BODYFACT

BODYFACT – DATENSCHUTZERKLÄRUNG

1. Einleitung, Zweck und rechtlicher Hintergrund

1.1. Zweck der Datenschutzerklärung

Zweck dieser Datenschutzerklärung (die „Datenschutzerklärung“) ist es, detailliert und transparent darzulegen, wie BodyFact (der „Dienstleister“ oder „Verantwortliche“) die personenbezogenen Daten von Nutzern, Kunden und Abonnenten im Zusammenhang mit der Nutzung von www.bodyfact.eu (und dessen Unterseiten), dem Einkauf im Onlineshop, der Inanspruchnahme abonnementbasierter Dienstleistungen sowie den mit Marketingkommunikationen verbundenen Tätigkeiten verarbeitet.

Die Datenschutzerklärung legt Folgendes fest:

- die Zwecke und Rechtsgrundlagen der Verarbeitung,
- die Kategorien der verarbeiteten Daten,
- die Aufbewahrungsfristen,
- das System der einzelnen Auftragsverarbeiter und Datenübermittlungen,
- die Garantien für internationale Datenübermittlungen,
- die Funktionsweise von Cookies und Cookie-Management-Systemen,
- die Rechte der betroffenen Personen und die Art und Weise ihrer Ausübung.

Der Verantwortliche verpflichtet sich zu einer transparenten und DSGVO-konformen Verarbeitung personenbezogener Daten und ist bestrebt, die Grundsätze „Privacy by Design“ und „Privacy by Default“ vollständig umzusetzen.

1.2. Angaben zum Verantwortlichen

Angabe	Daten
Firmenname	BODYFACT Kft.
Sitz	1029 Budapest, Csatlós utca 3. 1. em. 3. ajtó, UNGARN
Firmenregisternummer	01-09-454670
Steuernummer	33018346-2-41
Telefon	+36300707860
Datenschutzkontakt	privacy@bodyfact.eu
Kundenservice	hello@bodyfact.eu

Der Verantwortliche ist nicht verpflichtet, einen Datenschutzbeauftragten zu benennen; für die interne Kontrolle und Compliance ist jedoch ein Datenschutzverantwortlicher tätig.

1.3. Anwendbare Rechtsvorschriften

Die Verarbeitungstätigkeiten des Verantwortlichen unterliegen in erster Linie den folgenden auf EU-Ebene einheitlich anwendbaren Rechtsvorschriften:

- DSGVO — Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates
- ePrivacy-Richtlinie (2002/58/EG) und deren Umsetzung in dem für die Inanspruchnahme der Dienstleistung maßgeblichen Mitgliedstaat
- Kapitel V der DSGVO — internationale Datenübermittlungen

Soweit nach lokalem Recht anwendbar, können neben den vorgenannten Vorschriften auch die nationalen Rechtsvorschriften des Mitgliedstaats des gewöhnlichen Aufenthalts der betroffenen Person Anwendung finden, insbesondere in den Bereichen Verbraucherschutz, elektronischer Geschäftsverkehr und Direktmarketing. Für betroffene Personen in Ungarn umfasst dies insbesondere die folgenden Rechtsvorschriften:

- Ungarisches Datenschutzgesetz (Gesetz Nr. CXII von 2011 über die informationelle Selbstbestimmung und Informationsfreiheit, „Infotv.“)

- Ungarisches Gesetz über den elektronischen Geschäftsverkehr (Gesetz Nr. CVIII von 2001 über bestimmte Fragen des elektronischen Geschäftsverkehrs und der Dienste der Informationsgesellschaft, „Elektronikus kereskedelmi törvény“)
- Ungarisches Verbraucherschutzgesetz (Gesetz Nr. CLV von 1997 über den Verbraucherschutz, „Fogyasztóvédelmi törvény“)
- Gesetz Nr. C von 2003 über die elektronische Kommunikation
- Gesetz Nr. XLVIII von 2008 („Grt.“) — Vorschriften über Marketing-Einwilligungen

1.4. Persönlicher, sachlicher und räumlicher Geltungsbereich der Datenschutzerklärung

Persönlicher Geltungsbereich:

Die Datenschutzerklärung gilt für sämtliche Besucher, registrierten Nutzer, Kunden, Abonnenten des Onlineshops sowie Personen, die sich für Marketinglisten angemeldet haben (nachfolgend zusammen „betroffene Person“).

Sachlicher Geltungsbereich:

Sie gilt für sämtliche Verarbeitungstätigkeiten im Zusammenhang mit:

- Online-Käufen,
- Abonnements,
- Newslettern,
- Marketing (Werbung auf Facebook, Google, TikTok),
- Kundenservice,
- dem Affiliate-System,
- der Cookie-Verwaltung und webbasierten Tracking-Tools.

Räumlicher Geltungsbereich:

Die Datenschutzerklärung gilt für betroffene Personen, die den vom Verantwortlichen betriebenen Onlineshop aus dem Gebiet der Europäischen Union bzw. des Europäischen Wirtschaftsraums heraus nutzen, sofern die Voraussetzungen gemäß Artikel 3 DSGVO erfüllt sind, unabhängig vom Sitz des Verantwortlichen. Besondere Bestimmungen für betroffene Personen, die sich außerhalb des Gebiets der Europäischen Union/des Europäischen Wirtschaftsraums (einschließlich der Schweiz) aufhalten, sind in einem gesonderten Abschnitt dieser Datenschutzerklärung enthalten. Die Grundsätze für Datenübermittlungen in Drittländer werden in Kapitel 4 erläutert.

1.5. Verarbeitung personenbezogener Daten Minderjähriger

Voraussetzung für einen Kauf über den BodyFact-Onlineshop ist die Geschäftsfähigkeit, d. h., der Kunde muss eine volljährige natürliche Person sein, die das 18. Lebensjahr vollendet hat; dies erklärt der Kunde mit dem Abschluss der Bestellung. Die Produkte und Dienstleistungen von BodyFact werden dementsprechend ausschließlich an volljährige Personen verkauft.

Der Dienstleister führt keine technische oder dokumentenbasierte Überprüfung des Alters des Kunden durch und ist hierzu auch gesetzlich nicht verpflichtet. Besteht ein begründeter Verdacht, dass eine Bestellung von einer minderjährigen Person aufgegeben wurde, ist der Dienstleister berechtigt, die Bestellung zu stornieren, die damit verbundene Verarbeitung personenbezogener Daten zu beenden und/oder vom Kunden weitere Angaben zum Nachweis seines Alters anzufordern.

Die mit der Nutzung des Onlineshops, der Registrierung oder der Anmeldung zum Newsletter verbundenen Verarbeitungstätigkeiten beziehen sich ausschließlich auf volljährige und geschäftsfähige betroffene Personen; der Dienstleister stützt sich nicht auf eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten von Personen unter 18 Jahren und löscht solche Daten unverzüglich, sobald er von ihrer Verarbeitung Kenntnis erlangt.

1.6. Grundsätze der Datenverarbeitung

Der Verantwortliche verarbeitet personenbezogene Daten gemäß den in Artikel 5 DSGVO festgelegten Grundsätzen:

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
Jede Verarbeitungstätigkeit verfügt über eine Rechtsgrundlage, und den betroffenen Personen werden umfassende Informationen bereitgestellt.

2. Zweckbindung
Die Daten werden ausschließlich zu festgelegten Zwecken verarbeitet; bei einer Zweckänderung erfolgt die weitere Verarbeitung nur auf Grundlage einer neuen Rechtsgrundlage oder einer Einwilligung.

3. Datenminimierung
Es werden ausschließlich die erforderlichen Daten verarbeitet.

4. Richtigkeit
Der Verantwortliche stellt sicher, dass die Daten richtig sind; erforderlichenfalls können sie auf Antrag der betroffenen Person geändert werden.

5. Speicherbegrenzung
Die Daten werden nur so lange aufbewahrt, wie dies erforderlich ist.

6. Integrität und Vertraulichkeit
Geeignete technische und organisatorische Maßnahmen schützen die Daten (Verschlüsselung, Pseudonymisierung, Zugriffsprotokolle, Verwaltung von Zugriffsberechtigungen).

7. Rechenschaftspflicht
Der Verantwortliche ist dafür verantwortlich, dass die Verarbeitung in jeder Phase der DSGVO entspricht, und ist in der Lage, diese Einhaltung nachzuweisen.

1.7. Aktualisierung und Änderung der Datenschutzerklärung

Der Verantwortliche behält sich das Recht vor, die Datenschutzerklärung zu ändern, insbesondere:

- im Falle von Änderungen der Rechtsvorschriften,
- bei Einführung eines neuen Verarbeitungszwecks,
- bei Beauftragung eines neuen Dienstleisters.

Änderungen treten am Tag ihrer Veröffentlichung im Onlineshop in Kraft.

Bei wesentlichen Änderungen informiert der Verantwortliche die betroffenen Personen zusätzlich per E-Mail.

Führt eine Änderung für bereits zuvor erhobene personenbezogene Daten einen neuen Verarbeitungszweck ein und ist für den neuen Zweck die Einwilligung der betroffenen Person als Rechtsgrundlage erforderlich, wendet der Verantwortliche die Änderung auf die bereits vorhandenen Daten erst an, nachdem die betroffene Person ihre Einwilligung für den neuen Zweck erteilt hat oder — im Falle eines neuen Zwecks, der auf einem berechtigten Interesse beruht — nachdem der betroffenen Person die Möglichkeit zur Ausübung ihres Rechts auf Widerspruch eingeräumt wurde.

1.8. Datensicherheit und Risikomanagement

Der Verantwortliche wendet bei den Verarbeitungstätigkeiten insbesondere die folgenden Sicherheitsmaßnahmen an:

- HTTPS-Verschlüsselung,
- serverseitige Verschlüsselung (AES-256),
- Algorithmen zum Hashing von Passwörtern (bcrypt),

- Protokollierung von Zugriffen,
- Zugriffsberechtigungsstufen,
- regelmäßige Sicherheitsprüfungen,
- als organisatorische Maßnahme eine schriftliche Vertraulichkeitsverpflichtung für Mitarbeiter, die Zugang zu personenbezogenen Daten haben, sowie das „Need-to-know"-Prinzip (Zugriff ausschließlich in dem Umfang, der für die Erfüllung der jeweiligen beruflichen Aufgaben erforderlich ist),
- die integrierten Sicherheits- und Betrugspräventionssysteme von Shopify und Stripe sowie — sofern der Kunde diese Zahlungsart wählt — von PayPal.

BodyFact verfügt über ein „Data-Breach-Protokoll", das sicherstellt, dass im Falle einer Verletzung des Schutzes personenbezogener Daten die gemäß den Artikeln 33–34 DSGVO erforderlichen Maßnahmen ergriffen werden.

Wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat, informiert der Verantwortliche die betroffenen Personen gemäß Artikel 34 DSGVO auch unmittelbar.

2. Zwecke der Datenverarbeitung, Rechtsgrundlagen, Kategorien der verarbeiteten Daten und Aufbewahrungsfristen

Dieses Kapitel stellt die einzelnen Verarbeitungstätigkeiten getrennt nach Zweck und mit dem gemäß den Artikeln 13 und 14 DSGVO erforderlichen Detaillierungsgrad dar. Die Aufzählung umfasst sämtliche Verarbeitungstätigkeiten, die im Zusammenhang mit dem Onlineshop, der Marke BodyFact, den Kaufvorgängen, Abonnements und Marketingaktivitäten anfallen.

Ein Teil der Verarbeitungstätigkeiten beruht auf der **Vertragserfüllung** (Artikel 6 Absatz 1 Buchstabe b DSGVO), ein weiterer Teil auf einer **Rechtlichen Verpflichtung** (Buchstabe c), einem **Berechtigten Interesse** (Buchstabe f) oder einer ausdrücklichen **Einwilligung** (Buchstabe a).

2.1. Nutzung des Onlineshops (Aufrufen der Website)

Zweck:

Sicherstellung des technischen Betriebs des Onlineshops und einer fehlerfreien Erbringung der Dienstleistung.

Verarbeitete Daten:

- IP-Adresse
- Gerätetyp, Betriebssystem
- Browsertyp
- Zeitstempel
- Daten zu Seitenaufrufen
- notwendige Cookies (Session-ID)

Rechtsgrundlage:

Berechtigtes Interesse des Verantwortlichen – Artikel 6 Absatz 1 Buchstabe f DSGVO (Bereitstellung von Onlinediensten, Informationssicherheit)

Aufbewahrung:

Der Onlineshop kann für seinen Betrieb erforderliche Cookies (Sitzungskennungen) verwenden. Die genaue Bezeichnung, der Zweck und die Aufbewahrungsfrist der einzelnen Cookies sind in der auf der Website verfügbaren Cookie-Datenschutzerklärung (Cookie-Liste) angegeben.
Server-Logs: 30 Tage

2.2. Kauf / Aufgabe einer Bestellung (mit und ohne Registrierung)

Zweck: Abwicklung des Kaufvorgangs, Abschluss und Erfüllung des Vertrags.

Verarbeitete Daten:

- Name
- E-Mail-Adresse
- Rechnungsadresse
- Lieferadresse
- Telefonnummer
- Bestelldaten (Bestellnummer, Produkte, Preis)
- gewählte Zahlungsart
- Transaktionskennung des gewählten Zahlungsdienstleisters (Stripe bzw. — sofern der Kunde diese Zahlungsart wählt — PayPal); der Dienstleister speichert keine Zahlungsdaten (z. B. Bankkarten- oder PayPal-Kontodaten) und hat keinen Zugriff darauf; diese Daten werden ausschließlich vom jeweiligen Zahlungsdienstleister verarbeitet

Rechtsgrundlage:

Vertragserfüllung – Artikel 6 Absatz 1 Buchstabe b DSGVO

Der Kunde ist verpflichtet, die für die Bestellung erforderlichen Daten (Rechnungsdaten) anzugeben; bei Nichtbereitstellung dieser Daten kann der Dienstleister keine Rechnung ausstellen.

Aufbewahrung:

Rechnungsdaten: 8 Jahre (ungarisches Rechnungslegungsrecht)
Metadaten der Bestellungen: 5 Jahre (Verjährungsfrist nach dem ungarischen Bürgerlichen Gesetzbuch)
Lieferdaten: Erfüllung des Vertrags + 1 Jahr

Soweit die Verarbeitung zur Geltendmachung, Durchsetzung oder Verteidigung von Rechtsansprüchen erforderlich ist, erfolgt die Verarbeitung bis zum endgültigen Abschluss des Verfahrens, längstens jedoch bis zum Ablauf der Verjährungsfrist des jeweiligen Anspruchs.

2.3. Rechnungsstellung und Einhaltung der rechnungslegungsrechtlichen Vorschriften

Zweck:

Ausstellung und Aufbewahrung von Rechnungen aufgrund gesetzlicher Verpflichtungen.

Verarbeitete Daten:

- Name
- Rechnungsadresse
- Bestelldaten
- Zahlungsinformationen (keine Bankkartendaten!)

