PRIVACY STATEMENT FOR USERS

0. EXECUTIVE SUMMARY

0.1 Why, what, where, when, who, and how (long)

Why: In order for you to be able to open a payment account and use our services, we need to comply with relevant applicable know your customer (KYC) and anti-money laundry (AML) laws and legislation which requires KYC/AML verification (including transaction (and ongoing) monitoring, enhanced due diligence, sanctions & politically exposed persons screening).

In order to comply with KYC/AML requirements and render our services to you, we need to process some of your personal data as further described below.

What: We collect and process certain personal and non-personally identifiable information to offer, enable and improve our service and payment platform. The non-personally identifiable information includes transactional data and product usage data. For the (KYC/AML) verification service, we may ask you to provide certain personal data, such as your full name, email address, telephone number, date and place of birth, gender, nationality, driver's license/passport/ID details (including your picture), bank account details, debit/credit card details.

What else – rights: You will have all rights granted by applicable law, such as the right to know what information we hold, the right to be forgotten, and the right to amend, correct, delete, or block your personal information

What else – security: We have implemented a range of procedures, controls and measures to prevent unauthorized access to, and the misuse of, your personal data that we process.

When: Upon registration with HenriPay (or at any time thereafter), HenriPay may ask you to provide, update and complete relevant required personal information in its system through the website/app on which the HenriPay service is available to you. Please note not all services may be available to you if we do not have the required and requested relevant information from you.

Who: HenriPay is responsible for the data it collects and acts as a data controller. HenriPay may share the relevant personal information with banks, payment institutions and regulatory authorities (including central banks) where required, which shall also act as (independent or co-) data controller upon receipt of the relevant information. HenriPay and each (independent or co-) data controller shall each be solely responsible for the processing of personal data by itself or on its behalf in accordance with applicable data protection laws.

[Furthermore, HenriPay may share certain personal information with its affiliated group companies (e.g. for customer service) and trusted subcontractors. HenriPay is responsible for these parties (which act as data processor subject to a data processor agreement with HenriPay).]

How (long): We will collect and process your personal information in accordance with this privacy statement and retain your personal data for as long as necessary to manage our business relationship with you, provide HenriPay services to you, and comply with applicable laws, including those related to document retention. We will also retain some data to resolve disputes or claims with third parties and, if necessary, to conduct our business

The above is a general overview. Depending on the law that applies to you, we might be required to provide some additional information. Please find below more detailed information about the use and process of your personal information.

Glossary: appendix 1 includes a glossary with relevant privacy terms and their definitions.

0.2 BEWARE OF PHISHING AND FRAUDSTERS

We will never call, SMS or email to verify your account or ask by phone, email, text message (SMS), whatsApp or other form of messenger for your log in details (including one-time authentication code, PIN or CVV code) (also known as phishing). We will never ask you to log in to the Platform through a link in an email or text message.

Never enter your bank details, PINs, security codes or response codes on a website that you have accessed after clicking a link in an email, SMS or other message communication.

We will not call you to discuss problems with your account or possible fraud. We will never ask you by phone to transfer money.

Tips to prevent phishing, malware and scamming:

- *Always check the sender's email address. Never click on attachments or links in an unexpected or suspicious email.*
- *Always check if the link or URL address (website) in an email, SMS or text message is from https://henripay.com*
- *Make sure that your passwords are secure, strong, unique and change them regularly. And ensure that your telephone and smartphone, computer and laptop have the latest software and security updates installed. Only download apps from official (Apple or Google) app store.*
- *Do not share your personal data over the phone. Call us back if you do not trust our phone call.*
- *Check your account at least once every two weeks.*

1. INTRODUCTION, SCOPE AND DEFINITIONS

1.1 About HenriPay

1.1.1 We are HenriPay OÜ, a limited liability company, incorporated under the laws of Estonia and having its registered office at Harju maakond, Tallinn, Estonia, Kesklinna linnaosa, Narva mnt 5, 10117. Company code 16777340. HenriPay OÜ may be referred to in this document as 'we', 'us', 'our', or 'HenriPay'.

