BODYFACT

BODYFACT – PRIVACY POLICY

1. Introduction, Purpose and Legal Background

1.1. Purpose of the Privacy Policy

The purpose of this Privacy Policy (the "Privacy Policy") is to provide detailed and transparent information on how BodyFact (the "Service Provider" or "Controller") processes the personal data of Users, Customers and Subscribers in connection with the use of www.bodyfact.eu (and its subpages), purchases made in the Online Store, the use of subscription-based services, and activities related to marketing communications.

The Privacy Policy specifies:

- the purposes and legal bases of the processing,
- the categories of data processed,
- the retention periods,
- the system of individual Processors and Data transfers,
- the safeguards applicable to international Data transfers,
- the operation of cookies and cookie management systems,
- the rights of Data Subjects and the manner in which such rights may be exercised.

The Controller is committed to transparent and GDPR-compliant processing of personal data and seeks to fully implement the principles of "privacy by design" and "privacy by default".

1.2. Controller Details

Item	Data
Company name	BODYFACT Kft.
Registered office	1029 Budapest, Csatlós utca 3. 1. em. 3. ajtó, HUNGARY
Company registration number	01-09-454670
Tax number	33018346-2-41
Telephone	+36300707860
Data protection contact	privacy@bodyfact.eu
Customer service	hello@bodyfact.eu

The Controller is not required to appoint a Data Protection Officer; however, a data protection officer responsible for internal control and compliance operates within the organisation.

1.3. Applicable Legislation

The Controller's data processing activities are primarily governed by the following legislation applicable uniformly at EU level:

- GDPR — Regulation (EU) 2016/679 of the European Parliament and of the Council
- the ePrivacy Directive (2002/58/EC) and its implementation in the Member State applicable according to the use of the service
- Chapter V of the GDPR — international Data transfers

Where applicable under local law, in addition to the above, the national laws of the Member State of the Data Subject's habitual residence may also apply, in particular in the areas of consumer protection, electronic commerce and direct marketing. In the case of Data Subjects in Hungary, this includes in particular the following legislation:

- Hungarian Data Protection Act (Act CXII of 2011 on Informational Self-Determination and Freedom of Information, "Infotv.")

- Hungarian Electronic Commerce Act (Act CVIII of 2001 on Certain Issues of Electronic Commerce and Information Society Services, “Elektronikus kereskedelmi törvény”)
- Hungarian Consumer Protection Act (Act CLV of 1997 on Consumer Protection, “Fogyasztóvédelmi törvény”)
- Act C of 2003 on Electronic Communications
- Act XLVIII of 2008 (“Grt.”) — rules on marketing consents

1.4. Personal, Material and Territorial Scope of the Privacy Policy

Personal scope:

The Privacy Policy applies to all visitors, registered users, Customers, Subscribers of the Online Store and persons subscribed to marketing lists (hereinafter collectively referred to as the “Data Subject”).

Material scope:

It applies to all processing activities related to:

- online purchases,
- subscriptions,
- newsletters,
- marketing (Facebook, Google, TikTok advertising),
- customer service,
- the affiliate system,
- cookie management and web tracking tools.

Territorial scope:

The Privacy Policy applies to Data Subjects who use the Online Store operated by the Controller from within the territory of the European Union or the European Economic Area, where the conditions set out in Article 3 of the GDPR are met, irrespective of the Controller’s place of establishment. Specific provisions applicable to Data Subjects located outside the territory of the European Union/European Economic Area (including Switzerland) are set out in a separate section of this Privacy Policy. The principles governing Data transfers to third countries are described in Chapter 4.

1.5. Processing of Minors' Personal Data

Purchases through the BodyFact Online Store are subject to legal capacity, meaning that the Customer must be a natural person who has reached the age of 18 and is of full legal age; the Customer declares this by finalising the order. Accordingly, BodyFact's products and services are sold exclusively to persons of full legal age.

The Service Provider does not carry out technical or document-based verification of the Customer's age, nor is it legally required to do so. Where there are reasonable grounds to suspect that an order has been placed by a minor, the Service Provider is entitled to cancel the order, terminate the related processing of personal data, and/or request additional information from the Customer to verify their age.

Processing activities related to the use of the Online Store, registration or subscription to the newsletter apply exclusively to Data Subjects who are of full legal age and have legal capacity; the Service Provider does not rely on a legal basis for processing the personal data of persons under the age of 18 and, upon becoming aware of such data, shall delete it without undue delay.

1.6. Principles of Data Processing

The Controller processes personal data in accordance with the principles set out in Article 5 of the GDPR:

1. Lawfulness, fairness and transparency
Every processing activity has a legal basis, and Data Subjects are provided with comprehensive information.

2. Purpose limitation
Data are processed exclusively for specified purposes and, where the purpose changes, further processing is carried out only on the basis of a new legal basis or Consent.

3. Data minimisation
Only data that are necessary are processed.

4. Accuracy
The Controller ensures that the data are accurate; where necessary, they may be amended at the request of the Data Subject.

5. Storage limitation
Data are retained only for as long as necessary.

6. Integrity and confidentiality
Appropriate technical and organisational measures protect the data (encryption, pseudonymisation, access logs, access-rights management).

7. Accountability
The Controller is responsible for ensuring that processing complies with the GDPR at every stage and is able to demonstrate such compliance.

1.7. Updating and Amending the Privacy Policy

The Controller reserves the right to amend the Privacy Policy, in particular:

- in the event of changes in legislation,
- when introducing a new processing purpose,
- when engaging a new service provider.

Amendments shall take effect on the date of their publication on the Online Store.

In the event of a material change, the Controller shall also notify the Data Subjects by e-mail.

Where an amendment introduces a new processing purpose in respect of personal data collected previously, and the legal basis required for the new purpose is the Consent of the Data Subject, the Controller shall apply the amendment to the existing data only after the Data Subject has provided Consent for the new purpose or — where the new purpose is based on Legitimate interest — after the Data Subject has been provided with an opportunity to exercise the Right to object.

1.8. Data Security and Risk Management

In the course of processing activities, the Controller applies, in particular, the following security measures:

- HTTPS encryption,
- server-side encryption (AES-256),
- password hashing algorithms (bcrypt),
- access logging,
- access authorisation levels,
- regular security audits,

- as an organisational measure, written confidentiality obligations imposed on employees who have access to personal data, as well as the “need-to-know” principle (access limited exclusively to the extent necessary for the performance of the relevant duties),
- the built-in security and fraud-prevention systems of Shopify and Stripe, as well as PayPal where the Customer selects this payment method.

BodyFact maintains a “data breach protocol” ensuring that the measures required under Articles 33–34 of the GDPR are taken in the event of a Personal data breach.

Where a Personal data breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the Controller shall also directly inform the Data Subjects in accordance with Article 34 of the GDPR.

2. Data Processing Purposes, Legal Bases, Categories of Data Processed and Retention Periods

This chapter presents the individual data processing activities separately, by purpose, with the level of detail required under Articles 13 and 14 of the GDPR.
The list covers all processing activities that occur in connection with the Online Store, the BodyFact brand, purchasing processes, subscriptions and marketing activities.

Some processing activities are based on **Performance of a contract** (Article 6(1)(b) GDPR), others on a **Legal obligation** (Article 6(1)(c)), a **Legitimate interest** (Article 6(1)(f)), or explicit **Consent** (Article 6(1)(a)).

2.1. Use of the Online Store (Opening the Website)

Purpose:

Ensuring the technical operation of the Online Store and error-free provision of the service.

Data processed:

- IP address
- device type, operating system
- browser type
- timestamp
- page-view data

- essential cookies (session ID)

Legal basis:

Legitimate interest of the Controller – Article 6(1)(f) GDPR
(provision of online services, information security)

Retention:

The Online Store may use cookies necessary for its operation (session identifiers). The exact name, purpose and retention period of each cookie are specified in the Cookie Policy (Cookie List) available on the Website.
Server logs: 30 days

2.2. Purchase / Placing an Order (with and without Registration)

Purpose: The processing of the purchasing process, conclusion and performance of the contract.

Data processed:

- name
- e-mail address
- billing address
- delivery address
- telephone number
- order data (order number, products, price)
- selected payment method
- transaction identifier of the selected payment service provider (Stripe or - if the Customer selects this payment method - PayPal); the Service Provider does not store or have access to payment data (e.g. bank card or PayPal account data); such data are processed exclusively by the respective payment service provider

Legal basis:

Performance of a contract – Article 6(1)(b) GDPR

The Customer is required to provide the data necessary for placing the order (billing data); if such data are not provided, the Service Provider cannot issue the invoice.

Retention:

Billing data: 8 years (Hungarian Accounting Act)
Order metadata: 5 years (limitation period under the Hungarian Civil Code)
Delivery data: performance of the contract + 1 year

Where processing is necessary for the establishment, exercise or defence of legal claims, the processing period shall last until the proceedings have been finally concluded, but no longer than the applicable limitation period of the claim.

2.3. Invoicing and Accounting Legal Compliance

Purpose:

Issuing and retaining invoices as required by law.

Data processed:

- name
- billing address
- order data
- payment information (not bank card data!)

Legal basis:

Legal obligation – Article 6(1)(c) GDPR,
Hungarian Accounting Act (Act C of 2000 on Accounting, "Számviteli törvény"), Section 169

The issuance of an invoice is a mandatory statutory requirement (pursuant to Section 169 of the Hungarian Accounting Act); therefore, the contract cannot be performed without the provision of the invoice data.