Rechtsgrundlage:

Rechtliche Verpflichtung – Artikel 6 Absatz 1 Buchstabe c DSGVO,
Ungarisches Rechnungslegungsgesetz (Gesetz Nr. C von 2000 über die Rechnungslegung, „Számviteli törvény“), § 169

Die Ausstellung einer Rechnung ist eine zwingende gesetzliche Anforderung (gemäß § 169 des ungarischen Rechnungslegungsgesetzes); daher kann der Vertrag ohne Bereitstellung der Rechnungsdaten nicht erfüllt werden.

Aufbewahrung:

8 Jahre

2.4. Abonnementbasierte Dienstleistung (Subscription)

Zweck:

Verwaltung des Abonnements, Sicherstellung wiederkehrender Zahlungen und Versand von Benachrichtigungen.

Verarbeitete Daten:

- Name
- E-Mail-Adresse
- Art des Abonnements (monatlich / vierteljährlich)
- Stripe Subscription ID
- Bestellhistorie
- Statusänderungen (Pausierung, Änderung, Kündigung)

Rechtsgrundlage:

Vertragserfüllung – Artikel 6 Absatz 1 Buchstabe b DSGVO

Aufbewahrung:

2 Jahre nach Beendigung des Abonnements

Soweit die Verarbeitung zur Geltendmachung, Durchsetzung oder Verteidigung von Rechtsansprüchen erforderlich ist, erfolgt die Verarbeitung bis zum endgültigen Abschluss des Verfahrens, längstens jedoch bis zum Ablauf der Verjährungsfrist des jeweiligen Anspruchs.

2.5. Anmeldung zum Newsletter und Versand von Marketing-E-Mails

Zweck:

Marketingkommunikation sowie Versand von Angeboten und Aktionen an die betroffene Person.

Verarbeitete Daten:

- Name (optional)

- E-Mail-Adresse
- Zeitpunkt der Anmeldung
- technische Logs, die zum Nachweis der Anmeldung erforderlich sind
- Marketingpräferenzen
- Interaktionen im Zusammenhang mit Kampagnen (Öffnungen, Klicks) – pseudonymisiert

Rechtsgrundlage:

Ausdrückliche Einwilligung — Artikel 6 Absatz 1 Buchstabe a DSGVO.

Die Einzelheiten zur Einholung der Einwilligung und zu Direktmarketingmaßnahmen richten sich nach dem Recht des Mitgliedstaats des gewöhnlichen Aufenthalts der betroffenen Person (siehe Abschnitt 1.3); für betroffene Personen in Ungarn gilt dies insbesondere für § 6 des Ungarischen Werbegesetzes (Gesetz Nr. XLVIII von 2008 über die grundlegenden Anforderungen und bestimmte Beschränkungen wirtschaftlicher Werbetätigkeiten, „Grt.“).

Aufbewahrung:

Die zum Zweck des Newsletterversands verarbeiteten Daten (Name, E-Mail-Adresse) werden bis zum Widerruf der Einwilligung (Abmeldung bzw. Löschungs- oder Widerspruchsersuchen der betroffenen Person) verarbeitet.

Daten, die die Tatsache und den Zeitpunkt der Erteilung der Einwilligung nachweisen, werden im Hinblick auf die Geltendmachung und Verteidigung zivilrechtlicher Ansprüche 5 Jahre ab dem Widerruf der Einwilligung aufbewahrt.

2.6. Marketing- und Remarketing-Systeme (Meta, Google, TikTok)

Zweck:

Anzeige personalisierter Werbung auf externen Plattformen.

Verarbeitete Daten:

- E-Mail-Adresse (in gehashter Form zur Erstellung von Custom Audiences)
- IP-Adresse
- Cookie-Kennungen
- Gerätekennung

- von Pixeln erhobene Ereignisdaten (z. B. „Add to cart“, „Purchase“) — pseudonymisiert

Rechtsgrundlage:

Das Setzen und Auslesen von Cookies und Gerätekennungen erfolgt auf Grundlage der vorherigen Einwilligung der betroffenen Person gemäß den anwendbaren Vorschriften des jeweiligen Mitgliedstaats über elektronische Kommunikation/ePrivacy (siehe Abschnitt 1.3; für betroffene Personen in Ungarn insbesondere § 155 des Ungarischen Gesetzes über elektronische Kommunikation (Gesetz Nr. C von 2003 über die elektronische Kommunikation, „Eht.“)). Die anschließende Verarbeitung personenbezogener Daten — einschließlich der gehashten E-Mail-Adresse und der durch Pixel erhobenen Ereignisdaten — erfolgt auf Grundlage der ausdrücklichen Einwilligung der betroffenen Person gemäß Artikel 6 Absatz 1 Buchstabe a DSGVO.

Aufbewahrung:

Bis zum Ablauf der Cookies (in der Regel 90–180 Tage) oder bis zum Widerruf der Einwilligung.

Besonderer Hinweis:

Die Daten werden von Meta / Google in der Regel auf **Servern außerhalb der EU** verarbeitet → siehe Kapitel 6: Internationale Datenübermittlungen + SCC.

Im Hinblick auf bestimmte Tools von Meta und Google (z. B. Custom Audience, Customer Match) kann in einzelnen Phasen der Verarbeitung eine gemeinsame Verantwortlichkeit (Artikel 26 DSGVO) bestehen — siehe Kapitel 3.

2.7. Treuepunktesystem (Loyalty Program)

Zweck:

Gutschrift und Einlösung von Punkten sowie Verwaltung der Punkthistorie.

Verarbeitete Daten:

- E-Mail-Adresse
- Punkthistorie
- Kaufhistorie

Rechtsgrundlage:

Vertragserfüllung — Artikel 6 Absatz 1 Buchstabe b DSGVO. Die Registrierung für das Treuepunktesystem ist ein vom Kauf getrennter, freiwilliger Schritt, dem die betroffene

Person durch die ausdrückliche Zustimmung zu den Programmbedingungen beitritt; diese gesonderte Zustimmung bildet die Rechtsgrundlage.

Aufbewahrung:

Bis zur Löschung des Kontos

2.8. Affiliate-Programm (Refersion / Yotpo / andere)

Zweck:

Verwaltung der Provisionen von Influencern und Partnern sowie Kampagnen-Tracking.

Verarbeitete Daten:

- Name
- E-Mail-Adresse
- Affiliate-ID
- Provisionsdaten
- Anzahl der generierten Verkäufe
- Zahlungsdaten (Bankkontonummer oder PayPal — sofern vom Partner angegeben)

Rechtsgrundlage:

Vertragserfüllung – Artikel 6 Absatz 1 Buchstabe b DSGVO

Aufbewahrung:

5 Jahre nach Beendigung des Vertrags (Verjährungsfrist nach dem ungarischen Bürgerlichen Gesetzbuch)

Besonderer Hinweis:

Die für die Verarbeitung von Affiliate-Daten eingesetzten Dienstleister können personenbezogene Daten in mehreren Ländern verarbeiten:

- Im Falle von **Refersion** (Vereinigte Staaten) erfolgt die Datenübermittlung auf Grundlage der Standardvertragsklauseln (SCC) gemäß dem Beschluss (EU) 2021/914 der Kommission.
- Im Falle von **Yotpo** (primär Israel sowie die Vereinigten Staaten, das Vereinigte Königreich und die Europäische Union) erfolgt die Datenübermittlung nach Israel auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission für Israel, wonach Israel im Sinne der DSGVO als Drittland mit einem

angemessenen Schutzniveau gilt, ohne zusätzliche Garantien (SCC); die Datenübermittlung in das Vereinigte Königreich erfolgt auf Grundlage des Angemessenheitsbeschlusses EU–UK, ebenfalls mittels eines Angemessenheitsbeschlusses; für Datenübermittlungen in die Vereinigten Staaten verwendet der Dienstleister die Standardvertragsklauseln gemäß dem Beschluss (EU) 2021/914 der Kommission.

Weitere Informationen siehe Kapitel 6: Internationale Datenübermittlungen.

2.9. Kundenservice, Gewährleistungs-, Garantie- und Verbraucherschutzbeschwerden

Zweck:

Bearbeitung, Prüfung, Dokumentation und Erfüllung von Kundenserviceanfragen, Verbraucherbeschwerden sowie Gewährleistungs- und Garantieansprüchen.

Auf Grundlage der auf den Warenverkauf anwendbaren unionsrechtlichen Verbraucherschutzvorschriften (Richtlinie (EU) 2019/771 und deren Umsetzung in den Mitgliedstaaten) stehen dem Kunden Rechte hinsichtlich der Vertragsgemäßheit der Waren zu, einschließlich gesetzlicher Gewährleistungsrechte und — **Soweit nach lokalem Recht anwendbar** — Produktgewährleistungsrechte. Das Bestehen und der Umfang einer zwingenden bzw. freiwilligen Garantie sowie die Verfahrensregeln für die Bearbeitung von Gewährleistungs- und Garantieansprüchen richten sich nach dem auf die betroffene Person anwendbaren nationalen Recht.

Soweit nach lokalem Recht anwendbar, gilt für Kunden in Ungarn insbesondere Folgendes: Für die von BODYFACT vertriebenen Nahrungsergänzungsmittel besteht keine gesetzlich vorgeschriebene Garantiepflicht (die Produktgruppen, die der zwingenden Garantiepflicht unterliegen, werden in Anlage 1 zur Verordnung 10/2024 (VI. 28.) des Justizministers („10/2024. (VI. 28.) IM rendelet“) bestimmt); für bestimmte nicht als Lebensmittel einzustufende Zusatzprodukte von BODYFACT, insbesondere Shaker, übernimmt BODYFACT gemäß § 6:171 des Ungarischen Bürgerlichen Gesetzbuches (Gesetz Nr. V von 2013 über das Bürgerliche Gesetzbuch, „Ptk.“) eine freiwillige Garantie, deren Dauer und Bedingungen sowie die sich daraus ergebenden Rechte im der Ware beigefügten Garantieschein bzw. in den auf der Website veröffentlichten Garantieinformationen festgelegt sind; bei der Bearbeitung von Gewährleistungs- und Garantieansprüchen handelt der Dienstleister gemäß den Bestimmungen der Verordnung 19/2014 (IV. 29.) des Ministers für nationale Wirtschaft („19/2014. (IV. 29.) NGM rendelet“).

Über einen vom Kunden gemeldeten Gewährleistungs- oder Garantieanspruch nimmt der Dienstleister ein Protokoll auf, das insbesondere den Namen und die Kontaktdaten

des Kunden, den Gegenstand und die Gegenleistung des Vertrags, den Zeitpunkt der Erfüllung, die Beschreibung des gemeldeten Mangels, den vom Kunden geltend gemachten Anspruch sowie die Art der Erledigung des Anspruchs oder die Gründe für dessen Ablehnung enthalten kann.

Übernimmt der Dienstleister das Produkt zur Untersuchung, stellt er darüber eine Empfangsbestätigung aus, die die zur Identifizierung des Kunden erforderlichen Daten, die zur Identifizierung des Produkts erforderlichen Daten, den Zeitpunkt der Übernahme sowie den voraussichtlichen Zeitpunkt der Rückgabe des Produkts enthalten kann.

Verarbeitete Daten:

- Name
- E-Mail-Adresse
- Telefonnummer (sofern angegeben)
- Postanschrift oder Lieferadresse (sofern für die Bearbeitung erforderlich)
- Bestellnummer
- Angaben zum gekauften Produkt
- Zeitpunkt des Kaufs und der Erfüllung
- Inhalt der Beschwerde, des Gewährleistungs- oder Garantieanspruchs
- Beschreibung des gemeldeten Mangels
- zugehörige Dokumente und Nachweise (z. B. Rechnung, Foto, Protokoll, Korrespondenz)
- Daten der Kundenservice-Kommunikation
- Ticket- und Bearbeitungsdaten

Rechtsgrundlage:

- Artikel 6 Absatz 1 Buchstabe b DSGVO – Vertragserfüllung bzw. Ergreifen von Maßnahmen im Zusammenhang mit der Vertragserfüllung
- Artikel 6 Absatz 1 Buchstabe c DSGVO – Erfüllung einer für den Verantwortlichen geltenden Rechtlichen Verpflichtung, insbesondere verbraucherschutzrechtlicher, gewährleistungs- und garantierechtlicher Verpflichtungen

Art der Datenbereitstellung:

Die Bereitstellung personenbezogener Daten ist teilweise zur Erfüllung gesetzlicher Verpflichtungen und teilweise zur Prüfung und Bearbeitung einer Beschwerde, eines

Gewährleistungs- oder Garantieanspruchs erforderlich. Bei Fehlen der erforderlichen Daten kann die Prüfung oder Erfüllung des Anspruchs teilweise oder vollständig unmöglich werden.

Aufbewahrung:

Das über die Beschwerde aufgenommene Protokoll, die schriftliche Beschwerde und die darauf erteilte inhaltliche Antwort sind vom Dienstleister für den Zeitraum aufzubewahren, der durch die auf die betroffene Person anwendbaren nationalen verbraucherschutzrechtlichen Vorschriften vorgeschrieben ist, und auf Aufforderung der zuständigen Aufsichtsbehörde vorzulegen. **Soweit nach lokalem Recht anwendbar**, beträgt dieser Zeitraum für Kunden in Ungarn gemäß § 17/A Absatz 7 des Ungarischen Verbraucherschutzgesetzes (Gesetz Nr. CLV von 1997 über den Verbraucherschutz, „Fgytv.“) 3 Jahre ab dem Tag der Ablehnung der Beschwerde bzw. ab dem Tag der Übermittlung der inhaltlichen Antwort.

Andere Dokumente und personenbezogene Daten im Zusammenhang mit der Beschwerdebearbeitung und Kundenserviceabwicklung sowie Gewährleistungs- und Garantieansprüchen (insbesondere Korrespondenz, Anhänge und sonstige Nachweise) bewahrt der Dienstleister ab Abschluss der Beschwerde bzw. der endgültigen Erledigung des Anspruchs 5 Jahre auf.

Sofern ein Gesetz eine längere oder kürzere zwingende Aufbewahrungsfrist vorschreibt, handelt der Dienstleister gemäß den Bestimmungen des jeweiligen Gesetzes.

Soweit die Verarbeitung zur Geltendmachung, Durchsetzung oder Verteidigung von Rechtsansprüchen erforderlich ist, erfolgt die Verarbeitung bis zum endgültigen Abschluss des Verfahrens, längstens jedoch bis zum Ablauf der Verjährungsfrist des jeweiligen Anspruchs.

2.10. Qualitätsbeanstandung + Lebensmittelrückruf

Zweck:

Prüfung der Produktsicherheit und Führung gesetzlich vorgeschriebener Lebensmittelsicherheitsaufzeichnungen.

