



Privacy Policy

Version: 1.0

Published: 15/05/2024

Table of Contents

Document Control.....	3
Introduction	4
Responsibilities.....	5
Use of any hyperlinks and third-party views	6
Types of data we collect about you:	7
Legal Basis for Processing	9
How We Collect Your Data	12
Disclosure of Your Personal Data	13
International Transfers	14
Data Security	15
Data Retention	16
Your Legal Rights	17
Marketing Communications	19
Complaints	20
Definitions	21
Policy Review	23
Implementation of Policy	23

Document Control

Version History

Details of all changes made to this document are recorded in SharePoint.

Introduction

Name of Company: Mercury XRM LTD

Company Number: 08910193

Address: De Montfort House High Street, Coleshill, Warwickshire, B46 3BP

ICO Registration: ZA169800

Hyperlink: www.wearemercury.com

DPO Contact: DPO@wearemercury.com

This Privacy Policy sets out the basis on which Mercury xRM Limited, (“**the Company, Mercury**”) collects and processes your personal data as a data controller when you use or access our website or services.

Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it. By visiting www.wearemercury.com, (the “**Site**”) or using our services or apps, (“**Services**”) you are accepting and consenting to the practices described in this Privacy Policy.

Please note:

This Privacy Policy does not apply to any data you provide to us when we process personal data as a data processor i.e. where we process customer data within the cloud service we provide to you, as a business to business service provider.

The Site and Services are not intended for use by children and we do not knowingly collect information relating to children.

This Site and the Services are not intended for and shall not be used by anyone under the age of 18.

Responsibilities

Our Responsibilities

If you are a Mercury customer or supplier, if you use any of our products or services, enquire about our services, support our services, take part in our market research activities, interact with us online, email, live chat, call or write to us, or just visit our website, this Privacy Policy applies to you.

The following Privacy Policy sets out the personal data that we collect about you. This includes how and why we process your personal data, who we share it with, and lots of information about your rights and choices when it comes to the processing of your personal data.

We'll keep this Privacy Policy updated to show you all the things we do with your personal data. In certain circumstances, we may also provide an extra privacy notice, which will always refer to this page.

Your responsibilities

- ✓ To read this Privacy Policy
- ✓ If you are a Mercury customer, please also check the terms and conditions and policies between us as they may contain further details on how we collect and process your data.
- ✓ If you provide us with personal information about other people, or if others give us your information, we will only use that information for the specific reason for which it was provided to us. By submitting the information to us, you confirm that you have the right to authorise us to process it on your behalf in accordance with this Privacy Policy.

Use of any hyperlinks and third-party views

Neither Mercury nor any of our associates are responsible for the content of any other website, including any website through which you may have gained access to from this policy. We do not accept any liability in connection with any such websites or links.

Where we provide a hyperlink to a third party's website, we do so because we believe in good faith that such a website contains or may contain material which is relevant. Such a hyperlink does not signify that we have reviewed or approved of the connected third party's website or its contents – indeed in certain instances, a hyperlink may connect you to a third party's website containing views contradictory to those expressed on our site or otherwise held by us.

Any views or opinions of third parties are the personal views of the individuals or organisations that provided them and do not necessarily reflect the opinions or views of us.

Where we have provided you with a link to their privacy policy and their main business website. Please note that whilst we make every effort to keep these links up to date, there may be instances where the organisation has changed their website, and the link may no longer work. If that is the case, then please find their main website and their privacy policy can usually be found linked in the footer at the bottom of the main webpage.

Types of data we collect about you:

The Company only collects, processes, and holds personal data for the specific purposes or for other purposes expressly permitted by the GDPR). Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data.

‘Personal data’, or ‘personal information’, means any information about an individual from which that person can be identified. We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