1.1.2 We collect personal data via our Platform (app) and service and act in this respect as the data controller of your personal data.

1.1.3 The personal data that HenriPay collects in relation to its users depends on the context of the business relationship and their interaction with HenriPay, the choices the user makes, and the products, services and functions they use.

1.2 Privacy statement and acceptance

1.2.1 This privacy statement explains how HenriPay processes your personal data. 'You', 'your' or 'User' means you, the user of our service as made available on our website/app (the "**Platform**"), including any other natural person of whom the personal data is provided to HenriPay.

1.2.2 This privacy statement applies to every group company of HenriPay that is responsible for or involved in the processing of a User's personal data. Depending on the nature of the business relationship, various group companies of HenriPay may be responsible for the processing of that personal data.

1.2.3 To the extent permitted or required by law, by signing up for an account, registering (including uploading, submitting or otherwise enabling your personal data) and/or using our services, you hereby (i) accept, acknowledge (to have read and understood) and agree to this privacy statement, and (ii) give your explicit consent to HenriPay to collect, use, transfer, disclosure or process the personal data as from time to time provided or otherwise made available to us for purposes and to such recipients and locations as described in the privacy statement.

1.3 DPO

1.3.1 HenriPay has appointed a Data Protection Officer (DPO). If you have any questions about the processing of personal data after reading this Privacy Statement, you can contact our DPO via privacy@henripay.com. If you want to cancel your account or have any other questions about your account or our services, please contact our support via Support@henripay.com.

1.4 Minors

1.4.1 We collect and process personal data from minors only with parental consent when they become a user and use our services.

2. DATA COLLECTION

2.1 Personal data that HenriPay collects

2.1.1 Personal data that you – as a User – (may) provide to us includes:

- **Personal data**

  If you wish to open an account with us, we may collect relevant contact information from Users, such as first and last name, place/date of birth (if required), nationality, gender, (email) addresses, (mobile) telephone numbers, debit/credit card details (if required), (preferred) bank account details, counter IBAN, etc.

  Furthermore, we collect your social security numbers and/or other tax identification numbers including the type of identification document, the issuing date and the issuing institution

  In order to screen and verify your identity, we collect your picture of an identification document and video identification data made during the screening process when opening an account.

  Authentication methods based on biometrical data, such as fingerprint scans, are not stored, used or shared in a format that allows us to reproduce the biometrical data.

- **Transactional data**

  We collect information about your transactions (including transaction history), including the volume, price, value, currency, frequency and other relevant information for or in respect of transactions processed or paid through our service (including your bank account, debit/credit cards). This may include personally identifiable information.

- **Usage data**

  Information we collect automatically about how you use our Platform (i.e. app or website) and service (the "**Product Usage Data**"), including information on the device(s) you use (the "**Device Information**") and information on when, where and how you use our Platform and/or Software, including your IP address and info such as your browser type (the "**Log Data**"). For a more specific overview of what data and information (including personal data) is collected automatically, see below and our cookie statement [link].

- **Other data**

  When a User communicates with HenriPay, we may collect and process information about this communication. During calls with our customer service (including when being in queue or on hold), live listening and calls can be recorded for quality control and training purposes. These recordings can also be used for claims handling and fraud detection.

  Recordings are kept for a limited time before they are automatically deleted unless HenriPay has a legitimate interest in keeping the recording for longer. This only happens in exceptional cases, such as for fraud investigation, compliance, and legal purposes.

2.2 Information We Collect Automatically

2.2.1 Depending on the business relationship, HenriPay may also automatically collect information, some of which may be personal data. This data is collected when a User uses online services such as a registration form or a user account.

The data collected may include:

- Language settings
- IP address
- Place
- Device settings
- Device operating system
- Log information
- Time of use
- URL requested
- Status report

- User-agent (information about the browser version)
- Browsing history
- Browsing behaviour
- The type of data being viewed

2.2.2 Furthermore, we automatically collect and process the following information while using our service and platform:

- first and last names, phone numbers and email addresses of the contacts in your phone's address book;
- location data via GPS;
- uploaded images/content;
- device data of added devices and API-keys;
- added aliases (telephone numbers and email addresses);
- financial and banking data, product subscriptions and transaction history;
- cookies and usage data on how you use our products and services;
- marketing data (statistics related to our marketing campaigns and data to measure this);
- correspondence with HenriPay and support data (telephone, chat conversations, email, voice and screen recordings).

