

# MerchBee Privacy Policy

This applies to all MerchBee products, platforms, training, courses and services.

## Privacy Policy and GDPR Compliance Policy

Last updated: May 23<sup>rd</sup> - Website privacy notice

### 1. INTRODUCTION

This privacy notice provides you with details of how we collect and process your personal data through your use of our merchbee.com websites.

This applies to all MerchBee websites. By providing us with your data, you warrant to us that you are over 13 years of age. MerchBee is the data controller and we are responsible for your personal data (referred to as “we”, “us” or “our” in this privacy notice).

#### Contact Details

Our full details are:

Full name of legal entity: MerchBee LLC

Email address: [hello@merchbee.com](mailto:hello@merchbee.com)

Postal address: 830 International Dr, Orlando, Florida, 32827

It is very important that the information we hold about you is accurate and up to date. Please let us know if at any time your personal information changes by emailing us at [hello@merchbee.com](mailto:hello@merchbee.com).

### 2. WHAT DATA DO WE COLLECT ABOUT YOU, FOR WHAT PURPOSE AND ON WHAT GROUND WE PROCESS IT

Personal data means any information capable of identifying an individual. It does not include anonymised data.

We may process the following categories of personal data about you:

Communication Data that includes any communication that you send to us whether that be through the contact form on our website, through email, text, social media messaging, social media posting or any other communication that you send us. We process this data for the purposes of communicating with you, for record keeping and for the establishment, pursuance or defence of legal claims. Our lawful ground for this processing is our legitimate interests which in this case are to reply to communications sent to us, to keep records and to establish, pursue or defend legal claims.

Customer Data that includes data relating to any purchases of goods and/or services such as your name, title, billing address, delivery address email address, phone number, contact details, purchase details and your card details. We process this data to supply the goods and/or services you have purchased and to keep records of such transactions. Our lawful ground for this processing is the performance of a contract between you and us and/or taking steps at your request to enter into such a contract.

User Data that includes data about how you use our website and any online services together with any data that you post for publication on our website or through other online services. We process this data to operate our website and ensure relevant content is provided to you, to ensure the security of our website, to maintain back-ups of our website and/or databases and to enable publication and administration of our website, other online services and business. Our lawful ground for this processing is our legitimate interests which in this case are to enable us to properly administer our website and our business.

Technical Data that includes data about your use of our website and online services such as your IP address, your login data, details about your browser, length of visit to pages on our website, page views and navigation paths, details about the number of times you use our website, time zone settings and other technology on the devices you use to access our website. The source of this data is from our analytics tracking system. We process this data to analyse your use of our website and other online services, to administer and protect our business and website, to deliver relevant website content and advertisements to you and to understand the effectiveness of our advertising. Our lawful ground for this processing is our legitimate interests which in this case are to enable us to properly administer our website and our business and to grow our business and to decide our marketing strategy.

Marketing Data that includes data about your preferences in receiving marketing from us and our third parties and your communication preferences. We process this data to enable you to partake in our promotions such as competitions, prize draws and free give-aways, to deliver relevant website content and advertisements to you and measure or understand the effectiveness of this advertising. Our lawful ground for this processing is our legitimate interests which in this case are to study how customers use our products/services, to develop them, to grow our business and to decide our marketing strategy.

We may use Customer Data, User Data, Technical Data and Marketing Data to deliver relevant website content and advertisements to you (including Facebook adverts or other display advertisements) and to measure or understand the effectiveness of the advertising we serve you. Our lawful ground for this processing is legitimate interests which is to grow our business. We may also use such data to send other marketing communications to you. Our lawful ground for this processing is either consent or legitimate interests (namely to grow our business).

[NOTE SEE SECTION 4 BELOW]

**Sensitive Data** We do not collect any Sensitive Data about you. Sensitive data refers to data that includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data. We do not collect any information about criminal convictions and offences.

Where we are required to collect personal data by law, or under the terms of the contract between us and you do not provide us with that data when requested, we may not be able to perform the contract (for example, to deliver goods or services to you). If you don't provide us with the requested data, we may have to cancel a product or service you have ordered but if we do, we will notify you at the time.

We will only use your personal data for a purpose it was collected for or a reasonably compatible purpose if necessary. For more information on this please email us at [hello@merchbee.com](mailto:hello@merchbee.com). In case we need to use your details for an unrelated new purpose we will let you know and explain the legal grounds for processing. We may process your personal data without your knowledge or consent where this is required or permitted by law.

We may carry out automated decision making or any type of automated profiling.

For example if you engage with a marketing campaign - and we see you have already purchased product A, we will not offer you product A but instead product B.

This is the only kind of automated decision making.

### 3. HOW WE COLLECT YOUR PERSONAL DATA

We may collect data about you by you providing the data directly to us (for example by filling in forms on our site or by sending us emails). We may automatically collect certain data from you as you use our website by using cookies and similar technologies. Please see our cookie policy for more details about this, below on this page.