	<p>Contact details and Identity Data: Your name, contact address, business address, telephone number, email address, title, name and contact details of individuals authorised to access your account.</p>
	<p>Financial & Transaction Data Your bank account number, sort code, and bank details you provide to make payment for the products and services you purchase from us. Purchase and account history relating to the products and services which you have purchased or used, deliveries we have made to you. Information that allows us to understand your creditworthiness and financial position.</p>
	<p>Account Data CRM data – inclusive of Name, Email address, mobile number, address, emails and phone call summaries, Live chat history, and Screen recordings from support sessions.</p>
	<p>Communication Data Records of your discussions with our services team and other staff members, including call recordings, webchat, emails, transcripts and video recordings. When you share comments and opinions with us, ask us questions or make a complaint we will keep a record of this. This includes when you send us emails, phone our Services Team or contact us via web chat or through social media such as LinkedIn, Twitter or Facebook. Exercising your rights: if you exercise any of your statutory rights under data protection law, we will also keep a record of this and how we respond.</p>
	<p>Secondary Account Users Data Details of other people linked to your account i.e. secondary account holders</p>
	<p>Technical Data Your IP address, login information, device type, browser type and version, time zone setting, browser plug-in types, geolocation information about where you might be, operating system and version.</p>
	<p>Usage Data Information about how you use our website, products and services. Your URL clickstreams (the path you take through our websites), products/services viewed, page response times, download errors, how long you stay on our pages, what you do on those pages, how often, and other actions. Responses to surveys, competitions and promotions, including records of any surveys you respond to or your entry into any competitions we run.</p>

	<p>Special Category Data</p> <p>We do not collect, store or use special category data about you. This means 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 information about criminal convictions and offences either.</p>
	<p>Profile Data</p> <p>This includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.</p>
	<p>Marketing Communications Data</p> <p>This includes your preferences in receiving marketing from us and our third parties and your communication preferences.</p>
	<p>Location Data</p> <p>This includes GPS technology and other technology such as IP address used to determine your current location. Some of our location-enabled Services require your personal data for the feature to work.</p>
	<p>Aggregated Data</p> <p>We also collect, use and share aggregated data, such as statistical or demographic data that could be derived from your personal data but which is not considered personal data in law, as this data is anonymised and doesn't directly or indirectly reveal your identity.</p>
	<p>Data about changes in circumstance</p> <p>Should your circumstances change, we may also ask for the following to allow us to service your account.</p> <p>Documentation to support a change of name request or account management changes.</p> <p>Documentation to help us manage an account.</p>
	<p>Enquiries or Complaints Data</p> <p>We will obtain or request the following information if you contact us with an enquiry or complaint.</p> <p>Any information that you disclose to us as part of your enquiry or complaint.</p> <p>All the personal data which is necessary for us to deal with your enquiry, question or complaint, which will depend on the nature of your request. This may include processing agreements, legal documentation, and copies of cheques or bank statements.</p>

Legal Basis for Processing

Mercury will only use your personal data when the law allows us to. The law requires Mercury to have a legal basis for collecting and using your personal data. Mercury relies on one or more of the following legal bases:

- **Performance of a contract with you:**
Where Mercury needs to perform the contract we are about to enter into or have entered into with you.
- **Legal obligation:**
Mercury may use your personal data where it is necessary for compliance with a legal obligation that we are subject to. We will identify the relevant legal obligation when we rely on this legal basis.
- **Legitimate interests:**
Where it is necessary for Mercury's legitimate business interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example to prevent fraud and enable Mercury to give you the best and most secure customer experience.
- **Consent:**
Mercury relies on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example, if you subscribe to an email newsletter.

Performance of a Contract

Reason or purpose	Personal data used includes
Where requested by you we will provide you with a quotation for any of our products and services	<ul style="list-style-type: none"> • Contact and Identity Data • Secondary Account User Data • Account Data
To deliver our products and services to you	<ul style="list-style-type: none"> • Contact Data and Identity Data • Financial and Transaction Data • Account Data • Communications Data • Technical Data and Usage Data • Marketing Communications Data • Location Data • Aggregated Data
To collect payments for products and services, debt collection, manage your payment plans	<ul style="list-style-type: none"> • Contact and Identity Data • Financial and Transaction Data • Location Data • Technical Data
To deliver our service communications to you (such as invoices and annual statements), and tailor those communications to your circumstances	<ul style="list-style-type: none"> • Contact and Identity Data • Financial and Transaction Data
To manage and answer your complaints or questions. This includes communication media such as email, telephone, live online chat and social media.	<ul style="list-style-type: none"> • Contact and Identity Data • Financial and Transaction Data • Account Data • Communications Data • Technical Data • Usage Data

To comply with our legal obligations

Reason or purpose	Personal data used includes
To meet our data protection obligations; to verify your identity before we provide you with, or make amendments to information relating to your account, and to understand the information we hold about you.	All personal information relevant to performing these tasks.
To secure and protect our data processing network and infrastructure	All personal information relevant to performing these tasks.
Internal and statutory audits	All personal information relevant to performing these tasks.