Verarbeitete Daten:

- Name
- Kontaktdaten
- Bestelldaten
- Chargennummer

- für die Untersuchung angeforderte Fotos
- qualitätsbezogene Notizen

Rechtsgrundlage:

Rechtliche Verpflichtung (Lebensmittelsicherheitsvorschriften) – Artikel 6 Absatz 1 Buchstabe c DSGVO

Aufbewahrung:

5 Jahre
(auf Grundlage der Rückverfolgbarkeitsanforderungen des RASFF-Systems und der einschlägigen unionsrechtlichen lebensmittelrechtlichen Vorschriften)

2.11. Dokumentation und Widerruf der Einwilligung (Consent-Log)

Der Dienstleister erfasst die Tatsache und den Inhalt einer für die Verarbeitung personenbezogener Daten erteilten Einwilligung in einem elektronischen Register (dem „Consent-Log“). Das Register enthält den Zeitpunkt der Einwilligung, den Gegenstand der Einwilligung (z. B. Newsletter, Remarketing-Cookie) sowie die Quelle der Einwilligung (Website, Pop-up-Fenster, Formular). Zweck der Dokumentation der Einwilligung ist der Nachweis der gesetzlichen Compliance und die Gewährleistung der Ausübung der Rechte der betroffenen Person.

Die betroffene Person kann ihre Einwilligung jederzeit, ohne Angabe von Gründen und unentgeltlich auf folgende Weise widerrufen:

- über die Cookie-Verwaltungsoberfläche der Website,
- per E-Mail an privacy@bodyfact.eu,
- über den in Newslettern enthaltenen Abmeldelink.

Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung.

Auf Antrag der betroffenen Person erteilt der Dienstleister innerhalb von 30 Tagen Auskunft darüber, wann, auf welche Weise und zu welchem Zweck die Einwilligung erteilt wurde, und übersendet auf Antrag eine beglaubigte Kopie der relevanten Bestandteile des Einwilligungsregisters.

Die konkrete Aufbewahrungsfrist des Einwilligungsregisters wird je nach Art des Verarbeitungszwecks durch den jeweiligen Abschnitt festgelegt (bei Newsletter- und Marketingeinwilligungen gemäß Abschnitt 2.5, bei Cookie-Einwilligungen gemäß Abschnitt 6.2).

2.12. Cookie-Verwaltung und Cookie-Kennungen

Zweck:

Sicherstellung des Betriebs des Onlineshops, Analyse, Marketing und Verwaltung von Nutzerpräferenzen.

Die detaillierten Kategorien der Cookies sind in Abschnitt 5.2 (Kategorien der Cookies) aufgeführt.

Verarbeitete Daten:

- IP-Adresse
- Cookie-Kennung
- Gerätedaten
- Browsing-Ereignisse
- Ereignisprotokolle von Marketing-Pixeln

Rechtsgrundlage:

- notwendige Cookies: Berechtigtes Interesse des Verantwortlichen
- Analyse-/Marketing-Cookies: Einwilligung

Aufbewahrung:

Die genauen Aufbewahrungsfristen der einzelnen Cookie-Kategorien (notwendig, Präferenzen, Analyse, Marketing) sind in der auf der Website verfügbaren Cookie-Datenschutzerklärung (Cookie-Liste) angegeben, die über die CookieBot Consent-Management-Plattform fortlaufend auf dem aktuellen Stand gehalten wird.

2.13. Kundenbewertungen und Anfragen zur Kundenzufriedenheit

Zweck:

Nach Abschluss der Erfüllung einer Bestellung die Aufforderung an den Kunden, mittels einer automatisierten elektronischen Nachricht eine Bewertung abzugeben (Ziffer 15.3.1 der AGB), sowie die Verarbeitung personenbezogener Daten im Zusammenhang mit vom Kunden veröffentlichten Kundenbewertungen und nutzergenerierten Inhalten (UGC).

Verarbeitete Daten:

- Name (bei Veröffentlichung der Bewertung nach Wahl des Kunden vollständiger Name oder Initialen/Spitzname)
- E-Mail-Adresse
- Bestell-/Kaufkennung
- Text und Bewertungspunktzahl der abgegebenen Bewertung
- Zeitpunkt des Versands der Bewertungsaufforderung
- bei einer mit einem Anreiz verbundenen Anfrage: Tatsache, Zeitpunkt und Art der Erteilung der Einwilligung

Rechtsgrundlage:

Soweit die Bewertungsaufforderung ausschließlich zum Zweck einer Kundenzufriedenheitsbefragung oder zur Bitte um Abgabe einer Kundenbewertung versendet wird, keine werblichen Elemente enthält und nach dem einschlägigen nationalen Recht (siehe Abschnitt 1.3; für betroffene Personen in Ungarn insbesondere nach dem Grt.) nicht als Wirtschaftswerbung gilt, ist die Rechtsgrundlage für die Verarbeitung im Zusammenhang mit der Bewertungsaufforderung das Berechtigte Interesse des Dienstleisters (Artikel 6 Absatz 1 Buchstabe f DSGVO; Ziffer 15.3.1 der AGB).

Enthält die Bewertungsaufforderung zusätzlich einen in Abschnitt 2.13 dieser Datenschutzerklärung und Ziffer 15.7 der AGB genannten Anreiz (insbesondere einen Gutschein, Treuepunkte oder Rabatt), kann sie nach dem einschlägigen nationalen Recht (in Ungarn im Anwendungsbereich des Grt.) als Wirtschaftswerbung gelten. In diesem Fall darf die Nachricht ausschließlich auf Grundlage der vorherigen, freiwilligen, konkreten, auf angemessener Information beruhenden, ausdrücklichen und eindeutigen Einwilligung der betroffenen Person versendet werden (Artikel 6 Absatz 1 Buchstabe a DSGVO; für betroffene Personen in Ungarn § 6 Grt.; Ziffer 15.7.4 der AGB).

Auch bei einer auf Grundlage eines Berechtigten Interesses und ausschließlich zu Zwecken der Kundenzufriedenheit versendeten Anfrage wird der betroffenen Person die Möglichkeit zur Abmeldung bzw. zur Ausübung des Widerspruchsrechts gemäß Artikel 21 DSGVO eingeräumt; nach der Abmeldung versendet der Dienstleister keine weiteren Nachrichten dieser Art an den Kunden. Bei Bewertungsaufforderungen mit einem Anreiz, die auf einer Einwilligung beruhen, erfolgt die Erteilung und der jederzeitige, unentgeltliche Widerruf der Einwilligung (Abmeldung) auf dieselbe Weise wie die in Abschnitt 2.5 dieser Datenschutzerklärung beschriebene Newsletter-An- und Abmeldung.

Aufbewahrung:

Der Dienstleister bewahrt personenbezogene Daten im Zusammenhang mit Kundenbewertungen sowie Protokolldaten zum Nachweis von Einwilligungen ausschließlich so lange auf, wie dies erforderlich ist, unter Berücksichtigung des Zwecks der Verarbeitung, der einschlägigen gesetzlichen Verpflichtungen, der Notwendigkeit der Beilegung etwaiger Rechtsstreitigkeiten sowie der verbraucherschutz- und rechnungslegungsrechtlichen Vorschriften.

Die gesetzlich zwingend vorgeschriebenen konkreten Aufbewahrungsfristen sind in Abschnitt 2.14 (Gesetzlich vorgeschriebene Datenaufbewahrung) zusammengefasst.

Inhalte-Upload gegen Treuepunkte (Foto/Video):

Im Zusammenhang mit dem Treuepunktesystem erhält der Kunde die Möglichkeit, ein Foto oder Video des gekauften Produkts hochzuladen, wofür der Dienstleister Treuepunkte gutschreibt. Für die Nutzung der hochgeladenen Inhalte durch BODYFACT zu Marketingzwecken ist die ausdrückliche Einwilligung des Kunden erforderlich.

Verarbeitete Daten: das hochgeladene Foto oder Video; die Erklärung des Kunden über seine Berechtigung zum Hochladen des Inhalts; die Einwilligung des Kunden zur Nutzung zu Marketingzwecken; die Tatsache, der Zeitpunkt und die Art der Abgabe beider Erklärungen.

Rechtsgrundlage: ausdrückliche Einwilligung der betroffenen Person — Artikel 6 Absatz 1 Buchstabe a DSGVO. Der Schutz des Bildnisses bzw. Porträts Dritter, die gegebenenfalls auf dem hochgeladenen Inhalt erscheinen, unterliegt dem jeweils anwendbaren nationalen Recht (insbesondere den Vorschriften über Persönlichkeitsrechte am eigenen Bild); für dessen Einhaltung ist der hochladende Kunde durch die Annahme der folgenden zwei voneinander getrennten Erklärungen verantwortlich:

„☐ Ich bestätige, dass ich berechtigt bin, den hochgeladenen Inhalt zu teilen — es handelt sich um meinen eigenen Inhalt oder, sofern eine andere Person betroffen ist, wurde dieser mit deren Kenntnis und Einwilligung erstellt/geteilt. Sollte ein Dritter Einwände gegen die Nutzung erheben, kann BODYFACT den Inhalt unabhängig vom gemeldeten Problem nach eigenem Ermessen entfernen."

„☐ Ich willige ein, dass BODYFACT den hochgeladenen Inhalt zu Marketingzwecken wie folgt verwendet. [Weitere Informationen: Wie wir die hochgeladenen Inhalte verwenden]"

Die über den Link „Weitere Informationen" verfügbare ausführliche Information enthält den genauen Umfang der Nutzung (Onlineshop und Website, organische Social-Media-Plattformen, bezahlte Online-Werbung), die Berechtigung zur Bearbeitung des Inhalts sowie die Art und Weise des Widerrufs der Einwilligung.

Widerspricht eine vom Inhalt betroffene dritte Person — sei es der hochladende Kunde oder eine andere vom Inhalt betroffene Person — der Nutzung, entfernt der Dienstleister den Inhalt unverzüglich, spätestens jedoch innerhalb von **10 Werktagen** nach Eingang des Widerspruchs.

Aufbewahrung: bis zum Widerruf der Einwilligung bzw. — sofern kein Widerruf erfolgt — solange der Zweck der Nutzung zu Marketingzwecken besteht, längstens jedoch **3 Jahre**.

Rechte der betroffenen Person und Einschränkungen des Löschungsrechts:

Dem Kunden stehen insbesondere folgende Rechte zu: das Recht auf Auskunft, das Recht auf Berichtigung, das Recht auf Löschung, das Recht auf Einschränkung der Verarbeitung, das Recht auf Widerspruch gegen die Verarbeitung sowie das Recht auf Beschwerde.

Der Kunde ist berechtigt, seine Einwilligung jederzeit unentgeltlich zu widerrufen (sich abzumelden); der Widerruf berührt nicht die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung.

Der Kunde kann die Berichtigung, Einschränkung der Verarbeitung oder Löschung seiner personenbezogenen Daten im Zusammenhang mit einer von ihm veröffentlichten Bewertung verlangen. Der Dienstleister kann die Erfüllung eines Löschungsersuchens ganz oder teilweise verweigern, soweit die Verarbeitung personenbezogener Daten weiterhin zur Erfüllung einer Rechtlichen Verpflichtung, zur Geltendmachung, Durchsetzung oder Verteidigung von Rechtsansprüchen oder zu einem anderen gesetzlich bestimmten Zweck erforderlich ist.

Im Falle des Widerrufs der Einwilligung oder der Erfüllung eines Antrags auf Löschung der Bewertung beendet der Dienstleister für die Zukunft die öffentliche Anzeige der betreffenden Bewertung; er ist jedoch berechtigt, diejenigen Daten und Protokolldateien aufzubewahren, die zum Nachweis der Erteilung der Einwilligung, des Zustandekommens der Transaktion sowie der Rechtmäßigkeit der Verarbeitung erforderlich sind.

2.14. Gesetzlich vorgeschriebene bzw. auf einem Berechtigten Interesse beruhende Aufbewahrungsfristen

Aufgrund gesetzlicher Verpflichtungen des Dienstleisters bzw. — aufgrund seines Berechtigten Interesses an der Geltendmachung, Durchsetzung und Verteidigung von Rechtsansprüchen — gelten insbesondere folgende Aufbewahrungsfristen:

- Rechnungsdaten: 8 Jahre (Rechtliche Verpflichtung — ungarisches Rechnungslegungsrecht; siehe Abschnitt 2.3)

- Vertrags-/Bestelldaten: höchstens 5 Jahre, aufgrund eines Berechtigten Interesses unter Berücksichtigung der Verjährungsfrist nach dem auf die betroffene Person anwendbaren nationalen Recht (siehe Abschnitt 1.3); für betroffene Personen in Ungarn gilt die fünfjährige Verjährungsfrist gemäß § 6:22 des Ungarischen Bürgerlichen Gesetzbuches (Gesetz Nr. V von 2013 über das Bürgerliche Gesetzbuch, „Ptk.“) (siehe Abschnitt 2.2)
- Beschwerdeprotokoll, schriftliche Beschwerde und darauf erteilte inhaltliche Antwort: **Soweit nach lokalem Recht anwendbar**, für Kunden in Ungarn 3 Jahre (§ 17/A Absatz 7 des Ungarischen Verbraucherschutzgesetzes (Gesetz Nr. CLV von 1997 über den Verbraucherschutz, „Fgytv.“))
- sonstige Dokumentation zur Beschwerdebearbeitung und zum Kundenservice: 5 Jahre (siehe Abschnitt 2.9)
- lebensmittelsicherheitsbezogene Dokumentation: 5 Jahre (siehe Abschnitt 2.10)

Diese Aufzählung fasst die Aufbewahrungsfristen der oben ausführlich dargestellten Verarbeitungszwecke zusammen; im Falle einer Abweichung sind die detaillierten Regelungen des jeweiligen Abschnitts (2.2, 2.3, 2.9, 2.10) maßgeblich.

2.15. Zugriff auf Daten

Zugriff auf die Daten haben ausschließlich Mitarbeiter, die:

- Vertriebsaufgaben,
- Kundenserviceaufgaben,
- Marketingaufgaben,
- IT-Entwicklungsaufgaben

wahrnehmen und hierfür entsprechend berechtigt wurden.

3. Auftragsverarbeiter, gemeinsam Verantwortliche und Datenübermittlungen

Dieses Kapitel legt den Umfang aller Auftragsverarbeiter und Dienstleister fest, die im Rahmen der Tätigkeiten von BodyFact Zugriff auf personenbezogene Daten haben — unabhängig davon, ob sie als Auftragsverarbeiter oder als eigenständig Verantwortliche tätig werden.

Der Dienstleister nimmt ausschließlich solche Dienstleister in Anspruch, die die in der DSGVO festgelegten Anforderungen an Datensicherheit und Rechenschaftspflicht

erfüllen und mit denen entsprechende Vereinbarungen (Auftragsverarbeitungsverträge – AVV) bestehen.

3.1. Vom Verantwortlichen angewandte Sicherheitsmaßnahmen bei Datenübermittlungen

Der Verantwortliche bemüht sich, bei jeder Datenübermittlung die gemäß Artikel 32 der DSGVO erforderlichen Maßnahmen sicherzustellen:

- verschlüsselte Datenübertragungskanäle (HTTPS, TLS 1.2+)
- serverseitige Verschlüsselung
- Beschränkung des API-Zugriffs
- Protokollierung interner Zugriffe
- Zwei-Faktor-Authentifizierung
- Pseudonymisierung (insbesondere bei Marketing-Pixeln)

3.2. Fälle gemeinsamer Verantwortlichkeit (Artikel 26 DSGVO)

Bei bestimmten Marketinginstrumenten gelten der Dienstleister und die Plattform als gemeinsam Verantwortliche.

