External Privacy Notice

This Privacy Policy constitutes part of and should be read in conjunction with the Coin Rivet Terms and Conditions. This policy explains how we may collect, create, process, store, protect, disclose, share and transfer your Personal Data as part of our business operations.

(A) This Notice

Summary – This Notice
This Notice explains how we Process Personal Data. This Notice may be amended or updated from time to time, so please check it regularly for updates.

This Notice is issued by Galias Services, UAB (trading as Coin Rivet) a private limited liability company organised and existing under the laws of the Republic of Lithuania, legal entity code: 305705483, registered office address at Lvovo str. 25-104, Vilnius, Republic of Lithuania("**Coin Rivet**", "**we**", "**us**" and "**our**") and is addressed to individuals outside our organisation with whom we interact, including customers, visitors to our Sites, users of our Apps, other users of our Services, and visitors to our premises (together, "**you**"). Defined terms used in this Notice are explained in Section (S) below. For the purposes of this Notice, Coin Rivet is the Controller.

This Notice may be amended or updated from time to time to reflect changes in our practices with respect to the Processing of Personal Data, or changes in Applicable Law. We encourage you to read this Notice carefully, and to regularly check this page to review any changes we might make in accordance with the terms of this Notice. You can always find the latest version of this Privacy Policy here on this page.

(B) Collection of Personal Data

Summary – Collection of Personal Data
We collect or obtain Personal Data: when those data are provided to us (e.g., where you contact us); in the course of our relationship with you (e.g., if you make a purchase); when you make Personal Data public (e.g., if you make a public post about us on social media); when you download, install, or use any of our Apps; when you visit our Sites; when you register to use any of our Sites, Apps, or Services; or when you interact with any third party content or advertising on our Site or in our App. We may also receive Personal Data about you from third parties (e.g., law enforcement authorities).

Collection of Personal Data: We collect or obtain Personal Data about you from the following sources:

- Data provided to us: We obtain Personal Data when those data are provided to us (e.g., where you contact us *via* email or telephone, or by any other means, or when you provide us with your identity documents, or when you submit wage slips or other proof of funds documents, or when you provide other information required by Applicable Laws, or provide information otherwise required by us to provide the requested Services).
- Relationship data: We collect or obtain Personal Data in the ordinary course of our relationship with you (e.g., we provide a service to you).
- Data you make public: We collect or obtain Personal Data that you manifestly choose to make public, including *via* social media (e.g., we may collect information from your social media profile(s), if you make a public post about us).
- App data: We collect or obtain Personal Data when you download or use any of our Apps.
- Site data: We collect or obtain Personal Data when you visit any of our Sites or use any features or resources available on or through a Site.
- Registration details: We collect or obtain Personal Data when you use, or register to use, any of our Sites, Apps, or services.

- Content and advertising information: If you interact with any third party content or advertising on our Site or in our App (including third party plugins and cookies) we receive Personal Data from the relevant third party provider of that content or advertising.
- Third party information: We collect or obtain Personal Data from third parties who provide it to us (e.g., credit reference agencies; law enforcement authorities; identity service providers; global PEP and Sanctions watchlists; etc.).

Please note that third parties you interact with may have their own privacy policies, and we are not responsible for their operations or their use of data they collect. Information collected by third parties is governed by their privacy practices and we are not responsible for unauthorized third-party conduct. We encourage you to learn about the privacy practices of any relevant third parties.

(C) Creation of Personal Data

Summary – Creation of Personal Data
We create Personal Data about you (e.g., records of your interactions with us).

We also create Personal Data about you in certain circumstances, such as records of your interactions with us, and details of your past interactions with us. We may also combine Personal Data from any of our Sites, Apps, or Services, including where those data are collected from different devices.

(D) Categories of Personal Data we Process

Summary – Categories of Personal Data we Process
We Process: your personal details (e.g., your name); demographic data (e.g., your age); your contact details (e.g., your address); records of your consents; purchase details; payment details (e.g., your billing address); information about our Sites and Apps (e.g., the type of device you are using); details of your employer (where relevant); information about your interactions with our content or advertising; and any views or opinions you provide to us.

