PRIVACY AND COOKIES POLICY

Tedee E-Comerce

I. Foreword

This Privacy Policy and Cookie Policy set out the rules for the processing and protection of personal data provided by users, as well as the use of cookies and other technologies appearing on the Website and its subpages. For the purposes of this Policy, the term "Website" shall be understood to include all Tedee's e-commerce websites, namely:

- **www.tedee.com** (the main website),
- **www.tedee.com/shop** (the Tedee online store), and
- **proshop.tedee.com** (the B2B business store).

Any reference in this Policy to the "Website" should be construed as a reference to all of the above websites collectively.

II. Personal data controller

1. The controller of your personal data is Tedee spółka z ograniczoną odpowiedzialnością with its registered office in Warsaw (Karola Bohdanowicza Street 21/57, 02-127 Warsaw, Poland). Tedee sp. z o.o. is entered in the Register of Entrepreneurs of the National Court Register under number 0000712451 (District Court for the Capital City of Warsaw, 12th Commercial Division of the National Court Register), VAT ID (NIP): 7010795542, Business ID (REGON): 369188621, with a share capital of PLN 2,400,000. ("**Tedee**" or "**Controller**").

2. Tedee has not appointed a Data Protection Officer. For matters related to data protection, please contact us at e-mail: rodo@tedee.com or in writing to the Company's registered office address indicated above.

3. Personal data in accordance with this Privacy Policy is all information about an individual identified or identifiable by one or more factors, including device IP, location data, Internet ID and information collected through cookies and other similar technology.

4. Under the acronym GDPR is understood as the Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons in relation to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

III. Scope of personal data processed by the Controller

During your use of the Website, the Controller may process the following type of personal data:

a) Data you provide

In connection with the use of our website and services, you may be asked to provide your personal data. This primarily includes your name, contact details (e-mail address, phone number, shipping/billing address), and, in the case of purchases, also data necessary for the fulfillment of your order (e.g., delivery address, invoicing details including company name and VAT ID, if applicable).

You provide this data voluntarily, for example, when registering an account, placing an order in our online store, subscribing to our Newsletter, or filling in various contact forms on the website (general contact form, security vulnerability report form, product defect or hazard report form, cooperation/partnership form, etc.).

In these forms, we only collect the information that you choose to provide – usually such data as your name, e-mail address, phone number, and the content of your message or report (as well as any attachments you may include).

In the case of specialized forms, such as vulnerability reporting or product hazard reporting, we may also request information about the specific product (e.g., model, serial number, date and place of purchase) and a description of the problem/incident – however, this information relates to the product or incident, not directly to you, apart from your contact details as the reporting person.

b) Data collected automatically

During your visit to our website, certain data may be collected automatically through cookies and similar technologies. Such data may include, among others: the IP address of the device you are using, cookie identifiers, information about your browser and operating system, unique

device identifiers, as well as information about your activity on the website (e.g., pages viewed, time spent on the site, clicks on specific elements).

As a rule, this data does not allow us to identify you without additional information; however, it may be considered personal data if it is linked to you as an identified or identifiable user (e.g., when you have an account with us and cookie data is associated with it). Details regarding the use of cookies are provided in a later section of this Policy.

c) Data from communication:

If you contact us through the provided channels (e.g., by e-mail, telephone helpline, or social media), we will also process the information contained in such communication. This will primarily include identification and contact details (e.g., e-mail address, phone number, surname if it appears in the address or signature), as well as any personal data you include in the message content (e.g., order information, preferences, technical data regarding the reported issue, etc.). Such data will be used solely for the purpose of handling your message and resolving the matter you have raised.

IV. Purposes and bases of personal data processing by the Controller

1. Your personal data will be processed in order to:

a) Performance of a contract and provision of services

First and foremost, we process data in order to conclude and perform the contract to which you are a party, i.e., primarily for the operation of the Tedee online store – fulfilling your orders for devices and services, creating and maintaining your user account, delivering purchased products, handling potential returns, complaints, or warranty claims. This also includes ensuring the necessary functionalities of the website (e.g., maintaining the shopping cart, remembering login sessions) and ensuring the security of transactions and our platform (e.g., preventing hacking attacks or abuse).

Legal basis: Article 6(1)(b) GDPR (processing necessary for the performance of a sales contract or provision of a service).

b) Providing support and contacting you

We process your data in order to respond to inquiries submitted via contact forms (e.g., questions about our products, requests for an offer, business cooperation inquiries) and to

provide technical support or after-sales service. If you submit a query or report a problem, we use your data to get in touch with you and provide an answer or assistance.

