PRIVACY POLICY

To clearly and transparently explain our privacy practices when you use our services, we present our current Privacy Policy.

This document contains detailed information about your rights and our obligations, which we adhere to in order to ensure that the processing of personal data is carried out in accordance with applicable law and best practices.

The website may contain links to third-party websites or services. The controller is not responsible for the personal data processing policies or privacy practices of these third parties. The service providers we use in the operation of our websites declare that they conduct their activities in a manner similar to ours, that is, in compliance with applicable laws and with respect for the privacy of the individuals whose data they may process.

The website is not intended for persons under the age of 16. The Administrator does not knowingly process the data of persons under this age.

You are required to provide true, current, and complete information and to update it in the event of any changes. The administrator is not liable for the consequences of you providing false, incomplete, or outdated information.

To ensure the highest quality of service and operational efficiency, we use artificial intelligence (AI)-based tools in our operations. Below, we explain how we use them, what rights individuals have in this regard, and how we ensure compliance with applicable laws, particularly the Artificial Intelligence Act (AI Act).

By providing personal data to the Controller, the visitor declares that they are authorized to provide such data and that its processing by the Controller does not infringe upon the rights of third parties or applicable laws. In the case of providing third-party data, the visitor is obligated to ensure that they have an appropriate legal basis for sharing it.

DEFINITIONS

Organization – Gopackshot Studios Sp. z o.o., with its registered office at ul. Grabiszyńska 241, 53-234 Wrocław, Poland, registration number: KRS 0000470943, share capital: 10,000 PLN, Tax (VAT) number: PL8943167634.

Website – the websites *gopackshot.com* through which the Organization provides its services and conducts online sales.

Visitor – a person visiting the Organization's websites who does not log in to a specific User account or does not have one. A Visitor may become a User when they provide their personal data or otherwise disclose their identity to the Organization.

User – a person who uses the Organization's services, has a personal account, or orders goods or services provided by the Organization. A User may or may not be a customer. In the case of online purchases, during which individuals place orders (without registering an account, or with account registration), entries are created in the Organization's database systems, enabling the Organization to provide services to that individual, perform after-sales support on their behalf, and fulfill fiscal obligations by issuing the appropriate documents related to the purchases. Choosing not to create an account does not result in the cessation of personal data processing—the data is still processed as necessary to fulfill the contract between the individual and the Organization.

Cookies – pieces of information, known as cookies, sent by websites and stored on the end device used for the connection (computer, laptop, smartphone). Cookies may be mandatory (required) for the proper functioning of the websites or optional—providing information about the Visitor but not essential for the website's operation. During the first visit, the Visitor is asked to decide whether to allow the use of specific cookies associated with the Organization's solutions and technologies, as well as those of its external providers.

Tracking identifiers – these are mechanisms that track visits to the Website's pages using unique identifiers assigned by measurement service providers. The technology operates on the server side and is based on assigning unique codes to parameters such as device and browser characteristics. Together, they allow for the creation of a fairly unique device identifier that can be used to approximately identify Visitors.

AI System – a machine-based system designed to operate with varying levels of autonomy, which, once deployed, may demonstrate the ability to adapt and which, for explicit or implicit purposes, based on received input data, infer how to generate outputs, such as predictions, content, recommendations, or decisions that may affect the physical or virtual environment.

Vendor – An external entity that provides additional services to the Organization and supports its operations. Suppliers provide tools and services that enable the collection, analysis, and reporting of data regarding the effectiveness of online marketing activities, and they participate in the payment processing and optimization of the Websites. Their tools help carry out marketing activities by better targeting advertisements. Google Analytics and Microsoft Clarity are used to track how you use and interact with our website through behavioral metrics, heat maps, and session replays, which helps us improve our products and services and promote them to the market. Vendors have their own separate privacy policies: https://www.microsoft.com/pl-pl/privacy/privacystatement, https://support.google.com/analytics/answer/6004245

Business Partners – We collaborate with selected business partners ("Partners") who may request to include their own marketing content in our newsletters or other forms of content delivery, depending on the Visitor's choice. In such cases, Partners do not have access to recipients' personal data, and the content is sent by the Administrator without sharing data with the Partners. Marketing content from Partners is clearly marked and is informational or promotional in nature. Such content is placed only with the consent of the recipient of the marketing content to receive marketing communications from our Partners.