We may receive data from third parties such as analytics providers such as Google based outside the EU, advertising networks such as Facebook based outside the EU, such as search information providers such as Google based outside the EU, providers of technical, payment and delivery services, such as data brokers or aggregators.

We may also receive data from publicly available sources such as Companies House and the Electoral Register based inside the EU.

### 4. MARKETING COMMUNICATIONS

Our lawful ground of processing your personal data to send you marketing communications is either your consent or our legitimate interests (namely to grow our business).

Under the Privacy and Electronic Communications Regulations, we may send you marketing communications from us if (i) you made a purchase or asked for information from us about our goods or services or (ii) you agreed to receive marketing communications and in each case you have not opted out of receiving such communications since. Under these regulations, if you are a limited company, we may send you marketing emails without your consent. However you can still opt out of receiving marketing emails from us at any time. Before we share your personal data with any third party for their own marketing purposes we will get your express consent.

You can ask us or third parties to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you OR by emailing us at [hello@merchbee.com](mailto:hello@merchbee.com) at any time.

If you opt out of receiving marketing communications this opt-out does not apply to personal data provided as a result of other transactions, such as purchases, warranty registrations etc.

### 5. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with the parties set out below:

- Other companies in our group who provide services to us.
- Service providers who provide IT and system administration services.
- Professional advisers including lawyers, bankers, auditors and insurers
- Government bodies that require us to report processing activities.

Service providers for marketing technology and payment processing etc.

Third parties to whom we sell, transfer, or merge parts of our business or our assets. We require all third parties to whom we transfer your data to respect the security of your personal data and to treat it in accordance with the law. We only allow such third parties to process your personal data for specified purposes and in accordance with our instructions.

## 6. INTERNATIONAL TRANSFERS

We share your personal data within our group of companies which involves transferring your data outside the European Economic Area (EEA). We are subject to the provisions of the General Data Protection Regulations that protect your personal data. Where we transfer your data to third parties outside of the EEA, we will ensure that certain safeguards are in place to ensure a similar degree of security for your personal data. As such: We may transfer your personal data to countries that the European Commission have approved as providing an adequate level of protection for personal data by; or If we use US-based providers that are part of EU-US Privacy Shield, we may transfer data to them, as they have equivalent safeguards in place; or Where we use certain service providers who are established outside of the EEA, we may use specific contracts or codes of conduct or certification mechanisms approved by the European Commission which give personal data the same protection it has in Europe. If none of the above safeguards is available, we may request your explicit consent to the specific transfer. You will have the right to withdraw this consent at any time.

## 7. DATA SECURITY

We have put in place security measures to prevent your personal data from being accidentally lost, used, altered, disclosed, or accessed without authorisation. We also allow access to your personal data only to those employees and partners who have a business need to know such data. They will only process your personal data on our instructions and they must keep it confidential. We have procedures in place to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach if we are legally required to.

## 8. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. When deciding what the correct time is to keep the data for we look at its amount, nature and sensitivity, potential risk of harm from unauthorised use or disclosure, the processing purposes, if these can be achieved by other means and legal requirements.

For tax purposes the law requires us to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they stop being customers. In some circumstances we may anonymise your personal data for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

## 9. YOUR LEGAL RIGHTS

Under data protection laws you have rights in relation to your personal data that include the right to request access, correction, erasure, restriction, transfer, to object to processing, to portability of data and (where the lawful ground of processing is consent) to withdraw consent. You can see more about these rights at: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/> If you wish to exercise any of the rights set out above, please email us at [hello@merchbee.com](mailto:hello@merchbee.com). You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive or refuse to comply with your request in these circumstances. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you.

If you are not happy with any aspect of how we collect and use your data, you have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues ([www.ico.org.uk](http://www.ico.org.uk)). We should be grateful if you would contact us first if you do have a complaint so that we can try to resolve it for you.

## 10. THIRD-PARTY LINKS

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

## 11. COOKIES

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see below on this page.

# Cookie Policy

## COOKIE POLICY

### What's a cookie?

A "cookie" is a piece of information that is stored on your computer's hard drive and which records how you move your way around a website so that, when you revisit that website, it can present tailored options based on the information stored about your last visit. Cookies can also be used to analyse traffic and for advertising and marketing purposes. Cookies are used by nearly all websites and do not harm your system.

If you want to check or change what types of cookies you accept, this can usually be altered within your browser settings. You can block cookies at any time by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.

### How do we use cookies?

We use cookies to track your use of our website. This enables us to understand how you use the site and track any patterns with regards how you are using our website. This helps us to develop and improve our website as well as products and / or services in response to what you might need or want.

Cookies are either:

- Session cookies: these are only stored on your computer during your web session and are automatically deleted when you close your browser – they usually store an anonymous session ID allowing you to browse a website without having to log in to each page but they do not collect any personal data from your computer; or
- Persistent cookies: a persistent cookie is stored as a file on your computer and it remains there when you close your web browser. The cookie can be read by the website that created it when you visit that website again. [We use persistent cookies for Google Analytics.]