Hierzu gehören insbesondere:

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

Der Umfang der gemeinsamen Verantwortlichkeit wird durch die von den Plattformen bereitgestellten „Controller Addendum“-Vereinbarungen bestimmt.

Das Wesen der gemeinsamen Verantwortlichkeit ist wie folgt: Der Dienstleister ist dafür verantwortlich, dass er über eine rechtmäßige Rechtsgrundlage (die Einwilligung der betroffenen Person) für die Aktivierung der Custom-Audience- / Customer-Match-Funktion verfügt und die Daten gemäß den Vorgaben der Plattform (in der Regel in verschlüsselter, gehashter Form) an die Plattform übermittelt. Die jeweilige Plattform (Meta bzw. Google) ist für den Empfang, den Abgleich (Matching) und die Verwendung der Daten zu Werbezwecken in dem Umfang verantwortlich, der in ihrer eigenen Datenschutzerklärung und im Controller Addendum festgelegt ist. Der vollständige Text der Vereinbarung über die gemeinsame Verantwortlichkeit ist in der einschlägigen rechtlichen Dokumentation der jeweiligen Plattform verfügbar.

Die betroffene Person kann die in dieser Datenschutzerklärung festgelegten Rechte in erster Linie gegenüber dem Dienstleister ausüben; gemäß Artikel 26 Absatz 3 der DSGVO ist sie jedoch auch berechtigt, diese Rechte unmittelbar gegenüber Meta bzw. Google geltend zu machen.

3.3. Überprüfung der Auftragsverarbeiter

Der Verantwortliche überprüft die Auftragsverarbeiter jährlich:

- Compliance (DSGVO, Standardvertragsklauseln (SCC), Datenschutzprüfung)
- Aktualität der Auftragsverarbeitungsverträge
- Prüfung der Datensicherheitsmaßnahmen

4. Internationale Datenübermittlungen (SCC, TIA, technische und organisatorische Maßnahmen)

4.1. Rechtlicher Rahmen für internationale Datenübermittlungen

BodyFact nimmt im Rahmen bestimmter Verarbeitungstätigkeiten Dienstleister in Anspruch, deren Sitz oder Server sich außerhalb der Europäischen Union befinden. Hierzu gehören insbesondere:

- Shopify Inc.
- Stripe Inc.
- PayPal (Europe) S.à r.l. et Cie, S.C.A. sowie außerhalb des Europäischen Wirtschaftsraums ansässige Gesellschaften der PayPal-Gruppe, insbesondere PayPal, Inc., Vereinigte Staaten
- Klaviyo Inc.
- Meta Platforms Inc.
- Google LLC
- TikTok Inc.

Bei Nutzung der PayPal-Zahlungsmethode ist der primäre Vertragspartner des Kunden PayPal (Europe) S.à r.l. et Cie, S.C.A. mit Sitz im Europäischen Wirtschaftsraum; aufgrund der globalen Konzernstruktur und IT-Infrastruktur der PayPal-Gruppe können jedoch bestimmte personenbezogene Daten auch für außerhalb des Europäischen Wirtschaftsraums ansässige Gesellschaften der PayPal-Gruppe, insbesondere PayPal,

Inc. (Vereinigte Staaten), zugänglich werden. Daher gelten für die mit der Nutzung der PayPal-Zahlungsmethode verbundenen Verarbeitungstätigkeiten die in diesem Kapitel festgelegten Regelungen für internationale Datenübermittlungen.

Da die Datenverarbeitung durch diese Dienstleister häufig in den **Vereinigten Staaten** oder in einem anderen sogenannten „Drittland“ erfolgt, unterliegen solche Übermittlungen **Kapitel V der DSGVO**.

Eine Übermittlung personenbezogener Daten in ein Drittland ist nur dann rechtmäßig, wenn sie den in Artikel 46 der DSGVO vorgesehenen geeigneten Garantien entspricht.

4.2. Angewandte Garantien für Datenübermittlungen (Artikel 46 DSGVO)

Der Dienstleister wendet im Einklang mit der DSGVO folgende Garantien an:

4.2.1. Standardvertragsklauseln (SCC – einheitliche EU-Musterklauseln aus dem Jahr 2021)

Der Verantwortliche verwendet mit jedem Dienstleister, der personenbezogene Daten außerhalb der EU verarbeitet, **SCC**, die:

- rechtlich bindend sind,
- von der Europäischen Kommission genehmigt wurden,
- dem Datenimporteur Verpflichtungen hinsichtlich Datensicherheit und Datenschutz auferlegen.

BodyFact verwendet die am 4. Juni 2021 erlassenen neuen SCC (Module 1–4), abhängig von der konkreten Rolle des jeweiligen Dienstleisters.

4.2.2. Transfer Impact Assessment (TIA)

Zusätzlich zu den SCC erstellt oder prüft der Dienstleister für jeden relevanten Partner in einem Drittland ein **TIA**, in dessen Rahmen Folgendes bewertet wird:

- die rechtlichen Rahmenbedingungen des betreffenden Landes,
- die Möglichkeiten der Behörden zum Zugriff auf Daten,
- das technische Schutzniveau des Dienstleisters,
- die internen Compliance-Prozesse des Datenimporteurs.

Zweck des TIA ist die Feststellung, dass die übermittelten personenbezogenen Daten auch nach ihrem Verlassen der EU **ein der DSGVO entsprechendes Schutzniveau genießen**.

4.2.3. Technische und organisatorische Maßnahmen (TOM — Technical & Organisational Measures)

Vor einer Datenübermittlung in ein Drittland stellt der Dienstleister sicher, dass der Dienstleister mindestens die folgenden Sicherheitsmaßnahmen anwendet:

- **Verschlüsselung der Datenübertragung** (TLS 1.2+)
- **serverseitige Verschlüsselung** (AES-256 oder gleichwertig)
- **Pseudonymisierung und Hashing** (z. B. Hashing von E-Mail-Adressen zu Remarketing-Zwecken)
- **Protokollierung von Zugriffen**
- **Beschränkung von Zugriffsberechtigungen**
- **SOC2 / ISO 27001-Zertifizierung** (Stripe, Shopify, Klaviyo)
- **physische Sicherheit der Rechenzentren**
- **beschränkter Zugriff auf Nutzerdaten**
- **regelmäßige Sicherheitsprüfungen**

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

Datenübermittlungen in die Vereinigten Staaten erfolgen bei bestimmten Dienstleistern auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission zum EU–US-Datenschutzrahmen, soweit die betreffende US-Rechtseinheit und die konkrete Kategorie der Datenverarbeitung tatsächlich vom DPF-Zertifikat erfasst sind. Das Vorliegen einer DPF-Zertifizierung bedeutet nicht allein, dass sämtliche Verarbeitungstätigkeiten eines Dienstleisters automatisch auf Grundlage dieses Mechanismus erfolgen — der Dienstleister prüft die Anwendbarkeit des DPF für jeden Dienstleister und jede Datenkategorie gesondert und verwendet, soweit der DPF nicht anwendbar ist, die von der Europäischen Kommission genehmigten Standardvertragsklauseln (SCC) sowie ein Transfer Impact Assessment (TIA).

Der Dienstleister überprüft den DPF-Zertifizierungsstatus der in Abschnitt 4.3 aufgeführten Dienstleister regelmäßig, da sich der Zertifizierungsstatus im Laufe der

Zeit ändern kann. Der aktuelle Status der einzelnen Dienstleister kann im offiziellen DPF-Register (dataprivacyframework.gov) überprüft werden.

4.3. Konkrete von internationalen Datenübermittlungen betroffene Dienstleister und ihre Funktionen

4.3.1. Shopify Inc. (Kanada, USA)

- **Funktion:** Hosting, Betrieb des Onlineshops
- **Datenfluss:** IP-Adresse, Bestelldaten, Daten des Benutzerkontos
- **Rechtsgrundlage:** Vertragserfüllung, Berechtigtes Interesse
- **Garantie:** Der aktuelle Auftragsverarbeitungsvertrag (DPA) von Shopify benennt den EU–US-Datenschutzrahmen (DPF) sowie, sofern die betreffende Datenübermittlung nicht in den Anwendungsbereich des DPF fällt, die SCC als anwendbaren Mechanismus für Datenübermittlungen; der Dienstleister wendet auf Grundlage der jeweiligen Shopify-Rechtseinheit, des Datenverarbeitungsvorgangs und der Datenkategorie den geeigneten Mechanismus gemäß den jeweils geltenden Angaben von Shopify an, ergänzt durch ein TIA und Verschlüsselung als zusätzliche Garantien.

Hinweis:
Shopify verfügt aufgrund Kanadas über einen **Angemessenheitsstatus**, bestimmte Teilleistungen werden jedoch in den USA erbracht.

4.3.2. Stripe Inc. (USA)

- **Funktion:** Verarbeitung von Zahlungstransaktionen, Abonnementverwaltung
- **Datenfluss:** Transaktionsmetadaten, tokenisierte Zahlungskartendaten
- **Garantie:** primär der Angemessenheitsbeschluss im Rahmen des EU–US-Datenschutzrahmens (DPF), da Stripe, LLC über eine gültige DPF-Zertifizierung verfügt; soweit eine bestimmte Datenübermittlung nicht vom Zertifizierungsumfang erfasst ist, wendet der Dienstleister als zusätzliche Garantien SCC und ein TIA an
- **PCI-DSS-Konformität**

4.3.3. Klaviyo Inc. (USA)

- **Funktion:** Newsletter und Marketingautomatisierung
- **Datenfluss:** Name, E-Mail-Adresse, Kampagneninteraktionen
- **Garantie:** primär der Angemessenheitsbeschluss im Rahmen des EU–US-Datenschutzrahmens (DPF), da Klaviyo, Inc. über eine gültige DPF-Zertifizierung verfügt; soweit eine bestimmte Datenübermittlung nicht vom Zertifizierungsumfang erfasst ist, wendet der Dienstleister als zusätzliche Garantien SCC, Hashing und AES-256-Verschlüsselung an

4.3.4. Meta Platforms Inc. (USA)

- **Funktion:** Remarketing, zielgerichtete Werbung
- **Datenfluss:** Pixel-Ereignisdaten, Cookies, gehashte E-Mail-Adresse
- **Garantie:** primär der Angemessenheitsbeschluss im Rahmen des EU–US-Datenschutzrahmens (DPF), da Meta Platforms, Inc. und ihre hundertprozentigen US-Tochtergesellschaften über gültige DPF-Zertifizierungen verfügen, einschließlich der Kategorien Meta Business Tools, Meta Pixel, Conversions API sowie Ads and Measurement; soweit eine bestimmte Datenübermittlung nicht vom Zertifizierungsumfang erfasst ist, wendet der Dienstleister als zusätzliche Garantien die Controller Terms und SCC an
- in bestimmten Fällen gemeinsame Verantwortlichkeit

4.3.5. Google LLC (USA)

- **Funktion:** Analytik, Werbung, Remarketing
- **Datenfluss:** Cookies, IP-Adresse (teilweise anonymisiert), GA-Ereignisse
- **Garantie:** primär der Angemessenheitsbeschluss im Rahmen des EU–US-Datenschutzrahmens (DPF), da Google LLC und ihre hundertprozentigen US-Tochtergesellschaften über gültige DPF-Zertifizierungen verfügen, einschließlich der Datenübermittlungen im Zusammenhang mit Ads Services; soweit eine bestimmte Datenübermittlung nicht vom Zertifizierungsumfang erfasst ist, wendet der Dienstleister als zusätzliche Garantie SCC an
- IP-Anonymisierung, teilweise Nutzung von EU-Servern

4.3.6. TikTok Inc. (USA / Singapur)

- **Funktion:** Remarketing
- **Datenfluss:** Cookies, Pixel-Ereignisse
- **Garantie:** SCC + TIA (TikTok kann derzeit im offiziellen DPF-Register nicht als eine Rechtseinheit identifiziert werden, auf deren DPF-Zertifizierung der Dienstleister die Datenübermittlung sicher stützen könnte; daher erfolgt die Datenübermittlung nicht auf Grundlage des DPF, sondern auf Grundlage der SCC und der Transfer-Risikoanalyse (TIA), unter Berücksichtigung der jeweiligen TikTok-Rechtseinheit und des jeweiligen Datenflusses)

4.3.7. PayPal (Europe) S.à r.l. et Cie, S.C.A. (Luxemburg) / PayPal, Inc. (Vereinigte Staaten)

- **Funktion:** bei Nutzung der vom Kunden gewählten PayPal-Zahlungsmethode Verarbeitung und Durchführung der Zahlungstransaktion, Gewährleistung der Transaktionssicherheit und Betrugsprävention sowie Erfüllung der für PayPal geltenden zahlungsverkehrsrechtlichen, finanziellen, geldwäschepräventionsrechtlichen (AML/CFT) und sonstigen gesetzlichen Verpflichtungen;
- **Rechtsstellung:** PayPal handelt hinsichtlich der von PayPal festgelegten Zwecke und Mittel der Verarbeitung als eigenständig Verantwortlicher. Der Dienstleister übermittelt PayPal die für die Einleitung und Durchführung der Zahlungstransaktion erforderlichen Daten. Hinsichtlich der von PayPal als eigenständig Verantwortlichem durchgeführten Verarbeitungstätigkeiten besteht zwischen dem Dienstleister und PayPal kein Auftragsverarbeitungsverhältnis im Sinne von Artikel 28 der DSGVO;
- **Datenfluss:** abhängig insbesondere vom konkreten Zahlungsprozess und der Integration insbesondere Name, E-Mail-Adresse, Rechnungs- und Lieferdaten des Kunden, Bestellkennung, Transaktionsbetrag sowie PayPal-Transaktionskennung, soweit diese für die Zahlungstransaktion erforderlich sind;
- **internationale Datenübermittlungen:** abhängig von der Tätigkeit der internationalen Unternehmensgruppe von PayPal und den genutzten Dienstleistungen können personenbezogene Daten auch für PayPal-Gruppengesellschaften mit Sitz außerhalb des Europäischen Wirtschaftsraums sowie für andere Empfänger zugänglich werden, gegebenenfalls einschließlich PayPal, Inc. mit Sitz in den Vereinigten Staaten;

- **Garantien:** sofern personenbezogene Daten in ein Land außerhalb des Europäischen Wirtschaftsraums übermittelt werden, erfolgt die Übermittlung auf Grundlage der in Kapitel V der DSGVO vorgesehenen geeigneten Garantien, die auf die konkrete Datenübermittlung tatsächlich anwendbar sind, insbesondere — soweit anwendbar — auf Grundlage der von der Europäischen Kommission angenommenen Standarddatenschutzklauseln (SCC), unter Berücksichtigung der erforderlichen ergänzenden Maßnahmen und der Risikobewertung der Datenübermittlung, einschließlich des Transfer Impact Assessments (TIA).