2.3 Other information we receive from other sources

- **Other payment institutions**

  Other payment institutions (banks, credit card companies, etc) may share certain personal data with us. This can include your credit card details, bank account, phone number, country, your email address and your name. To learn more about the data processing that occurs when making use of the services offered by these third parties, see relevant third party' privacy statement for more information.

- **Data related to requests from law enforcement and tax authorities**

  Law enforcement or tax authorities may contact HenriPay with additional information about Users in the event that they are affected by an investigation.

- **Fraud detection & prevention, risk management & compliance**

  In certain cases, and as permitted by applicable law, HenriPay may need to collect data from third-party sources for fraud detection and prevention, risk management, and compliance purposes (e.g. sanction/PEP screening).

3. PROCESSING PURPOSES AND SHARING

3.1 Purposes

3.1.1 HenriPay uses the previously described information about Users, some of which may be personal data, where relevant, for the following purposes:

A. Registration and administration

HenriPay uses account information, contact details, and financial information to manage and maintain the business relationship with the User and to render its service to you. This also applies to registration and verification purposes.

B. Render its service (including verification service and customer service)

HenriPay uses the information provided by Users, which may include personal data to provide and support its services.

C. Other activities, including marketing

If a potential User has not yet completed the online registration, HenriPay may send a reminder to complete the registration process. We believe that this extra service is useful for our (future) Users because it allows them to complete the registration without having to re-enter all registration details.

HenriPay may invite Users to complete user/product reviews, ratings and scores and attend (online) events, seminars, webinars that may be relevant or interesting to them or where they can share crypto or Fiat Gateway related products and services. We may also use personal data to provide and host online forums that allow Users to find answers to frequently asked questions about the range and use of HenriPay's products and services.

Marketing (e.g. newsletters): To the extent relevant to the business relationship, HenriPay may use personal data for communication, including providing information about its systems or product updates, sending HenriPay newsletters, and inviting Users to participate in references, promotions, or for other marketing communications. When we use personal information to send direct marketing messages electronically not for or related to our service, we offer an active opt-in option.

D. Communication with users

For any User who has signed up for an account, HenriPay may have (access to) communication with you (telephone, chatbot, email, Platform). We may use automated systems to review, scan and analyze communications for the following purposes:

- Safety
- Fraud prevention
- Compliance with legal and regulatory requirements
- Research nasty possible misconduct
- Product development and improvement
- Research
- Customer engagement (including providing information or offers to Users that we think may be of interest to them)
- Customer or technical support

Communications sent or received using HenriPay's means of communication are received and stored by HenriPay. We do not record all calls. If a call is recorded, each recording is kept for a limited time before being automatically deleted. This is the case unless we have determined that it is necessary to keep the recording for fraud investigation or legal purposes.

E. Analysis, improvement and research

HenriPay uses the information provided to us, which may include personal data, for analytical and research purposes. This is part of our commitment to improve HenriPay's products and services and to improve the user experience in respect of our Platform and Service (e.g. customize the content, user experience and layout of the Platform).

The data can also be used for identification of IT or network issues, testing purposes, troubleshooting and improving the functionality and quality of HenriPay's online services. We may also record some live sessions using tools such as Hotjar and invite users to participate in surveys and other market research from time to time.

Certain Users may be invited to join a user forum to communicate with HenriPay and/or to exchange experiences with other Users.

Please refer to the information HenriPay provides when you are invited to participate in a survey, market research or to join an online Platform to understand how your personal data may be treated differently than described in this Privacy Statement.

F. Security, fraud detection, administration and prevention

We process the information provided to us, which may include personal data, to investigate, prevent and detect fraud and other illegal acts and to manage our Platform (including Service and system administration). This may include personal data that a User has provided to HenriPay, for example for security and verification purposes as part of the registration process, personal data collected

automatically, or personal data obtained from external sources (including from guests). We also use the information to identify mal-intended usage of our Platform, Service and/or Software, prevent fraud, money laundering and unauthorized use of our Service, Platform and Software.