Retention:

8 years

2.4. Subscription Service

Purpose:

Managing the subscription, ensuring recurring payments and sending notifications.

Data processed:

- name

- e-mail address
- subscription type (monthly / quarterly)
- Stripe subscription ID
- order history
- status changes (suspension, modification, cancellation)

Legal basis:

Performance of a contract – Article 6(1)(b) GDPR

Retention:

2 years following termination of the subscription

Where processing is necessary for the establishment, exercise or defence of legal claims, the processing period shall last until the proceedings have been finally concluded, but no longer than the applicable limitation period of the claim.

2.5. Newsletter Subscription and Sending Marketing E-mails

Purpose:

Marketing communications and sending offers and promotions to the Data Subject.

Data processed:

- name (optional)
- e-mail address
- date and time of subscription
- technical logs necessary to verify the subscription
- marketing preferences
- interactions relating to campaigns (openings, clicks) – pseudonymised

Legal basis:

Explicit Consent — Article 6(1)(a) GDPR.

The detailed rules governing the obtaining of Consent and direct marketing communications apply under the law of the Member State of the Data Subject's habitual residence (see Section 1.3); for Data Subjects in Hungary, this means in particular Section 6 of the Hungarian Advertising Act (Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Economic Advertising Activities, "Grt.").

Retention:

Data processed for the purpose of sending newsletters (name, e-mail address) are processed until Consent is withdrawn (unsubscription or the Data Subject's request for erasure or objection).

Data evidencing the fact and time of granting Consent are retained for 5 years from withdrawal of Consent, having regard to the establishment, exercise and defence of civil-law claims.

2.6. Marketing and Remarketing Systems (Meta, Google, TikTok)

Purpose:

Displaying personalised advertisements on external platforms.

Data processed:

- e-mail address (in hashed form for creating custom audiences)
- IP address
- cookie identifiers
- device identifier
- event data collected by pixels (e.g. "Add to cart", "Purchase") — pseudonymised

Legal basis:

The placement and reading of cookies and device identifiers are based on the Data Subject's prior Consent pursuant to the applicable Member State electronic communications/ePrivacy rules (see Section 1.3; for Data Subjects in Hungary, in particular Section 155 of the Hungarian Electronic Communications Act (Act C of 2003 on Electronic Communications, "Eht.")). The subsequent processing of personal data — including the hashed e-mail address and event data collected by pixels — is based on the Data Subject's explicit Consent under Article 6(1)(a) GDPR.

Retention:

Until the cookies expire (generally 90–180 days), or until withdrawal of Consent.

Special note:

The data are generally processed by Meta / Google on **servers located outside the EU** → see Chapter 6: International Data Transfers + SCCs.

With regard to certain Meta and Google tools (e.g. Custom Audience, Customer Match), joint controllership (Article 26 GDPR) may exist at certain stages of the processing — see Chapter 3.

2.7. Loyalty Points System (Loyalty Program)

Purpose:

Crediting and redeeming points and managing point history.

Data processed:

- e-mail address
- point history
- purchase history

Legal basis:

Performance of a contract — Article 6(1)(b) GDPR. Registration for the loyalty points system is a voluntary step separate from the purchase, to which the Data Subject expressly joins by accepting the terms of the program; this separate acceptance constitutes the legal basis.

Retention:

Until deletion of the account

2.8. Affiliate Program (Refersion / Yotpo / Other)

Purpose:

Managing commissions payable to influencers and partners and campaign tracking.

Data processed:

- name
- e-mail address
- affiliate ID
- commission data
- number of generated sales
- payment data (bank account number or PayPal — if provided by the partner)

Legal basis:

Performance of a contract – Article 6(1)(b) GDPR

Retention:

5 years following termination of the contract (limitation period under the Hungarian Civil Code)

Special note:

Service providers used for affiliate-related data processing may process personal data in several countries:

- In the case of **Refersion** (United States), the Data transfer is based on the Standard Contractual Clauses (SCCs) pursuant to Commission Decision (EU) 2021/914.
- In the case of **Yotpo** (primarily Israel, as well as the United States, United Kingdom and European Union), Data transfers to Israel are based on the European Commission's adequacy decision concerning Israel, according to which Israel is regarded as a third country providing an adequate level of protection for GDPR purposes, without separate safeguards (SCCs); Data transfers to the United Kingdom are based on the EU–UK adequacy decision, likewise by means of an adequacy decision; with regard to Data transfers to the United States, the service provider applies the Standard Contractual Clauses pursuant to Commission Decision (EU) 2021/914.

For further information, see Chapter 6: International Data Transfers.

2.9. Customer Service, Statutory Warranty, Commercial Warranty and Consumer Protection Complaints

Purpose:

Handling, investigating, documenting and fulfilling customer service enquiries, consumer complaints, and statutory warranty and commercial warranty claims.

Under EU consumer protection legislation applicable to the sale of goods (Directive (EU) 2019/771 and its implementation in the Member States), the Customer has rights relating to conformity of the goods with the contract, including statutory warranty rights and — **Where applicable under local law** — product warranty rights. The existence and scope of mandatory or voluntary commercial warranty, as well as the procedural rules governing the handling of statutory warranty and commercial warranty claims, are determined by the national law applicable to the Data Subject.

Where applicable under local law, in the case of Customers in Hungary, this means the following: dietary supplement products marketed by BODYFACT are not subject to mandatory statutory warranty under Hungarian law (the category of products subject to mandatory statutory warranty is defined in Annex 1 to Decree 10/2024 (VI. 28.) of the Minister of Justice ("10/2024. (VI. 28.) IM rendelet")); BODYFACT provides a voluntary commercial warranty for certain non-food ancillary products, in particular shakers, pursuant to Section 6:171 of the Hungarian Civil Code (Act V of 2013 on the Civil Code, "Ptk."), the duration and conditions of which, as well as the rights arising from the commercial warranty, are set out in the warranty certificate accompanying the product and in the warranty information published on the Website; in handling statutory warranty and commercial warranty claims, the Service Provider acts in accordance with the provisions of Decree 19/2014 (IV. 29.) of the Minister for National Economy ("19/2014. (IV. 29.) NGM rendelet").

The Service Provider shall draw up a record of any statutory warranty or commercial warranty claim reported by the Customer, which may include, in particular, the Customer's name and contact details, the subject matter and consideration of the contract, the date of performance, a description of the reported defect, the claim asserted by the Customer, and the manner in which the claim is settled or the grounds for its rejection.

Where the Service Provider takes possession of the product for the purpose of examination, it shall issue an acknowledgement of receipt, which may contain the data necessary to identify the Customer, the data necessary to identify the product, the date of receipt and the expected date of return of the product.

Data processed:

- name
- e-mail address
- telephone number (if provided)
- postal address or delivery address (if necessary for handling the matter)
- order number
- details of the purchased product
- date of purchase and performance
- content of the complaint, statutory warranty or commercial warranty claim
- description of the reported defect
- related documents and evidence (e.g. invoice, photograph, record, correspondence)

- customer service communications
- ticketing and case-handling data

Legal basis:

- Article 6(1)(b) GDPR – Performance of a contract and taking measures at the request of the Data Subject prior to entering into a contract
- Article 6(1)(c) GDPR – compliance with a Legal obligation applicable to the Controller, in particular consumer protection, statutory warranty and commercial warranty obligations

Nature of the provision of data:

The provision of personal data is required partly for compliance with statutory obligations and partly for the investigation and handling of complaints, statutory warranty or commercial warranty claims. Without the necessary data, the investigation or fulfilment of the claim may become partially or entirely impossible.

Retention:

The record of the complaint, the written complaint and the substantive response to the complaint must be retained by the Service Provider for the period prescribed by the national consumer protection legislation applicable to the Data Subject and must be presented upon request by the competent supervisory authority. **Where applicable under local law**, for Customers in Hungary, this period is 3 years from the date of rejection of the complaint or the date on which the substantive response was sent, pursuant to Section 17/A(7) of the Hungarian Consumer Protection Act (Act CLV of 1997 on Consumer Protection, "Fgytv.").

Other documents and personal data relating to complaint handling and customer service, as well as statutory warranty and commercial warranty claims (in particular correspondence, attachments and other evidence), are retained by the Service Provider for 5 years from the closure of the complaint or the final settlement of the claim.

Where any legislation prescribes a longer or shorter mandatory retention period, the Service Provider shall act in accordance with the provisions of such legislation.

Where processing is necessary for the establishment, exercise or defence of legal claims, the processing period shall last until the proceedings have been finally concluded, but no longer than the applicable limitation period of the claim.

2.10. Quality Complaints + Food Recall

Purpose:

Investigating product safety and maintaining mandatory food safety records.

Data processed:

- name
- contact details
- order data
- batch number
- photographs requested for the investigation
- quality management notes

Legal basis:

Legal obligation (food safety requirements) – Article 6(1)(c) GDPR

Retention:

5 years
(based on the traceability requirements of the RASFF system and the applicable EU food law)

2.11. Recording and Withdrawal of Consent (Consent Log)

The Service Provider records the fact and content of Consent given for the processing of personal data in an electronic register (the "consent log"). The register contains the date and time of Consent, the subject matter of the Consent (e.g. newsletter, remarketing cookie), and the source of the Consent (Website, pop-up window, form). The purpose of documenting Consent is to demonstrate legal compliance and ensure the exercise of Data Subject rights.