4.4. Transparenz des Dienstleisters: Zugänglichkeit der SCC

Auf Antrag der betroffenen Person gewährt der Dienstleister Zugang zu **den relevanten Teilen der SCC-Dokumente**, unter Berücksichtigung der folgenden Aspekte:

- Geschäftsgeheimnisse der Dienstleister dürfen nicht offengelegt werden,
- SCC-Module oder Anhänge können teilweise zur Verfügung gestellt werden,
- der Verantwortliche bearbeitet den Antrag innerhalb von 30 Tagen.

4.5. Vorbehalt des Dienstleisters hinsichtlich eines Wechsels von Dienstleistern

Der Dienstleister ist berechtigt, künftig andere Auftragsverarbeiter einzusetzen, sofern diese:

- geeignete Garantien bieten (Artikel 46 DSGVO),
- SCC anwenden,
- ein nachgewiesenes Datenschutzniveau aufweisen (ISO 27001 / SOC2),
- die Anforderungen der DSGVO erfüllen.

4.6. Ausschluss von Datenübermittlungen in besonderen Fällen

Der Dienstleister übermittelt personenbezogene Daten nicht:

- in verbotene Länder (EU-Sanktionsliste),
- an einen Dienstleister ohne angemessenen Schutz,
- an einen Partner, der die SCC nicht unterzeichnet,
- oder an einen Partner, der keine TIA- oder TOM-Anforderungen übernimmt.

4.7. Risikoanalyse und Monitoring

Die Risikoeinstufung internationaler Datenübermittlungen wird jährlich überprüft:

- Aktualisierung der TIA,
- Austausch bei einer neuen SCC-Version,
- Überprüfung praktischer Audits der Dienstleister,
- Verfolgung der Empfehlungen des ICO / EDPB,
- Sicherstellung der Einhaltung der Schrems-II-Anforderungen.

4.8. Rechte der betroffenen Person bei internationalen Datenübermittlungen

Die betroffene Person ist berechtigt:

- Auskunft darüber zu verlangen, in welches Land die Daten übermittelt werden,
- eine Kopie der relevanten Teile der SCC anzufordern,
- gegen eine auf dem Berechtigten Interesse beruhende Datenübermittlung Widerspruch einzulegen,
- eine Beschwerde bei der Aufsichtsbehörde einzulegen.

5. Verwendung von Cookies und Cookie-Management

5.1. Zwecke und Rechtsgrundlagen der Verwendung von Cookies

Die Website von BodyFact (nachfolgend: die „Website“) verwendet Cookies und sonstige Tracking-Technologien für den Betrieb der Website, ein personalisiertes Nutzererlebnis, statistische Analysen und Marketingaktivitäten.

Die Zwecke der Verwendung von Cookies sind:

1. **Gewährleistung des Betriebs der Website**
   – Anmeldung, Warenkorbfunktion, Sicherheitsfunktionen, Aufrechterhaltung der Sitzung.
2. **Speicherung von Nutzerpräferenzen**
   – Spracheinstellungen, regionsspezifische Funktionen, vom Nutzer ausgewählte Cookie-Einstellungen.

3. **Analyse und Leistungsmessung**
   – Messung des Website-Verkehrs, Identifizierung von Fehlern, Optimierung von Funktionen.

4. **Marketing und Remarketing**
   – Anzeige personalisierter Werbung
   – Durchführung zielgerichteter Kampagnen auf Grundlage des Nutzerverhaltens.

Rechtsgrundlagen:

- **Erforderliche Cookies:** Artikel 6 Absatz 1 Buchstabe b der DSGVO – Vertragserfüllung (z. B. Warenkorbfunktion, Durchführung des Zahlungsvorgangs), und/oder Artikel 6 Absatz 1 Buchstabe f der DSGVO – Berechtigtes Interesse des Verantwortlichen (z. B. IT-Sicherheit, Betrugsprävention).
- **Nicht erforderliche Cookies:** Artikel 6 Absatz 1 Buchstabe a der DSGVO – die vorherige, freiwillige Einwilligung der betroffenen Person.

Nicht erforderliche Cookies dürfen beim erstmaligen Laden der Website ohne eine über das Cookie-Management-System erteilte Einwilligung nicht aktiviert werden.

Zur Gewährleistung des Betriebs der Website, zur Verbesserung des Nutzererlebnisses sowie zu statistischen und Marketingzwecken verwendet der Verantwortliche verschiedene Arten von Cookies. Dieses Kapitel beschreibt ausschließlich die Arten, Zwecke und Aufbewahrungsfristen der Cookies. Die detaillierten Regelungen zur Einwilligungsverwaltung im Zusammenhang mit der Verwendung von Cookies sind in Kapitel 6 enthalten.

5.2. Kategorien von Cookies

Die folgenden Kategorien werden auf Grundlage der DSGVO, des ePrivacy-Rahmens und der Regeln von CookieBot bestimmt.

5.2.1. Erforderliche (essential) Cookies

Diese Cookies sind für den Betrieb der Website unerlässlich. Für ihre Installation ist keine Einwilligung erforderlich.

Funktionen:

- Sitzungskennung (session ID)
- Aufrechterhaltung des Anmeldestatus

- Warenkorbfunktion
- Durchführung des Zahlungsvorgangs
- Sicherheit, Betrugsprävention
- Speicherung der Cookie-Einwilligungseinstellungen

Typische Beispiele:

- Shopify essential cookies
- Cloudflare security cookies
- CookieBot „consent“-Status-Cookie

5.2.2. Präferenz-Cookies (functionality / preferences)

Diese Cookies ermöglichen ein personalisiertes Nutzererlebnis.

Funktionen:

- Speicherung der ausgewählten Sprache
- Region, Währung
- Speicherung bevorzugter Einstellungen
- teilweise Ausfüllung von Formularen

Sie dürfen nur mit Einwilligung aktiviert werden.

5.2.3. Analyse-Cookies (analytics)

Der Dienstleister kann zu Analysezwecken die folgenden Dienste verwenden:

- Google Analytics 4
- Shopify Analytics
- Hotjar (sofern aktiviert)

Die verarbeiteten Daten können beispielsweise Folgendes umfassen:

- Zeitpunkt des Besuchs
- Verhaltensdaten (Seitenaufrufe, Klicks)
- Geräte- und Browserdaten
- teilweise anonymisierte IP-Adresse

Für die Installation von Analyse-Cookies ist eine Einwilligung erforderlich.

5.2.4. Marketing- und Remarketing-Cookies

Hierzu gehören:

- Meta (Facebook) Pixel
- Google Ads Remarketing-Tag
- TikTok Pixel
- Klaviyo Web-Tracking
- Shopify Marketing-Cookies

Verarbeitete Daten:

- Seitenaufrufe
- Kaufereignisse (view content, add to cart, initiation, purchase)
- gehashte E-Mail-Adresse (zu Remarketing-Zwecken)
- Muster des Nutzerverhaltens

Marketing-Cookies dürfen ausschließlich nach Erteilung einer Einwilligung aktiviert werden.

5.3. Möglichkeiten des Cookie-Managements für die betroffene Person

Die betroffene Person verfügt hinsichtlich der Cookies über folgende Rechte und Möglichkeiten:

5.3.1. Erteilung oder Verweigerung der Einwilligung

Beim ersten Besuch der Website wird eindeutig ein Cookie-Banner angezeigt, über das die betroffene Person:

- alle Cookies akzeptieren,
- bestimmte Kategorien auswählen,
- alle Cookies ablehnen

kann.

5.3.2. Änderung oder Widerruf der Einwilligung

Die Einwilligung kann jederzeit über folgende Möglichkeiten widerrufen werden:

- „Cookie-Einstellungen“ / „Cookie Settings“
- oder durch Öffnen des CookieBot-Panels.

Der Widerruf berührt nicht die Rechtmäßigkeit der Verarbeitung, die auf Grundlage der Einwilligung bis zu deren Widerruf erfolgt ist.

5.3.3. Browsereinstellungen

Die betroffene Person kann Cookies auch in ihrem Browser löschen, insbesondere durch:

- Löschen von Cookies
- privaten Modus
- Blockierungseinstellungen
- Deaktivierung von Drittanbieter-Cookies

5.3.4. Einstellungen auf mobilen Geräten

Die folgenden Werbekennungen können ebenfalls eingeschränkt oder gelöscht werden:

- Apple IDFA
- Google Advertising ID

5.4. Aufbewahrungsfrist der Cookies

Je nach Art werden Cookies für folgende Zeiträume gespeichert:

- Sitzungscookies → bis zum Schließen des Browsers
- Präferenz-Cookies → 1–12 Monate
- Analyse-Cookies → 1–24 Monate
- Marketing-Cookies → 1–24 Monate (Meta, TikTok, Ads)

CookieBot zeigt die Aufbewahrungsfrist jedes einzelnen Cookies in einer monatlich aktualisierten Liste an.

6. Cookie-Einwilligungsverwaltungssystem (Consent Manager)

BodyFact installiert nicht erforderliche Cookies ausschließlich auf Grundlage der vorherigen, freiwilligen, spezifischen, angemessen informierten und ausdrücklichen Einwilligung der betroffenen Person gemäß Artikel 6 Absatz 1 Buchstabe a der DSGVO sowie den geltenden Rechtsvorschriften über elektronische Kommunikation.

Zur Verwaltung der Einwilligungen verwendet der Verantwortliche die Einwilligungsverwaltungsplattform CookieBot (Cybot A/S, Dänemark), die sicherstellt, dass einwilligungspflichtige Cookies ausschließlich nach der aktiven Zustimmung der betroffenen Person aktiviert werden.

Der Verantwortliche behält sich das Recht vor, anstelle von CookieBot ein anderes Einwilligungsverwaltungssystem mit gleichwertigem oder höherem Standard einzusetzen, sofern dieses die einschlägigen datenschutzrechtlichen Anforderungen erfüllt.

6.1. CookieBot als Einwilligungsverwaltungssystem

CookieBot gewährleistet insbesondere:

- die Einholung der Einwilligung der Besucher;
- die Protokollierung der Einwilligungsdatensätze;
- die Speicherung des Einwilligungsstatus;
- die Blockierung nicht erforderlicher Cookies bis zur Erteilung der Einwilligung;
- die automatische Identifizierung und Kategorisierung der verwendeten Cookies;
- die Auditierbarkeit der Einwilligungsprotokolle.

CookieBot ermöglicht es der betroffenen Person, für jede Cookie-Kategorie gesondert über die Erteilung, Verweigerung oder den Widerruf der Einwilligung zu entscheiden.

6.2. Protokollierung und Aufbewahrung der Einwilligung

CookieBot protokolliert im Zusammenhang mit der Einwilligung insbesondere folgende Daten:

- Datum und Uhrzeit der Einwilligung;
- die IP-Adresse der betroffenen Person in anonymisierter Form;
- die ausgewählten Cookie-Kategorien;

- die Versionsnummer des Einwilligungs-Banners;
- die Domain der betroffenen Person;
- technische Einwilligungskennung (Consent ID).

Die Aufbewahrungsfrist der Einwilligungsprotokolle beträgt grundsätzlich 12 Monate.

Zweck der Protokollierung ist die Erfüllung des Grundsatzes der Rechenschaftspflicht gemäß der DSGVO und die Sicherstellung der Nachweisbarkeit einer rechtmäßigen Einwilligung.

6.3. Blockierung von Cookies bis zur Erteilung der Einwilligung

Beim ersten Besuch der Website blockiert CookieBot automatisch das Laden sämtlicher nicht erforderlicher Cookies und damit verbundener Skripte.

Hierzu können insbesondere gehören:

- Google Analytics;
- Google Ads;
- Meta Pixel;
- TikTok Pixel;
- Klaviyo-Tracking-Lösungen;
- Shopify-Cookies zu Analyse- oder Marketingzwecken.

Diese Cookies und die damit verbundenen Technologien dürfen ausschließlich nach vorheriger Einwilligung der betroffenen Person aktiviert werden.

Dies stellt die Einhaltung der Anforderungen der DSGVO und des ePrivacy-Rahmens durch die Website sicher.

6.4. Erneuerung der Einwilligung (Re-consent)

Die Einwilligung gilt für einen Zeitraum von höchstens 12 Monaten als gültig; danach kann das System eine erneute Einwilligung anfordern.

Der Verantwortliche ist insbesondere in folgenden Fällen berechtigt, eine erneute Einwilligung anzufordern:

a) Einführung einer neuen Cookie-Kategorie;
b) Integration eines neuen Drittanbieter-Dienstleisters;

c) wesentliche Änderung der Zwecke der Cookies;
d) Änderung der geltenden Rechtsvorschriften.

Zweck der erneuten Einwilligung ist die Aufrechterhaltung der fortlaufenden Rechtmäßigkeit.

6.5. Automatisches Cookie-Verzeichnis und Aktualisierung

CookieBot erfasst, identifiziert und kategorisiert die auf der Website verwendeten Cookies regelmäßig und automatisch.

Dies dient insbesondere folgenden Zwecken:

- Identifizierung neuer Cookies;
- Entfernung nicht mehr verwendeter Cookies;
- Aktualisierung der Cookie-Kategorien;
- Aktualisierung der Rechtsgrundlagen und Beschreibungen im Zusammenhang mit den Cookies.

Das aktuelle Cookie-Verzeichnis ist über die auf der Website verfügbare CookieBot-Oberfläche fortlaufend zugänglich.

6.6. Änderung und Widerruf der Einwilligung

Die betroffene Person ist jederzeit berechtigt:

- die Einwilligung zu ändern;
- die Einwilligung zu widerrufen;
- die Cookie-Einstellungen neu zu konfigurieren.

Der Widerruf der Einwilligung berührt nicht die Rechtmäßigkeit der vor dem Widerruf erfolgten Verarbeitung.

Die betroffene Person kann diese Rechte jederzeit über die auf der Website verfügbare Oberfläche „Cookie-Einstellungen“ ausüben.

6.7. Auditierbarkeit und Compliance-Dokumentation

Der Verantwortliche gewährleistet mithilfe von CookieBot:

- die Protokollierbarkeit der Einwilligungen;

- die Rückverfolgbarkeit der Einwilligungsdatensätze;
- die Aufrechterhaltung der Compliance-Dokumentation;
- die Nachweisbarkeit gegenüber der Aufsichtsbehörde.

Durch dieses System kann der Verantwortliche insbesondere nachweisen:

- dass nicht erforderliche Cookies ohne Einwilligung nicht aktiviert werden;
- dass die Einwilligung freiwillig und informiert erfolgt;
- dass die Einwilligung jederzeit widerrufen werden kann.

6.8. Integrationen von Drittanbietern und Datenübermittlungen

CookieBot verwaltet insbesondere integriert:

- die Shopify-Cookie-Konfiguration;
- die Blockierung von Google-Tag-Manager-Skripten;
- die Aktivierung von Meta Pixel;
- das Laden von TikTok Pixel;
- die Klaviyo-Codes für die Marketingautomatisierung.