Legal basis: Article 6(1)(f) GDPR, i.e., our legitimate interest in responding to your inquiry and ensuring a high quality of service (where the inquiry does not directly arise from a contract). However, if your inquiry relates to steps leading to the conclusion of a contract or the performance of an already concluded contract (e.g., asking about a product before purchase, requesting assistance with order fulfillment), the legal basis may also be Article 6(1)(b) GDPR (processing necessary at your request in connection with entering into/performance of a contract).

c) Handling security (vulnerability) reports and product defect/hazard reports

If you report a potential security vulnerability in our systems or products, or an incident or hazard related to our device (e.g., via the "Report Vulnerability" or "Report Product Hazard" form), we use the data you provide in order to analyze and address the reported vulnerability or hazard. We may need to contact you to obtain additional information or to inform you about the outcome of your report – however, we will only do so if you consent by selecting the relevant option in the form (e.g., by checking the box "I agree to be contacted for further clarification or corrective actions"). If you do not wish us to contact you, you can submit your report anonymously or without giving such consent – in that case, we will use the provided information solely for internal remediation and corrective measures, without responding back to you.

Legal basis: Article 6(1)(f) GDPR, i.e., our legitimate interest in ensuring the security of our products, services, and users' information. This interest includes the ability to receive and respond to security-related reports and, where consent has been given, to contact the reporting person for clarification or to provide thanks.

d) Newsletter and own marketing communication

If you subscribe to our Newsletter, we will process your data in order to send you e-mails containing information about our products, news, promotions, or tips (in line with the scope of consent provided at the time of subscription). When registering for the Newsletter, we ask you to provide your e-mail address and first name, as well as your country and preferred communication language – we use this information to personalize the content we send (e.g., ensuring you receive messages in the appropriate language).

Legal basis: Article 6(1)(b) GDPR – performance of the Newsletter service agreement, which you enter into with us when subscribing (we understand this as delivering the commercial information service you requested). In addition, to the extent that certain marketing communication may not be strictly necessary for the performance of this service, the legal basis is our legitimate interest (Article 6(1)(f) GDPR) in conducting direct marketing of our own products and services. Please note that you can unsubscribe from the Newsletter at any time – each e-mail contains a footer link allowing you to unsubscribe, or you can contact us directly regarding this matter.

e) Direct marketing to customers (own materials)

If you have purchased our products or otherwise use our services, we may, within the scope permitted by law, send you information about similar Tedee products or services (e.g., updates, complementary offers) to the e-mail address you provided. We carry out such activities based on our legitimate interest in direct marketing (Article 6(1)(f) GDPR).

However, we respect your privacy – if you do not wish to receive this type of communication, you may object (opt out) at any time. Each such message contains an appropriate link or unsubscribe instructions.

f) External marketing and analytics (advertising profiling, targeted ads)

With your prior consent, we may process your data for external marketing purposes, i.e., displaying targeted advertisements for our products on third-party websites and applications (e.g., on social media platforms), as well as analyzing the effectiveness of such ads and general marketing statistics. This is mainly done through cookies and marketing pixels operating on our website – if you consent to marketing cookies, our partners (e.g., Facebook/Meta, TikTok) may use them to collect information about your activity on our site and tailor ads shown to you later in their services. Analytical tools (e.g., Google Analytics) also operate only if you consent to analytical cookies – these tools collect statistical data on website traffic, helping us understand how users interact with the site and improve its features and offerings.

Legal basis: Article 6(1)(a) GDPR, i.e., the user's voluntary consent expressed through cookie settings (cookie banner) or another clear affirmative action (e.g., consent given in account settings). Without your consent, analytical or marketing cookies will not be activated.

g) Compliance with legal obligations

In certain situations, the law requires us to process your data. This mainly concerns accounting and tax obligations (e.g., storing sales documents and invoices containing your data – based on accounting and tax regulations) as well as obligations arising from warranty, guarantee, and consumer protection laws (e.g., handling complaints or contract withdrawals).

Legal basis: Article 6(1)(c) GDPR – compliance with a legal obligation to which we are subject. Data processed for these purposes will be stored for as long as required by the relevant regulations (details are provided in the section on retention periods).

h) Establishment, exercise, or defense of claims

We may also process your data where it is necessary to safeguard our legitimate interests in establishing, pursuing, or defending legal claims (e.g., in the event of a dispute, debt collection, or proceedings before law enforcement authorities or courts).

Legal basis: Article 6(1)(f) GDPR (the controller's legitimate interest in protecting its rights). Data will be used for this purpose only where necessary and for the period required by law (e.g., until the final resolution of the dispute).

V. Cookies and similar technologies

Our Website uses cookies and similar technologies (such as tracking pixels) to ensure its proper functioning and to improve your browsing experience. Cookies are small text files sent by a website and stored on your device (computer, smartphone, etc.) while browsing.

Categories of cookies used: during your first visit, we display a cookie banner that allows you to give consent for the use of specific categories of non-essential cookies. We use cookies for the following purposes:

- **Necessary (technical) cookies**: these are cookies required for the proper functioning of the website and available features, which is why they cannot be disabled in our consent panel (you can block them in your browser, but the website may then not work correctly). These cookies enable basic actions such as maintaining the user session after logging in, remembering the contents of the shopping cart, and adjusting the interface (e.g., language or currency selection). Without these cookies, our online store would not be able to provide you with services. Therefore, we rely on telecommunications

law provisions that allow the use of strictly necessary cookies (Article 173(3) of the Polish Telecommunications Law).

