PRIVACY POLICY

This policy was last modified on 26th Nov 2018.

At Spitfire Audio, we are committed to maintaining the trust and confidence of visitors to our website, and users of our products and services. In particular, we want you to know that Spitfire Audio is not in the business of buying, selling, renting or trading email lists with other companies and businesses for marketing purposes.

In this Privacy Policy, we've provided lots of detailed information on when and why we collect your personal information, how we use it, the limited conditions under which we may disclose it to others and how we keep it secure.

You can contact us with data information requests by emailing James Bellamy on dataprotection@spitfireaudio.com, or alternatively get in touch via our support page, who can pass on your request to the right person.

COOKIES POLICY

WHAT ARE COOKIES?

Like most websites, spitfireaudio.com uses cookies to collect information. Cookies are small data files which are placed on your computer or other devices (such as smartphones or tablets) as you browse this website. They are used to remember when your computer or device accesses our website, and also help us keep track of information needed as you move from page to page (for example, the contents of your shopping cart).

Cookies are essential for the effective operation of our websites and to help you shop with us online. They are also used to tailor the products and services offered and advertised to you, both on our websites and elsewhere.

INFORMATION COLLECTED

Some cookies collect information about browsing and purchasing behaviour when you access this website via the same computer or device. This includes information about pages viewed, products purchased or added to your cart and your journey around a website. We do not use cookies to collect or record information on your name, address or other contact details. Spitfire Audio can use cookies to monitor your browsing and purchasing behaviour.

HOW ARE COOKIES MANAGED?

The cookies stored on your computer or other device when you access our websites are designed by:

- Spitfire Audio, or on behalf of Spitfire Audio, and are necessary to enable you to a make purchases on our website.
- Third parties who collect analytical data (namely Google Analytics, Facebook Pixel and Zendesk).

WHAT ARE COOKIES USED FOR?

The main purposes for which cookies are used are:

0. For technical purposes essential to effective operation of our website, particularly in relation to online transactions and site navigation.

0. To enable Spitfire Audio to collect information about your browsing and shopping patterns, including to monitor the success of campaigns, competitions etc.

HOW DO I DISABLE COOKIES?

If you want to disable cookies you need to change your website browser settings to reject cookies. How you can do this will depend on the browser you use. Further details on how to disable cookies for the most popular browsers are set out below:

- For Microsoft Internet Explorer
- For Google Chrome
- For Safari
- For Mozilla Firefox
- For Opera
- For Safari on iPhone
- For Chrome on iPhone
- For Android Browser

WHAT HAPPENS IF I DISABLE COOKIES?

This depends on which cookies you disable, but in general the website will not operate properly if cookies are switched off. If you only disable third party cookies, you will not be prevented from making purchases on our sites. If you disable all cookies, you will be unable to complete a purchase on our site, some buttons will become inactive, and some navigation functionality will be lost.

OUR CUSTOMER DATABASE

We are a data controller as defined by the GDPR ("A controller determines the purposes and means of processing personal data"). We are registered with the UK Information Commissioner's Office (https://ico.org.uk/) with registration number ZA170164.

We have our own customer database which is stored on servers inside the EU (Ireland), and is never transferred, duplicated or backed up outside of the EU. Stringent measures are in place to prevent unauthorised access to this database, including IP locking and strong "need to know basis" access policies.

WHO HAS ACCESS?

Access to the raw data is limited to a very small handful of people who legitimately need to use it within Spitfire, as well as senior partners at our third party web development company, Switchplane, who administer the database for us (you can read their privacy policy at https://www.switchplane.com/privacy/).

Our customer experience team and finance teams, via the administration section of our website, have access to all customer details including name, postal address, email address, order history, transaction and stored wish list items. Only the head of department can access the raw underlying data.

Our web development teams, both internally, and employed by our third party provider work with an anonymised copy of the live database (the same underlying data, but with all references to identifiable personal information scrambled, including names, email addresses, postal addresses, & phone numbers).

Access keys for our various third party services are stored securely external to the code to which developers have access.

MARKETING

SIGNING UP FOR OUR MAILING LIST

Our home page contains a form you can use to sign up to our mailing list (sometimes known as our newsletter). In using it you'll be opting in to receiving all 3 categories of emails we send (explained below), however you can update your preferences at any time using this link (which will also be included in every email we send you). You can unsubscribe altogether in the same place.

After you've given us your email using this form, we'll send you a confirmation email, and you'll need to click the confirm button to affirm that you opt in and that the email address you used is valid.