We Process the following categories of Personal Data about you:

- Personal details: given name(s); preferred name; and photograph, pictures of identity documents and any relevant data contained within those documents, pictures of billing documents and the extracted data, proof of salary and earnings
- Demographic information: gender; date of birth / age; nationality; salutation; title; and language preferences.
- Contact details: correspondence address; telephone number; email address; details of Personal Assistants, where applicable; messenger app details; online messaging details; and social media details.
- Consent records: records of any consents you have given, together with the date and time, means of consent and any related information (e.g., the subject matter of the consent).
- Purchase details: records of purchases and prices.
- Payment details: invoice records; payment records; crypto currency wallets received from: crypto currency wallets sent to;
- Data relating to our Sites and Apps: device type; operating system; browser type; browser settings; IP address; language settings; dates and times of connecting to a Site; App usage statistics; App settings; QR codes; dates and times of connecting to an App; location data, and other technical communications information (some of which may constitute Personal Data); username; password; security login details; aggregate statistical information.

(E) Sensitive Personal Data

Summary – Sensitive Personal Data

We do not seek to collect or otherwise Process Sensitive Personal Data. Where we need to Process Sensitive Personal Data for a legitimate purpose, we do so in accordance with Applicable Law.

We do not seek to collect or otherwise Process Sensitive Personal Data in the ordinary course of our business. Where it becomes necessary to Process your Sensitive Personal Data for any reason, we rely on one of the following legal bases:

- Compliance with Applicable Law: We may Process your Sensitive Personal Data where the Processing is required or permitted by Applicable Law (e.g., to comply with our diversity reporting obligations);
- Detection and prevention of crime: We may Process your Sensitive Personal Data where the Processing is necessary for the detection or prevention of crime (e.g., the prevention of fraud);
- Establishment, exercise or defence of legal rights: We may Process your Sensitive Personal Data where the Processing is necessary for the establishment, exercise or defence of legal rights; or
- Consent: We may Process your Sensitive Personal Data where we have, in accordance with Applicable Law, obtained your prior, express consent before Processing your Sensitive Personal Data (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).

If you provide Sensitive Personal Data to us, you must ensure that it is lawful for you to disclose such data to us, and you must ensure a valid legal basis applies to the Processing of those Sensitive Personal Data.

(F) Purposes of Processing and legal bases for Processing

Summary – Purposes of Processing and legal bases for Processing

We Process Personal Data for the following purposes: providing our Sites, Apps, and Services to you; compliance checks; operating our business; communicating with you; managing our IT systems; health and safety; financial management; conducting surveys; ensuring the security of our premises and systems; conducting investigations where necessary; compliance with Applicable Law; improving our Sites, Apps, and services; fraud prevention; and recruitment and job applications.

The legal basis for the Processing of your Personal Data is dependent on the context in which we collect it and the purposes for which it is used. The purposes for which we Process Personal Data, subject to Applicable Law, and the legal bases on which we perform such Processing, are as follows:

Processing activity	Legal basis for Processing
• Provision of Sites, Apps, and services: providing our Sites, Apps, or services; providing promotional items upon request; and communicating with you in relation to those Sites, Apps, or services.	• The Processing is **necessary in connection with any contract** that you have entered into with us, or to take steps prior to entering into a contract with us; or • We have **a legitimate interest** in carrying out the Processing for the purpose of providing our Sites, Apps, or Services (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).

• Compliance checks: fulfilling our regulatory and/or compliance obligations; 'Know Your Client' checks; and confirming and verifying your identity; use of credit reference agencies; and screening against government and/or law enforcement agency sanctions lists and other legal restrictions.	• The Processing is necessary for **compliance with a legal obligation**; or • The Processing is **necessary in connection with any contract** that you have entered into with us, or to take steps prior to entering into a contract with us; or • We have **a legitimate interest** in carrying out the Processing for the purpose of fulfilling our regulatory and compliance obligations (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).
• Operating our business: operating and managing our Sites, our Apps, and our Services; providing content to you; displaying advertising and other information to you; communicating and interacting with you *via* our Sites, our Apps, or our Services; and notifying you of changes to any of our Sites, our Apps, or our Services.	• The Processing is **necessary in connection with any contract** that you have entered into with us, or to take steps prior to entering into a contract with us; or • We have **a legitimate interest** in carrying out the Processing for the purpose of providing our Sites, our Apps, or our Services to you (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).
• Communications and marketing: communicating with you *via* any means (including *via* email, telephone, text message, social media, post or in person) to provide news items and other information in which you may be interested, subject always to obtaining your prior opt-in consent to the extent required under Applicable Law; maintaining and updating your contact information where appropriate; and obtaining your prior, opt-in consent where required.	• The Processing is **necessary in connection with any contract** that you have entered into with us, or to take steps prior to entering into a contract with us; or • We have **a legitimate interest** in carrying out the Processing for the purpose of contacting you, subject always to compliance with Applicable Law (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).
Processing activity	**Legal basis for Processing**
• Management of IT systems: management and operation of our communications, IT and security systems; and audits (including security audits) and monitoring of such systems.	• The Processing is necessary for **compliance with a legal obligation**; or • We have **a legitimate interest** in carrying out the Processing for the purpose of managing and maintaining our communications and IT systems (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms).
• Health and safety: health and safety assessments and record keeping; providing a safe and secure environment at our premises; and compliance with related legal obligations.	• The Processing is necessary for **compliance with a legal obligation**; or • We have **a legitimate interest** in carrying out the Processing for the purpose of ensuring a safe environment at our premises (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • The Processing is necessary to protect the **vital interests** of any individual.
• Financial management: sales; finance; corporate audit; and vendor management.	• We have **a legitimate interest** in carrying out the Processing for the purpose of managing and operating the financial affairs of our business (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).