Soweit die Verwendung von Cookies eine Datenübermittlung in ein Drittland beinhaltet, wendet der Verantwortliche die in Kapitel 4 (Internationale Datenübermittlungen) festgelegten Garantien an — einschließlich, soweit anwendbar, des Angemessenheitsbeschlusses im Rahmen des EU–US-Datenschutzrahmens (DPF) und, sofern dieser nicht anwendbar ist, der von der Europäischen Kommission angenommenen Standardvertragsklauseln (SCC) sowie des damit verbundenen Transfer Impact Assessments (TIA).

6.9. Transparenz und fortlaufende Compliance

Der Verantwortliche überprüft regelmäßig den Umfang der auf der Website verwendeten Cookies, den Mechanismus zur Verwaltung der Einwilligungen und die damit verbundenen Datenverarbeitungspraktiken, um eine fortlaufende Rechtmäßigkeit, Transparenz und Compliance sicherzustellen.

Die betroffene Person erhält über die CookieBot-Oberfläche jederzeit detaillierte Informationen über die Art, den Zweck, den Anbieter und die Aufbewahrungsfrist der Cookies.

7. Rechte der betroffenen Personen und Ausübung ihrer Rechte

7.1. Allgemeine Grundsätze der Rechte der betroffenen Personen (Artikel 12 DSGVO)

Der Dienstleister stellt sicher, dass die Ausübung der Rechte der betroffenen Personen:

- unentgeltlich,
- transparent,
- leicht zugänglich,
- in verständlicher und klarer Form erfolgt,
- ohne unangemessene Verzögerung, spätestens jedoch innerhalb von 30 Tagen erfolgt.

Der Dienstleister kann die Erfüllung von Anträgen von der Überprüfung der Identität der antragstellenden Person abhängig machen, insbesondere wenn die Identifizierung aus der Ferne erfolgt (z. B. per E-Mail).

Die Frist für die Beantwortung kann in begründeten Fällen um weitere 2 Monate verlängert werden. Hierüber informiert der Dienstleister die betroffene Person vorab.

7.2. Recht auf Information (Artikel 13–14 DSGVO)

Die betroffene Person hat das Recht, Kenntnis zu erlangen über:

- welche personenbezogenen Daten verarbeitet werden,
- die Zwecke und Rechtsgrundlagen der Verarbeitung,
- die Kategorien der verarbeiteten Daten,
- die Aufbewahrungsfrist der Verarbeitung,
- die Empfänger von Datenübermittlungen,
- die Herkunft der personenbezogenen Daten (wenn diese nicht von der betroffenen Person bereitgestellt wurden),
- das Vorliegen von Datenübermittlungen in Drittländer und die hierfür geltenden Garantien,

- die Rechte der betroffenen Person und die zur Verfügung stehenden Rechtsbehelfe.

Der Dienstleister stellt diese Informationen:

- in der Datenschutzerklärung,
- während des Kaufvorgangs,
- bei der Anmeldung zum Newsletter,
- und bei der Beantwortung von Anträgen betroffener Personen

zur Verfügung.

7.3. Recht auf Auskunft (Artikel 15 DSGVO)

Die betroffene Person hat das Recht, vom Dienstleister eine Bestätigung darüber zu erhalten, ob:

- ihre personenbezogenen Daten verarbeitet werden, und
- falls dies der Fall ist, kann sie Auskunft darüber verlangen:

1. welche Daten verarbeitet wurden,
2. zu welchen Zwecken,
3. auf welcher Rechtsgrundlage,
4. an wen die Daten übermittelt wurden,
5. für welchen Zeitraum die Daten verarbeitet werden,
6. welche Rechte ihr zustehen.

Die betroffene Person kann eine elektronische Kopie ihrer personenbezogenen Daten (z. B. PDF, CSV) verlangen.

Das Recht auf Auskunft ist eingeschränkt, wenn seine Ausübung die Rechte anderer Personen oder Geschäftsgeheimnisse verletzen würde.

7.4. Recht auf Berichtigung (Artikel 16 DSGVO)

Die betroffene Person hat das Recht, Folgendes zu verlangen:

- die Berichtigung unrichtiger personenbezogener Daten,
- die Vervollständigung unvollständiger Daten.

Der Dienstleister nimmt die Berichtigung unverzüglich vor und informiert darüber jeden Empfänger, dem die fehlerhaften Daten zuvor übermittelt wurden, es sei denn, dies würde einen unverhältnismäßigen Aufwand erfordern.

7.5. Recht auf Löschung („Recht auf Vergessenwerden“) – Artikel 17 DSGVO

Die betroffene Person kann die Löschung ihrer personenbezogenen Daten verlangen, wenn:

1. der Zweck der Verarbeitung weggefallen ist,
2. sie ihre Einwilligung widerrufen hat und keine andere Rechtsgrundlage besteht,
3. sie der auf dem berechtigten Interesse beruhenden Verarbeitung widerspricht,
4. die Verarbeitung unrechtmäßig ist,
5. eine rechtliche Verpflichtung die Löschung vorschreibt,
6. es sich bei einem Dienst der Informationsgesellschaft um Daten eines Kindes handelt.

Die Löschung kann verweigert werden, wenn die Verarbeitung:

- zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Abrechnungsdaten),
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist,
- aufgrund buchhalterischer oder steuerrechtlicher Verpflichtungen nicht gelöscht werden darf.

Bei der Erfüllung von Löschungsanträgen:

- löscht der Dienstleister das Benutzerkonto (soweit vorhanden),
- löscht er die in Marketingsystemen gespeicherten Daten (Klaviyo usw.),
- löscht er die in Shopify gespeicherten Profildaten,
- anonymisiert er Transaktionen (unter Beachtung gesetzlicher Aufbewahrungspflichten).

7.6. Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO)

Die betroffene Person kann die Einschränkung der Verarbeitung verlangen, wenn:

- sie die Richtigkeit der personenbezogenen Daten bestreitet,

- die Verarbeitung unrechtmäßig ist und sie die Löschung ablehnt,
- der Dienstleister die Daten nicht mehr benötigt, die betroffene Person diese jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt,
- die betroffene Person der auf dem berechtigten Interesse beruhenden Verarbeitung widersprochen hat (während des Prüfungszeitraums).

Während der Einschränkung dürfen die Daten:

- nicht gelöscht,
- nicht verarbeitet,
- ausschließlich gespeichert

werden,

ausgenommen:

- mit Einwilligung der betroffenen Person,
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
- zum Schutz einer anderen Person,
- aus wichtigen Gründen des öffentlichen Interesses.

7.7. Recht auf Datenübertragbarkeit (Artikel 20 DSGVO)

Die betroffene Person hat das Recht, diejenigen Daten:

- die sie dem Dienstleister bereitgestellt hat,
- deren Verarbeitung auf einer Einwilligung oder einem Vertrag beruht,
- und die automatisiert verarbeitet werden,

in einem strukturierten, gängigen und maschinenlesbaren Format (z. B. CSV, JSON) zu erhalten.

Die betroffene Person kann auch die direkte Übermittlung der Daten von einem Dienstleister an einen anderen verlangen, sofern dies technisch machbar ist.

7.8. Recht auf Widerspruch (Artikel 21 DSGVO)

Die betroffene Person ist jederzeit berechtigt, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen, wenn diese:

- auf einem berechtigten Interesse beruht, oder
- dem Zweck der Direktwerbung dient.

Folge des Widerspruchs:

- der Dienstleister darf die personenbezogenen Daten nicht weiterverarbeiten,
- es sei denn, er weist nach, dass zwingende schutzwürdige Gründe für die Verarbeitung bestehen.

Bei Direktwerbung (z. B. Newsletter):

Der Widerspruch führt automatisch zur unverzüglichen Löschung der Daten aus der Marketingdatenbank.

7.9. Automatisierte Entscheidungsfindung und Profiling (Artikel 22 DSGVO)

Der Dienstleister führt keine automatisierte Entscheidungsfindung durch, die gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, und verwendet kein Profiling, das erhebliche Auswirkungen auf die betroffene Person hat.

Im Rahmen seiner Marketingaktivitäten kann der Dienstleister in bestimmten Fällen Profiling durchführen (insbesondere durch Segmentierung mittels Klaviyo und Meta Ads), um der betroffenen Person Angebote anzuzeigen, die ihren Interessen entsprechen. Diese Art der Segmentierung zu Marketingzwecken stellt keine nach Artikel 22 DSGVO verbotene automatisierte Entscheidungsfindung dar, weil:

- sie keine erheblichen rechtlichen Auswirkungen hat,
- sie den rechtlichen Status der betroffenen Person nicht berührt,
- sie ausschließlich der zielgerichteten Werbung dient.

7.10. Ausübung der Rechte der betroffenen Person

Die betroffene Person kann die in dieser Datenschutzerklärung festgelegten Rechte schriftlich per E-Mail, auf dem Postweg oder über die auf der Website verfügbare Kontaktoberfläche ausüben.

Der Verantwortliche bearbeitet und beantwortet Anträge betroffener Personen ohne unangemessene Verzögerung, spätestens jedoch innerhalb der in Artikel 12 Absatz 3 DSGVO festgelegten Frist.

7.11. Recht auf Beschwerde und Recht auf gerichtlichen Rechtsschutz

7.11.1. Beschwerde bei einer Aufsichtsbehörde

Gemäß Artikel 77 Absatz 1 DSGVO hat die betroffene Person das Recht, eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes einzureichen. Die Kontaktdaten der Aufsichtsbehörden der einzelnen Mitgliedstaaten sind auf der Website des Europäischen Datenschutzausschusses (EDPB) verfügbar.

Betroffene Personen in Ungarn — sowie jede andere betroffene Person, die sich an die ungarische Aufsichtsbehörde wenden möchte — können sich an folgende Behörde wenden:

Ungarische Nationale Behörde für Datenschutz und Informationsfreiheit (NAIH)
H-1055 Budapest, Falk Miksa utca 9–11.
Telefon: +36 1 391 1400
E-Mail: ugyfelszolgalat@naih.hu
Web: www.naih.hu

7.11.2. Recht auf gerichtlichen Rechtsschutz

Die betroffene Person ist berechtigt, sich an folgendes Gericht zu wenden:

- das am Sitz des Dienstleisters zuständige Gericht, oder
- das am Wohnsitz / gewöhnlichen Aufenthaltsort der betroffenen Person zuständige Gericht.

8. Technische und organisatorische Maßnahmen (TOM)

8.1. Allgemeine Grundsätze der Datensicherheit (Art. 32 DSGVO)

Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen ein, um die kontinuierliche Sicherheit der verarbeiteten personenbezogenen Daten hinsichtlich

- Vertraulichkeit
- Integrität
- Verfügbarkeit

- Authentizität

zu gewährleisten.

Bei der Festlegung der anzuwendenden Maßnahmen berücksichtigt der Verantwortliche:

- die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung,
- das Ausmaß des Risikos für die Rechte und Freiheiten der betroffenen Personen,
- den Stand der Technik und die Kosten,
- die besten verfügbaren Branchenpraktiken.

8.2. Technische Datensicherheitsmaßnahmen

Der Verantwortliche und die von ihm beauftragten Auftragsverarbeiter gewährleisten den technischen Schutz auf mehreren Ebenen.

8.2.1. Datenverschlüsselung

Verschlüsselung der Datenübertragung

- HTTPS-/TLS-1.2- oder neuere Protokolle
- Verschlüsselung der Datenkommunikation mit den Systemen von Shopify, Stripe, Klaviyo, Meta, Google und TikTok

Verschlüsselung gespeicherter Daten

- serverseitige AES-256-Verschlüsselung
- tokenisierte Zahlungskartendaten (Stripe)
- gehashte E-Mail-Adressen zu Marketingzwecken (SHA-256 oder gleichwertig)

Der Verantwortliche speichert niemals Zahlungskartendaten – Zahlungstransaktionen werden ausschließlich von Stripe abgewickelt, das über eine PCI-DSS-Zertifizierung verfügt.

8.2.2. Pseudonymisierung und Anonymisierung

In Marketing- und Analysesystemen angewandte Verfahren:

- gehashte E-Mail-Adressen zu Remarketing-Zwecken

- Anonymisierung von IP-Adressen in Google Analytics
- tokenisierte Benutzerkennungen

Die Pseudonymisierung minimiert das Risiko der Identifizierung von Profilen.

8.2.3. Zugriffsschutz und Berechtigungsmanagement

Der Verantwortliche:

- verwendet ein rollenbasiertes Zugriffskontrollsystem (RBAC),
- gewährt Zugriff ausschließlich Personen, für die dieser Zugriff zur Erfüllung ihrer beruflichen Aufgaben unbedingt erforderlich ist,
- schreibt eine Multi-Faktor-Authentifizierung (MFA) vor.

Alle Zugriffsberechtigungen:

- werden regelmäßig überprüft,
- werden bei Beendigung des Beschäftigungsverhältnisses unverzüglich entzogen,
- werden protokolliert.

8.2.4. System- und Infrastrukturschutz

Der Verantwortliche setzt branchenübliche:

- Firewalls,
- Intrusion-Prevention-Systeme (IPS),
- DDoS-Schutz (Cloudflare / Shopify),
- Richtlinien zur Versionskontrolle und Aktualisierung,
- kontinuierliches Schwachstellen-Monitoring

ein.

Die Hosting-Dienste und Server:

- verfügen über eine ISO-27001- oder SOC-2-Zertifizierung,
- befinden sich in kontrollierten Rechenzentren,
- verfügen über physische Sicherheitssysteme (24/7-Sicherheitsdienst, Zutrittskontrolle, Kameras).

8.2.5. Sicherungskopien und Wiederherstellung

Der Verantwortliche gewährleistet:

- die automatisierte Erstellung täglicher und wöchentlicher Datensicherungen,
- eine versionierte Speicherung von Backups,
- serverseitige Redundanz,
- die Nutzung geografisch voneinander getrennter Rechenzentren,
- ein Verfahren zur schnellen Wiederherstellung im Falle von Dienstunterbrechungen (Disaster-Recovery-Plan).

Die Backups werden zusätzlich verschlüsselt.

8.2.6. Protokollierung, Monitoring und Auditing

Der Verantwortliche und seine Auftragsverarbeiter:

- führen eine kontinuierliche Systemprotokollierung durch,
- protokollieren Administratorzugriffe,
- archivieren Ereignisprotokolle,
- führen regelmäßige interne und externe Audits durch (Shopify, Stripe, Klaviyo: SOC 2).

Sicherheitsprotokolle werden für einen festgelegten Zeitraum, typischerweise 12–24 Monate, aufbewahrt.

8.3. Organisatorische und administrative Datensicherheitsmaßnahmen

Zusätzlich zu den technischen Maßnahmen wendet der Verantwortliche Regelungen und Verfahren auf Organisationsebene an.

8.3.1. Datenschutz- und Datensicherheitsrichtlinie

Die internen Richtlinien des Verantwortlichen umfassen:

- Verfahren der Datenverarbeitung,
- die Festlegung von Datenschutzverantwortlichkeiten,
- Verfahren zur Behandlung von Datenschutzvorfällen,

- Regeln für die Dokumenten- und Aktenverwaltung,
- Aufbewahrungsfristen für Daten.