- **Functional cookies**: these are cookies that are not strictly necessary for the functioning of the website, but they make it easier to use and improve its functionality. They allow us to remember your preferences and settings (such as your selected country and site language, or preferred communication method), so that the website is better tailored to you on future visits. Functional cookies may also be used to integrate with external tools that facilitate website use – e.g., to display trust certificates and badges (such as our Trusted Shops certificate) or to operate a live chat, if available. We use these cookies only if you consent to them in the cookie settings. If you do not consent, personalized features and some services may be limited.

- **Analytical cookies**: this category of cookies allows us to collect anonymous statistics about visits and how our website is used. For this purpose, we use tools such as Google Analytics provided by Google Ireland Ltd. Analytical cookies collect information such as the number of visitors, traffic sources, time spent on the site, clicks on specific elements, etc. This data helps us understand which content and features are popular and which need improvement. We process this aggregated data to improve the structure and content of the website. These cookies are only activated with your consent. You can enable or disable them via our cookie management banner. If you do not consent, analytics will not be carried out and your visit will not be included in Google Analytics statistics.

- **Marketing (advertising) cookies**: these cookies are used for marketing purposes, including ad profiling. With them, we and our advertising partners can present you with ads tailored to your interests – both on our site and elsewhere (e.g., on social media platforms such as Facebook, Instagram, or TikTok, as well as within the Google advertising network). Marketing cookies enable remarketing, i.e., showing you our ads when you visit other sites based on the fact that you have already visited our site or viewed specific products. They also allow us to measure the effectiveness of campaigns (e.g., checking if you clicked on an ad and made a purchase). Such cookies are implemented through our partners' marketing tools, including: Facebook Pixel (Meta Platforms Ireland Ltd.), TikTok Pixel (TikTok Information Technologies UK Ltd.), Google Ads/AdWords (Google Ireland Ltd.), and Awin network cookies (an affiliate

network used to settle commissions with partners referring customers to our store). Marketing cookies are used only with your consent. If you do not consent, we will not load these tools in your browser, and the ads you see (ours and those of other companies) may be less tailored to your preferences.

Cookie lifespan

Cookies may be stored on your device for varying periods of time. We use both session cookies, which exist until you close your browser (after which they are automatically deleted), and persistent cookies, which remain on your device for a specified period or until you manually delete them. The exact storage times of individual cookies depend on their purpose and are defined in the settings of the relevant tool (e.g., Google Analytics cookies may be stored for up to 14 months, Facebook Pixel cookies typically for 90 days, etc.). You can also find information about storage periods in your browser settings or in the privacy policies of our partners.

Managing cookies

You have full control over cookies. During your first visit, you can adjust your preferences using our cookie banner (accept all, reject all, or choose individual categories). You can also change your decisions at any time – a link to cookie settings is available in the footer of our website, allowing you to reopen the consent management panel and modify your choices. In addition, you can manage cookies through your web browser settings – most browsers allow you to block cookies from all or selected websites, as well as delete cookies that have already been stored. Please note, however, that blocking necessary cookies may result in our website not functioning properly, and some features may become unavailable. Detailed instructions for configuring cookies in the most popular browsers can be found in the help sections of those browsers (e.g., for Chrome, Firefox, Safari, Edge – cookie management instructions are available on their official websites).

VI. Contact and reporting forms

Our websites provide various forms that allow you to share information or requests with us. Data collected through these forms is processed solely for the purposes for which the forms are made available and includes only the data you voluntarily provide. Below we describe the key forms and how we use the data collected through them:

a) General contact form (e.g., “How can we help?”, “Contact us”)

This form allows you to send us a message on any matter – e.g., a product inquiry, a request for technical support, or feedback. In this form, we usually ask for your name, e-mail address, phone number, as well as the subject and content of your message. This data is used solely to contact you and respond to your inquiry. In some cases, the form may also include additional consent options for marketing communication ("Receive feedback requests and customer service information").

If you check this option, you agree that we may later send you, for example, surveys to evaluate our services or additional information about our offerings. This is optional – if you do not provide this consent, we will not use your data from this form for any purpose other than replying to your current message.

The legal basis for processing data from the contact form is our legitimate interest in responding (Article 6(1)(f) GDPR), and for any optional marketing consent – Article 6(1)(a) GDPR (consent, which you can withdraw at any time).

b) Vulnerability report form ("Report Vulnerability")

This form is used by experts or users to report potential security vulnerabilities in our systems or applications. We ask for contact details (although you may also report anonymously by providing only a pseudonym or a reply-only e-mail address) and a description of the problem (e.g., whether it concerns an application, technical details, steps to reproduce the issue, etc.).

Contact details are used solely for communication regarding the report – for example, to confirm receipt, thank you for the information, request clarification, or provide feedback on the resolution.