The Data Subject may withdraw Consent at any time, without giving reasons and free of charge, by the following means:

- via the cookie management interface of the Website,
- by e-mail at privacy@bodyfact.eu,
- via the unsubscribe link included in newsletters.

Withdrawal of Consent does not affect the lawfulness of processing based on Consent before its withdrawal.

At the request of the Data Subject, the Service Provider shall provide information within 30 days on when, how and for what purpose Consent was given and shall send, upon request, a certified copy of the relevant elements of the Consent register.

The specific retention period of the Consent register is determined by the relevant processing purpose, as specified in the applicable section (for newsletter and marketing Consent, Section 2.5; for cookie Consent, Section 6.2).

2.12. Cookie Management and Cookie Identifiers

Purpose:

Ensuring the operation of the Online Store, analytics, marketing and management of user preferences.

The detailed categories of cookies are set out in Section 5.2 (Categories of Cookies).

Data processed:

- IP address
- cookie identifier
- device data
- browsing events
- event logs generated by marketing pixels

Legal basis:

- necessary cookies: Legitimate interest of the Controller
- analytics / marketing cookies: Consent

Retention:

The exact retention periods of the individual cookie categories (necessary, preference, analytics, marketing) are specified in the Cookie Policy (Cookie List) available on the Website, which is continuously kept up to date through the CookieBot consent management platform.

2.13. Customer Reviews and Customer Satisfaction Enquiries

Purpose:

Following fulfilment of an order, inviting the Customer to submit a review by means of an automated electronic message (Section 15.3.1 of the Terms and Conditions), as well

as processing personal data relating to customer reviews and user-generated content (UGC) published by the Customer.

Data processed:

- name (where the review is published, at the Customer's choice, either full name or initials/nickname)
- e-mail address
- order/purchase identifier
- text and rating of the submitted review
- date and time the review invitation was sent
- in the case of an incentive-based enquiry: the fact, date and manner of granting Consent

Legal basis:

Where the review invitation is sent exclusively for the purpose of conducting a customer satisfaction survey or requesting a customer review, does not contain any advertising elements, and does not constitute commercial advertising under the applicable national law (see Section 1.3; for Data Subjects in Hungary, in particular the Grt.), the legal basis for the processing relating to the review invitation is the Service Provider's Legitimate interest (Article 6(1)(f) GDPR; Section 15.3.1 of the Terms and Conditions).

Where the review invitation also contains an incentive as referred to in Section 2.13 of this Privacy Policy and Section 15.7 of the Terms and Conditions (in particular a coupon, loyalty points or discount), it may constitute commercial advertising under the applicable national law (in Hungary, for the purposes of the Grt.). In such cases, the message may be sent exclusively on the basis of the Data Subject's prior, voluntary, specific, informed, explicit and unambiguous Consent (Article 6(1)(a) GDPR; for Data Subjects in Hungary, Section 6 of the Grt.; Section 15.7.4 of the Terms and Conditions).

Even in the case of an enquiry sent on the basis of Legitimate interest and exclusively for customer satisfaction purposes, the Data Subject is provided with the possibility to unsubscribe and to exercise the Right to object under Article 21 GDPR; following unsubscription, the Service Provider shall not send the Customer any further messages of this nature. In the case of review invitations containing an incentive and based on Consent, the granting and withdrawal of Consent at any time and free of charge (unsubscription) shall take place in the same manner as the newsletter subscription and unsubscription mechanism described in Section 2.5 of this Privacy Policy.

Retention:

The Service Provider retains personal data relating to customer reviews and logging data used to demonstrate Consent only for as long as necessary, taking into account the purpose of the processing, applicable statutory obligations, the need to resolve any disputes, and consumer protection and accounting requirements.

The specific retention periods mandatorily prescribed by law are summarised in Section 2.14 (Statutory Data Retention).

Content Upload in Exchange for Loyalty Points (Photo/Video):

In connection with the loyalty points system, the Customer is given the opportunity to upload a photograph or video of the purchased product in exchange for loyalty points credited by the Service Provider. The Customer's explicit Consent is required for BODYFACT to use the uploaded content for marketing purposes.

Data processed: the uploaded photograph or video; the Customer's statement regarding their right to upload the content; the Customer's Consent to marketing use; the fact, date and manner in which both statements were provided.

Legal basis: explicit Consent of the Data Subject — Article 6(1)(a) GDPR. The protection of the image/portrait of third parties who may appear in the uploaded content is subject to the applicable national law (in particular rules concerning personality rights relating to a person's image/portrait); responsibility for ensuring this rests with the uploading Customer, through acceptance of the following two separate declarations:

"☐ I confirm that I am entitled to share the uploaded content — it is my own content, or, where another person is concerned, it was created/shared with that person's knowledge and consent. If a third party raises an objection to its use, BODYFACT may remove the content at its own discretion, irrespective of the reported issue."

"☐ I consent to BODYFACT using the uploaded content for marketing purposes as follows. [More information: How we use the uploaded content]"

The detailed information available through the "More information" link specifies the exact scope of use (Online Store and Website, organic social media platforms, paid online advertising), the right to edit the content, and the method of withdrawing Consent.

If a third party affected by the content — whether the uploading Customer or another person affected by the content — objects to its use, the Service Provider shall remove the content without undue delay and no later than **10 business days** following receipt of the objection.

Retention: until withdrawal of Consent or, in the absence of withdrawal, for as long as the purpose of the marketing use remains applicable, but for no longer than **3 years**.

Rights of the Data Subject and limitations on erasure:

The Customer has, in particular, the following rights: the Right of access, the Right to rectification, the Right to erasure, the Right to restriction of processing, the Right to object to processing, and the Right to lodge a complaint.

The Customer may withdraw Consent at any time and free of charge (unsubscribe); withdrawal does not affect the lawfulness of processing carried out before withdrawal.

The Customer may request rectification, restriction of processing or erasure of personal data relating to a review published by the Customer. The Service Provider may refuse to comply with an erasure request in whole or in part where processing of the personal data remains necessary for compliance with a Legal obligation, for the establishment, exercise or defence of legal claims, or for another purpose specified by law.

Where Consent is withdrawn or a request for deletion of a review is fulfilled, the Service Provider shall discontinue the public display of the relevant review for the future; however, it may retain data and log files necessary to demonstrate that Consent was given, that the transaction was concluded, and that the processing was lawful.

2.14. Statutory and Legitimate-Interest-Based Data Retention Periods

The following principal retention periods apply on the basis of the Service Provider's statutory obligations and — based on its Legitimate interest in the establishment, exercise and defence of legal claims — as follows:

- billing data: 8 years (Legal obligation — Hungarian Accounting Act; see Section 2.3)
- contractual/order data: up to 5 years, based on Legitimate interest and taking into account the limitation period under the national law applicable to the Data Subject (see Section 1.3); for Data Subjects in Hungary, this is the 5-year limitation period under Section 6:22 of the Hungarian Civil Code (Act V of 2013 on the Civil Code, "Ptk.") (see Section 2.2)
- complaint record, written complaint and substantive response: **Where applicable under local law**, for Customers in Hungary, 3 years (Section 17/A(7) of the Hungarian Consumer Protection Act (Act CLV of 1997 on Consumer Protection, "Fgytv."))
- other complaint-handling and customer-service documentation: 5 years (see Section 2.9)
- food safety documentation: 5 years (see Section 2.10)

This list summarises the retention periods applicable to the processing purposes detailed above; in the event of any discrepancy, the detailed rules set out in the relevant section (2.2, 2.3, 2.9, 2.10) shall prevail.

2.15. Access to Data

Access to the data is restricted exclusively to employees who:

- perform sales,
- customer service,
- marketing,
- IT development

functions and have been granted the relevant authorisation.

3. Processors, Joint Controllers and Data Transfers

This chapter defines the scope of all processors and service providers that have access to personal data in the course of BodyFact's activities — whether acting as a Processor or as an independent Controller.

The Service Provider uses only service providers that comply with the data security and accountability requirements set out in the GDPR and with whom appropriate agreements (Data Processing Agreement – DPA) are in place.

3.1. Security measures applied by the Controller during data transfers

For every data transfer, the Controller seeks to ensure the measures required under Article 32 of the GDPR:

- encrypted data transmission channels (HTTPS, TLS 1.2+)
- server-side encryption
- restriction of API access
- logging of internal access
- two-factor authentication
- pseudonymisation (in particular in the case of marketing pixels)

3.2. Cases of joint controllership (Article 26 GDPR)

In the case of certain marketing tools, the Service Provider and the platform qualify as joint Controllers.

This includes in particular:

- Meta (Facebook) Custom Audience / Pixel
- Google Ads Customer Match

The scope of the joint controllership is determined by the “Controller Addendum” agreements provided by the platforms.

The essence of the joint controllership is as follows: the Service Provider is responsible for ensuring that it has a lawful legal basis (the Data Subject’s Consent) for activating the Custom Audience / Customer Match function and for transmitting the data to the platform in accordance with the platform’s requirements (typically in encrypted, hashed form). The platform (Meta and Google, respectively) is responsible for receiving, matching and using the data for advertising purposes, to the extent specified in its own Privacy Policy and the Controller Addendum. The full text of the joint controllership agreement is available in the relevant legal documentation of the platform.