Account – a set of resources and settings created for the User within the Organization's Services, used to manage services, including making online purchases or providing online services.

EEA – European Economic Area – a free trade zone and common market comprising the member states of the European Union and the European Free Trade Association (EFTA), with the exception of Switzerland.

GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

I. PERSONAL DATA CONTROLLER

The Organization is the Data Controller for personal data processed on the Website or Websites. The Data Controller has appointed a Data Protection Officer, who can be contacted regarding matters related to privacy, security, and the processing of personal data, including the rights and obligations of the Data Controller. You can contact the DPO at: *dpo@gopackshot.com* or by sending written correspondence to the Organization's registered office address provided above, marked "Data Protection Officer":

Gopackshot Studios Sp. z o.o.
ul. Grabiszyńska 241
53-234 Wrocław, Poland

In the case of interactions carried out through or with the assistance of third-party solutions, in particular social media, the Organization acts as a joint data controller. In such cases, the relevant regulations contained in the respective statements of these providers apply with regard to data protection and privacy.

II. METHODS OF COLLECTING PERSONAL DATA

Scenarios for possible forms of personal data collection:

1. Information is provided voluntarily by Visitors and Users during registration, when contacting us via electronic forms, or through messaging platforms.

2. Information collected automatically is data gathered by servers hosting the Services, whether owned by the Organization or by Providers supporting this process or delivering content and materials (e.g., fonts, video content, or CSS scripts). Information obtained in this manner includes, among other things, the website address (URL) of the requested page, the date and time of the request, device data (e.g., hardware model and operating system type), browser type, and data regarding the IP addresses from which the connection originates (both directly and indirectly—via a proxy).

3. Information transmitted automatically is not used in a form that would allow it to be directly linked to Visitors' personal data. However, this data may enable selected solution providers to identify individuals with a high degree of probability and, to a certain extent, monitor their online activity—through mechanisms using unique identifiers. The Organization itself does not carry out such activities, relying solely on aggregated statistical data provided by Providers who have the capability to link the context of a connection to a specific individual, particularly when that individual is browsing websites while logged into social media platforms or associated messaging services.

4. Some parts of the Services may include social media tools. Their purpose is to enable the exchange of information between registered users of these social media platforms and to make it easier for them to share links to content on . However, it should be noted that such interactions are inextricably linked to the processing of personal data in the context of the services provided by social media platforms. The entities responsible for a given social media platform may use this method to identify correlations between individuals and products or services.

5. The Organization does not have access to, nor does it perform any actions on, the data that Visitors or Users send from the Services to social media platforms—such actions are carried out by the users of the respective social media platform themselves, and the effects of such personal

data processing should be referred to the relevant privacy policies of the respective social media provider.

6. Personal data may be obtained indirectly from social media providers, where the identity of individuals interacting with the Organization's profiles on social media may be disclosed. Each user of such platforms sets their privacy settings within their account, and details regarding the relevant privacy policies can be found at:

   - https://www.facebook.com/privacy/
   - https://about.instagram.com/safety
   - https://www.youtube.com/howyoutubeworks/our-commitments/protecting-user-data/
   - https://www.tiktok.com/legal/page/eea/privacy-policy/pl
   - https://www.linkedin.com/legal/privacy-policy

7. The Websites may also contain elements related to the Organization's activities that require the provision of specific data—for example, in connection with payment options or installment purchases.

