishing content of all types. This category of data may include texts, images, videos, audio files, and other multimedia content published across various platforms and media. Content data are not limited to the content itself but also include metadata providing information about the content, such as tags, descriptions, authorship details, and publication dates.

Contract data: Contract data are specific details pertaining to the formalisation of an agreement between two or more parties. They document the terms under which services or products are provided, exchanged, or sold. This category of data is essential for managing and fulfilling contractual obligations and includes both the identification of the contracting parties and the specific terms and conditions of the agreement. Contract data may encompass the start and end dates of the contract, the nature of the agreed-upon services or products, pricing arrangements, payment terms, termination rights, extension options, and special conditions or clauses. They serve as the legal foundation for the relationship between the parties and are crucial for clarifying rights and duties, enforcing claims, and resolving disputes.

Controller: "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Inventory data: Inventory data encompass essential information required for the identification and management of contractual partners, user accounts, profiles, and similar assignments. These data may include, among others, personal and demographic details such as names, contact information (addresses, phone numbers, email addresses), birth dates, and specific identifiers (user IDs). Inventory data form the foundation for any formal interaction between individuals and services, facilities, or systems, by enabling unique assignment and communication.

Log data: Protocol data, or log data, refer to information regarding events or activities that have been logged within a system or network. These data typically include details such as timestamps, IP addresses, user actions, error messages, and other specifics about the usage or operation of a system. Protocol data is often used for analyzing system issues, monitoring security, or generating performance reports.

Meta, communication and process data: Meta-, communication, and procedural data are categories that contain information about how data is processed, transmitted, and managed. Meta-data, also known as data about data, include information that describes the context, origin, and structure of other data. They can include details about file size, creation date, the author of a document, and modification histories. Communication data capture the exchange of information between users across various channels, such as email traffic, call logs, messages in social networks, and chat histories, including the involved parties, timestamps, and transmission paths. Procedural data describe the processes and operations within systems or organisations, including workflow documentations, logs of transactions and activities, and audit logs used for tracking and verifying procedures.

Payment Data: Payment data comprise all information necessary for processing payment transactions between buyers and sellers. This data is crucial for e-commerce, online banking, and any other form of financial transaction. It includes details such as credit card numbers, bank account information, payment amounts, transaction dates, verification numbers, and billing information. Payment data may also contain information on payment status, chargebacks, authorizations, and fees.

Personal Data: "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing: The term "processing" covers a wide range and practically every handling of data, be it collection, evaluation, storage, transmission or erasure.

Usage data: Usage data refer to information that captures how users interact with digital products, services, or platforms. These data encompass a wide range of information that demonstrates how users utilise applications, which features they prefer, how long they spend on specific pages, and through what paths they navigate an application. Usage data can also include the frequency of use, timestamps of activities, IP addresses, device information, and location data. They are particularly valuable for analysing user behaviour, optimising user experiences, personalising content, and improving products or services. Furthermore, usage data play a crucial role in identifying trends, preferences, and potential problem areas within digital offerings