HenriPay may also use personal data to facilitate investigation and enforcement by competent authorities, if necessary. For these purposes, personal data may be shared with law enforcement authorities.

HenriPay may also use personal data for risk assessment and security purposes, including user authentication, and we use external service providers for third-party risk management. These providers help us assess the business risk profile of our Users. They may also provide us with due diligence reports from third parties, which, as permitted by applicable law, may contain potential information about criminal convictions and owner or User violations.

G. Legal, regulatory and compliance

In certain cases, HenriPay must use the information provided (which may include personal data) to handle and resolve legal disputes or for regulatory investigations, risk management and (regulatory) compliance. We may also use it to enforce our agreement(s) with Users or to resolve any complaint or claim involving a User, and in accordance with internal rules and procedures.

In addition, we may need to share information about Users (including personal data) where required to do so by law or strictly necessary to respond to requests from competent authorities. This includes tax authorities, central banks, courts, other government and public authorities, or local municipalities (for example, regarding short-term rental laws).

Finally, HenriPay may use personal data for AML verification and KYC related purposes and obligations (including sanction screening for 'politically exposed persons' (PEPs) and sanctioned individuals).

If we use automated means to process personal data that produces legal effects or significantly affects you or other natural persons, we will take appropriate measures to safeguard your or the other person's rights and freedoms. This includes the right to human intervention.

3.2 Legal grounds

3.2.1 First of all, HenriPay strongly believes that the User should be in control of its personal data. Therefore and save as set out otherwise below, HenriPay will at all times obtain your consent before processing personal data for any services you wish to use from HenriPay, including for marketing and profiling purposes or as otherwise required by law.

3.2.2 Purpose A and B: In addition to the consent, HenriPay assumes the legal basis that the processing of personal data for purposes A and B is also necessary for the execution of the agreement between the User and HenriPay. If the required information is not provided, HenriPay may not be able to fully service a User and provide its services (such as the verification service), nor will we be able to provide customer service.

3.2.3 Purposes C to G: HenriPay relies on its legitimate interest to provide its services to, or obtain services from Users, to prevent and combat misuse, fraud and crimes, and to improve its services, analyse the use of our products and services for the purpose of improving them, for information and system security purposes or for offering you a better user experience. When we use personal data to serve the legitimate interest of HenriPay or a third party, we will always balance the rights and interests of the data subject and the protection of their information against the rights and interests of HenriPay and/or the third party.

3.2.4 Purpose F and G: HenriPay also relies, where applicable, on compliance with legal obligations (such as lawful law enforcement requests and compliance with financial laws for AML/KYC purposes (including sanction screening)).

3.2.5 Important notice: you can at all times withhold or withdraw your consent without detriment. If you wish to object to the processing as set out under C to G and cannot find a way to opt out directly (for example in your account settings), please contact HenriPay at compliance@HenriPay.com.

3.3 Automatic decisions

3.3.1 When you use our services, automated decisions can be made about you, which will include profiling. Automatic decisions with the use of your personal data can be made for monitoring how our services

are used to detect fraud, money laundering, and other crimes and prevent the continuation of misuse of our services.

3.3.2 You have the right to request a manual review of automatic decisions.

4. SHARE WITH OTHERS

4.1 Sharing with affiliated group companies

4.1.1 To support the use of HenriPay services, your information (which may include personal data) may be shared with or within HenriPay affiliates. This is done for the purposes described below, subject to any contractual terms.