The Data Subject may primarily exercise the rights specified in this Privacy Policy against the Service Provider; however, pursuant to Article 26(3) of the GDPR, the Data Subject is also entitled to enforce these rights directly against Meta and Google, respectively.

3.3. Auditing of Processors

The Controller reviews the Processors annually:

- compliance (GDPR, SCCs, data protection audit)
- up-to-dateness of Data Processing Agreements
- review of data security measures

4. International Data Transfers (SCCs, TIA, Technical and Organisational Measures)

4.1. Legal framework for international data transfers

In the course of certain processing activities, BodyFact uses service providers whose registered office or servers are located outside the European Union.
Such service providers include in particular:

- Shopify Inc.
- Stripe Inc.
- PayPal (Europe) S.à r.l. et Cie, S.C.A., as well as members of the PayPal Group located outside the European Economic Area, in particular PayPal, Inc., United States
- Klaviyo Inc.
- Meta Platforms Inc.
- Google LLC
- TikTok Inc.

Where the PayPal payment method is used, the Customer's primary contractual partner is PayPal (Europe) S.à r.l. et Cie, S.C.A., established in the European Economic Area; however, due to the global structure and IT infrastructure of the PayPal Group, some personal data may also become accessible to members of the PayPal Group located outside the European Economic Area, in particular PayPal, Inc. (United States). Accordingly, the international data transfer rules set out in this chapter apply to processing activities associated with the use of the PayPal payment method.

As the processing of data by these service providers frequently takes place in the **United States** or in another so-called "third country", such transfers are governed by **Chapter V of the GDPR**.

A transfer of personal data to a third country is lawful only if it complies with the appropriate safeguards set out in Article 46 of the GDPR.

4.2. Transfer safeguards applied (Article 46 GDPR)

In accordance with the GDPR, the Service Provider applies the following safeguards:

4.2.1. Standard Contractual Clauses (SCCs – standardised EU model clauses of 2021)

The Controller applies **SCCs** with every service provider that processes personal data outside the EU, which:

- are legally binding,
- have been approved by the European Commission,
- impose data security and data protection obligations on the data importer.

BodyFact applies the new SCCs issued on 4 June 2021 (Modules 1–4), depending on the specific role of the service provider.

4.2.2. Transfer Impact Assessment (TIA)

In addition to SCCs, the Service Provider prepares or reviews a **TIA** for each relevant partner in a third country, assessing:

- the legal environment of the country concerned,
- the authorities' possibilities of accessing data,
- the service provider's level of technical protection,
- the data importer's internal compliance processes.

The purpose of the TIA is to establish that the personal data transferred continue to receive **a level of protection compliant with the GDPR** after leaving the EU.

4.2.3. Technical and Organisational Measures (TOMs — Technical & Organisational Measures)

Before transferring data to a third country, the Service Provider verifies that the service provider applies at least the following security measures:

- **encryption of data in transit** (TLS 1.2+)
- **server-side encryption** (AES-256 or equivalent)
- **pseudonymisation and hashing** (e.g. e-mail hashing for remarketing purposes)
- **access logging**
- **restriction of access rights**
- **SOC2 / ISO 27001 certification** (Stripe, Shopify, Klaviyo)

- **physical data centre security**
- **restricted access to user data**
- **regular security audits**

4.2.4. EU–US Data Privacy Framework (Data Privacy Framework, DPF)

Transfers of data to the United States are, in the case of certain service providers, carried out on the basis of the European Commission's adequacy decision concerning the EU–US Data Privacy Framework, provided that the relevant US legal entity and the specific category of processing are actually covered by the DPF certification. The existence of DPF certification does not in itself mean that all processing activities of a service provider automatically take place on the basis of this mechanism — the Service Provider assesses the applicability of the DPF on a provider-by-provider and data-category basis and, where the DPF does not apply, uses the standard contractual clauses (SCCs) approved by the European Commission and a Transfer Impact Assessment (TIA).

The Service Provider regularly reviews the DPF certification status of the service providers listed in Section 4.3 at regular intervals, as certification status may change over time. The current status of individual service providers can be verified in the official DPF register (dataprivacyframework.gov).

4.3. Specific service providers involved in international data transfers and their roles

4.3.1. Shopify Inc. (Canada, USA)

- **function:** hosting, operation of the Online Store
- **data flow:** IP address, order data, user account data
- **legal basis:** Performance of a contract, Legitimate interest
- **safeguard:** Shopify's current Data Processing Agreement (DPA) identifies the EU–US Data Privacy Framework (DPF) and — if the relevant data transfer does not fall within the scope of the DPF — SCCs as the applicable data transfer mechanism; the Service Provider applies the appropriate mechanism based on the specific Shopify entity, processing activity and data category, in accordance with Shopify's applicable statements, with a TIA and encryption as supplementary safeguards

Note:
Due to Canada, Shopify has **adequate country status**, but certain sub-services are performed in the USA.

4.3.2. Stripe Inc. (USA)

- **function:** processing of payment transactions, subscription management
- **data flow:** transaction metadata, tokenised payment card data
- **safeguard:** primarily the adequacy decision under the EU–US Data Privacy Framework (DPF), given that Stripe, LLC holds a valid DPF certification; if a particular data transfer does not fall within the scope of the certification, the Service Provider applies SCCs and a TIA as supplementary safeguards
- **PCI-DSS compliance**

4.3.3. Klaviyo Inc. (USA)

- **function:** newsletters and marketing automation
- **data flow:** name, e-mail address, campaign interactions
- **safeguard:** primarily the adequacy decision under the EU–US Data Privacy Framework (DPF), given that Klaviyo, Inc. holds a valid DPF certification; if a particular data transfer does not fall within the scope of the certification, the Service Provider applies SCCs, hashing and AES-256 encryption as supplementary safeguards

4.3.4. Meta Platforms Inc. (USA)

- **function:** remarketing, ad targeting
- **data flow:** pixel event data, cookies, hashed e-mail
- **safeguard:** primarily the adequacy decision under the EU–US Data Privacy Framework (DPF), given that Meta Platforms, Inc. and its wholly owned US subsidiaries hold valid DPF certifications, including the Meta Business Tools, Meta Pixel, Conversions API, and Ads and Measurement categories; if a particular data transfer does not fall within the scope of the certification, the Service Provider applies Controller Terms and SCCs as supplementary safeguards
- in certain cases, joint controllership

4.3.5. Google LLC (USA)

- **function:** analytics, advertising, remarketing
- **data flow:** cookies, IP address (partially anonymised), GA events
- **safeguard:** primarily the adequacy decision under the EU–US Data Privacy Framework (DPF), given that Google LLC and its wholly owned US subsidiaries hold valid DPF certifications, including data transfers carried out in connection with Ads Services; if a particular data transfer does not fall within the scope of the certification, the Service Provider applies SCCs as a supplementary safeguard
- IP anonymisation, partial use of EU servers

4.3.6. TikTok Inc. (USA / Singapore)

- **function:** remarketing
- **data flow:** cookies, pixel events
- **safeguard:** SCCs + TIA (TikTok currently cannot be identified in the official DPF register as an entity on which the Service Provider could safely base the data transfer; therefore, the data transfer is not based on the DPF, but on SCCs and the Transfer Impact Assessment (TIA), taking into account the relevant TikTok entity and data flow)

4.3.7. PayPal (Europe) S.à r.l. et Cie, S.C.A. (Luxembourg) / PayPal, Inc. (United States)

- **function:** where the PayPal payment method selected by the Customer is used, processing and execution of payment transactions, ensuring the security of transactions and preventing fraud, as well as fulfilling the payment services, financial, anti-money laundering (AML/CFT) and other statutory obligations applicable to PayPal;
- **legal status:** PayPal acts as an independent Controller with regard to the purposes and means of processing determined by PayPal. The Service Provider transfers to PayPal the data necessary for initiating and processing the payment transaction. With regard to processing activities carried out by PayPal as an independent Controller, no Processor relationship within the meaning of Article 28 of the GDPR exists between the Service Provider and PayPal;

- **data flow:** depending in particular on the specific payment process and integration, the Customer's name, e-mail address, billing and delivery details, order identifier, transaction amount and PayPal transaction identifier, as required for the payment transaction;
- **international data transfers:** depending on the operation of PayPal's international corporate group and the services used, personal data may also become accessible to PayPal Group entities located outside the European Economic Area or to other recipients, including, where applicable, PayPal, Inc., located in the United States;
- **safeguards:** where personal data are transferred to a country outside the European Economic Area, the transfer is carried out on the basis of the appropriate safeguards specified in Chapter V of the GDPR that are actually applicable to the relevant transfer, in particular — where applicable — on the basis of the standard data protection clauses (SCCs) adopted by the European Commission, taking into account the necessary supplementary measures and the transfer risk assessment, including the Transfer Impact Assessment (TIA).

4.4. Transparency provided by the Service Provider: availability of SCCs

Upon request by the Data Subject, the Service Provider provides access to **relevant parts of the SCC documents**, taking into account the following:

- the business secrets of service providers may not be disclosed,
- SCC modules or annexes may be provided in partial form,
- the Controller shall process the request within 30 days.

4.5. The Service Provider reserves the right to change service providers

The Service Provider is entitled to engage other Processors in the future, provided that they:

- provide appropriate safeguards (Article 46 GDPR),
- apply SCCs,
- have a verified level of data security (ISO 27001 / SOC2),
- comply with the requirements of the GDPR.