• Security: physical security of our premises (including records of visits to our premises); CCTV recordings; and electronic security (including login records and access details).	• The Processing is necessary for **compliance with a legal obligation**; or • We have **a legitimate interest** in carrying out the Processing for the purpose of ensuring the physical and electronic security of our business and our premises (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms).
• Investigations: detecting, investigating and preventing breaches of policy, and criminal offences, in accordance with Applicable Law.	• The Processing is necessary for **compliance with a legal obligation**; or • We have **a legitimate interest** in carrying out the Processing for the purpose of detecting, and protecting against, breaches of our policies and Applicable Laws (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms).
• Legal proceedings: establishing, exercising and defending legal rights.	• The Processing is necessary for **compliance with a legal obligation**; or • We have **a legitimate interest** in carrying out the Processing for the purpose of establishing, exercising or defending our legal rights (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms).
• Legal compliance: compliance with our legal and regulatory obligations under Applicable Law.	• The Processing is **necessary for compliance with a legal obligation**.
• Improving our Sites, Apps, and services: identifying issues with our Sites, our Apps, or our Services; planning improvements to our Sites, our Apps, or our Services; and creating new Sites, Apps, or Services.	• We have **a legitimate interest** in carrying out the Processing for the purpose of improving our Sites, our Apps, or our services (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).
• Fraud prevention: Detecting, preventing and investigating fraud.	• The Processing is necessary for **compliance with a legal obligation** (especially in respect of applicable employment law); or • We have **a legitimate interest** in carrying out the Processing for the purpose of detecting, and protecting against, fraud (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms).
• Recruitment and job applications: recruitment activities; advertising of positions; interview activities; analysis of suitability for the relevant position; records of hiring decisions; offer details; and acceptance details.	• The Processing is necessary for **compliance with a legal obligation** (especially in respect of applicable employment law); or • We have **a legitimate interest** in carrying out the Processing for the purpose of recruitment activities and handling job applications (to the extent that such legitimate interest is not overridden by your interests, fundamental rights, or freedoms); or • We have obtained **your prior consent** to the Processing (this legal basis is only used in relation to Processing that is entirely voluntary – it is not used for Processing that is necessary or obligatory in any way).

(G) Disclosure of Personal Data to third parties

Summary – Disclosure of Personal Data to third parties
We disclose Personal Data to: legal and regulatory authorities; our external advisors; our Processors; any party as necessary in connection with legal proceedings; any party as necessary for investigating, detecting or preventing criminal offences; any purchaser of our business; and any third party providers of advertising, plugins or content used on our Sites or our Apps.

We disclose Personal Data within Coin Rivet, for legitimate business purposes and the operation of our Sites, Apps, or services to you, in accordance with Applicable Law. In addition, we disclose Personal Data to:

- you and, where appropriate, your appointed representatives;
- any legal and regulatory authorities, upon request, or for the purposes of reporting any actual or suspected breach of Applicable Law or regulation;
- accountants, auditors, lawyers and other outside professional advisors to Coin Rivet, subject to binding contractual obligations of confidentiality;
- third party Processors and associated Processors (such as payment services providers; including but not limited to Luxon Payments Limited etc.), located anywhere in the world, subject to the requirements noted below in this Section (G);
- any relevant party, law enforcement agency or court, to the extent necessary for the establishment, exercise or defence of legal rights;
- any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
- any relevant third party acquirer(s), in the event that we sell or transfer all or any relevant portion of our business or assets (including in the event of a reorganization, dissolution or liquidation); and
- any relevant third party provider, where our Sites and our Apps use third party advertising, plugins or content. If you choose to interact with any such advertising, plugins or content, your Personal Data may be shared with the relevant third party provider. We recommend that you review that third party's privacy policy before interacting with its advertising, plugins or content.