At this point we'll ask you for your name, but giving it to us is optional. The single piece of mandatory information we need from you in order to subscribe you is a valid email address.

- Products

- If you opt in to this category we'll tell you about new and upcoming products and significant updates or changes to existing products. We'll also use this category to send messages about upcoming promotional pricing events in our shop (such as the promotions we run for Black Friday or our Wish List campaigns).

- LABS

- This selection will ensure you'll be among the first to access our free libraries; along with new music, videos, and interviews which relate to the infinite LABS programme. Let's all become something.

- Community

- With this, we'll keep you abreast of our editorial and educational Journal content including Quick Tips, Creative Cribs, Ones to Watch, and much more. We'll also announce all the exclusive events and competitions we're planning, and share social media activity we think might interest you.

You can also opt to join our mailing list during the process of creating an account. You will be opted into all 3 categories above if you opt in, but you can update your preferences at any time (using this form).

WHERE WE KEEP OUR MAILING LIST

We use Mailchimp to host our mailing list. This is a US-based company which is a member of the US-EU Privacy Shield scheme, indicating that their data protection policies comply with GDPR. Their privacy policy is here. They store our data outside the EU.

Apart from your email address and (optionally) your name, Mailchimp also tracks your interactions with our campaigns (opens, clicks) as well as detecting if the email is marked as spam or doesn't get delivered (bounces). They also track whether or not you have unsubscribed.

Every message we send from this platform has an unsubscribe button, and the option to update your mailing preferences.

Additionally, we send some promotional email campaigns via our own website, usually where the message relies on us knowing more information about you. Examples of this include our wish list campaign emails (for which we need to know which products are in your wish list) or "affiliation" messages (e.g. to let Spitfire Symphonic Strings owners know that we have released an Expansion Pack).

We maintain synchronicity between your preferences in our own database, and your preferences on Mailchimp (whichever way round you choose to edit them).

One caveat you should note is that if you change your email address directly using Mailchimp's supplied form, and don't make the same adjustment on your Spitfire account, we will be unable to maintain sync between both sets of preferences, and you may receive emails you don't expect.

HOW LONG WE'LL KEEP YOU ON OUR MAILING LIST

We'll keep you on our mailing list until you unsubscribe so long as you occasionally open our messages.

Once a year we'll remove people from our list who have not opened any of our emails in the previous 12 months.

THE LEGAL BASIS WE USE FOR MARKETING MESSAGES WE SEND

Where we have not obtained explicit consent from our customers for sending of marketing messages, we may still use the legitimate interests legal basis to send direct messages. We've conducted a comprehensive legitimate interests assessment to justify this which you can read here.

CREATING A SPITFIRE AUDIO ACCOUNT

Certain activities you might perform on our website require you to have a Spitfire Audio account. These include:

- Buying products
- Downloading and installing products
- Storing a personal "wish list" of products you are interested in
- Submitting a customer service request (* see Zendesk section below)
- Applying for a student discount

When you create an account, we ask for your first and last names, your email address and a password, and also ask whether you'd like to opt in to our mailing list (MORE ABOVE).

Your password is stored encrypted using an industry standard password hashing mechanism which isn't reversible, so nobody, including us, can find out what your password is in plain text. We encourage our customers to use difficult to guess passwords or passphrases, and to use a password manager to discourage password sharing between websites (we use Lastpass at Spitfire).

HOW YOU CAN KEEP YOUR DATA UP TO DATE

You will find a comprehensive suite of pages which you can use to update your data on our website. Alternatively, if you create a support ticket we can update it for you.

HOW YOU CAN FIND OUT WHAT DATA WE HOLD

Known under the GDPR as a "Subject Data Access Request," you can request that we supply you with all the data we hold on you at any time. To make this easy for you, we have created a page in your account area here: http://www.spitfireaudio.com/my-account/my-information/. A print optimised version is available on the same page.

HOW LONG DO WE KEEP YOUR DATA

We will retain your Spitfire Audio account indefinitely unless you ask us to delete it (which you can do by submitting a support ticket).

If you have ever bought anything from us we are required by law to retain financial records for at least 6 years, so we will not be able to completely remove you if you have made any orders more recently than this (see OUR SHOP section below).

OUR SHOP

If you buy something from us, we will ask for some additional information from you in order to process your payment, deliver you your purchases and continue to support them in future. This is to enable us to fulfill our contractual obligation to you which begins at the point of sale.