8. When providing information to the Administrator via contact forms, email, or other communication channels, visitors should provide only the data necessary to handle the inquiry or perform the service in question.

9. The Administrator is not liable for the provision of personal data exceeding the scope required to fulfill the purpose of the correspondence, in particular specially protected (sensitive) data or data concerning third parties.

III. LEGAL BASIS FOR THE PROCESSING OF PERSONAL DATA

As the Controller, the Organization collects personal data based on various grounds, described below along with a brief justification:

1. In order to enable the handling of any complaints, claims, and requests, as well as to respond to questions, the Organization may process certain personal data provided during registration or in the contact form. In such cases, the legal basis is the individual's conscious action aimed at providing contact details to the Organization—that is, part of the performance of the contract pursuant to Article 6(1)(b) of the GDPR, or it may be a legitimate interest, i.e., Article 6(1)(f) of the GDPR, consisting in the provision of electronic services and in building positive relationships with Users based on reliability and loyalty.

2. The organization may also process data necessary for billing purposes, including: first name, last name, and, if applicable, the name of the company under which business activities are conducted; registered address; Tax Identification Number (NIP) and National Business Registry Number (REGON); address details; and information regarding bank transfers and bank account numbers. The legal basis is the fulfillment of a legal obligation incumbent upon the Controller under Article 6(1)(c) of the GDPR.

3. The Controller may also process personal data based on explicit consent (i.e., voluntary, specific, informed, and unambiguous consent). In such cases, prior to the collection or processing of

personal data, clear information will be provided regarding the purpose and scope for which consent may be granted. Any person granting consent has the right to withdraw it at any time. The mere use of certain contact forms constitutes consent for the Organization to respond to the messages received, either by replying or by conducting further correspondence.

4. Based on a legitimate interest, i.e., Article 6(1)(f) of the GDPR, the Organization carries out activities promoting its services independently or in collaboration with Business Partners.

5. When using services provided through Meta platforms, individuals independently decide whether to interact with a service operating on Facebook or Instagram. These activities may include subscribing, commenting on content, tagging, or sharing content further.

6. Tracking identifiers are used only after obtaining the Visitor's consent, in accordance with the regulations on privacy in electronic communications.

IV. USE OF PERSONAL DATA

1. The primary purpose of the Data Controller in collecting personal data is to provide online sale of services. These purposes are linked to other activities—namely, creating and managing User accounts, conducting business correspondence, and facilitating contact. Some information is required to process payment transactions. Certain information may also be used to customize the Website to individual needs, including for interactive communication and other additional services.

2. The Website may also include optional registration for selected services, surveys, and questionnaires requesting additional information relevant to a specific purpose.

3. Measurement data transmitted from Visitors' devices while browsing the Website may be used to design and create better solutions, customize operations, improve the Website, and provide advice and assistance regarding the services provided.

4. Some data may be provided voluntarily; however, failure to provide it will make it impossible to deliver (or continue delivering) the relevant products or services.

5. The Data Controller may use the information collected based on explicit consent to create personalized marketing and advertising offers. This type of advertising may be displayed through visible elements on the Website, on social media platforms, or in popular search engines.

6. Information about Visitors and Users may be used by third parties such as Suppliers or social media platforms, which may independently link the Organization's context to specific individuals visiting the websites. Such activities do not result in the direct processing of personal data by the Organization, which does not have access to it. The use of third-party services is implemented through the acceptance of consents upon the first (or subsequent, after deleting cookies) visit to the Website, where each visitor can specify whether they want the mechanisms of a given Provider to be enabled within the Website. General acceptance constitutes consent to enable all Provider solutions. It is also possible to selectively choose them or reject all additional solutions that are not strictly necessary for the operation of the Website.

7. The scope of possible processing purposes by social media providers depends on how they manage profiling and ad display. This may be based on user consent or can be disabled by using paid social media accounts, which are designed to eliminate or limit ads. The Organization uses social media ads but does not know which individuals the ads are displayed to—only the provider of the social media platform has this information.