If we engage a third-party Processor to Process your Personal Data, the Processor will be subject to binding contractual obligations to: (i) only Process the Personal Data in accordance with our prior written instructions; and (ii) use measures to protect the confidentiality and security of the Personal Data; together with any additional requirements under Applicable Law. Third party processors we use regularly, but may change from time to time, include but are not limited to:

- Jumio;
- Comply Advantage; and
- Chainalysis.

(H) Profiling

Summary – Profiling
Personal Data are subject to automated decision-making and Profiling.

We Process Personal Data for the purposes of automated decision-making and Profiling, which is carried out for the following purposes:

Profiling activity	Logic of the Profiling activity	Consequences for you

Credit scoring	Where we engage a third party (e.g., a credit reference agency) to provide us with information about your credit score and/or credit history. This information is analysed to determine the most appropriate terms on which to offer you credit, where applicable.	This Profiling activity may affect whether you are able to obtain credit, and the interest rates applicable to any such credit.
Transaction Monitoring	We engage a third party to analyse transactions to highlight suspicious behaviour and potentially block suspicious transactions.	This profiling activity may mean that transactions are rejected or delayed if the activity is suspicious we may also report suspicious activity to the relevant regulatory bodies or law enforcement agencies.
Crypto Transaction Monitoring	We scan all incoming and outgoing wallet addresses, to prevent the use of our platforms for money laundering or other financial crime. This includes send source addresses or destination addresses to third parties to analyse against interaction with known bad actors.	This activity may mean that your wallet is frozen if cryptocurrency associated with known bad actors is sent to the system. This will result in us sending a suspicious activity report to the relevant regulatory bodies or law enforcement agencies.
KYC Identification	We engage a third party to collect information and analyse it for KYC purposes, this information is then removed from their system and stored on ours.	This profiling activity may mean that sign up is rejected or delayed if we may also need to provide this information relevant regulatory bodies or law enforcement agencies.

(I) International transfer of Personal Data

Summary – International transfer of Personal Data
We transfer Personal Data to recipients in other countries. Where we transfer Personal Data from the EEA to a recipient outside the EEA that is not in an Adequate Jurisdiction, we do so on the basis of Standard Contractual Clauses.

Because of the international nature of our business, we transfer Personal Data within Coin Rivet and to third parties as noted in Section (G) above, in connection with the purposes set out in this Notice. For this reason, we transfer Personal Data to other countries that may have different laws and data protection compliance requirements to those that apply in the country in which you are located.

Where we transfer your Personal Data from the EEA to recipients located outside the EEA who are not in Adequate Jurisdictions, we rely primarily on the European Commission's Standard Contractual Clauses to facilitate the international and onward transfer of Personal Data. You are entitled to request a copy of our Standard Contractual Clauses using the contact details provided in Section (R) below.

Please note that when you transfer any Personal Data directly to a recipient outside the EEA, we are not responsible for that transfer of your Personal Data. We will nevertheless Process your Personal Data, from the point at which we receive those data, in accordance with the provisions of this Notice.

(J) Data security

Summary – Data security
We implement appropriate technical and organisational security measures to protect your Personal Data. Please ensure that any Personal Data that you send to us are sent securely.

We have implemented appropriate technical and organisational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, and other unlawful or unauthorised forms of Processing, in accordance with Applicable Law.

Because the internet is an open system, the transmission of information *via* the internet is not completely secure. Although we will implement all reasonable measures to protect your Personal Data, we cannot guarantee the security of your data transmitted to us using the internet – any such transmission is at your own risk and you are responsible for ensuring that any Personal Data that you send to us are sent securely.

Furthermore, we cannot ensure or warrant the security or confidentiality of information you transmit to us or receive from us by Internet or wireless connection, including email, phone, or SMS, since we have no way of protecting that information once it leaves and until it reaches us.

(K) Data accuracy

Summary – Data accuracy
We take every reasonable step to ensure that your Personal Data are kept accurate and up-to-date and are erased or rectified if we become aware of inaccuracies.