Because it is in our legitimate interests as a business to use your information:

Reason or purpose	Personal data used includes
To maintain, develop and improve our Mercury products and services e.g. for quality assurance purposes, to optimise our business processes and procedures, to support efficient business operations and the management and training of our staff, to analyse the performance of webpages and provide you with relevant content	<ul style="list-style-type: none"> Your contact details and the contact details of people associated with your account Your account information and details of other people linked to your account Financial & transaction information Purchase and account history Lifestyle and demographic insight information How you use our online applications and websites Location information Advertising and direct marketing preferences and responses Technical data including video recordings
Identify, and let you know about Mercury products and services that may interest you.	<ul style="list-style-type: none"> Your contact details and the contact details of people associated with your account Your Account information and details of other people linked to your account Financial & transaction information Purchase and account history Business and demographic insight information Advertising and direct marketing preferences and responses Technical data including video recordings
Develop new products and services e.g. new products and technology, new website or online functionality.	<ul style="list-style-type: none"> Your contact details and the contact details of people associated with your account Account information and details of other people linked to your account Financial information Purchase and account history Technical data including video recordings
Management information reporting. This includes the creation of aggregated and anonymised information for further use It is important to be clear that for the use of Management Information, personal data is not accessed in its raw format directly by management.	<ul style="list-style-type: none"> Your contact details and the contact details of people associated with your account Account information and details of other people linked to your account Financial & transaction information Technical data including video recordings
For market research purposes, to help us continually improve our offering to our customer	All personal information relevant to performing these tasks.
Direct Marketing. If you have not specifically consented to receive direct marketing, we will only send you direct marketing materials where we are allowed to by law. However, we will never send you direct marketing materials where you have opted out of receiving direct marketing communications	<ul style="list-style-type: none"> Your contact details and the contact details of people associated with your account Your account information and details of other people linked to your account How you use our online applications and websites Advertising and direct marketing preferences and responses
Protection of our staff	All personal information relevant to performing these tasks.
Staff training	All personal information relevant to performing these tasks.
For the establishment, exercise or defence of legal claims	All personal information relevant to performing these tasks.
Debt recovery relating to former Mercury customers	<ul style="list-style-type: none"> Your contact details and the contact details of people associated with your account Account information and details of other people linked to your account Financial information Transaction and payment information Purchase and account history

Where we have your consent:

Reason or purpose	Personal data used includes
<p>Direct Marketing - To provide you with information about products and services that we think you'd benefit from in accordance with your marketing preferences</p>	<ul style="list-style-type: none"> • Your contact details • Direct Marketing preferences • Technical data including video recordings
<p>Push notifications within our online applications (please note that revoking these permissions may require you to do this within your device e.g. disabling cookies)</p>	<ul style="list-style-type: none"> • Your contact details and the contact details of people associated with your account • Account information and details of other people linked to your account • Technical data

How We Collect Your Data

We use different methods to collect data from and about you including via:

Direct Interactions:

You may give us your Identity, Contact and Financial Data when you fill in forms or correspond with us by post, phone, email or otherwise. This includes personal data you provide when you register to use our Site or to receive our newsletter, agree to use our Services, create an account to Services, request marketing to be sent to you, search for a product or request a demonstration on our Site, participate in discussion boards or other social media functions on our Site, enter a competition, promotion or survey, attend a conference or webinar, give us feedback or contact us, when you report a problem with our Site or Services, make a complaint or exercise your statutory rights, or contact us via social media.

Purchases:

If you make purchases via our Site or within any Services, or register for an event or webinar, we may require you to provide your Identity, Contact, Financial and Transaction Data.

Community:

If you register for an online community that we provide, or connect with other company's products or apps, you may need to provide us with Identity, Contact, Profile and Technical Data.

Automated Technologies or Interactions:

As you interact with our Services, Sites or emails, we automatically collect Technical Data about your device, browsing actions, patterns, Location Data and Usage Data. We collect this personal data by using cookies, server logs, web beacons, pixels, and other similar technologies, and your use of our Site and Services. We may also receive Technical Data and Location Data about you if you visit other websites using our cookies. Please see the Cookie section below for further details.

PERSONAL DATA WE RECEIVE FROM OTHER SOURCES

We work closely with the third parties set out in our Third Party Supplier List (Available on request) which includes, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies and we may receive the following personal data about you from them:

Technical Data:

From analytics providers, advertising networks and search information providers.

Contact, Transaction and Financial Data:

From providers of technical, payment and delivery services or from cloud accounting systems that store email and names of persons who sent invoices by email.