If you do not wish to be contacted, you may omit identifying details (e.g., write "N/A" in the name field and provide an anonymous e-mail if you wish). We will still accept and review such reports. The legal basis is our legitimate interest (Article 6(1)(f) GDPR) in maintaining the security of our systems and networks. Data from this form (particularly contact details of the reporter) is not made public without the reporter's consent. However, we may publish information about the identified vulnerability and its remediation (without personal data of the reporter), in line with our transparency policy.

c) Product hazard/defect report form ("Report Product Hazard")

This form allows you to report any safety incidents or defects related to the use of our hardware products (e.g., if you notice that a device is malfunctioning in a potentially hazardous way). The form requires basic contact details (name, e-mail, phone number) as well as product information (model, serial number if available, purchase date and place) and a description of the incident/risk. Contact details will be used to reach out to you if necessary to gather additional information, provide corrective instructions, or inform you about the outcome (e.g., whether the product requires servicing, whether the issue is already known, etc.). Data is processed based on our legitimate interest (Article 6(1)(f) GDPR) in ensuring product safety and customer protection, as well as fulfilling product safety monitoring obligations. In addition, such reports may help us meet legal obligations regarding product safety (e.g., reporting duties towards market surveillance authorities if the report concerns a serious risk) – in this respect, the additional legal basis may be Article 6(1)(c) GDPR (compliance with a legal obligation). The form also includes an optional consent field for feedback – similar to vulnerability reports, we respect your choice and will contact you only if you provide such consent.

d) Cooperation/partnership forms ("Become a partner", "Cooperation contact")

If you are interested in business cooperation with Tedee (e.g., becoming our distributor, integrator, or partner), you may use a dedicated form. We ask for information identifying you and your company (e.g., name, e-mail, company name, position, phone number) as well as a description of your cooperation proposal. This data will be used to evaluate your proposal and to contact you for further discussions. The legal basis is taking steps at your request prior to entering into a potential cooperation agreement (Article 6(1)(b) GDPR) or our legitimate interest in establishing and maintaining business relations (Article 6(1)(f) GDPR). Data from these forms is not used for marketing purposes unrelated to the proposed cooperation, unless you separately consent to it.

All of the above form data is provided voluntarily. However, providing certain information may be necessary for us to take the action you request. Mandatory fields are marked with an asterisk (*) – failure to complete them may prevent us from contacting you or processing your report. We ensure that data collected through the forms is not used for purposes other than those stated (unless we obtain your separate consent for additional purposes).

VII. Data recipients

As part of providing our services and operating the website, we work with various external entities to whom we may transfer your data – always on the basis of an appropriate data processing agreement or when they act as independent controllers under the law or your consent. We ensure that only the data necessary to perform a given service is shared. Below are the main categories of recipients of your personal data:

a) **Hosting and IT infrastructure providers:** your data on the website and store is stored on secure servers of external hosting companies we use. Currently, our hosting providers include SiteGround Spain S.L. and Convesio – these entities provide the server infrastructure for our site (storing the website database, files, backups, etc.). They may potentially access your data stored on the servers (e.g., account or order data) but process it solely on our instructions and for the purpose of ensuring the continuous operation of the service.

b) **CDN and security provider:** we use Cloudflare, Inc. (USA) to improve website speed and security (Content Delivery Network, DDoS protection, etc.). This means that all requests to our website go through Cloudflare's globally distributed servers. As a result, Cloudflare may process your IP address and other technical connection data as part of traffic filtering and acceleration. Cloudflare acts as a processor on our behalf and is bound by Standard Contractual Clauses (see the section on transfers outside the EEA). Cloudflare may also use necessary cookies for security purposes (e.g., to recognize malicious traffic); however, these are technical cookies essential for the secure functioning of the service.

c) **Analytics providers:** to collect statistics and analyze website traffic, we use Google Analytics (provided by Google Ireland Limited). Google may have access to the data collected via Google Analytics cookies (if you consent to them). This data (e.g., your IP address – shortened/anonymized, device identifier, website usage events) is processed by Google on our behalf to prepare aggregated reports and statistics for us. We have signed a data processing agreement with Google. However, note that Google may also use the collected data for its own purposes (e.g., service improvement, if permitted by their policy – in aggregated form). You can find Google's Privacy Policy here: https://policies.google.com/privacy. Important: we use settings that anonymize your IP address (shortened before storage on servers) to further protect your privacy.

d) **Marketing and advertising partners:** our website includes marketing tools that, with your consent, collect data for ad profiling and remarketing. Accordingly, recipients of some of your data may include:

- Meta Platforms Ireland Ltd. – provider of Facebook Pixel and related Facebook/Instagram Ads tools. With your consent to marketing cookies, information about your activity on our site (e.g., products viewed, purchases made) may be transmitted to Meta and used to target our ads on Facebook and Instagram. Meta may combine this data with your Facebook/Instagram profile data (if you are logged in) and act as an independent controller in line with its privacy policy. We do not share personal identifiers (like your name or e-mail) with Meta, only online identifiers and browser events. Meta's Privacy Policy: https://www.facebook.com/privacy/explanation

- TikTok Information Technologies UK Ltd. – provider of TikTok Pixel, used for displaying Tedee ads on TikTok. Similarly, if you consent, events from your visit (e.g., browsing, clicks, purchases) may be shared with TikTok to personalize ads. TikTok may act as a joint controller of this data, processing it according to its Privacy Policy: https://www.tiktok.com/legal/page/global-privacy-policy