4.6. Exclusion of data transfers in special cases

The Service Provider does not transfer personal data:

- to prohibited countries (EU sanctions list),
- to a service provider without adequate protection,
- to a partner that does not sign the SCCs,
- or to a partner that does not undertake to comply with TIA or TOM requirements.

4.7. Risk assessment and monitoring

The risk classification of international data transfers is reviewed annually:

- updating of TIAs,
- replacement in the event of a new version of the SCCs,
- review of practical service provider audits,
- monitoring of ICO / EDPB recommendations,
- ensuring Schrems II compliance.

4.8. Rights of the Data Subject in the event of international data transfers

The Data Subject is entitled to:

- request information on the country to which the data are transferred,
- request a copy of the relevant parts of the SCCs,
- object to transfers based on Legitimate interest,
- lodge a complaint with the Supervisory Authority.

5. Use of Cookies and Cookie Management

5.1. Purposes and legal basis of the use of cookies

The BodyFact website (hereinafter: the “Website”) uses cookies and other tracking technologies for its operation, personalised user experience, statistical analysis and marketing activities.

The purposes of using cookies are:

1. **Ensuring the operation of the Website**
   – login, shopping cart functionality, security features, maintenance of the session.
2. **Storage of user preferences**
   – language settings, region-specific functionality, cookie settings selected by the user.
3. **Analytics and performance measurement**
   – measuring Website traffic, identifying errors, optimising functionalities.
4. **Marketing and remarketing**
   – displaying personalised advertisements
   – running targeted campaigns based on user behaviour.

Legal bases:

- **Necessary cookies:** Article 6(1)(b) of the GDPR – Performance of a contract (e.g. operation of the shopping cart and payment process), and/or Article 6(1)(f) of the GDPR – the Controller's Legitimate interest (e.g. IT security, fraud prevention).
- **Non-essential cookies:** Article 6(1)(a) of the GDPR – the Data Subject's prior, voluntary Consent.

Non-essential cookies may not be activated upon the first loading of the Website without Consent given through the cookie management system.

For the purpose of ensuring the operation of the Website, improving the user experience, and for statistical and marketing purposes, the Controller uses various types of cookies. This chapter describes exclusively the types, purposes and Retention periods of cookies. The detailed rules governing Consent management relating to the use of cookies are set out in Chapter 6.

5.2. Categories of cookies

The following categories are defined on the basis of the GDPR, the ePrivacy framework and the CookieBot rules.

5.2.1. Necessary (essential) cookies

These cookies are essential for the operation of the Website. Their installation does not require Consent.

Functions:

- session identifier (session ID)
- maintaining login status
- shopping cart functionality
- operation of the payment process
- security, fraud prevention
- storage of cookie Consent settings

Typical examples:

- Shopify essential cookies
- Cloudflare security cookies
- CookieBot “consent” status cookie

5.2.2. Preference cookies (functionality / preferences)

These cookies provide a personalised user experience.

Functions:

- saving the selected language
- region, currency
- retaining preferred settings
- partial completion of forms

They may only be activated with Consent.

5.2.3. Analytics cookies (analytics)

The Service Provider may use the following services for analytical purposes:

- Google Analytics 4
- Shopify Analytics
- Hotjar (if activated)

The data processed may include, for example:

- time of visit
- behavioural data (page views, clicks)

- device and browser data
- partially anonymised IP address

Consent is required for the installation of analytics cookies.

5.2.4. Marketing and remarketing cookies

These include:

- Meta (Facebook) Pixel
- Google Ads remarketing tag
- TikTok Pixel
- Klaviyo web tracking
- Shopify marketing cookies

Data processed:

- page views
- purchase events (view content, add to cart, initiation, purchase)
- hashed e-mail address (for remarketing purposes)
- user behavioural patterns

Marketing cookies may only be activated after Consent.

5.3. Cookie management options available to the Data Subject

The Data Subject has the following rights and options regarding cookies:

5.3.1. Giving or refusing Consent

Upon the first visit to the Website, a cookie banner is clearly displayed, where the Data Subject may:

- accept all cookies,
- select certain categories,
- reject all cookies.

5.3.2. Modifying or withdrawing Consent

Consent may be withdrawn at any time through:

- “Cookie Settings”
- or by opening the CookieBot panel.

Withdrawal does not affect the lawfulness of processing based on Consent before its withdrawal.

5.3.3. Browser settings

The Data Subject may also delete cookies in their browser by using:

- cookie deletion
- private mode
- blocking settings
- blocking third-party cookies

5.3.4. Mobile device settings

The following advertising identifiers may likewise be restricted or deleted:

- Apple IDFA
- Google Advertising ID

5.4. Cookie Retention period

Depending on their type, cookies are retained for:

- session cookies → until the browser is closed
- preference cookies → 1–12 months
- analytics cookies → 1–24 months
- marketing cookies → 1–24 months (Meta, TikTok, Ads)

CookieBot displays the Retention period of each individual cookie in a list updated monthly.

6. Cookie Consent Management System (Consent Manager)

BodyFact installs non-essential cookies exclusively on the basis of the Data Subject's prior, voluntary, specific, appropriately informed and explicit Consent pursuant to Article 6(1)(a) of the GDPR and the applicable legislation governing electronic communications.

For the management of Consent, the Controller uses the CookieBot consent management platform (Cybot A/S, Denmark), which ensures that cookies requiring Consent are activated only following the Data Subject's active approval.

The Controller reserves the right to use, instead of CookieBot, another consent management system of equivalent or higher standard, provided that such system complies with the applicable data protection requirements.

6.1. CookieBot as a consent management system

CookieBot provides in particular:

- obtaining Consent from visitors;
- logging Consent records;
- storing the status of Consent;
- blocking non-essential cookies until Consent is given;
- automatically identifying and categorising the cookies used;
- ensuring the auditability of Consent logs.

CookieBot enables the Data Subject to make a separate decision for each cookie category as to whether to give, refuse or withdraw Consent.

6.2. Logging and Retention of Consent

In connection with Consent, CookieBot logs in particular the following data:

- date and time of Consent;
- the Data Subject's IP address in anonymised form;
- selected cookie categories;
- version number of the Consent banner;
- the Data Subject's domain;

- technical Consent identifier (Consent ID).

The Retention period of Consent logs is generally 12 months.

The purpose of logging is to comply with the principle of accountability under the GDPR and to ensure that lawful Consent can be demonstrated.

6.3. Blocking of cookies until Consent is given

Upon the first visit to the Website, CookieBot automatically blocks the loading of all non-essential cookies and related scripts.

This may include in particular:

- Google Analytics;
- Google Ads;
- Meta Pixel;
- TikTok Pixel;
- Klaviyo tracking solutions;
- Shopify cookies for analytics or marketing purposes.

These cookies and related technologies may only be activated following the Data Subject's prior Consent.

This ensures the Website's compliance with the requirements of the GDPR and ePrivacy framework.

6.4. Renewal of Consent (Re-consent)

Consent is considered valid for a maximum period of 12 months, after which the system may request renewed Consent.

The Controller is entitled to request renewed Consent in particular in the following cases:

a) introduction of a new cookie category;
b) integration of a new third-party service provider;
c) a material change in the purposes of the cookies;
d) a change in applicable legislation.

The purpose of renewed Consent is to maintain continuous lawfulness.

6.5. Automatic cookie register and updating

CookieBot regularly and automatically scans, identifies and categorises the cookies used on the Website.

The purposes include in particular:

- identification of new cookies;
- removal of discontinued cookies;
- updating of cookie categories;
- keeping the Legal bases and descriptions relating to cookies up to date.

The current cookie register is continuously accessible through the CookieBot interface available on the Website.

6.6. Modification and withdrawal of Consent

The Data Subject is entitled at any time to:

- modify Consent;
- withdraw Consent;
- reconfigure cookie settings.

Withdrawal of Consent does not affect the lawfulness of processing carried out before the withdrawal.

The Data Subject may exercise these rights at any time through the “Cookie Settings” interface available on the Website.

6.7. Auditability and compliance documentation

The Controller ensures through CookieBot:

- the logging of Consent;
- the retrievability of Consent records;
- the maintenance of compliance documentation;
- the ability to demonstrate compliance to the Supervisory Authority.

Through this system, the Controller is able to demonstrate in particular:

- that non-essential cookies are not activated without Consent;

- that Consent is voluntary and informed;
- that Consent can be withdrawn at any time.

6.8. Third-party integrations and data transfers

CookieBot manages in an integrated manner, in particular:

- the Shopify cookie configuration;
- blocking of Google Tag Manager scripts;
- activation of Meta Pixel;
- loading of TikTok Pixel;
- Klaviyo marketing automation codes.

Where the use of cookies involves a Data transfer to a Third country, the Controller applies the safeguards specified in Chapter 4 (International Data Transfers) — including, where applicable, the adequacy decision under the EU–US Data Privacy Framework (DPF), and, in its absence, the Standard Contractual Clauses (SCCs) adopted by the European Commission and the associated Transfer Impact Assessment (TIA).

6.9. Transparency and continuous compliance

The Controller regularly reviews the scope of cookies used on the Website, the Consent management mechanism and the related data processing practices in order to ensure continuous lawfulness, transparency and compliance.

The Data Subject may at any time obtain detailed information through the CookieBot interface regarding the type, purpose, provider and Retention period of the cookies.