8.3.2. Mitarbeiterschulung und Vertraulichkeit

Der Verantwortliche gewährleistet:

- eine jährliche Datenschutzschulung,
- Schulungen zu Datenlecks und Phishing,
- die Unterzeichnung von Vertraulichkeitsverpflichtungen,
- die Vermittlung von Datensicherheitsverfahren.

Alle Mitarbeiter sind verpflichtet, die Datenschutzvorschriften einzuhalten.

8.3.3. Garantien für Auftragsverarbeiter und vertragliche Garantien

Der Verantwortliche schließt ausschließlich Verträge mit Auftragsverarbeitern, die:

- über einen schriftlichen Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO verfügen,
- nachweislich DSGVO-konform sind,
- Übermittlungen in Drittländer auf Grundlage der in Kapitel 4 festgelegten Garantien durchführen (primär des EU-US Data Privacy Framework und, sofern dieses nicht anwendbar ist, der Standardvertragsklauseln (SCC)),
- angemessene Sicherheitsgarantien bieten.

Alle Auftragsverarbeiter erfüllen folgende Anforderungen:

- Verpflichtungen zur Datensicherheit,
- Meldung von Sicherheitsvorfällen,
- Zusammenarbeit bei der Bearbeitung von Anfragen betroffener Personen,
- Gewährleistung der Auditierbarkeit.

8.4. Reaktion auf Verletzungen des Schutzes personenbezogener Daten

Zur Vermeidung und Behandlung von Verletzungen des Schutzes personenbezogener Daten:

1. wendet der Verantwortliche ein spezielles Verfahren zur Behandlung von Datenschutzvorfällen an,
2. bestimmt er ein Untersuchungsteam zur Bewertung der Situation,
3. protokolliert er den Vorfall und dessen Umstände,
4. bestimmt er den eingetretenen Schaden und das damit verbundene Risiko,
5. ergreift er Maßnahmen zur Beendigung des Ereignisses.

Meldepflicht gegenüber der Aufsichtsbehörde:

Der Verantwortliche meldet eine Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden der NAIH, wenn diese:

- ein Risiko für die Rechte oder Freiheiten der betroffenen Personen darstellt.

Benachrichtigung der betroffenen Person:

Die betroffene Person wird informiert, wenn:

- der Vorfall ein hohes Risiko für die betroffene Person darstellt.

Die Benachrichtigung enthält:

- die Art des Vorfalls,
- den Zeitpunkt des Eintritts,
- die betroffenen Daten,
- die möglichen Folgen,
- die ergriffenen Maßnahmen,
- mögliche weitere Schritte.

8.5. Zertifizierungen und Compliance-Nachweise

Die Partner des Verantwortlichen können über folgende Zertifizierungen verfügen:

- ISO 27001 (Shopify, Google, Klaviyo)
- SOC 2 Type II (Stripe, Shopify, Klaviyo)
- PCI-DSS (Stripe – Zahlungsabwicklung)
- ISO/IEC 27701 – Erweiterung für den Datenschutz (bestimmte Dienstleister)

Diese gewährleisten die Einhaltung von Sicherheitsstandards auf Branchenebene.

8.6. Kontinuierliche Verbesserung der Datensicherheit

Der Verantwortliche überprüft regelmäßig:

- technologische Entwicklungen,
- neue Sicherheitsbedrohungen,
- die Sicherheit der Dienstleisterkette (Shopify, Stripe, Klaviyo usw.),
- Empfehlungen des EDPB und der NAIH,
- den aktuellen rechtlichen Status der in Kapitel 4 beschriebenen Garantien für internationale Datenübermittlungen (DPF, SCC, TIA).

Soweit erforderlich, führt er zusätzliche Schutzmaßnahmen ein.

8.7. Datenschutz-Folgenabschätzung

Der Verantwortliche führt gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung (DSFA) bei der Planung von Verarbeitungstätigkeiten durch, wenn diese – insbesondere bei der Einführung neuer digitaler Dienstleistungen – voraussichtlich ein hohes Risiko für die Grundrechte und Freiheiten der betroffenen Personen zur Folge haben können. Der Verantwortliche konsultiert die Aufsichtsbehörde im Einklang mit den geltenden Vorschriften vorab hinsichtlich des Ergebnisses der Datenschutz-Folgenabschätzung und der erforderlichenfalls vorgesehenen Abhilfemaßnahmen.

9. Aufbewahrungsfristen und Löschungsregeln

9.1. Allgemeine Grundsätze der Aufbewahrungsfristen

Der Dienstleister verarbeitet personenbezogene Daten nur so lange, wie dies erforderlich ist und im Zusammenhang mit dem Zweck der Verarbeitung steht, unter Berücksichtigung von:

- Artikel 5 Absatz 1 Buchstabe e DSGVO („Grundsatz der Speicherbegrenzung“),
- den gesetzlichen Aufbewahrungspflichten nach dem Rechnungslegungs- und Steuerrecht (ungarisches Rechnungslegungsgesetz (Gesetz Nr. C von 2000 über die Rechnungslegung, „Számviteli törvény“), § 169),
- den sich aus den Rechtsvorschriften über den elektronischen Geschäftsverkehr ergebenden Verpflichtungen,
- etwaigen bestehenden Rechtsansprüchen,

- der Dauer der Erfüllung von Kundenverträgen.

Soweit die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, dauert die Verarbeitung bis zum endgültigen Abschluss des Verfahrens, längstens jedoch bis zum Ablauf der für den jeweiligen Anspruch geltenden Verjährungsfrist. Diese Regel gilt ergänzend für sämtliche in diesem Kapitel und in anderen Abschnitten der Datenschutzerklärung festgelegten Aufbewahrungsfristen, wenn hinsichtlich der betreffenden Datenkategorie ein Rechtsstreit oder Rechtsanspruch entsteht.

Nach Ablauf der Aufbewahrungsfristen:

- werden die Daten gelöscht, oder
- sofern eine Löschung aufgrund einer gesetzlichen Verpflichtung nicht möglich ist → erfolgt eine irreversible Anonymisierung.

9.2. Konkrete Aufbewahrungsfristen nach Datenart

Die nachstehende Tabelle legt die Aufbewahrungsfristen für die vom Dienstleister verarbeiteten Datenkategorien fest.

9.2.1. Kauf- und Vertragsdaten

Datenart	**Aufbewahrungsfrist**	**Rechtsgrundlage / Hinweis**
Bestell-Metadaten	5 Jahre	Berechtigtes Interesse unter Berücksichtigung der Verjährungsfrist nach dem auf die betroffene Person anwendbaren nationalen Recht (siehe §§ 1.3 und 2.2); bei betroffenen Personen in Ungarn die fünfjährige Verjährungsfrist gemäß § 6:22 des ungarischen Bürgerlichen Gesetzbuches (Gesetz Nr. V von 2013 über das Bürgerliche Gesetzbuch, „Polgári Törvénykönyv“)
Versanddaten	Erfüllung + 1 Jahr	Siehe § 2.2

Datenart	Aufbewahrungsfrist	Rechtsgrundlage / Hinweis
Rechnungsdaten	8 Jahre	Ungarisches Rechnungslegungsgesetz (Gesetz Nr. C von 2000 über die Rechnungslegung, „Számviteli törvény“), § 169; siehe § 2.3
Buchführungs-/Rechnungslegungsbelege von Abonnementtransaktionen (Stripe Subscriptions)	8 Jahre	Gesetzliche Verpflichtung nach dem ungarischen Rechnungslegungsgesetz (Gesetz Nr. C von 2000 über die Rechnungslegung, „Számviteli törvény“), § 169. Diese Zeile bezieht sich ausschließlich auf die zum Abonnement gehörenden Rechnungslegungsbelege; die abweichende, kürzere Aufbewahrungsfrist für Abonnementverwaltungsdaten (Konto- und Statusdaten) ist in § 2.4 festgelegt.
Daten im Zusammenhang mit der Vertragserfüllung	Bis zur Erfüllung des Vertrags + 5 Jahre	Berechtigtes Interesse unter Berücksichtigung der Verjährungsfrist nach dem auf die betroffene Person anwendbaren nationalen Recht

Der Dienstleister darf die vorstehenden Daten nicht früher löschen, selbst wenn die betroffene Person die Löschung verlangt.

9.2.2. Daten des Benutzerkontos

Datenart	Aufbewahrungsfrist	Hinweis
Benutzerkonto (Shopify account)	Bis zur Löschung des Kontos	Kann auf Antrag der betroffenen Person gelöscht werden

Datenart	Aufbewahrungsfrist	Hinweis
Inaktive Konten	Nach 24 Monaten Inaktivität	Der Dienstleister kann die Daten aufgrund seines berechtigten Interesses löschen oder anonymisieren

9.2.3. Newsletter-Anmeldung und Marketingdaten

Datenart	Aufbewahrungsfrist	Rechtsgrundlage / Hinweis
E-Mail-Adressen von Newsletter-Abonnenten	Bis zum Widerruf der Einwilligung	DSGVO Artikel 6 Absatz 1 Buchstabe a
Protokolldaten zum Nachweis der Einwilligung (Tatsache, Zeitpunkt und Quelle der Einwilligung)	5 Jahre ab Widerruf der Einwilligung	DSGVO Artikel 6 Absatz 1 Buchstabe f – berechtigtes Interesse (Geltendmachung, Ausübung und Verteidigung zivilrechtlicher Ansprüche)
Abgemeldete E-Mail-Adressen in der „Suppression List“	24 Monate	Zum Nachweis, dass keine weiteren Marketingnachrichten versendet werden
Marketinginteraktionen (Klaviyo: Öffnungen, Klicks)	24 Monate	Branchenübliche Praxis, Statistik
Gehashte Identifikatoren von Remarketing-Listen	180–540 Tage	Regeln von Meta / Google Ads

9.2.4. Kundendienst- und Kundenservicedaten

Datenart	Aufbewahrungsfrist	Hinweis
Kundendienstkorrespondenz	12 Monate	Beschwerden, Qualitätssicherung
Beschwerdedaten	5 Jahre; bei dem über die Beschwerde aufgenommenen Protokoll, der schriftlichen	§ 17/A Absatz 7 des ungarischen Verbraucherschutzgesetzes (Gesetz Nr. CLV von 1997 über den Verbraucherschutz, „Fogyasztóvédelmi törvény“)

Datenart	Aufbewahrungsfrist	Hinweis
	Beschwerde und einer Kopie der darauf erteilten sachlichen Antwort: 3 Jahre	(Beschwerdeprotokoll, schriftliche Beschwerde und sachliche Antwort: 3 Jahre, einschließlich der Verpflichtung zur Vorlage gegenüber der zuständigen Behörde); sonstige Beschwerdedaten und Dokumente: 5 Jahre. Soweit dies zur Geltendmachung von Rechtsansprüchen erforderlich ist, dauert die Verarbeitung bis zum endgültigen Abschluss des Verfahrens, längstens jedoch bis zum Ablauf der Verjährungsfrist des Anspruchs.
Qualitätsbeanstandungen und zugehörige Dokumente	5 Jahre	Archivierung der Untersuchungen im Zusammenhang mit dem 72-Stunden-SLA. Soweit dies zur Geltendmachung von Rechtsansprüchen erforderlich ist, dauert die Verarbeitung bis zum endgültigen Abschluss des Verfahrens, längstens jedoch bis zum Ablauf der Verjährungsfrist des Anspruchs.

9.2.5. Daten zur Lebensmittelsicherheit und zu Rückrufen

Datenart	Aufbewahrungsfrist	Hinweis
Chargennummernverwaltung und Daten zur Rückverfolgbarkeit des Herstellers	5 Jahre	Lebensmittelrechtliche Vorschriften
Rückrufmitteilungen	5 Jahre	Behördliche Compliance

Datenart	Aufbewahrungsfrist	Hinweis
Daten zu Entschädigungsleistungen	5 Jahre	Geltendmachung zivilrechtlicher Ansprüche

9.2.6. Cookies und Online-Identifikatoren

Die maßgeblichen Aufbewahrungsfristen für die einzelnen Cookie-Kategorien sind in § 5.4 („Cookie-Aufbewahrungsfrist“) festgelegt; die genauen Aufbewahrungsfristen für einzelne Cookies werden in der auf der Website verfügbaren Cookie-Liste festgelegt, die durch die automatische monatliche Überprüfung von CookieBot aktualisiert wird.

Cookies können manuell oder durch den Widerruf der Einwilligung gelöscht werden.

9.2.7. Logdaten und Protokolldateien

Datenart	Aufbewahrungsfrist	Hinweis
Systemprotokolle	12–24 Monate	Aus Sicherheitsgründen
Protokolle der Administratorzugriffe	12 Monate	Zu Audit-Zwecken
Protokolle von Datenschutzvorfällen	5 Jahre	Aufgrund der Meldepflichten nach der DSGVO

9.2.8. Daten im Zusammenhang mit Kundenbewertungen

Datenart	Aufbewahrungsfrist	Rechtsgrundlage / Hinweis
Daten aus Nachrichten zur Kundenzufriedenheits-/Bewertungsanfrage (ohne Werbeinhalt)	12 Monate ab Versand	DSGVO Artikel 6 Absatz 1 Buchstabe f – berechtigtes Interesse (§ 15.3.1 der AGB)
Nachricht zur Bewertungsanfrage mit einem Anreiz (Gutschein,	Bis zum Widerruf der Einwilligung; Protokolldaten zum Nachweis der	DSGVO Artikel 6 Absatz 1 Buchstabe a; § 6 des ungarischen Werbegesetzes (Gesetz Nr. XLVIII von 2008 über

Datenart	**Aufbewahrungsfrist**	**Rechtsgrundlage / Hinweis**
Treuepunkte, Rabatt) und Daten zur Einwilligung	Einwilligung 5 Jahre ab Widerruf	die grundlegenden Anforderungen und bestimmte Beschränkungen der kommerziellen Werbung, „Grt.“) (§ 15.7.4 der AGB)
Veröffentlichten Kundenbewertungen und nutzergenerierte Inhalte (UGC) – ausgenommen Foto-/Video-Uploads für Treuepunkte, siehe nachfolgende Zeile	Bis zum Widerruf der Einwilligung bzw. bis zum Löschungsantrag; nach Beendigung der öffentlichen Darstellung werden die zu Beweiszwecken erforderlichen Protokolldaten für 5 Jahre ab Beendigung der öffentlichen Darstellung aufbewahrt	Einwilligung der betroffenen Person; im Falle eines Rechtsanspruchs berechtigtes Interesse des Dienstleisters zu Beweiszwecken
Für Treuepunkte hochgeladene Inhalte (Foto/Video)	Bis zum Widerruf der Einwilligung bzw. – sofern kein Widerruf erfolgt – höchstens 3 Jahre ab dem Upload	DSGVO Artikel 6 Absatz 1 Buchstabe a; siehe § 2.13

9.3. Maßnahmen nach Ablauf der Aufbewahrungsfristen

Nach Ablauf der Aufbewahrungsfrist wird der Dienstleister:

1. die betreffenden personenbezogenen Daten löschen oder
2. sie irreversibel anonymisieren, sofern eine Aufbewahrung gesetzlich vorgeschrieben ist, ihre personenbezogene Eigenschaft jedoch nicht mehr erforderlich ist.