Identity and Contact Data:

From providers of chat/communication/helpdesk services with customers including via email. From providers of email communications service providers. from CRM service providers who manage contacts and keep a record of communications/ interactions with customers.

PERSONAL DATA we collect from other sources:

We also collect personal data about you from publicly available sources. We may combine this information with personal data provided by you. This helps us update, expand, and analyse our records, identify new customers, and create more tailored advertising to provide services that may be of interest to you. We also use this for targeted advertising, delivering relevant email content, determining eligibility and verifying Contact Data. Sources we use includes:

- Publicly available sources such as Companies House.
- Data that is published about you on social media profiles: such as LinkedIn, Facebook, Twitter.
- Credit, anti-fraud agencies and the Police or other law enforcement agencies.

Disclosure of Your Personal Data

Personal data we share with third parties. We may share your personal data where necessary with third parties for the purposes set out in the tables above.

Below is a summary of the types of third parties used:

- Any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.
- Business partners, suppliers and sub-contractors for the performance of any contract we enter into with them or you to provide services such as IT and system administration services, email communications, hosting services, backup services, credit card processing, research, development, marketing and customer support.
- Analytics and search engine providers that assist us in the improvement and optimisation of our Site and Services.
- Tax authorities, regulators and other authorities who require reporting of processing activities in certain circumstances.
- Advertisers and advertising networks that require the data to select and serve relevant adverts to you and others. We do not disclose personal data about identifiable individuals to our advertisers, but we may provide them with Aggregated Data about our users. We may also use such Aggregated Data to help advertisers reach the kind of audience they want to target (for example, women living in London). We may make use of the personal data we have collected from you to enable us to comply with our advertisers' wishes by displaying their advertisements to that target audience.
- Credit reference agencies for the purpose of assessing your credit score where this is a condition of us entering into a contract with you.

Personal data we disclose to third parties. We may disclose your personal data where necessary to third parties:

- If we choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets.
- If we or a member of our group of companies or substantially all of their assets are acquired by a third party, in which case personal data held by them about their customers will be one of the transferred assets.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms and conditions, terms of use and/or any other legal agreements; or to protect our rights, property, safety, our customers or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We use Aggregated Data in the normal course of operating our business; for example, sharing Aggregated Data with other Site or Services users, our customers or publicly to show trends or benchmark the general use of our Site and Services. We also use Aggregated Data for the purposes of testing our IT systems, data analysis, improving the Site and Services and development.

We require all third parties to respect the security of your personal data and to treat it in accordance with applicable law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

International Transfers

Our Services are global, and your personal data may be stored and processed in any country where we have operations, or our staff are located. When we share your personal data within our group of companies this may involve transferring your personal data to our overseas offices in The USA and Australia.

We may transfer your personal data to service providers that carry out certain functions on our behalf. This may involve transferring personal data outside your country of residence to countries with laws that do not provide the same data protection as your country of residence. When we share your personal data with our service providers, who are identified in our Third Party Supplier List, this will involve transferring your personal data to the country set out in the Third Party Supplier List for each service provider.

European Data

When we transfer UK, EU or Swiss personal data to countries whose laws do not provide the same level of data protection as the UK, the EU or Switzerland, we always ensure that a similar degree of protection is afforded to your data by ensuring that one of the following applicable safeguards is in place:

- We will only transfer UK personal data outside of the UK to: (i) countries deemed by the ICO to provide an adequate level of protection for UK personal data; or (ii) entities located outside of the UK with whom standard contractual terms approved for use in the UK which give the transferred personal data the same protection as it has in the UK have been entered into, for example, the International Data Transfer Addendum, (IDTA) to the European Commission's standard contractual clauses for international data transfers or binding corporate rules (BCRs); or (iii) entities located in the USA certified under the UK Extension to the EU-U.S. DPF; or (iv) any entity located outside of the UK that is subject to any other transfer mechanism, bespoke contract, approved code of conduct or certification scheme approved by the ICO.
- We will only transfer EU personal data outside of the EEA to: (i) countries deemed by the European Commission to provide an adequate level of protection for EU personal data; or (ii) entities located outside of the EEA with whom standard contractual terms approved for use in the EU which give the transferred personal data the same protection as it has in the EU have been entered into, for example, the European Commission's standard contractual clauses for international data transfers, (EU SCCs) or binding corporate rules (BCRs); or (iii) entities located in the USA certified under the EU-U.S. DPF; or (iv) any entity located outside of the EEA that is subject to any other transfer mechanism, bespoke contract, approved code of conduct or certification scheme approved by the European Commission.
- We will only transfer Swiss personal data outside of Switzerland to (i) countries deemed by the Swiss Data Protection Authority to provide an adequate level of protection for Swiss personal data; or (ii) entities located outside of Switzerland with whom standard contractual terms approved for use in Switzerland which give the transferred personal data the same protection as it has in Switzerland have been entered into, for example the European Commission's standard contractual clauses for international data transfers, (EU SCCs) or binding corporate rules (BCRs); or (iii) entities located in the USA certified under the Swiss-U.S. DPF; or (iv) any entity located outside of Switzerland that is subject to any other transfer mechanism, bespoke contract, approved code of conduct or certification scheme approved by the Swiss Data Protection Authority.