7. Rights of Data Subjects and Exercise of Their Rights

7.1. General principles governing the rights of Data Subjects (Article 12 of the GDPR)

The Service Provider ensures that the exercise of the rights of Data Subjects is:

- free of charge,
- transparent,

- easily accessible,
- carried out in an intelligible and clear manner,
- carried out without undue delay and, at the latest, within 30 days.

The Service Provider may make the fulfilment of requests conditional upon verification of the identity of the person making the request, particularly where the person is identified remotely (e.g. by e-mail).

Where justified, the response deadline may be extended by a further 2 months, of which the Service Provider shall inform the Data Subject in advance.

7.2. Right to information (Articles 13–14 of the GDPR)

The Data Subject has the right to obtain information about:

- what personal data are processed,
- the purposes and Legal bases of the processing,
- the categories of data processed,
- the Retention period of the processing,
- the recipients of Data transfers,
- the source of the personal data (where the data were not provided by the Data Subject),
- the fact of Data transfers to Third countries and the safeguards applicable thereto,
- the rights of the Data Subject and available legal remedies.

The Service Provider provides this information:

- in the Privacy Policy,
- during the purchasing process,
- when subscribing to the newsletter,
- and when responding to requests made by Data Subjects.

7.3. Right of access (Article 15 of the GDPR)

The Data Subject has the right to obtain confirmation from the Service Provider as to whether:

- their personal data are being processed, and
- if so, they may request access to:

1. what data have been processed,
2. for what purposes,
3. on what Legal basis,
4. to whom the data have been transferred,
5. for what period the data are processed,
6. what rights they have.

The Data Subject may request an electronic copy of their personal data (e.g. PDF, CSV).

The right of access is subject to limitations where its exercise would adversely affect the rights of others or trade secrets.

7.4. Right to rectification (Article 16 of the GDPR)

The Data Subject has the right to request:

- rectification of inaccurate personal data,
- completion of incomplete data.

The Service Provider shall carry out the rectification without undue delay and shall notify every recipient to whom the inaccurate data were previously disclosed, unless this would require disproportionate effort.

7.5. Right to erasure ("right to be forgotten") – Article 17 of the GDPR

The Data Subject may request the erasure of their personal data where:

1. the purpose of the processing has ceased to exist,
2. they have withdrawn their Consent and there is no other Legal basis,
3. they object to processing based on Legitimate interest,
4. the processing is unlawful,
5. erasure is required by a Legal obligation,
6. in the case of an information society service, the data concern a child.

Erasure may be refused where the processing:

- is necessary for compliance with a Legal obligation (billing data),
- is necessary for the establishment, exercise or defence of legal claims,
- cannot be erased due to accounting or tax obligations.

When fulfilling requests for erasure, the Service Provider:

- deletes the user account (if any),
- deletes data stored in marketing systems (Klaviyo, etc.),
- deletes profile data stored in Shopify,
- anonymises transactions (subject to statutory Retention requirements).

7.6. Right to restriction of processing (Article 18 of the GDPR)

The Data Subject may request restriction of processing where:

- they contest the accuracy of the personal data,
- the processing is unlawful and they oppose the erasure of the personal data,
- the Service Provider no longer needs the data, but the Data Subject requires them for the establishment, exercise or defence of legal claims,
- the Data Subject has objected to processing based on Legitimate interest (during the verification period).

During the restriction period, the data:

- may not be erased,
- may not be processed,
- may only be stored,

except:

- with the Data Subject's Consent,
- for the establishment, exercise or defence of legal claims,
- for the protection of another person,
- for important public interest reasons.

7.7. Right to data portability (Article 20 of the GDPR)

The Data Subject has the right to receive data:

- which they have provided to the Service Provider,
- the processing of which is based on Consent or a contract,
- and which are processed by automated means,

in a structured, commonly used and machine-readable format (e.g. CSV, JSON).

The Data Subject may also request the direct transfer of the data from one service provider to another, where technically feasible.

7.8. Right to object (Article 21 of the GDPR)

The Data Subject has the right to object at any time to the processing of their personal data where such processing:

- is based on Legitimate interest, or
- serves the purpose of direct marketing.

Consequences of an objection:

- the Service Provider may no longer process the personal data,
- unless it demonstrates compelling legitimate grounds for the processing.

In the case of direct marketing (e.g. newsletters):

The objection automatically results in the immediate deletion of the data from the marketing database.

7.9. Automated decision-making and profiling (Article 22 of the GDPR)

The Service Provider does not carry out automated decision-making that produces legal effects concerning the Data Subject or similarly significantly affects them, and does not conduct profiling that produces significant effects concerning the Data Subject.

In the course of its marketing activities, the Service Provider may in certain cases conduct profiling (in particular through segmentation using Klaviyo and Meta Ads) for the purpose of displaying offers corresponding to the Data Subject's interests. This type of marketing-oriented segmentation does not constitute prohibited automated decision-making under Article 22 of the GDPR because:

- it does not produce significant legal effects,

- it does not affect the Data Subject's legal status,
- it is used solely for advertising targeting.

7.10. How Data Subjects may exercise their rights

The Data Subject may exercise the rights specified in this Privacy Policy in writing by e-mail, postal mail or via the contact interface available on the Website.

The Controller shall process and respond to requests made by Data Subjects without undue delay and, at the latest, within the time limit specified in Article 12(3) of the GDPR.

7.11. Right to lodge a complaint and right to seek judicial remedy

7.11.1. Lodging a complaint with a Supervisory Authority

Pursuant to Article 77(1) of the GDPR, the Data Subject has the right to lodge a complaint with the Supervisory Authority in the Member State of their habitual residence, place of work or the place of the alleged infringement. The contact details of the Supervisory Authorities of the individual Member States are available on the website of the European Data Protection Board (EDPB).

Data Subjects in Hungary — as well as any other Data Subject wishing to lodge a complaint with the Hungarian Supervisory Authority — may contact:

Hungarian National Authority for Data Protection and Freedom of Information (NAIH)
H-1055 Budapest, Falk Miksa utca 9–11.
Telephone: +36 1 391 1400
E-mail: ugyfelszolgalat@naih.hu
Web: www.naih.hu

7.11.2. Right to seek judicial remedy

The Data Subject has the right to bring proceedings before:

- the court having jurisdiction at the registered seat of the Service Provider, or
- the court having jurisdiction according to the Data Subject's place of residence / habitual residence.

8. Technical and Organizational Measures (TOM)

8.1. General Principles of Data Security (Article 32 GDPR)

The Controller implements appropriate technical and organizational measures to ensure the continuous protection of the processed personal data in terms of:

- confidentiality
- integrity
- availability
- authenticity

When determining the measures to be applied, the Controller takes into account:

- the nature, scope, context and purposes of the processing,
- the degree of risk posed to the rights and freedoms of Data Subjects,
- the state of technology and the costs,
- the best available industry practices.

8.2. Technical Data Security Measures

The Controller and its contracted Processors ensure technical protection at multiple levels.

8.2.1. Data Encryption

Encryption of Data Transfers

- HTTPS / TLS 1.2 or later protocols
- Encryption of data communications with Shopify, Stripe, Klaviyo, Meta, Google and TikTok systems

Encryption of Data at Rest

- server-side AES-256 encryption
- tokenized payment card data (Stripe)
- hashed email addresses for marketing purposes (SHA-256 or equivalent)

The Controller never stores payment card data – payment transactions are handled exclusively by Stripe, with PCI-DSS certification.

8.2.2. Pseudonymization and Anonymization

Practices applied in marketing and analytics systems:

- hashed email addresses for remarketing purposes
- IP address anonymization in Google Analytics
- tokenized user identifiers

Pseudonymization minimizes the risk of identifying profiles.

8.2.3. Access Protection and Access Rights Management

The Controller:

- applies a role-based access control (RBAC) system
- grants access only to persons for whom such access is strictly necessary for the performance of their work
- requires multi-factor authentication (MFA)

All access rights:

- are reviewed regularly,
- are revoked immediately upon termination of employment,
- are logged.

8.2.4. System and Infrastructure Protection

The Controller applies industry-standard:

- firewalls,
- intrusion prevention systems (IPS),
- DDoS protection (Cloudflare / Shopify),
- version control and update policies,
- continuous vulnerability monitoring.

The hosting services and servers:

- have ISO 27001 or SOC 2 certification,
- are located in controlled data centres,
- employ physical security systems (24/7 security, access control, cameras).

8.2.5. Backups and Recovery

The Controller ensures:

- automated daily and weekly data backups,
- versioned backup storage,
- server-side redundancy,
- the use of geographically separate data centres,
- a rapid recovery procedure in the event of service outages (disaster recovery plan).

Backups are subject to separate encryption.

8.2.6. Logging, Monitoring and Auditing

The Controller and its Processor partners:

- perform continuous system logging,
- log administrator access,
- archive event logs,
- conduct regular internal and external audits (Shopify, Stripe, Klaviyo: SOC 2).

Security logs are retained for a defined period, typically 12–24 months.

8.3. Organizational and Administrative Data Security Measures

In addition to technical measures, the Controller applies organization-level policies and procedures.

8.3.1. Data Processing and Data Security Policy

The Controller's internal policies include:

- data processing procedures,

- definition of data protection responsibilities,
- incident management procedures,
- document and records management rules,
- data retention periods.

8.3.2. Employee Training and Confidentiality

The Controller ensures:

- annual data protection training,
- data leakage and phishing training,
- execution of confidentiality undertakings,
- communication of data security procedures.