- Google Ireland Ltd. – in connection with Google Ads/AdWords and Google Tag Manager, which may be used for remarketing and tracking ad conversions. For example, if you came to our site by clicking a Google ad, the conversion tracking tool (Google Ads) saves an identifier linking your visit/purchase to that ad (helping us assess ad effectiveness). With marketing cookies enabled, we may also use Google functions to display our ads on other sites (Google Display Network) based on products you viewed with us (remarketing). Google's Privacy Policy: https://policies.google.com/privacy

- Awin AG – affiliate marketing partner. Awin is an affiliate network we work with to reward partners (publishers) who refer customers to our store. If you visit us via an affiliate link (e.g., from an external review site), a cookie identifying this situation is stored in your browser. If you make a purchase, Awin may receive transaction details (order value, referrer partner ID, possibly your order ID) to calculate partner commissions. We do not share your contact or personal details with Awin – only the minimum required for affiliate settlement. Awin acts as an independent controller

of affiliate network data. More on Awin's data processing: https://www.awin.com/pl/polityka-prywatnosci

- Other advertising and social partners: our site may include buttons linking to social media (Facebook, Instagram, Twitter, LinkedIn, etc.) or embedded content (e.g., a YouTube video). Clicking such buttons or playing embedded content may result in some data being transferred to the respective external providers (e.g., that you visited our website). Simply browsing our site does not transmit your data to these services unless you interact with them. Once you do, processing is governed by the respective providers' privacy policies (e.g., YouTube/Google, Facebook/Meta).

e) **CRM / customer support system provider:** for efficient customer service and contact management, we use HubSpot (HubSpot, Inc., USA or HubSpot Ireland Ltd.). HubSpot may process the data you provide in forms (e.g., contact form, reports) and your activity data on our site if linked (e.g., when you click a link in our email or visit our site from such an email – this may be recorded to track communication history). HubSpot acts as a processor on our behalf and complies with GDPR (including Standard Contractual Clauses approved by the European Commission). Data in HubSpot is used solely to manage our relationship with you (e.g., so we can view your inquiry history and preferences in one place) and, where applicable, to send marketing materials if you consented. HubSpot's Privacy Policy: https://legal.hubspot.com/privacy-policy.

f) **Newsletter/e-mail marketing provider:** for sending newsletters and bulk e-mails, we use FreshMail (FreshMail Sp. z o.o., Kraków, Poland). If you subscribed to our Newsletter, your e-mail (and any other details you provided during sign-up, such as your name) is stored on FreshMail's servers and used to send you our messages. FreshMail acts as a processor – processing your data only on our instructions and solely for Newsletter delivery. FreshMail ensures confidentiality and technical/organizational safeguards compliant with GDPR. We have a data processing agreement with FreshMail. FreshMail's Privacy Policy: https://freshmail.pl/polityka-prywatnosci/.

g) **Payment operators:** for online purchases via our store, payments are processed by external payment providers. This means that once you choose a payment method, you are redirected to a secure payment service (e.g., PayU, PayPal, Stripe, Przelewy24, or another available provider) to complete your payment. We do not process or store your payment card or financial details – these go directly to the chosen payment operator.

From the operator, we only receive confirmation of the transaction status (e.g., payment successful) and possibly your transaction ID in their system. The payment operator becomes an independent controller of your data in the context of processing the transaction – they apply their own terms and privacy policies, which you should review when choosing a payment method (these are usually provided during the payment process). We provide the payment operator only with the minimum data needed to identify the transaction (e.g., amount, order number, currency, selected product/service). If you require an invoice, we process your invoicing data ourselves, but the payment itself is handled by the operator.

h) **Courier/shipping companies:** to deliver purchased products, we work with logistics and courier companies (e.g., DHL, UPS, DPD, InPost, or others depending on your location and choice). For this purpose, we provide the courier with the necessary delivery details: recipient's name, delivery address, contact phone number (so the courier can reach you), and possibly e-mail (for parcel tracking notifications). The courier processes this data as an independent controller for the delivery service (based on the contract with you or us). Courier companies are obliged to protect this data and use it only for delivery purposes.

i) **Partners operating review and trust programs:** we value customer feedback and participation in purchase protection programs. Therefore, after completing an order, some of your basic data may be shared with partners operating such programs, but only where the service is explicitly used or linked to your purchase. For example:

   - If you choose to leave a review on Trustpilot, we may share your email address and details of your purchase with Trustpilot A/S (Copenhagen, Denmark), so that they can invite you to provide feedback about our store. Trustpilot acts as an independent data controller and will process your personal data in accordance with its own Privacy Policy (available on their website). Similarly, if after your purchase you request to leave a review via the Trustpilot system, our store may initiate the sending of such an invitation to you.

j) **Entities providing legal, audit, and consultancy services:** where necessary, we may share your data with our legal advisors, law firms, or auditing entities, but only to the extent required and in connection with specific purposes (e.g., pursuing claims, consulting on legal obligations, compliance audits). These entities are bound by

professional or contractual confidentiality obligations and are required to ensure the protection of your data.

k) **Public authorities:** we may disclose your personal data to competent state or judicial authorities if they request it on a valid legal basis. This may include, for example, the police, prosecutor's office, courts, tax authorities, or the data protection supervisory authority (PUODO). In such cases, we are obliged to provide the data pursuant to a legal requirement. We always verify that the request is legally justified and disclose no more data than necessary.