WHAT DATA DO WE COLLECT

We ask for your name, email address, company name (if applicable), your registered card billing address, your delivery address (only if you ordered a hard drive), your phone number (which we use as part of our fraud checking process), your credit card number (unless you use Paypal), expiry date and CVS code ("the last 3 digits on the back of the card").

WHO DEALS WITH OUR PAYMENTS

Our Payment Service Provider is Sage Pay (formerly Protx) – the largest independent payment service provider (PSP) in the UK and Ireland.

Sage Pay provides a secure payment gateway (Level 1 PCI DSS), processing payments for thousands of online businesses, including ours. It is Sage Pay’s utmost priority to ensure that transaction data is handled in a safe and secure way.

Sage Pay uses a range of secure methods such as fraud screening, IP address blocking and 3D secure. Once on the Sage Pay systems, all sensitive data is secured using the same internationally recognised 256-bit encryption standards.

Sage Pay is PCI DSS (Payment Card Industry Data Security Standard) compliant to the highest level and maintains regular security audits. They are also regularly audited by the banks and banking authorities to ensure that their systems are impenetrable.

Sage Pay is an active member of the PCI Security Standards Council (PCI SSC) that defines card industry global regulation.

All data transfer between our server and Sage Pay is over HTTPS which means it is encrypted in transit, and can only be unencrypted by the intended recipient.

Sage Pay retain your card information in order that we can refund all or part of your transaction in future, but we only have access to the last 4 digits, card name and CVS code.

We don't make use of any kind of token which would enable us to take another payment in future on the same card (even if you asked us to).

After a payment is successful, Sage Pay provide us with an automated fraud score which combined with other measures of our own, we use to make an automated decision to either process the order immediately or hold for investigation by one of our customer experience team.

We also take payments using Paypal (whose GDPR compliant privacy policy is here), though Sage Pay act as an intermediary for these transactions, so your data is passed to Paypal using Sage Pay's fully PCI compliant systems, rather than directly from our servers.

After a successful transaction, we have access to the billing address, name and email address of the Paypal account which was used to make the transaction, which we recognise may not be the same as the Spitfire Audio account holder. We don't make use of this information for anything. We use the transaction references for accounting purposes.

WHO HAS ACCESS TO FINANCIAL DATA?

Access to our Sage Pay and Paypal data is restricted to our customer experience and finance teams (both of whom legitimately need it to be able to carry out their jobs). The heads of our web and operations teams (including at our external partners Switchplane) also have access in order to be able to manage the integration with our site, and act as tier 3 level support in case of unusually problematic transactions. The Customer Experience team has access to Paypal principally so that they can request and confirm manual payments.

TRANSACTIONAL EMAILS

Email	When and what?	Legal basis
Order confirmation	Confirms that we have received your order and the amount you spent. Includes link to your invoice	Contractual obligation - we need to confirm your order has been successful
Purchase is ready	After fraud checking has finished and your order has been fully processed, we'll send this message to let you know it is ready to be downloaded. This email also contains your serial number(s), if applicable.	Contractual obligation - this is part of us delivering the product to you

Hard drive in progress	If you've ordered a hard drive, we'll send you a quick email to let you know we've started to build it.	Legitimate interests - we think it polite and reasonable to let you know your order is in progress
Hard drive dispatched	When your hard drive is shipped we'll let you know, and give you a shipping tracking reference.	Legitimate interests - we think it is reasonable for us to let you know that your order is on its way
Product Updates	We typically offer free updates to products during their lifetime. This message is to let you know when one is available for something you own.	Legitimate interests - we think you'll want to know that there have been improvements to a product you own. This is part of our ongoing commitment to our customers.

OUR PRODUCTS

INSTALLING

Our Spitfire Application software requires you to have an account on our website. Logging into your account via the app allows it to know which products you own. All communication with our server is transferred over HTTPS.

During the install process we log information about the progress of your download and install, including your operating system and IP address. We do this so that our customer experience team can diagnose problems more effectively if something goes wrong, as well as for the purpose of recognising and preventing unusual download activity (for example, a single purchase being downloaded simultaneously in several different countries may indicate piracy). This data may also be used statistically to help us improve the quality, reliability and speed of our download service.

UPDATING

We typically offer free updates to our products during their lifetime, either to fix bugs or to add new features. In order for us to be able to to send these to you, we must retain your account email address and your order history. If you'd like to opt out of future updates, you can (by contacting support), though since installing an update is entirely optional and older versions of our products may conceivably stop working, we'd recommend that you don't.