To obtain a copy of any of the above these contractual safeguards, please contact us as set out at the end of this Privacy Policy.

Please note that our Site and Services are accessible via the internet and may potentially be accessed by anyone around the world. Other users may access the Site or Services from outside the EEA, Switzerland or the UK. This means that where you chose to post your personal data on our Site or within the Services, it could be accessed from anywhere around the world and therefore a transfer of your personal data outside of the EEA, Switzerland or the UK may be deemed to have occurred.

Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. For example, all information you provide to us is stored on our secure servers. Any credit card information or payment transactions will be encrypted using SSL technology.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of the Site or Services, you are responsible for keeping this password confidential. We ask you not to share any password with anyone. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Unfortunately, the transmission of information via the Internet is not completely secure. Although we will endeavour to protect your personal data, we cannot guarantee the security of your personal data transmitted to our Site or the Services. Any transmission is at your own risk. Once we have received your personal data, we will use strict procedures and security features to try to prevent unauthorised access.

Data Retention

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint if we reasonably believe there is a prospect of litigation in respect of our relationship with you, to comply with law enforcement requests, maintain security, prevent fraud and abuse, resolve disputes, enforce our legal agreements, or fulfil your request to “unsubscribe” from further messages from us.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements. Usually, this will be for as long as we provide access to the Site or Services to you, your account with us remains open or any period set out in any relevant contract you have with us.

By law, we must keep basic information about our customers (including Contact Data, Identity Data, Financial Data and Transaction Data) for 6 years after they cease being customers for tax purposes.

In some circumstances, we will anonymise your personal data (so that it can no longer be associated with you) after your account has been closed and we may use this for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

Please note: After you have closed your account or deleted information from your account, any information you have shared with others will remain visible. We do not control data that other users may have copied from the Site or Services. Your profile may continue to be displayed in the services of others (e.g. search engine results) until they refresh their cache.

Your Legal Rights

You have several rights under the Data Protection Law in relation to your personal data. You only have the benefits of some of the rights in limited circumstances, which depend on the legal reason why we collected your personal data.

	<h3>You have the right to request access to your personal data</h3> <p>This is commonly known as a “data subject request”. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.</p>
	<h3>You have the right to request rectification of personal data we hold about you</h3> <p>This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.</p>
	<h3>You have the right to request export your data to you or a third party</h3> <p>We will give you a copy of all the personal data applicable to this right in CSV or JSON format so that you can access it and / or provide it to another service. If you ask us and it is technically possible, we will directly transfer the data to the other service for you. We will not do so to the extent that this involves disclosing data about any other individual. Please note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.</p>
	<h3>You have the right to request the erasure of your personal data in certain circumstances</h3> <p>This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request</p>
	<h3>Right to Request a Restriction on Processing</h3> <p>This enables you to ask us to suspend the processing of your personal data in one of the following scenarios: (i) if you want us to establish the data’s accuracy; (ii) where our use of the data is unlawful but you do not want us to erase it; (iii) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (iv) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.</p>
	<h3>Right to Object to processing</h3> <p>You have the right to object to processing where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.</p>



You have the right to object to direct marketing

You can object at any time to the processing of your personal data for direct marketing purposes.



You have the right to withdraw consent at any time

Where we are relying on consent to process your personal data as the legal basis for using your data, you can withdraw consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

How to exercise your rights

If you wish to exercise any of the above rights please contact our Mercury DPO: DPO@wearemercury.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. Alternatively, we could refuse to comply with your request in these circumstances.

We will try to respond to all legitimate requests within 30 days and will deal with requests we receive from you, in accordance with the provisions of Data Protection Law. Occasionally it could take us longer if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

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.