Data transfers within a corporate group: currently, Tedee sp. z o.o. is not part of an international corporate group that would involve intra-group data transfers. If, in the future, your data is to be shared with related entities (e.g., subsidiaries, strategic partners), we will inform you accordingly and ensure a proper legal basis and adequate safeguards for such transfer.

VIII. Data transfers outside the EEA

As a rule, we store your personal data within the European Economic Area (EEA), where our main service providers are also located (e.g., hosting servers in the EU, databases in the EU). However, when using certain tools and services, your data may be transferred to countries outside the EEA (so-called third countries). In particular, this may concern:

- **United States (USA):** some of our providers are based in the USA or have servers located there (e.g., Cloudflare, HubSpot, some Google or Meta servers may be located in the USA). In such cases, the transfer of data to the USA takes place on the basis of the Standard Contractual Clauses approved by the European Commission, which oblige the recipient in the USA to protect the data in line with EU standards. In addition, where possible, we apply supplementary security measures (e.g., data encryption, IP anonymization in Google Analytics). Note: in July 2023, the European Commission adopted an adequacy decision for the EU–US Data Privacy Framework, which may apply to some of our U.S. providers (if they have joined the program). We will rely on this mechanism if it covers the relevant recipient and your data transfer – meaning that data may be transferred to entities certified under the Privacy Framework, ensuring compliance with EU requirements.

- **United Kingdom (UK):** some marketing data may be transferred to TikTok Information Technologies UK Ltd. (due to the use of TikTok Pixel). Following Brexit, the UK is treated as a third country; however, it currently benefits from an adequacy decision of the European Commission, confirming that UK law provides a level of protection equivalent to the EU GDPR. This means that data transfers to the UK may take place as if within the EEA – without additional authorizations.

- **Other countries outside the EEA:** when using social media or global tools, your data may occasionally be transferred to other third countries (e.g., Switzerland – headquarters of Awin AG; or other data center locations of global service providers). In each case, we ensure that such transfers take place in accordance with Chapter V of the GDPR, i.e., with the application of appropriate safeguards (e.g., Standard Contractual Clauses, Binding Corporate Rules, or – where applicable – based on an exception under Article 49 GDPR). If you would like to obtain a copy of the safeguards applied or information on where your data has been made available, please contact us.

We always make sure that every data transfer outside the EEA complies with the law – in particular, we transfer data only to recipients that guarantee an adequate level of protection. Your rights and the security of your data remain our priority also in the context of international transfers.

IX. Data retention periods

We process your personal data no longer than necessary for the purposes for which it was collected. This means that retention periods vary depending on the type of data and the purpose of processing. Below are the main rules regarding data retention:

- **Data processed for the performance of a contract (sales/services**): data related to fulfilling your orders, contracts, and the provision of services (e.g., purchase information, account data, transaction history) will be stored for the duration of the contract and until the expiry of potential claims arising from it. Under applicable civil law, the standard limitation period for claims is currently 6 years (for property-related claims, including sales contracts, with some exceptions), while claims for periodic benefits and those related to business activity expire after 3 years. Some consumer claims (e.g., warranty claims) may be pursued within 2 years of product delivery. In practice, for legal security, we may store sales-related data for up to 6 years from the

end of the calendar year in which the contract was performed (this is also often required by tax law – see below). After this period, the data may be archived (if needed for statistical purposes) or permanently deleted/anonymized.

- **Financial and accounting data**: documents containing your data that constitute accounting records (e.g., VAT invoices, receipts) must be stored for 5 tax years from the end of the financial year in which the document was issued. For example, invoices from 2025 must be stored until the end of 2030. This retention period arises from accounting and tax regulations. Legal basis: Article 74 of the Accounting Act, Article 86 of the Tax Ordinance. After this period, documents are deleted or anonymized in line with procedures.
- **Data processed based on legitimate interest**: if we process your data on the basis of our legitimate interest (Article 6(1)(f) GDPR) – e.g., for customer support, own marketing, or securing claims – we will store it until such interest no longer exists or you effectively object. This means that:
    - data used for ongoing communication with you (e.g., e-mail correspondence, CRM data) is stored as long as necessary to handle your case, and after communication ends, it may be archived for the limitation period of claims (as above) or shorter if further retention is not required;
    - data used for direct marketing (e.g., customer e-mail address for information about similar products) is stored until you object or unsubscribe from such messages (or until our interest ceases, e.g., if we stop offering those products);
    - data processed for IT security purposes (system logs, incident data) is stored for up to 2 years from collection, unless exceptionally required for longer (e.g., logs related to a major incident may be stored until claims related to it expire).
- **Data processed on the basis of consent: if the legal basis for processing your data is your consent (Article 6(1)(a) GDPR)** – this applies, for example, to external marketing (marketing cookies), the Newsletter, or other optional consents – we will process the data until you withdraw your consent. You have the right to withdraw consent at any time (e.g., by unsubscribing from the newsletter, changing cookie settings). Withdrawal of consent does not affect the lawfulness of processing before its withdrawal. After consent is withdrawn, data may be retained in a limited scope solely to demonstrate compliance (i.e., proof that we had your consent and that you withdrew it, which is our legal obligation under GDPR – such metadata on consent may be stored for up to 5 years for audit purposes).