WATERMARKING AND ENCRYPTION

Our Kontakt and Kontakt Player libraries are watermarked to help protect us against software piracy. Watermarks are encoded on our server in advance, and allocated to individuals by our automated order processor when they buy. They contain no personally identifiable data in themselves, though we can work out who a watermarked file belongs to if we need to by referring to our allocation records.

Our standalone plugins (e.g. BT Phobos, Hans Zimmer Strings) are encrypted for use only on your individual computer(s). To achieve this our Spitfire Application software reads certain bits of system information from your machine then uses it to generate a key which is unique to your machine. Only this key is sent back to our server where it is used to encrypt some of the files we send you. No personally identifiable information is used at any time during this process.

LOGGING

None of our products besides our Spitfire Application (installer software, details above) communicates with our servers in any way, either for statistical purposes, or to pass usage or personal data of any kind.

CUSTOMER EXPERIENCE

At Spitfire we want happy customers. To help us to help you, we will often need to know a little bit about you.

ZENDESK

We use US-based company Zendesk (https://www.zendesk.co.uk/) as our customer support ticketing system and to provide live chat customer service. You can find full details of their comprehensive compliance with data protection regulations here: https://www.zendesk.co.uk/company/customers-partners/eu-data-protection/

Your data may be stored on servers outside of the EU, but Zendesk are a certified member of the EU-US Privacy Shield Scheme (see item 13 in their data protection policy) as well as the US-Swiss Safe Harbor scheme which demonstrates that they process data to a GDPR-compliant standard.

LIVE CHAT

If you choose to get in touch with our support team via our live chat service we'll ask you for your name and email address however if you choose not to tell us, you can still talk to us, and the chat will only be retained in Zendesk against an anonymous visitor number. Note that the nature of some enquiries may mean we have to insist on you telling us your account or other sensitive personal details during the chat in order to be able to fulfill your requirements.

If you do give us an email address and subsequently create an account at spitfireaudio.com using the same email address, the chat you initiated before you had an account will be attached to the account you subsequently create.

When you start a chat your browser will report to Zendesk your IP address, which browser (and version) you're using, which operating system you're using, your approximate location (City & Country) and the URL of the page you're looking at at the point the chat begins.

PHONE

If you call us, we will collect your caller ID (ie. phone number) if available, and store a recording of the call against this phone number. During the call we will ask for your name and account details (if applicable), and will add all this information into your account. If you call us from the same number at a later date, we can retrieve this account information the next time you call.

If you block the sending of your caller ID, and don't tell us who you are during the call, only the recording will be saved against an anonymous ID number.

CREATING A SUPPORT TICKET

In order to be able to create a support ticket in our system, we ask you to log in to your Spitfire Audio account. We can then log you into Zendesk using a process called Single Sign On. With this, we confirm to Zendesk that you have a valid account with us via a secure exchange of tokenised data. There's no need for you to have a separate password to access Zendesk. They don't have any record of your Spitfire Audio password, even in encrypted form.

You can see all your own activity on Zendesk at the following URL (you will be redirected to the spitfireaudio.com website to log in first if necessary): https://spitfireaudio.zendesk.com/hc/en-us/requests

In the process of servicing your request, we may ask for additional personal or financial information or details of your order history or your hardware and software, and all such information will be retained with the ticket for future reference.

KNOWLEDGEBASE & COMMUNITY

All knowledgebase articles we publish allow customers to comment. You must be logged into your account to do this. There is also a community section where you can chat to other Spitfire customers and Spitfire Customer Experience Advocates.

Your comments will be visible to anyone on the internet, and we will publish your account name alongside your comment. You can delete your own comments at any time.

You can see all your own comments by clicking here: https://spitfireaudio.zendesk.com/hc/contributions/posts

HOW LONG WE KEEP YOUR DATA FOR

We retain all customer service tickets indefinitely. This is to ensure that we have a full case history of any problems you may have experienced in the past, and can refer back to these when necessary. We are happy to delete your full Zendesk history upon request. Please create a support ticket and ask.

EDUCATIONAL DISCOUNTS

We offer educational discounts to students & teachers in schools, colleges and universities. To qualify for this, we ask you to create an account, and submit documented proof that you are a student or teacher. This may be in the form of a college ID card, a payslip, a bank statement or a letter from the institution, and will often contain personally identifiable information, and / or a photograph of you.

We further recognise that by the nature of the scheme, it is possible that we will be collecting information about people who are under the age of 18. Consequently, we are careful to restrict access to these documents to just the customer experience team who process them.

We retain the documents for 30 days from the date we process the request, after which they are automatically deleted. This is sufficient to help us deal with any enquiries which may arise during purchase in most cases. In rare cases, we may ask you to re-submit your documents if your enquiry falls outside of the 30 day period.