8. Visitor data is subject to profiling (automated decision-making), enabling Visitors to receive more tailored content or services. Profiling may influence how products are presented, but it does not result in significant legal consequences for the Visitor nor does it otherwise significantly affect the data subjects.

9. If such additional parameters are required by external providers, they may be processed both by the Administrator and by Providers associated with the Website's services—based on the explicit consent of the data subject.

10. By accepting the mailing terms and conditions, individuals may receive newsletters containing information about services, additional features, promotions, or other related services provided by Administrator and its group of business partners. This does not imply the transfer of Recipients' personal data to business partners, and consent to the mailing terms and conditions may be withdrawn at any time.

11. The Recipient may change their newsletter subscription preferences by adjusting the settings with the Provider that handles the distribution on behalf of the Administrator. They may also unsubscribe from the service there.

12. Additionally, if appropriate consent is granted, selected Recipient data may be shared with Business Partners, who will then be able to send personalized materials. This practice is clearly indicated on the Websites and is not equivalent to the Providers monitoring traffic on the Websites; rather, it constitutes a separate, explicitly identified activity.

V. DATA SHARING

1. In certain cases, based on consent or unambiguous actions constituting consent, the Administrator may share personal data with commercial entities.

2. The websites use service providers that operate systems supporting our operations including schedule online appointments:

   Cal.com, Inc.
   2261 Market Street #4382; San Francisco, CA 94114, United States

   Hetzner Online GmbH (HRB 6089)
   Industriestrasse 25, 91710 Gunzenhausen, Germany

3. Partners operate exclusively on the basis of strictly defined rules—including personal data processing agreements concluded in accordance with Article 28 of the GDPR, along with the mandatory requirement to maintain the confidentiality of all personal data with which they come into contact.

4. As a data controller, the organization may disclose personal data in specific cases to entities such as legal advisors, in connection with the establishment, exercise, or defense of legal claims, to comply with legal requirements, or to respond to lawful requests in the context of legal proceedings, to protect rights and property, including to enforce contracts, comply with court orders, subpoenas, or other legal notices related to legal proceedings.

5. Additionally, under certain circumstances, the Controller may be required by law to disclose the processed personal data upon request by authorized authorities.

6. The same applies to Suppliers, who may be required to disclose Visitors' personal data associated with the Services.

7. Certain Visitor data may be disclosed to third parties at the Visitors' express request. This may occur when integrating the Website's services with other providers whose solutions may communicate with the Website to provide additional features, such as product reviews. The points of such data exchange are clearly marked, and before any action is taken, consent must be given (by accepting the terms or taking action: opt-in) to prevent the accidental or unintentional disclosure of data.

VI. ARTIFICIAL INTELLIGENCE (AI)

The Administrator may use IT tools based on artificial intelligence (AI) solutions to streamline operations, improve service quality, analyze service performance, and automate selected technical processes. These systems may support:

- analysis of the Website's operation and its functionality,
- handling user inquiries,
- organizing and processing information,
- support for administrative and technical processes.

When using such tools, the Controller applies the principle of data minimization and transfers to AI systems only the data necessary to perform a specific function. The AI tools used fall into the category of systems with limited or minimal risk and do not make decisions that produce significant legal effects on individuals or otherwise significantly affect them.

If the processing of personal data involves the use of external AI technology providers, the Controller ensures that it cooperates exclusively with entities that guarantee an adequate level of personal data protection and enters into appropriate agreements with them governing the rules of data processing in accordance with the provisions of the GDPR.

The Controller does not use personal data provided through the use of the Website to train artificial intelligence models, unless this is explicitly stated in separate information or is inherent to the nature of a given feature.

The AI solutions used by the Controller do not make decisions that produce significant legal effects on individuals within the meaning of Article 22 of the GDPR.