The purposes for sharing data within the HenriPay group of companies are:

A. to offer, provide or make available services and products and to provide (customer) support;

B. to prevent, detect and investigate fraud and other illegal activities;

C. for analytical, quality, and product improvement purposes (including monitoring conversations by live listening or recording for quality and training purposes);

D. marketing activities (including news items) from which you can easily unsubscribe or unsubscribe) and to personalize online services (including personalized offers and promotions);

E. communication purposes (by email, telephone, or post) for the above purposes (including survey, market research, reviews, or ratings) or as necessary under our agreement with you;

F. legal purposes, including the handling of complaints, claims, legal claims, and for the detection of fraud (in which cases any telephone conversations may be recorded);

G. to ensure compliance with applicable (financial and privacy) laws or law enforcement.

With a view to purpose A, and insofar as applicable, HenriPay relies on the legal basis that the processing of personal data is necessary for the performance of the agreement with you for the purchase, booking, reservation, order, or use of the product or service as offered by the travel provider.

HenriPay further relies on its legitimate interest and that of its group companies to receive, process, and share personal data as described under B to G. This is to provide services to or obtain services from Users, including to improve the services and prevent fraud or other illegal acts. When personal data is used to serve the legitimate interest of HenriPay or a third party, HenriPay will always balance the rights and interests of the person concerned in protecting their personal data and the rights and interests of HenriPay or the third party.

For purpose G, HenriPay also relies on compliance with legal obligations where applicable (such as lawful law enforcement requests or enforcing its terms and conditions for use of the service and compliance with financial laws for AML/KYC purposes (including sanction screening)).

Finally, where needed under applicable law, HenriPay will obtain your consent prior to processing your personal data, including for email marketing purposes or as otherwise required by law.

If you wish to object to the processing as set out under B to G, and cannot find a way to unsubscribe directly (for example in your account settings), please contact HenriPay at compliance@HenriPay.com

4.2 Sharing with third parties

4.2.1 We share Users' information (which may include personal data) with third parties, as permitted by law and as set out in paragraph 8 and described below:

(a) banks and financial institutions (including payment service providers). We may transfer, disclose, share or otherwise enable your personal data with banks and financial institutions (including payment service providers) to (i) render our service to you (e.g. process payment transactions from you) and (ii) allow them to offer, facilitate or provide their product or service to you (including further process, execute or receive payment transactions from you). Depending on the product or service used, ordered or booked by you, the details we share

can include your name, contact and payment/bank account details and any other information you specified or included in transfer or payment order or when using the relevant service or product of the relevant bank and financial institution (including payment service provider). The banks and financial institutions shall also act as (co-) data controller upon receipt of the relevant information. HenriPay and of the foregoing shall each be solely responsible for the processing of personal data by itself or on its behalf in accordance with applicable data protection laws. The payment service provider acts as data processor (see below for more information).

(b) Service providers (including suppliers, auxiliaries, and subcontractors). We share personal information with selected and trusted third-party service providers that support us when rendering services and making our products available (e.g. payment service providers), prevent and detect fraud, store data and otherwise support our business processes, or so that they can conduct business on our behalf.

(c) To the extent that you have signed up for an account, we may share your personal data with trusted partners which conduct KYC/AML verification and screening of sanctions lists as required by applicable law.

(d) Forced disclosure. When required by law, strictly necessary for the performance of our services, in legal proceedings, or to protect our rights or the rights of users, we disclose personal data to law enforcement agencies, research organizations or group companies.

As applicable and unless indicated otherwise, for purposes (a), (b) and (c) HenriPay relies on the legal basis that the processing of personal data is necessary for the performance of a contract, and for purposes (a) to (c), HenriPay (also) relies on its legitimate interests to share, process, enable and receive personal data, and, where applicable, for (c) and (d) on compliance with legal obligations (such as lawful law enforcement requests).

Third party's to which you (wish to) transfer funds, may also ask for additional personal data, for instance to provide their services, or to comply with local regulations and restrictions. If available, please read the privacy statement of the relevant Fiat Gateway to understand how they process your personal data and how to enforce your rights.

4.3 Sharing and disclosure of aggregated data

4.3.1 We may share information with third parties in an aggregated form and/or another form in which the recipient cannot identify you, for example for industry analysis or demographic profiling.