EDUCATIONAL DISCOUNT APPLICATION EMAILS

Email	When and what?	Legal basis
Educational discount application was successful	If you apply for an educational discount, we'll send you a message confirming that you have been approved and offering you the appropriate discount codes.	Consent - by applying for this discount scheme, you agree that we'll have to communicate the outcome to you.
Educational discount application was not successful	If you are not approved for an educational discount for any reason, we'll let you know in an email.	Consent - by applying for this discount scheme, you agree that we'll have to communicate the outcome to you.
Educational discount application follow up message	If you are not approved for an educational discount, we may follow up with you in a personal email to ask for further details. You can choose not to engage with this message if you wish.	Legitimate interests - by applying for the scheme we take that to mean that you'd like us to do all we can to help you secure your discount.

TRUSTPILOT

We use a third party company - Trustpilot - to collect, analyse and display reviews relating to our customers' experience with our service and our products themselves. After purchase, we share the order number, email address and the name of the product that you have bought with Trustpilot in order to send a request to you by email for a review of our service and the product that you have bought.

If you choose to leave a review:

0. Service ratings and reviews are displayed on Trustpilot's own site in order that potential customers can look Spitfire Audio up and see our average rating and read any reviews that have been left.
0. Product ratings and reviews are displayed on our product pages along with the average rating.

In both cases, moderation of reviews is only possible under Trustpilot's own terms, Spitfire Audio does not have the ability to edit or delete reviews left using Trustpilot. Trustpilots own privacy policy can be found here: https://uk.legal.trustpilot.com/end-user-privacy-terms.

If you wish to unsubscribe from Trustpilot's mailing list, please follow the instructions here.

FINANCE

SUN SYSTEMS

We use financial software Sun Systems for our accounts. All data resides in the EU. Their privacy policy is here. No personally identifiable customer information is transferred into this system, only transaction references, and sales ledger data. Access is limited to our finance team. We retain financial records for the statutory six years.

ANALYTICS AND STATISTICS

We use a few different technologies to track behaviour on our site.

GOOGLE ANALYTICS

When someone visits spitfireaudio.com we use a third party service, Google Analytics, to collect standard internet log information (e.g. geographical location, OS and browser information, and details of visitor behaviour patterns. We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make, and do not allow Google to make, any attempt to find out the identities of those visiting our website. Besides members of our own internal marketing team, the other third parties who have access to Google Analytics information are:

- London-based marketing agency Found, who use the data to help us with Search Engine Optimisation and to plan marketing campaigns (their privacy policy is available to read here).
- Switchplane, who administer the analytics service integration on our behalf.

FACEBOOK PIXEL

When someone visits spitfireaudio.com we use a third party service, Facebook Pixel, to collect standard internet log information and details of visitor behaviour (e.g. which pages they visit, whether they add something to their cart or their wish list). We do this to find out things such as the number of visitors to the various parts of the site. This information is only processed in a way which does not identify anyone. We do not make any attempt to find out the identities of those visiting our website.

OUR DATA BREACH POLICY

WHAT IS A DATA BREACH?

We consider a data breach to be one or more of the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record)
- Equipment theft or failure
- System failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Human error
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

INVESTIGATION AND CONTAINMENT

If we discover or are notified of any of the above:

- We will firstly determine whether the breach is ongoing, and if so, take immediate measures to stop it and minimise its impact.

- Secondly, we will investigate the extent and severity of the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. This investigation will consider the following:

- the type of data involved
- its sensitivity
- the protections which are in place (e.g. encryptions)
- what has happened to the data (e.g. has it been lost or stolen)
- whether the data could be put to any illegal or inappropriate use
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

NOTIFICATION

After investigating the breach, we will determine whether it is necessary to report it to the Information Commissioner's Office (ICO), and if so, will do so within a maximum of 72 hours of becoming aware of the breach, if possible.

Every incident will be assessed on a case by case basis. The following will be considered:

- Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
- Whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?)
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Whether there are any legal / contractual notification requirements
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact us for further information or to ask questions on what has occurred.

We will consider notifying third parties such as the police, insurers, banks or credit card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

We will consider whether our marketing team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

An internal record will be kept of any personal data breach, regardless of whether notification was required.

EVALUATION AND RESPONSE

Once the initial incident is contained, we will carry out a full review of the causes of the breach, the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie including identifying potential weak points within existing security measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Staff awareness

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Spitfire Audio board.