We take every reasonable step to ensure that:

- your Personal Data that we Process are accurate and, where necessary, kept up to date; and
- any of your Personal Data that we Process that are inaccurate (having regard to the purposes for which they are Processed) are erased or rectified without delay.

From time to time we may ask you to confirm the accuracy of your Personal Data.

(L) Data minimisation

Summary – Data minimisation
We take every reasonable step to limit the volume of your Personal Data that we Process to what is necessary.

We take every reasonable step to ensure that your Personal Data that we Process are limited to the Personal Data reasonably necessary in connection with the purposes set out in this Notice.

(M) Data retention

Summary – Data retention
We take every reasonable step to ensure that your Personal Data are only retained for as long as they are needed in connection with a lawful purpose.

We take every reasonable step to ensure that your Personal Data are only Processed for the minimum period necessary for the purposes set out in this Notice. The criteria for determining the duration for which we will retain your Personal Data are as follows:

(1) we will retain Personal Data in a form that permits identification only for as long as:

(a) we maintain an ongoing relationship with you (e.g., where you are a user of our services, or you are lawfully included in our mailing list and have not unsubscribed); or

(b) your Personal Data are necessary in connection with the lawful purposes set out in this Notice, for which we have a valid legal basis (e.g., where your personal data are included in a contract between us and you, and we have a legitimate interest in processing those data for the purposes of operating our business and fulfilling our obligations under that contract; or where we have a legal obligation to retain your Personal Data

Plus (2) the duration of:

(a) any applicable limitation period under Applicable Law (i.e., any period during which any person could bring a legal claim against us in connection with your Personal Data, or to which your Personal Data are relevant); and

(b) an additional two (2) month period following the end of such applicable limitation period (so that, if a person brings a claim at the end of the limitation period, we are still afforded a reasonable amount of time in which to identify any Personal Data that are relevant to that claim),

and:

(3) in addition, if any relevant legal claims are brought, we continue to Process Personal Data for such additional periods as are necessary in connection with that claim.

During the periods noted in paragraphs (2)(a) and (2)(b) above, we will restrict our Processing of your Personal Data to storage of, and maintaining the security of, those data, except to the extent that those data need to be reviewed in connection with any legal claim, or any obligation under Applicable Law.

Once the periods in paragraphs (1), (2) and (3) above, each to the extent applicable, have concluded, we will either:

- permanently delete or destroy the relevant Personal Data; or
- anonymize the relevant Personal Data.

(N) Your legal rights

Summary – Your legal rights
Subject to Applicable Law, you may have a number of rights, including: the right not to provide your Personal Data to us; the right of access to your Personal Data; the right to request rectification of inaccuracies; the right to request the erasure, or restriction of Processing, of your Personal Data; the right to object to the Processing of your Personal Data; the right to have your Personal Data transferred to another Controller; the right to withdraw consent; and the right to lodge complaints with Data Protection Authorities. In some cases it will be necessary to provide evidence of your identity before we can give effect to these rights.

Subject to Applicable Law, you may have the following rights regarding the Processing of your Relevant Personal Data:

- the right not to provide your Personal Data to us (however, please note that we will be unable to provide you with the full benefit of our Sites, Apps, or services, if you do not provide us with your Personal Data – e.g., we might not be able to process your requests without the necessary details);
- the right to request access to, or copies of, your Relevant Personal Data, together with information regarding the nature, Processing and disclosure of those Relevant Personal Data;
- the right to request rectification of any inaccuracies in your Relevant Personal Data; • the right to request, on legitimate grounds:

  - erasure of your Relevant Personal Data; or
  - restriction of Processing of your Relevant Personal Data;
- the right to have certain Relevant Personal Data transferred to another Controller, in a structured, commonly used and machine-readable format, to the extent applicable;
- where we Process your Relevant Personal Data on the basis of your consent, the right to withdraw that consent (noting that such withdrawal does not affect the lawfulness of any Processing performed prior to the date on which we receive notice of such withdrawal, and does not prevent the Processing of your Personal Data in reliance upon any other available legal bases); and
- the right to lodge complaints regarding the Processing of your Relevant Personal Data with a Data Protection Authority (in particular, the Data Protection Authority of the EU Member State in which you live, or in which you work, or in which the alleged infringement occurred, each if applicable).