Cookies can also be categorised as follows:

- Strictly necessary cookies: These cookies are essential to enable you to use the website effectively, such as when buying a product and / or service, and therefore cannot be turned off. Without these cookies, the services available to you on our website cannot be provided. These cookies do not gather information about you that could be used for marketing or remembering where you have been on the internet.
- Performance cookies: These cookies enable us to monitor and improve the performance of our website. For example, they allow us to count visits, identify traffic sources and see which parts of the site are most popular.
- Functionality cookies: These cookies allow our website to remember choices you make and provide enhanced features. For instance, we may be able to provide you with news or updates relevant to the services you use. They may also be used to provide services you have requested such as viewing a video or commenting on a blog. The information these cookies collect is usually anonymised.

# Data Processor Policy

## Definitions:

Data Protection Legislation: all applicable data protection laws including General Data Protection Regulation ((EU) 2016/679) ("GDPR") and any applicable national data protection legislation, regulations and secondary legislation from time to time in force in the jurisdiction of the Controller and/or the Processor relating to the processing of Personal Data, and where relevant the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426). DATA PROTECTION All definitions used in this clause shall have the definition set out in the Data Protection Legislation. The Controller and the Processor acknowledge that the Controller is the controller and the Processor is the processor and that the Controller retains control of the Personal Data and remains responsible for its compliance obligations under Data Protection Legislation. The Processor may process the Personal Data categories and Data Subject types set out in this Agreement. Each party agrees to comply with all applicable requirements of the Data Protection Legislation. The Processor shall: implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of Data Protection Legislation and ensure the protection of the rights of the Data Subject; only authorise a third party ("sub-processor") to process the Personal Data if (i) the Processor has obtained the prior written consent from the Controller for each appointment of a sub-processor (or the sub-processor's name is set out in Schedule and (ii) the Processor and the sub-processor enter into a written contract containing terms the same as those set out in this clause, in particular, in relation to data security measures and (iii) the Processor maintains control over all Personal Data it shares with the sub-processor and (iv) the Processor ensures that the sub-processor does not process the Personal Data except on instructions from the Data Controller (unless required to do so by Union or Member State law);

process the Personal Data only on documented instructions from the Controller, unless required to do so by Data Protection Legislation to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; ensure that persons authorised to process the personal data (such as its employees) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; ensure that is has in place appropriate technical and organisational measures, reviewed and approved by the Controller, to ensure a level of security appropriate to the risk (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of Natural Persons) including, where appropriate, the pseudonymisation and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident and a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of processing. Account shall also be taken of the risks that are presented by the processing in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed; taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights set out in Chapter III of the GDPR; assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the GDPR (data breach) taking into account the nature of processing and the information available to the Processor; at the choice of the Controller, delete or return all the Personal Data to the Controller after the termination or expiry of this Agreement and delete existing copies (unless Union or Member State law requires storage of the Personal Data); make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller; assist the Controller in ensuring

compliance with the requirement to carry out Data Protection Impact Assessments as set out in Article 35 of GDPR, taking into account the nature of processing and the information available to the Processor; immediately inform the Controller, if in the opinion of the Processor, an instruction from the Controller infringes Data Protection Legislation; promptly comply with any request by or instruction from the Controller to process the Personal Data, or to stop, mitigate or remedy any unauthorised processing; keep all Personal Data confidential and not disclose such data to third parties unless specifically authorised in writing by the Controller or as required by law. If the Processor is required by law, court, regulator or supervisory authority to process or disclose any Personal Data, the Processor will first inform the Controller of this and allow the Controller to object or challenge the requirement, unless the law prohibits the Processor from informing the Controller; not transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining the Controller's prior written consent (except where the Processor is required to transfer such data by Union or Member State law, in which case the Processor shall inform the Controller of such legal requirement before processing takes place, unless any law prohibits such disclosure on important grounds of public interest) and (i) there is an appropriate safeguard or derogation for such transfer in accordance with part V of the GDPR; keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Controller, using the schedule set out in schedule 3 or in such form as the Controller may require from time to time (Records) and shall send the Records to the Controller on a monthly basis (or such other period as required by the Controller).

### **What Personal Information We Collect**

When You create a MerchBee User Account, purchase a product, download a software update, or contact us, we collect a variety of information, including Your name, mailing address, phone number, e-mail address, and contact preferences. When payment, or payment information, is required, we will direct You to submit credit card information through a third-party such as Stripe. When You, as a MerchBee Account Holder, acquire information regarding Your customers and then enable the upload that information to MerchBee via MWS API for managing your customer emails and sales/profit tracking, MerchBee will store whatever personal information regarding Your customers that You have uploaded via MWS API on MerchBee production servers for the purpose of providing accounting and CRM-like functionality.