In cases where AI tools utilize infrastructure or service providers located outside the European Economic Area, data transfers are conducted using appropriate safeguards required by the provisions of the GDPR.

The Controller takes measures to ensure the transparency of the technological solutions used and monitors their operation in terms of data security and compliance with applicable laws.

The controller ensures human oversight of the operation of the AI systems used. Responsible individuals have the ability to verify and correct decisions made by the system, which is particularly important in the event of an objection or the filing of a complaint.

VII. DATA SECURITY

1. All activities performed on the Services are subject to technical and organizational security measures, such as encryption, which involves encoding information entered by Users or Visitors or displayed to them in such a way that it can only be read by the Users' or Visitors' browsers and the servers hosting the Services.

2. As part of our commitment to the security of the Websites, security tests and independent audits by specialists are conducted periodically, and the latest software versions are used.

3. At the same time, however, since it is technically impossible to guarantee that every data transmission over the Internet is completely secure, despite making every effort to ensure the protection of personal data, the Data Controller cannot ensure or otherwise guarantee the complete security of information transmitted by Users and Visitors via the network.

4. In the event of a personal data breach, the Data Controller acts in accordance with Articles 33 and 34 of the GDPR, including assessing and classifying the incident and notifying the supervisory authority within 72 hours if the nature of the incident so requires.

5. In the event of detecting security incidents related to the processing of personal data that may pose a risk of infringing the rights or freedoms of natural persons, the Controller—in accordance with Article 34 of the GDPR—notifies the data subjects, indicating the possible consequences of the incident and recommended actions to mitigate the potential effects of the incident.

VIII. RETENTION – DATA RETENTION PERIOD

Personal data is stored for no longer than is necessary to fulfill the purposes for which it was collected, unless applicable laws require longer retention. In particular, this includes:

1. Accounts on the Website for the purpose of providing services and related support, as well as other services in accordance with the agreement.

2. After the Account is deleted, the data will be anonymized, except for data necessary to establish, pursue, or defend claims.

3. If the provision of the service involves the fulfillment of tax and legal obligations, the necessary data will be processed for the period required by law (most often 5 years from the date of fulfillment of the tax and legal obligation).

4. Data processed on the basis of consent will be processed until such consent is withdrawn or until the service for which consent was granted is terminated.

Furthermore, information that may to some extent identify personal data is stored for a period corresponding to the lifecycle of the cookies stored on your devices. These settings can be changed in any modern browser or by deleting the cookies.

IX. TRANSFER OF DATA TO THIRD COUNTRIES

Personal data is generally not transferred outside the European Economic Area (EEA). The key servers used are located in Poland or the EEA, and our Partners have their headquarters within the European Economic Area.

1. When data is jointly managed with social media providers, there is a possibility that Visitors' data may be processed by these providers if this results from Visitors' consent to the use of the Providers' solutions.

2. In the event of data transfers outside the EEA, such processing is permitted only by entities that use the European Commission's Standard Contractual Clauses (SCCs) or the EU–US Data Privacy Framework (DPF) compliance mechanisms. The Controller assumes that these entities process data in accordance with their declarations within the EEA or in accordance with accepted principles ensuring a level of privacy protection no less than that required by the GDPR.

3. Detailed information and settings regarding the processing of personal data by social media providers can be found on their privacy pages. These are typically referred to as Privacy Policies, Privacy Centers, or Privacy Settings within account profiles.

X. RIGHTS

In connection with the processing of personal data, every individual has a number of rights, the exercise of which the Controller is obligated to ensure. These rights may be exercised by submitting a request in writing or via the email address provided at the beginning of this Policy.

Every individual whose data is processed has the right to:

1. Access to your data pursuant to Article 15 of the GDPR. Specifically, this includes the right to obtain confirmation as to whether your personal data is being processed and, if so:

   a) to access your personal data,
   b) to obtain information about the purposes of processing, the recipients or categories of recipients of such data, the planned retention period or the criteria for determining that period, the rights granted under the GDPR and the right to lodge a complaint with a supervisory authority, the source of such data, and automated decision-making, including profiling.
   c) Obtain a copy of their personal data.