5. SECURITY, PROTECTION AND CROSS BORDER TRANSFER

5.1 You have access to your personal data via your account.

5.2 We have procedures and controls in place to prevent unauthorized access to and misuse of personal data.

5.3 We employ industry-standard security measures designed to protect the security of all information submitted through the Software. We use appropriate business systems, controls and procedures to protect and secure information, including personal data. We also use security procedures and technical and physical restrictions to access and use the personal information on our servers. Only authorized personnel have access to personal data in the context of their work.

5.4 Please be aware that your data might be transferred to, processed, and stored in the United States or other non-EEA jurisdictions. Whenever we transfer your personal information out of the EEA to the U.S. or countries not deemed by the European Commission to provide an adequate level of personal information protection, the transfer will be based on a data transfer mechanism recognized by the European Commission as providing adequate protection for personal information.

6. DATA RETENTION

6.1 We retain personal data for as long as it is deemed necessary to manage the business relationship with a User, to provide HenriPay services to a User, and to comply with applicable laws (including

those relating to the retention of documents), disputes, or claims with any parties, and if otherwise necessary to enable us to conduct our business.

6.2 We are legally obliged to retain certain data for a minimum of 5 to 7 years after ending the customer relationship and in other cases up to 10 years, as in the case of accounting obligations. We are able to store personal data for longer periods with a valid legal ground, or when the data is sufficiently pseudonymised or anonymised.

6.3 Upon termination of the agreement with you, we will in any event delete all your personal data after 10 years after termination of the agreement (or for certain relevant personal information such longer period as required by law).

6.4 Any personal data we hold about you as a User is subject to this privacy statement and our internal retention guidelines. If you have any questions about the specific retention periods for the different types of personal data we process, please contact HenriPay at privacy@henripay.com.

7. YOUR CHOICES AND RIGHTS

7.1 Depending on where you are located or the entity of HenriPay that processes your personal data, different rights may apply to the processing of that data, as set out in this privacy statement (see below for more information). As applicable:

- You can ask us for a copy of the personal data we hold about you,
- You can notify us of any changes to your personal information, or you can ask us to correct the personal information we hold about you,
- In certain situations, you can ask us to delete, block, amend, or restrict the personal information we hold about you, or you can object to certain ways in which we use your personal information,
- In certain situations, you can also ask us to send the personal data you provide to us to a third party.

7.2 Where we use your personal information based on your consent, you have the right to withdraw that consent at any time, subject to applicable law. Where we process your personal data on the basis of legitimate interest or public interest, you also have the right to object at any time, subject to applicable law.

7.3 Regardless of your location or the HenriPay entity you have a contract with, we rely on our Users to ensure that the personal information we hold is complete, accurate, and current. Always inform us in good time of any changes or inaccuracies in your personal data.

7.4 To protect your privacy and security, we will verify your identity before responding to such request, and your request will be answered within a reasonable timeframe. We may not be able to allow you to access certain personal data in some cases e.g. if your personal data is connected with personal data of other persons, or for legal reasons. In such cases, we will provide you with an explanation why you cannot obtain this information. We may also deny your request for deletion or rectification of your personal data if you have future/ongoing service with us or due to statutory provisions, especially those affecting our accounting processes, processing of claims, for fraud detection or prevention purposes, and mandatory data retention, which may prohibit deletion or anonymization.

7.5 Below we have outlined the rights GDPR grants you and what this means for you in the context of your activities with HenriPay.

(i) Right to be informed (Article 13 GDPR): We provide you with the necessary information regarding the collection and usage of your personal data through this Privacy Statement.

(ii) Right to access personal data (Article 15(1) GDPR): If you file a data access request, we will provide you with a copy of all the personal data we have collected about you. You also have the right to receive this information in a way that is structured, commonly used, and machine-readable.

(iii) Right to request deletion of personal data (Article 17(1) GDPR): We will delete the personal data we have collected about you upon request, provided you are no longer an active user

with us and we are not legally required to keep the data. Certain information may be retained due to Estonian law requirements.

(iv) Right to rectification of incorrect or incomplete information (Article 16(1) GDPR): If you notice anything incorrect or incomplete in your personal information, let us know, and we will rectify it as soon as possible.

(v) Right to object to processing of personal data (Article 21(1) GDPR): You can object to the processing of your personal data based on legitimate interest. We will assess your request and consider whether there's an overriding reason to continue processing the data. Objections may not apply if there's a legal obligation or contractual necessity.