- **Newsletter data**: if you are a Newsletter subscriber, your data will be processed for as long as the Newsletter service is provided, i.e., until you unsubscribe (cancel the subscription). After unsubscribing (withdrawal of consent/termination of the agreement), your data may be stored for a short time to document the withdrawal of consent (see above) or possibly longer if linked with our other systems (e.g., if you are also a registered customer). In such a case, we may retain the information that you do not wish to receive the Newsletter to avoid accidental mailings in the future (so-called internal "opt-out list").
- **Special retention periods:** for certain categories of data, specific retention periods apply under the law. For example:
    - Complaint data – we must store complaint documentation for at least 1 year after resolution (under the Consumer Rights Act). In practice, for evidential purposes, we may keep complaint correspondence and data for the limitation period of claims (up to 6 years, as with contracts).
    - Product safety reports – if a report concerns an issue that may trigger legal obligations (e.g., notifying market surveillance authorities, corrective actions), documentation may be stored for the period required by product safety laws (at least for the product's lifetime or the statutory period necessary to demonstrate compliance).
    - System logs – general server logs (HTTP connection records) are usually stored for 30 days (for security and error diagnostics) and then automatically overwritten or deleted. Exceptions apply to logs linked to significant security events, which may be stored longer as noted above.

After the above retention periods, your data is deleted or anonymized (i.e., irreversibly de-identified so it can no longer be linked to you). Anonymized information may still be used for statistical, analytical, or reporting purposes – but it will no longer constitute personal data.

X. Your rights

You have certain rights in connection with the processing of your personal data. Below we outline these rights together with explanations:

- **Right of access** – you have the right to obtain confirmation from us as to whether we are processing your personal data and, if so, to access that data along with information on,

for example, the purposes, scope, and methods of processing. At your request, we will provide you with a copy of your personal data being processed (the first copy is free of charge; for additional copies, we may charge an administrative fee in accordance with the GDPR).

- **Right to rectification** – you have the right to request without undue delay the correction of inaccurate personal data concerning you, as well as to have incomplete data completed (taking into account the purposes of processing). If you notice that any of your data is incorrect or has changed (e.g., surname, address), please contact us – we will update it.
- **Right to erasure ("right to be forgotten")** – you have the right to request the deletion of your personal data in the cases provided for in Article 17 GDPR, including when the data is no longer needed for the purposes for which it was collected, when you withdraw consent (and there is no other legal basis for processing), or when you have lodged an effective objection and there are no overriding legitimate grounds for processing. Please note that the right to erasure is not absolute – in certain situations we may not be able to delete your data immediately, for example where processing is necessary to comply with a legal obligation (e.g., we cannot delete transaction history while the law requires us to retain it) or to establish or defend legal claims. In all cases, we will inform you whether your request has been fulfilled or explain the reasons why it cannot be fully met.
- **Right to restriction of processing** – you have the right to request that we temporarily restrict the processing of your data (other than storing it) in the cases specified in Article 18 GDPR. This applies, for example, when you contest the accuracy of the data (for the time needed to verify it), when you believe we are processing data unlawfully but do not want it erased, or when you have lodged an objection – until it is determined whether our legitimate grounds override your objection. If processing is restricted, we will only store your data and carry out other operations solely with your consent, or for the establishment, exercise or defence of legal claims, or to protect the rights of another person, or for important public interest reasons.
- **Right to data portability** – insofar as we process your data on the basis of your consent (Article 6(1)(a)) or on the basis of a contract (Article 6(1)(b)) and by automated means, you have the right to receive your data from us in a structured, commonly used, machine-readable format (e.g., CSV, JSON, XML) and to transmit it to another controller. You also have the right to request that we transmit such data directly to another controller of your choice, where technically feasible. This right applies only to data you have provided

to us, for example via a form or account. It does not cover our internal assessments or derived data.