All employees are required to comply with data protection requirements.

8.3.3. Processor and Contractual Safeguards

The Controller enters into contracts only with Processors that:

- have entered into a written Data Processing Agreement (DPA) (Article 28 GDPR),
- are demonstrably GDPR-compliant,
- carry out transfers to third countries on the basis of the safeguards specified in Chapter 4 (primarily the EU–US Data Privacy Framework and, in its absence, SCCs),
- provide appropriate security safeguards.

All Processors comply with the following:

- data security obligations,
- notification of security incidents,
- cooperation in handling Data Subject requests,
- ensuring auditability.

8.4. Personal Data Breach Response

For the prevention and handling of personal data breaches, the Controller:

1. applies a dedicated incident response protocol,
2. appoints an investigation team to assess the situation,
3. logs the incident and its circumstances,
4. determines the damage and risk resulting from the incident,
5. takes measures to terminate the event.

Notification obligation to the supervisory authority:

The Controller shall notify the NAIH of a personal data breach within 72 hours if it:

- poses a risk to the rights or freedoms of Data Subjects.

Notification of the Data Subject:

The Data Subject shall be informed where:

- the incident poses a high risk to the Data Subject.

The notification shall include:

- the nature of the incident,
- the time of occurrence,
- the data affected,
- the possible consequences,
- the measures taken,
- any further steps available.

8.5. Certifications and Compliance Certifications

The Controller's partners may hold the following certifications:

- ISO 27001 (Shopify, Google, Klaviyo)
- SOC 2 Type II (Stripe, Shopify, Klaviyo)
- PCI-DSS (Stripe – payment processing)
- ISO/IEC 27701 – privacy extension (certain service providers)

These ensure compliance with industry-level security standards.

8.6. Continuous Data Security Improvement

The Controller regularly reviews:

- technological developments,
- new security threats,
- the security of the service provider chain (Shopify, Stripe, Klaviyo, etc.),
- EDPB and NAIH recommendations,
- the current legal status of the safeguards concerning international data transfers described in Chapter 4 (DPF, SCC, TIA).

Where necessary, it implements additional protective measures.

8.7. Data Protection Impact Assessment

In accordance with Article 35 GDPR, the Controller carries out a Data Protection Impact Assessment (DPIA) when planning data processing operations if such processing may, in particular in the case of introducing new digital services, result in a high risk to the fundamental rights and freedoms of Data Subjects. The Controller consults the Supervisory Authority in advance, in accordance with the applicable rules, regarding the outcome of the Data Protection Impact Assessment and any necessary mitigating measures.

9. Retention Periods and Deletion Rules

9.1. General Principles of Data Retention Periods

The Service Provider processes personal data only for as long as necessary and in connection with the purpose of the processing, taking into account:

- Article 5(1)(e) of the GDPR (the “principle of storage limitation”),
- accounting and tax-law retention obligations (Hungarian Accounting Act (Act C of 2000 on Accounting, “Számviteli törvény”), Section 169),
- obligations arising from e-commerce legislation,
- any legal claims that may exist,
- the duration of the performance of customer contracts.

Where processing is necessary for the establishment, exercise or defence of legal claims, the processing period shall last until the final conclusion of the proceedings, but in any event no longer than the limitation period applicable to the claim. This rule shall apply as a supplementary rule to all retention periods specified in this Chapter and in other sections of the Privacy Policy where a dispute or legal claim arises in relation to the relevant category of data.

After the expiry of the retention periods:

- the data shall be deleted, or
- where deletion is not possible due to a statutory requirement → the data shall be irreversibly anonymised.

9.2. Specific Retention Periods by Data Type

The table below specifies the retention periods applicable to the categories of data processed by the Service Provider.

9.2.1. Purchase and Contractual Data

Data type	**Retention period**	**Legal basis / Remark**
Order metadata	5 years	Legitimate interest, with regard to the limitation period under the national law applicable to the Data Subject (see Sections 1.3 and 2.2); in the case of Data Subjects in Hungary, the five-year limitation period under Section 6:22 of the Hungarian Civil Code (Act V of 2013 on the Civil Code, “Polgári Törvénykönyv”)
Shipping data	Performance + 1 year	See Section 2.2
Invoice data	8 years	Hungarian Accounting Act (Act C of 2000 on Accounting, “Számviteli törvény”), Section 169; see Section 2.3

Data type	Retention period	Legal basis / Remark
Accounting/bookkeeping records of subscription transactions (Stripe Subscriptions)	8 years	Statutory obligation under the Hungarian Accounting Act (Act C of 2000 on Accounting, "Számviteli törvény"), Section 169. This row applies exclusively to accounting records relating to the subscription; the shorter retention period applicable to subscription-management data (account and status data) is specified in Section 2.4.
Data related to the performance of the contract	Until performance of the contract + 5 years	Legitimate interest, with regard to the limitation period under the national law applicable to the Data Subject

The Service Provider may not delete the above data earlier, even if the Data Subject requests deletion.

9.2.2. User Account Data

Data type	Retention period	Remark
User account (Shopify account)	Until deletion of the account	May be deleted at the request of the Data Subject
Inactive accounts	After 24 months of inactivity	The Service Provider may delete or anonymise the data on the basis of its legitimate interest

9.2.3. Newsletter Subscriptions and Marketing Data

Data type	Retention period	Legal basis / Remark
E-mail addresses of newsletter subscribers	Until withdrawal of Consent	GDPR Article 6(1)(a)

Data type	Retention period	Legal basis / Remark
Consent-verification log data (fact, date and source of the Consent)	5 years from withdrawal of Consent	GDPR Article 6(1)(f) – legitimate interest (establishment, exercise and defence of civil-law claims)
Unsubscribed e-mail addresses in the "suppression list"	24 months	For the purpose of demonstrating that no further marketing messages are sent
Marketing interactions (Klaviyo: opens, clicks)	24 months	Industry practice, statistics
Hashed identifiers of remarketing lists	180–540 days	Meta / Google Ads rules

9.2.4. Customer Service Data

Data type	Retention period	Remark
Customer service correspondence	12 months	Complaints, quality assurance
Complaint data	5 years; in the case of the complaint record, written complaint and copy of the substantive response: 3 years	Section 17/A(7) of the Hungarian Consumer Protection Act (Act CLV of 1997 on Consumer Protection, "Fogyasztóvédelmi törvény") (complaint record, written complaint and substantive response: 3 years, with an obligation to present them to the authority); other complaint data and documents: 5 years. Where necessary for the exercise of legal claims, processing shall continue until the proceedings are finally concluded, but no longer than the limitation period applicable to the claim.
Quality complaints and related documents	5 years	Archiving of investigations related to the 72-hour SLA. Where necessary for the exercise of legal claims, processing shall continue until the proceedings are finally concluded,

Data type	Retention period	Remark
		but no longer than the limitation period applicable to the claim.

9.2.5. Food Safety and Recall Data

Data type	Retention period	Remark
Batch-number management and manufacturer traceability data	5 years	Food industry regulations
Recall notifications	5 years	Regulatory compliance
Compensation data	5 years	Exercise of civil-law claims

9.2.6. Cookies and Online Identifiers

The indicative retention periods for the individual cookie categories are set out in Section 5.4 (“Cookie Retention Period”); the exact retention periods for individual cookies are specified in the Cookie List available on the Website and updated through CookieBot’s automated monthly scanning.

Cookies may be deleted manually or by withdrawing Consent.

9.2.7. Log Data and Log Files

Data type	Retention period	Remark
System logs	12–24 months	Security reasons
Logs of administrator access	12 months	Audit purposes
Incident logs	5 years	Due to GDPR notification obligations

9.2.8. Data Related to Customer Reviews

Data type	Retention period	Legal basis / Remark
Data contained in customer satisfaction / review invitation messages (without advertising content)	12 months from sending	GDPR Article 6(1)(f) – legitimate interest (Section 15.3.1 of the GTC)
Review invitation message containing an incentive (coupon, loyalty points, discount) and Consent data	Until withdrawal of Consent; Consent-verification log data for 5 years from withdrawal	GDPR Article 6(1)(a); Section 6 of the Hungarian Advertising Act (Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising, "Grt.") (Section 15.7.4 of the GTC)
Published customer review and user-generated content (UGC) — excluding photo/video uploads for loyalty points, see the row below	Until withdrawal of Consent or until a deletion request; after termination of public display, the log data necessary for evidentiary purposes shall be retained for 5 years from termination of the public display	Consent of the Data Subject; in the event of a legal claim, the Service Provider's legitimate interest for evidentiary purposes
Content uploaded in exchange for loyalty points (photo/video)	Until withdrawal of Consent or — in the absence of withdrawal — for a maximum of 3 years from the upload	GDPR Article 6(1)(a); see Section 2.13

9.3. Actions Following the Expiry of Retention Periods

Upon expiry of the retention period, the Service Provider shall:

1. delete the relevant personal data, or
2. irreversibly anonymise it where retention is required by law but its personal nature is no longer necessary.

Anonymisation may involve:

- hashing,
- creation of aggregated statistical data,
- irreversible data processing.

9.4. Handling of Deletion Requests

Upon a deletion request from the Data Subject, the Service Provider shall:

- delete or anonymise the account,
- remove the data from marketing systems,
- delete or deactivate cookies,
- request deletion by partner Processors as well (Shopify, Klaviyo, Meta, etc.).