2. Request rectification of data (Article 16 of the GDPR). Data subjects have the right to rectify and supplement the personal data they have provided. With respect to other personal data, they have the right to request rectification of such data (if it is inaccurate) and to have it supplemented (if it is incomplete).

3. Request the erasure of data pursuant to Article 17 of the GDPR. Data subjects have the right to request the erasure of all or some of their personal data if:

    a) The personal data is no longer necessary for the purposes for which it was collected or processed;
    b) the processing was based on consent, and that consent has been withdrawn;
    c) an objection has been raised to the use of the data for marketing purposes;
    d) the personal data is being processed unlawfully.

4. Notwithstanding a request to delete personal data due to an objection, the Controller may retain certain personal data to the extent necessary for the purposes of establishing, exercising, or defending legal claims, as well as to fulfill legal obligations. At , this applies in particular to personal data including: first name, last name, email address, and log history records of our Services, retained for the purpose of handling complaints and claims related to the use of services.

5. Requests to restrict data processing (based on Article 18 of the GDPR). Data subjects have the right to request the restriction of the use of their personal data in the following cases:

    a) when the accuracy of their personal data is disputed—in which case the Controller restricts its use for the time necessary to verify the accuracy of the data, but for no longer than 7 days,
    b) when the processing of data is unlawful, and instead of erasure, restriction of use has been requested;
    c) when the personal data is no longer necessary for the purposes for which it was collected or used, but is needed to establish, exercise, or defend legal claims;
    d) when an objection has been raised against the use of the data—in which case the restriction applies for the time necessary to assess whether, due to a specific situation, the protection of interests, rights, and freedoms outweighs the interests pursued by the Controller.

6. Right to data portability (Article 20 of the GDPR). Data subjects have the right to receive the personal data they have provided and then transmit it to another data controller of their choice. They also have the right to request that the personal data be transmitted directly to such another controller, provided this is technically feasible. In such a case, personal data may be transmitted in the form of files and document types that are commonly used, machine-readable, and allow the received data to be transferred to another data controller.

7. Objections to data processing under Article 21 of the GDPR. Data subjects have the right to object at any time to the use of their personal data if it is processed on the basis of the Controller's legitimate interest. If the objection is justified and there is no other legal basis for processing the personal data, it will be deleted with respect to the uses for which the objection was raised.

8. Withdrawal of consent to the processing of personal data. With regard to personal data processed on the basis of consent, you have the right to withdraw such consent. This right may be exercised by changing the settings in the User's profile to enable or disable consent for specific processing purposes, or by writing to the Data Controller at the email address provided at the beginning of this Policy.

9. Lodging a complaint with a supervisory authority (Article 77 of the GDPR). If data subjects believe that their right to the protection of personal data or other rights granted under the GDPR

have been infringed, they have the right to lodge a complaint with the President of the Personal Data Protection Office.

How long does the Controller take to comply with requests?

If, in the exercise of the rights listed above, the Controller receives a request, it will comply with or refuse to comply with it without delay, but no later than within one month of receiving it. However, if—due to the complex nature of the request or the number of requests—it is not possible to fulfill the request within one month, it will be fulfilled within the following two months, and the data subject will be informed in advance of the intended extension of the deadline.

XI. CHANGES TO THE PRIVACY POLICY

In line with technological developments and changes in legal regulations, the Administrator adapts the Privacy Policy accordingly, amending or supplementing its provisions as necessary.

Data subjects will be informed of any changes or additions by posting relevant information on the Website, and in the case of significant changes, by sending separate notifications to the provided email address.

This Privacy Policy does not limit any rights to which individuals are entitled under the service agreement or applicable laws.