Subject to Applicable Law, you may also have the following additional rights regarding the Processing of your Relevant Personal Data:

- **the right to object, on grounds relating to your particular situation, to the Processing of your Relevant Personal Data by us or on our behalf; and**
- **the right to object to the Processing of your Relevant Personal Data by us or on our behalf for direct marketing purposes.**

This does not affect your statutory rights.

To exercise one or more of these rights, or to ask a question about these rights or any other provision of this Notice, or about our Processing of your Personal Data, please use the contact details provided in Section (R) below. Please note that:

- in some cases it will be necessary to provide evidence of your identity before we can give effect to these rights; and
- where your request requires the establishment of additional facts (e.g., a determination of whether any Processing is non-compliant with Applicable Law) we will investigate your request reasonably promptly, before deciding what action to take.

(O) Cookies and similar technologies

Summary – Cookies and similar technologies
We Process Personal Data by using Cookies and similar technologies. For more information, please see our Cookie Policy.

When you visit a Site or use an App we will typically place Cookies onto your device, or read Cookies already on your device, subject always to obtaining your consent, where required, in accordance with Applicable Law. We use Cookies to record information about your device, your browser and, in some cases, your preferences and browsing habits. We Process Personal Data through Cookies and similar technologies, in accordance with our Cookie Policy.

(P) Terms and Conditions

Summary – Terms and Conditions
Our Terms of Use govern all use of our Sites, Apps and our Services.

All use of our Sites, Apps, or services is subject to our Terms and Conditions. We recommend that you review our Terms and Conditions regularly, in order to review any changes we might make from time to time.

(Q) Direct marketing

Summary – Direct marketing

We Process Personal Data to contact you with information regarding Sites, Apps, or services that may be of interest to you. You may unsubscribe for free at any time.

We Process Personal Data to contact you *via* email, telephone, direct mail or other communication formats to provide you with information regarding Sites, Apps, or services that may be of interest to you. If we provide Sites, Apps, or services to you, we may send information to you regarding our Sites, Apps, or services, upcoming promotions and other information that may be of interest to you, using the contact details that you have provided to us, subject always to obtaining your prior opt-in consent to the extent required under Applicable Law.

You may unsubscribe from our promotional email list at any time by simply clicking on the unsubscribe link included in every promotional email we send. After you unsubscribe, we will not send you further promotional emails, but in some circumstances we will continue to contact you to the extent necessary for the purposes of any Sites, Apps, or services you have requested.

(R) Contact details

Contact details for Coin Rivet are as follows:

Coin Rivet Group
107 Leadenhall street
London
EC3A 4AF

Email: support@coinrivet.com

(S) Definitions

- "**Adequate Jurisdiction**" means a jurisdiction that has been formally designated by the European Commission as providing an adequate level of protection for Personal Data.

- "**App**" means any application made available by us (including where we make such applications available *via* third party stores or marketplaces, or by any other means).

- **Applicable Laws**" means any applicable statutes, laws, ordinances, orders, judgments, decrees, rules or regulations issued by any government authority, and any judicial or administrative interpretation of any of these;

- "**Cookie**" means a small file that is placed on your device when you visit a website (including our Sites). In this Notice, a reference to a "Cookie" includes analogous technologies such as web beacons and clear GIFs.

- "**Controller**" means the entity that decides how and why Personal Data are Processed. In many jurisdictions, the Controller has primary responsibility for complying with applicable data protection laws.

- "**Data Protection Authority**" means an independent public authority that is legally tasked with overseeing compliance with applicable data protection laws.

- "**EEA**" means the European Economic Area.

- "**Personal Data**" means information that is about any individual, or from which any individual is directly or indirectly identifiable, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

- "**Process**", "**Processing**" or "**Processed**" means anything that is done with any Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- "**Processor**" means any person or entity that Processes Personal Data on behalf of the Controller (other than employees of the Controller).

- "**Profiling**" means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- "**Relevant Personal Data**" means Personal Data in respect of which we are the Controller.

- "**Sensitive Personal Data**" means Personal Data about race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, any actual or alleged criminal offences or penalties, national identification number, or any other information that are deemed to be sensitive under Applicable Law.

- **Services** has the same meaning as defined in clause 4.1 of the Coin Rivet Terms and Conditions

- "**Standard Contractual Clauses**" means template transfer clauses adopted by the European Commission or adopted by a Data Protection Authority and approved by the European Commission.

- "**Site**" means any website operated, or maintained, by us or on our behalf.