Marketing Communications

We may use your Identity Data, Contact Data, Technical Data, Usage Data and Profile Data to form a view on which products, services and offers may be of interest to you so that we can send you relevant marketing communications.

Direct marketing: You will receive marketing communications if you “opt in” to receive marketing communications from us when you registered on our Site or within the Services, or if you enquired about, or have purchased any of our goods or services and you have not opted out of receiving such marketing.

Third Party Marketing: We will obtain your express opt-in consent before we share your personal data with any third party for their own direct marketing purposes.

Opting out of Marketing: You can ask us to stop sending you marketing communications at any time by logging into the Site or Services and unchecking the relevant boxes to adjust your marketing preferences or by following the “opt out” or “unsubscribe” links within any marketing communication sent to you.

Once you “opt out” or “unsubscribe”, you will no longer receive any marketing communications from us. You will however still receive service related communications that are essential for administrative or customer service purposes, for example relating to orders, billing, updates, checking that your contact details are up to date and support issues.

Please note that where we send push notifications from time to time in order to update you about any service updates, events and promotions we may be running, if you no longer wish to receive these communications, please disable these in the settings on your device.

Complaints

Our intention is to meet the highest standards when collecting and using personal data. For this reason, we take the complaints we receive very seriously. We encourage users to notify us if they think that our collection or use of personal data is unfair, misleading or inappropriate. If you have any complaints about our use of your personal data, please contact us as set out at the beginning of this Privacy Policy or you have the right to make a complaint to your local data protection supervisory authority.

For UK individuals:

The Information Commissioner's Office at, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, England.

Our EU representative is:

VeraSafe at VeraSafe Ireland Ltd, Unit 3D North Point House, North Point Business Park, Cork T23AT2P, Ireland. If you wish to raise a question please contact via their contact form [here](#), quoting "Mercury" in the subject line. Or by calling: +420 228 881 031.

Definitions

“Agreement”	the agreement between the Data Controller and the Data Processor for the provision of the Services;
“Customer Data”	means all data provided to the Data Processor within the Services when used or accessed by the Data Controller, its Affiliates and any end-users;
“Data Controller”	means the Customer;
“Data Processor”	means Mercury, including as applicable any “Service Provider” as that term is defined in US State Privacy Laws;
“Data Protection Legislation”	means all laws and regulations, including laws and regulations of the European Union, the European Economic Area, their member states and the United Kingdom any amendments, replacements or renewals thereof, applicable to the processing of Personal Data, including where applicable the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, the EU GDPR, the UK GDPR, the FADP, the UK Data Protection Act 2018, US State Privacy Laws, The Australian Privacy Act 1988 (Cth) No. 119 1988 (as amended) and any applicable national implementing laws, regulations and secondary legislation relating to the processing of the Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426);
“Data Subject”	has the same meaning as in Data Protection Legislation or means a “Consumer” as that term is defined in US State Privacy Laws;
“DPA”	means this data processing agreement together with its Schedules 1 and 2;
“EEA”	means the European Economic Area (all EU member states, plus Iceland, Liechtenstein, and Norway);
“EU GDPR”	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation);
“FADP”	means the Swiss Federal Act on Data Protection of the 1 st of September 2023, as amended from time to time;
“Personal Data”	has the meaning given to it by Data Protection Legislation;
“Restricted Transfer”	means: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy

	regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and
	(iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission;
“SCCs”	means: (i) where the EU GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN , (“ EU SCCs ”); and (ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR published at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/ , (“ UK SCCs ”); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority; (“ Swiss SCCs ”)
“Sub-Processor”	means any third party (including Data Processor Affiliates) engaged directly or indirectly by the Data Processor to process Personal Data under this DPA in the provision of the Services to the Data Controller;
“Supervisory Authority”	means a governmental or government chartered regulatory body having binding legal authority over a party;
“UK GDPR”	means the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;
“US State Privacy Laws”	means the following US state data protection or privacy laws and regulations applicable to the party's Processing of Personal Data: California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CTDPA), and Utah Consumer Privacy Act (UCPA) and the Connecticut Data Privacy Act (CTDPA) in each case as may be amended or superseded from time to time.

Policy Review

The Company shall review this Policy not less than annually and otherwise as required to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the Company Data Protection Officer and/or Chief Technology Officer.

Implementation of Policy

This Policy shall be deemed effective as of May 2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Rachel Fuller

Position: Risk And Compliance Executive

Date: May 2024

Next Review: May 2025

Initials: RF