Die Anonymisierung kann insbesondere erfolgen durch:

- Hashing,
- Erstellung aggregierter statistischer Daten,
- irreversible Datenverarbeitung.

9.4. Bearbeitung von Löschungsanträgen

Auf Antrag der betroffenen Person auf Löschung wird der Dienstleister:

- das Konto löschen oder anonymisieren,
- die Daten aus den Marketingsystemen entfernen,
- Cookies löschen oder deaktivieren,
- auch bei den Partner-Auftragsverarbeitern die Löschung veranlassen (Shopify, Klaviyo, Meta usw.).

Folgende Daten können nicht gelöscht werden:

- Rechnungsdaten,
- buchhalterische Transaktionsdaten,
- Daten, die zur Aufbewahrung und Verteidigung von Rechtsansprüchen erforderlich sind.

9.5. Gesetzliche und Rechenschaftspflichten

Der Dienstleister:

- überprüft die Regelungen zur Datenaufbewahrung jährlich,
- dokumentiert diese im Rahmen von Audits,
- aktualisiert die Datenschutzerklärung im Falle von Änderungen.

Gemäß dem Grundsatz der Rechenschaftspflicht ist der Dienstleister verpflichtet:

- nachzuweisen, dass angemessene Aufbewahrungsfristen angewendet werden,
- die Durchführung der Löschungen nachzuweisen,
- das Verzeichnis der Verarbeitungstätigkeiten auf dem aktuellen Stand zu halten.

10. Empfänger, Auftragsverarbeiter und Datenübermittlungen

10.1. Einleitende Bestimmungen

Der Verantwortliche setzt im Rahmen seiner Datenverarbeitung ausschließlich Auftragsverarbeiter und Datenempfänger ein, die:

- die Anforderungen der Art. 28 und 46 DSGVO erfüllen;
- sich zur Einhaltung der Pflichten eines Auftragsverarbeiters verpflichten;
- über angemessene technische und organisatorische Maßnahmen (TOM) verfügen;
- schriftliche Auftragsverarbeitungsverträge abschließen;
- bei Übermittlungen personenbezogener Daten in Drittländer die in Kapitel 4 genannten Garantien (vorrangig das EU-US Data Privacy Framework, soweit erforderlich SCC und TIA) sowie ergänzende technische Schutzmaßnahmen gewährleisten.

10.2. Detaillierte Liste der Auftragsverarbeiter

Die nachstehende Liste enthält die für den Betrieb von BodyFact erforderlichen Auftragsverarbeiter, deren jeweilige Rolle, die Kategorien der verarbeiteten Daten sowie die Garantien für die Einhaltung der DSGVO.

Gemäß Art. 28 DSGVO schließt der Verantwortliche ausschließlich mit solchen Auftragsverarbeitern Verträge ab, die sich schriftlich zur Einhaltung der Pflichten nach der DSGVO verpflichten. Die folgenden Abschnitte beschreiben die wichtigsten Auftragsverarbeiter für die wesentlichen Funktionsbereiche sowie die von ihnen verarbeiteten Datenkategorien und die Garantien für die rechtliche Konformität.

10.2.1. Shopify Inc.

Rolle: Betrieb des Webshop-Systems (Auftragsverarbeiter & Verantwortlicher / gemischte Funktion)
Land: Kanada + USA
Drittland: Ja
Garantien: siehe Abschnitt 4.3.1 (vorrangig DPF, soweit erforderlich SCC), ergänzt durch ISO 27001- und SOC-2-Zertifizierungen

Verarbeitete Daten:

- Name, E-Mail-Adresse, Telefonnummer
- Lieferadresse
- Bestelldaten, Warenkorbdaten
- IP-Adresse, Geräteinformationen
- Kontodaten, Anmeldedaten

Hinweis: Kanada gilt für die betreffenden Datenverarbeitungsvorgänge als Land mit angemessenem Datenschutzniveau. Für in den Vereinigten Staaten erbrachte Teilleistungen wendet Shopify den in Abschnitt 4.3.1 beschriebenen Mechanismus an (vorrangig DPF, soweit erforderlich SCC).

10.2.2. Stripe Inc.

Rolle: Zahlungsdienstleister, Verwaltung von Abonnements
Land: USA
Drittland: Ja
Garantien: siehe Abschnitt 4.3.2 (vorrangig DPF), ergänzt durch die PCI-DSS-Level-1-Zertifizierung

Verarbeitete Daten:

- Transaktionsmetadaten
- tokenisierte Kartendaten (für BodyFact nicht zugänglich)
- Rechnungsdaten
- Abonnementstatus, Zahlungsbelastungen
- IP-Adresse, Geräteinformationen

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

Rolle: Erbringung von Zahlungsdienstleistungen, sofern PayPal als Zahlungsmethode ausgewählt wird (eigenständiger Verantwortlicher hinsichtlich der Verarbeitung von Zahlungstransaktionen, der Betrugsprävention und der Erfüllung gesetzlicher Pflichten – siehe Abschnitt 4.3.7)

Land: Luxemburg (EU); konzerninterne Datenübermittlungen in die USA (PayPal, Inc.)

Drittland: Ja, aufgrund von Datenübermittlungen innerhalb der PayPal-Gruppe außerhalb des EWR

Garantien: Soweit personenbezogene Daten in ein Land außerhalb des Europäischen Wirtschaftsraums übermittelt werden, erfolgt die Übermittlung auf Grundlage der für die jeweilige Übermittlung nach Kapitel V der DSGVO tatsächlich anwendbaren geeigneten Garantien, insbesondere – soweit anwendbar – auf Grundlage der von der Europäischen Kommission angenommenen Standardvertragsklauseln (SCC), unter Berücksichtigung der erforderlichen ergänzenden Maßnahmen und der Risikobewertung der Datenübermittlung einschließlich einer Transfer Impact Assessment (TIA).

Verarbeitete Daten:

- Name
- E-Mail-Adresse
- für die Transaktion erforderliche Rechnungs-/Lieferadresse
- Bestellnummer und Bestellbetrag
- PayPal-Transaktions-ID
- sofern der Kunde über ein PayPal-Konto verfügt: Daten, die aufgrund des eigenständigen Rechtsverhältnisses zwischen dem Kunden und PayPal verarbeitet werden

10.2.4. Klaviyo Inc.

Rolle: E-Mail-Marketing, Newsletter, Automatisierung
Land: USA
Garantien: siehe Abschnitt 4.3.3 (vorrangig DPF), ergänzt durch AES-256-Verschlüsselung und SOC-2-Zertifizierung

Verarbeitete Daten:

- Name, E-Mail-Adresse
- Kaufhistorie (sofern synchronisiert)
- Kampagneninteraktionen (Öffnungen, Klicks)
- Präferenzen, Interessen (Profilfelder)
- gehashte E-Mail-Adresse zu Remarketing-Zwecken

10.2.5. Meta Platforms Inc. (Facebook/Instagram)

Rolle: Marketing und Remarketing
Land: USA
Garantien: siehe Abschnitt 4.3.4 (vorrangig DPF), ergänzt durch Controller Terms; hinsichtlich der gemeinsamen Verantwortlichkeit siehe Abschnitt 3.2

Verarbeitete Daten:

- Pixel-Ereignisdaten (Pageview, Purchase)
- gehashte E-Mail-Adresse (Custom Audience)

- Cookies, Online-Identifikatoren
- Remarketing-Listen

Hinweis: In bestimmten Fällen liegt eine gemeinsame Verantwortlichkeit (Joint Controllership) vor.

10.2.6. Google LLC

Rolle: Analyse + Werbung + Remarketing
Land: USA
Garantien: siehe Abschnitt 4.3.5 (vorrangig DPF), ergänzt durch IP-Anonymisierung

Verarbeitete Daten:

- Cookies
- IP-Adresse (anonymisiert)
- Ereignisdaten (GA4)
- Remarketing-Identifikatoren (Ads)

10.2.7. TikTok Inc.

Rolle: Remarketing
Land: USA / Singapur
Garantien: siehe Abschnitt 4.3.6 (SCC + TIA; DPF derzeit nicht anwendbar)

Verarbeitete Daten:

- Pixel-Ereignisdaten
- Cookies
- Marketinginteraktionen

10.2.8. Cloudflare, Inc.

Rolle: Sicherheitsinfrastruktur, CDN, DDoS-Schutz
Land: USA + weltweit

Garantien: Vorrangig das EU-US Data Privacy Framework (DPF) gemäß dem Angemessenheitsbeschluss, da Cloudflare, Inc. über eine gültige DPF-Zertifizierung verfügt. Gemäß dem Cloudflare Data Processing Addendum, v6.4, stellen Übermittlungen auf Grundlage dieses Mechanismus keine eingeschränkten

Übermittlungen dar. Sollte die Zertifizierung beendet oder ungültig werden, erfolgt die Übermittlung auf Grundlage eines alternativen Mechanismus gemäß dem Cloudflare DPA, vorrangig SCC und erforderlichenfalls ergänzenden Maßnahmen. Zusätzliche Garantie: ISO-27001-Zertifizierung.

Verarbeitete Daten:

- IP-Adresse
- Browserkennung
- verkehrstechnische Daten

Cloudflare verarbeitet ausschließlich die für die Erbringung der Dienstleistungen erforderlichen Daten und verwendet diese nicht für Marketingzwecke.

10.2.9. CookieBot (Cybot A/S)

Rolle: Verwaltung von Cookie-Einwilligungen
Land: Dänemark (EU)
Garantien: Anbieter mit Sitz in der EU; SCC sind nicht erforderlich

Verarbeitete Daten:

- Einwilligungsstatus
- IP-Adresse (anonymisiert)
- Cookie-Einstellungen
- Consent ID
- Banner-Versionsnummer

10.2.10. Refersion, Inc.

Rolle: Verwaltung des Affiliate-Programms, Provisionsverfolgung
Land: USA
Drittland: Ja
Garantien: SCC + TIA (siehe Abschnitt 2.8)

Verarbeitete Daten:

- Name und E-Mail-Adresse des Affiliate-Partners
- Affiliate-ID
- Provisionsdaten, generierter Umsatz
- Zahlungsdaten (Bankkontonummer oder PayPal)

10.2.11. Yotpo Ltd.

Rolle: Verwaltung des Treuepunkteprogramms, Kundenbewertungen und nutzergenerierter Inhalte (UGC)
Land: Israel (Sitz); die Verarbeitung kann außerdem in den USA, im Vereinigten Königreich und in der Europäischen Union erfolgen
Drittland: Ja

Garantien: Übermittlungen nach Israel erfolgen auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission für Israel; Übermittlungen in das Vereinigte Königreich erfolgen auf Grundlage des EU-UK-Angemessenheitsbeschlusses; Übermittlungen in die USA erfolgen auf Grundlage von SCC (siehe Abschnitt 2.8). EU-GDPR-Vertreter: SMSBump Ltd. (Bulgarien).

Verarbeitete Daten:

- Daten zu Treuepunkten
- Texte von Kundenbewertungen
- hochgeladene Foto-/Videoinhalte (UGC), zusammen mit den in Abschnitt 2.13 beschriebenen Nutzungsberechtigungen und Marketing-Einwilligungen

10.2.12. Kurierdienste (GLS, DHL, DPD, MPL usw.)

Rolle: Paketzustellung
Land: EU
Garantien: Auftragsverarbeitungsvertrag

Verarbeitete Daten:

- Name
- Adresse
- Telefonnummer
- E-Mail-Adresse
- Paketidentifikationsnummer

10.2.13. Buchhalter / Steuerberater / Buchhaltungspartner

Rolle: Erfüllung gesetzlicher Verpflichtungen
Land: Ungarn / EU
Garantien: Auftragsverarbeitungsvertrag

Verarbeitete Daten:

- Rechnungsdaten
- Buchhaltungsunterlagen
- Transaktionsdaten

10.2.14. Behörden und Gerichte

Rolle: gesetzlich vorgeschriebene Datenübermittlung

Verarbeitete Daten:

- Rechnungsdaten
- Transaktionsdaten
- Unterlagen zur Bearbeitung von Beschwerden
- für Gerichts- und Rechtsverfahren erforderliche Daten

Diese Übermittlungen bedürfen keiner Einwilligung (Art. 6 Abs. 1 lit. c DSGVO – Erfüllung einer rechtlichen Verpflichtung bzw. in begründeten Fällen Art. 6 Abs. 1 lit. f DSGVO – berechtigtes Interesse, z. B. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen).

Sonstige Datenübermittlungen: Eine Datenübermittlung erfolgt ausschließlich, wenn eine gesetzliche Verpflichtung besteht, insbesondere an die für den Sitz des Verantwortlichen zuständigen Behörden, beispielsweise die ungarische Steuer- und Zollbehörde (NAV) oder die ungarische Datenschutzbehörde (NAIH), sowie gegebenenfalls an zuständige Behörden anderer Mitgliedstaaten. Die Übermittlung erfolgt jeweils auf Grundlage von Art. 6 Abs. 1 lit. c DSGVO bzw. im Rahmen des jeweiligen behördlichen Verfahrens.

10.3. Zusammenfassung der Datenübermittlungen in Drittländer und der Compliance-Garantien

Bei den folgenden Dienstleistern kann eine Übermittlung personenbezogener Daten außerhalb der EU erfolgen:

Dienstleister	Land	Garantie
Shopify Inc.	Kanada/USA	siehe Abschnitt 4.3.1
Stripe Inc.	USA	siehe Abschnitt 4.3.2
Klaviyo Inc.	USA	siehe Abschnitt 4.3.3
Meta Platforms	USA	siehe Abschnitt 4.3.4
Google LLC	USA	siehe Abschnitt 4.3.5
TikTok	USA / Singapur	siehe Abschnitt 4.3.6
PayPal (Europe) S.à r.l. et Cie, S.C.A. / PayPal, Inc.	Luxemburg (EU) / USA	siehe Abschnitt 4.3.7
Cloudflare	USA	DPF (vorrangig); bei Beendigung der Zertifizierung SCC – siehe Abschnitt 10.2.8
Refersion, Inc.	USA	SCC + TIA (siehe Abschnitt 2.8)
Yotpo Ltd.	Israel / USA / UK / EU	Angemessenheitsbeschluss (Israel, UK) / SCC (USA) – siehe Abschnitt 2.8

Alle Übermittlungen in Drittländer entsprechen Art. 46 DSGVO.

11. Kontaktdaten des Verantwortlichen

Kontakt und Rechtsbehelfe

Verantwortlicher: BODYFACT Kft.
Sitz und Postanschrift: Csatlós utca 3. 1/3, 1029 Budapest, Ungarn
Kundenservice-E-Mail: hello@bodyfact.eu
Datenschutzangelegenheiten: privacy@bodyfact.eu