- **Right to object** – you have the right at any time to object to the processing of your personal data carried out on the basis of our legitimate interests (Article 6(1)(f)), including profiling on this basis.
    - **Objection based on your particular situation**: if you raise such an objection, we must cease processing the data covered by the objection, unless we can demonstrate compelling legitimate grounds for processing that override your interests, rights, and freedoms, or grounds for the establishment, exercise, or defence of legal claims.
    - **Objection to direct marketing**: if your data is processed for direct marketing purposes (e.g., sending marketing emails), you have the unconditional right to object at any time – in which case we will immediately stop such processing. You can raise an objection, for example, by email. For marketing emails, the simplest way to object is to click the unsubscribe link provided in the footer of each message – this is equivalent to an objection to further marketing.
- **Right to withdraw consent** – where processing is based on your consent, you have the right to withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal (i.e., up until consent is withdrawn, processing remains lawful). Once withdrawn, we will cease processing your data for the purpose for which consent was given. For example: if you withdraw consent to marketing cookies, we will stop collecting data for those purposes and remove/disable such cookies; if you withdraw consent to receiving the Newsletter, we will stop sending you emails. You can withdraw consent in the same way as it was given (e.g., by changing settings on our site, clicking the link in an email, or emailing us with a withdrawal notice).

How to exercise your rights

You may contact us in any convenient way – preferably by sending an e-mail to GDPR@tedee.com or in writing to our registered office address (as indicated above). You may also use the contact form available on our website. Please specify in your request which right and which data it concerns, to help us process it correctly and promptly. We reserve the right, in case of doubt as to the identity of the requesting person, to ask for additional information to confirm identity (this is to protect your data from being disclosed to an unauthorized person).

We aim to respond to your requests without undue delay, and no later than within one month of receipt. This period may be extended by a further two months if necessary (we will inform you of the extension and reasons for the delay). The exercise of most rights is free of charge. Only in cases of manifestly unfounded or excessive requests (e.g., repetitive requests made very frequently) may we, in accordance with the GDPR, refuse to act or charge a reasonable fee (you will be informed in advance in such cases).

Right to lodge a complaint with a supervisory authority –
If you believe that we are processing your data in breach of applicable laws, you have the right to lodge a complaint with the relevant supervisory authority for data protection. In Poland, this is the President of the Personal Data Protection Office (PUODO). Address: ul. Stawki 2, 00-193 Warsaw. Detailed information on how to file a complaint can be found on the authority's website: https://uodo.gov.pl/

However, before taking this step, we encourage you to contact us – we will do our best to clarify any concerns and resolve the matter amicably.

XI. Voluntary provision of data

Providing your personal data is voluntary; however, in many cases it is a condition for using our services or website features. This means that if you do not provide the required data, we will not be able to carry out certain actions:

- **Account and orders**: providing the data marked as mandatory during account registration or when placing an order (e.g., first name, last name, delivery address, e-mail, phone number) is necessary for us to accept and process your order. Without this data, purchasing products in our online store will not be possible.
- **Contact forms**: in contact forms, we usually require at least contact details (e.g., e-mail address) and a short description of your inquiry – without this we would not be able to respond to your message. Providing additional details in the message is voluntary but may help us provide a complete answer.
- **Service/safety reports**: providing contact details in product or safety reports is not mandatory; however, if you do not provide them, we will not be able to inform you of the outcome of the analysis or ask for further details – your report will be processed anonymously based on the available information.

- **Newsletter**: providing an e-mail address (and confirming your subscription) is required to receive the Newsletter. Without it, we cannot send you messages, and without your consent we cannot add you to our subscriber list.

In all cases where we collect your data, we indicate which fields/information are necessary (marked, for example, with an asterisk). Other data is optional – it may be helpful, but its omission will not have negative consequences.

Please note that if you provide us with data of third parties (e.g., naming another person as the delivery recipient, recommending our product to a friend, etc.), you may only do so with their consent and within the limits permitted by law. In such cases, it is your responsibility to inform the person about sharing their data and to acquaint them with this Privacy Policy.

XII. Automated decision-making and profiling

We want to assure you that you are not subject to decisions based solely on automated processing that would produce legal effects concerning you or similarly significantly affect you (i.e., we do not apply fully automated decisions, without human involvement, that would materially impact your rights).

Some of your data may be subject to profiling, but only in a way that does not produce legal effects or significantly affect you. The profiling we carry out involves, for example, automated analysis or prediction of your preferences based on your browsing history on our website (using cookies) – this allows us to tailor ads or offers to what might interest you. Such profiling is carried out on the basis of your consent (for marketing cookies) or our legitimate interest (our own marketing toward existing customers) and is intended primarily to better match marketing content to your needs. However, we do not make any decisions based on profiling that would have serious consequences for you – e.g., we do not refuse to conclude a contract with you or differentiate prices solely on the basis of profiling data.

If in the future we were to make any significant decisions in an automated way, you would be informed about this separately, and we would provide you with the possibility to contest such a decision and obtain human intervention, in accordance with Article 22 GDPR.

XIII. Updates and changes to this Privacy Policy

We make every effort to ensure that this Privacy Policy accurately reflects the actual processing of personal data within our website and business activities. As our services evolve and in response to legal or technological developments, the content of this Policy may change. We will inform you in advance of any material changes to the Policy by means of a notice on our website or, where relevant to the services you use (e.g., the Newsletter), by email.

The current version of this Privacy Policy is always available on our website (under the "Privacy Policy" section). Each version is marked with its effective date. We encourage you to review the Policy regularly to stay informed about any updates.

Version history:

- Rev. 1.0 – April, 1, 2022
- Rev. 1.1 – August, 22, 2025