The following data cannot be deleted:

- invoice data,
- accounting records relating to transactions,
- data necessary for the retention and defence of legal claims.

9.5. Statutory and Accountability Obligations

The Service Provider shall:

- review its data retention policy annually,
- document it during audits,
- update the Privacy Policy in the event of amendments.

In accordance with the principle of accountability, the Service Provider shall be required to:

- demonstrate that appropriate retention periods are applied,
- verify that deletions have been carried out,
- keep its records of processing activities up to date.

10. Recipients, Data Processors and Data Transfers

10.1. Introductory provisions

In the course of its data processing activities, the Data Controller uses only data processors and data recipients that:

- comply with Articles 28 and 46 of the GDPR;
- undertake to fulfil their obligations as data processors;
- have appropriate technical and organisational measures (TOMs) in place;
- enter into written data processing agreements;
- in the event of transfers of personal data to third countries, provide the safeguards specified in Chapter 4 (primarily the EU–US Data Privacy Framework, and where applicable, SCCs and a TIA), supplemented by additional technical safeguards.

10.2. Detailed list of data processors

The following list identifies the data processors required for the operation of BodyFact, their respective roles, the types of data processed and the safeguards ensuring GDPR compliance.

Pursuant to Article 28 of the GDPR, the Data Controller enters into agreements only with data processors that undertake in writing to comply with their obligations under the GDPR. The following sections describe the main data processors used for key functions, together with the principal categories of data processed and the safeguards ensuring legal compliance.

10.2.1. Shopify Inc.

Role: operation of the webshop system (data processor & controller / mixed)
Country: Canada + USA
Third country: Yes
Safeguards: see Section 4.3.1 (primarily DPF, and where necessary SCCs), supplemented by ISO 27001 and SOC 2 certifications

Data processed:

- name, e-mail address, telephone number

- shipping address
- order data, cart data
- IP address, device information
- account data, login data

Note: Canada is considered an adequate country for the relevant data processing activities. For services performed in the United States, Shopify applies the mechanism described in Section 4.3.1 (primarily DPF, and where necessary SCCs).

10.2.2. Stripe Inc.

Role: payment service provider, subscription management
Country: USA
Third country: Yes
Safeguards: see Section 4.3.2 (primarily DPF), supplemented by PCI-DSS Level 1 certification

Data processed:

- transaction metadata
- tokenised card data (not accessible to BodyFact)
- billing data
- subscription status, payment charges
- IP address, device information

10.2.3. PayPal (Europe) S.à r.l. et Cie, S.C.A.

Role: provision of payment services where PayPal is selected as the payment method (independent controller in relation to payment transaction processing, fraud prevention and legal compliance – see Section 4.3.7)

Country: Luxembourg (EU); intra-group data flows to the United States (PayPal, Inc.)

Third country: Yes, due to data flows outside the EEA within the PayPal group

Safeguards: where personal data is transferred to a country outside the European Economic Area, the transfer is carried out on the basis of the appropriate safeguards actually applicable to the relevant transfer under Chapter V of the GDPR, including, where applicable, the Standard Contractual Clauses (SCCs) adopted by the European

Commission, together with the necessary supplementary measures and transfer risk assessment, including a Transfer Impact Assessment (TIA).

Data processed:

- name
- e-mail address
- billing/shipping address required for the transaction
- order ID and amount
- PayPal transaction ID
- where the Customer has a PayPal account: data processed in connection with the Customer's independent contractual relationship with PayPal

10.2.4. Klaviyo Inc.

Role: e-mail marketing, newsletters, automation
Country: USA
Safeguards: see Section 4.3.3 (primarily DPF), supplemented by AES-256 encryption and SOC 2 certification

Data processed:

- name, e-mail address
- purchase history (if synchronised)
- campaign interactions (opens, clicks)
- preferences, interests (profile fields)
- hashed e-mail address for remarketing purposes

10.2.5. Meta Platforms Inc. (Facebook/Instagram)

Role: marketing and remarketing
Country: USA
Safeguards: see Section 4.3.4 (primarily DPF), supplemented by Controller Terms; for joint controllership, see Section 3.2

Data processed:

- Pixel event data (pageview, purchase)

- hashed e-mail address (Custom Audience)
- cookies, online identifiers
- remarketing lists

Note: In certain cases, joint controllership applies.

10.2.6. Google LLC

Role: analytics + advertising + remarketing
Country: USA
Safeguards: see Section 4.3.5 (primarily DPF), supplemented by IP anonymisation

Data processed:

- cookies
- IP address (anonymised)
- event data (GA4)
- remarketing identifiers (Ads)

10.2.7. TikTok Inc.

Role: remarketing
Country: USA / Singapore
Safeguards: see Section 4.3.6 (SCC + TIA; DPF is currently not applicable)

Data processed:

- Pixel event data
- cookies
- marketing interactions

10.2.8. Cloudflare, Inc.

Role: security infrastructure, CDN, DDoS protection
Country: USA + worldwide

Safeguards: primarily the EU–US Data Privacy Framework (DPF) adequacy decision, as Cloudflare, Inc. maintains a valid DPF certification. Under the Cloudflare Data Processing Addendum, v6.4, transfers carried out under this mechanism do not

constitute restricted transfers. If the certification ceases or becomes invalid, transfers shall rely on an alternative mechanism under the Cloudflare DPA, primarily SCCs and, where necessary, supplementary measures. Additional safeguard: ISO 27001 certification.

Data processed:

- IP address
- browser identifier
- traffic-related technical data

Cloudflare processes only the data necessary for the provision of its services and does not use such data for marketing purposes.

10.2.9. CookieBot (Cybot A/S)

Role: cookie consent management
Country: Denmark (EU)
Safeguards: EU-based provider; SCCs are not required

Data processed:

- consent status
- IP address (anonymised)
- cookie preferences
- Consent ID
- banner version number

10.2.10. Refersion, Inc.

Role: affiliate programme management, commission tracking
Country: USA
Third country: Yes
Safeguards: SCC + TIA (see Section 2.8)

Data processed:

- affiliate partner's name and e-mail address
- affiliate ID
- commission data, generated revenue

- payment data (bank account number or PayPal)

10.2.11. Yotpo Ltd.

Role: loyalty programme, customer reviews and user-generated content (UGC) management
Country: Israel (registered office); processing may also take place in the United States, the United Kingdom and the European Union
Third country: Yes

Safeguards: transfers to Israel are based on the European Commission's adequacy decision concerning Israel; transfers to the United Kingdom are based on the EU–UK adequacy decision; transfers to the United States are carried out on the basis of SCCs (see Section 2.8). EU GDPR representative: SMSBump Ltd. (Bulgaria).

Data processed:

- loyalty point data
- text of customer reviews
- uploaded photo/video content (UGC), together with the permissions and marketing consent declarations detailed in Section 2.13

10.2.12. Courier services (GLS, DHL, DPD, MPL, etc.)

Role: parcel delivery
Country: EU
Safeguards: data processing agreement

Data processed:

- name
- address
- telephone number
- e-mail address
- parcel tracking/identification number

10.2.13. Accountant / Tax Advisor / Accounting Partner

Role: fulfilment of statutory obligations
Country: Hungary / EU
Safeguards: data processing agreement

Data processed:

- invoice data
- accounting documents
- transaction data

10.2.14. Authorities and courts

Role: data transfers based on statutory obligations

Data processed:

- invoice data
- transaction data
- complaint-handling records
- data necessary for legal proceedings

These transfers do not require consent (GDPR Article 6(1)(c) – compliance with a legal obligation, and where justified, Article 6(1)(f) – legitimate interest, e.g. the establishment, exercise or defence of legal claims).

Other data disclosures: data is transferred only where a statutory obligation exists, including, in particular, to authorities competent at the Data Controller's registered office, such as the Hungarian Tax and Customs Administration (NAV) and the Hungarian National Authority for Data Protection and Freedom of Information (NAIH), and, where justified, to the competent authority of another Member State. Such transfers are carried out on the legal basis of Article 6(1)(c) of the GDPR or within the framework of the relevant official proceedings.

10.3. Summary of third-country data transfers and compliance safeguards

The following service providers may involve transfers of personal data outside the EU:

Service Provider	Country	Safeguard
Shopify Inc.	Canada/USA	see Section 4.3.1
Stripe Inc.	USA	see Section 4.3.2
Klaviyo Inc.	USA	see Section 4.3.3
Meta Platforms	USA	see Section 4.3.4
Google LLC	USA	see Section 4.3.5
TikTok	USA / Singapore	see Section 4.3.6
PayPal (Europe) S.à r.l. et Cie, S.C.A. / PayPal, Inc.	Luxembourg (EU) / USA	see Section 4.3.7
Cloudflare	USA	DPF (primarily); if certification ceases, SCC – see Section 10.2.8
Refersion, Inc.	USA	SCC + TIA (see Section 2.8)
Yotpo Ltd.	Israel / USA / UK / EU	adequacy decision (Israel, UK) / SCC (USA) – see Section 2.8

All transfers to third countries comply with Article 46 of the GDPR.

11. Contact Details of the Data Controller

Contact and legal remedies

Data Controller: BODYFACT Kft.
Registered office and postal address: 1029 Budapest, Csatlós utca 3. 1/3 – Hungary**:**
Customer service e-mail: hello@bodyfact.eu
Data protection matters: privacy@bodyfact.eu