(vi) Right to request restriction of processing of personal data (Article 18 GDPR): You can request the temporary suspension of processing your personal data if:

- you contest the accuracy of the information;
- processing is unlawful but you want us to retain the data;
- processing is unlawful, but you need us to maintain the information for legal reasons, or
- you have objected to the processing, and we are evaluating your request.

(vii) Right not to be subject to automated decisions (Article 22 GDPR): We will manually review any personal data subject to automated decisions in the past.

(viii) Right to lodge a complaint with data protection supervisory authority (Article 77 GDPR): You have the right to lodge a complaint with the Estonian Privacy Authority if you believe the processing of your personal data violates the GDPR.

8. THIRD PARTIES WE USE

8.1 We use the following third parties, which act as our data processor (unless indicated otherwise), subject to an appropriate data processing agreement, or which jointly offer products and services with us.

Integrated Finance: offering of technology to be able to provide issuing of IBAN's so consumers can load, manage and send funds form within the HenriPay application.

Clear Bank: underlying licensed entity that owns the NL IBANs on behalf of clients who have opened an IBAN within the HenriPay Application. They are a licensed entity and allowed by the DNB to offer banking services to consumers.

Comply Advantage: transaction monitoring for and on behalf of HenriPay to ensure we comply with all the anti-money laundering and fraud detection requirements as prescribed by applicable laws.

Transact Payments Malta Limited: is the underlying licensed entity that issues you with payment accounts within the HenriPay Application. They are a licensed e-money institution and are regulated by the Malta Financial Services Authority.

Wallester AS: issuing of Visa Debit cards (personal debit cards) to consumers and also to offer shared card solutions inside of 'Splitty'.

Moneythor Pte. Ltd: a software tool which utilises data by accessing and leveraging open banking data, give clear insights in customer behaviour at their benefit so they can manage, grow and budget their money better as well as track their carbon footprint and refer friends with rewards. We can enrich data, make personal financial management easy, offer budgeting tools and give insights in carbon footprint on every transaction as well as a referral management system so our clients can refer and earn money easily.

9. DISCLAIMER

9.1 We are not responsible for any interception or interruption of any communications through the internet or for changes to or losses of data. Users of the Software are responsible for maintaining the security of any password (which needs to be unique and strong) or another form of authentication

involved in obtaining access to password protected. To protect you and your data, we may suspend your use of any of the software, without notice, pending an investigation, if any breach of security is suspected.

10. CONTACT US AND COMPLAINTS

10.1 If you have any questions, wishes, complaints or comments about how we process your personal data, or if you would like to exercise any of the rights you have under this Privacy Statement, please contact us at compliance@HenriPay.com. You can also contact your local data protection authority.

10.2 We handle privacy-specific questions, requests, and concerns reported to us using internal policies and procedures based on applicable privacy laws, regulations, and guidelines. We regularly review and improve this policy and procedures, also taking into account User feedback.

11. CHANGES TO THIS PRIVACY STATEMENT

This privacy statement may be amended or supplemented from time to time. If we intend to make material changes or changes that affect you, we will always contact you in advance. An example of this type of change would be if we started processing your personal data for purposes not described above.

Version: 2 July 2024.

APPENDIX 1 – Glossary and definitions

Some useful terms and definitions:

"**Algorithm**" means a computational procedure or set of instructions and rules designed to perform a specific task, solve a particular problem, or produce a machine learning or AI model.

"**Anonymization**" means the process in which individually identifiable data is altered in such a way that it no longer can be related back to a given individual.

"**Automated processing**" means a processing operation that is performed without any human intervention.

"**Caching**" means the saving of local copies of downloaded content, reducing the need to repeatedly download content.

"**Cookie**" means a small text file stored on a client machine that may later be retrieved by a web server from the machine. Cookies allow web servers to keep track of the end user's browser activities, and connect individual web requests into a session. Cookies can also be used to prevent users from having to be authorized for every password protected page they access during a session by recording that they have successfully supplied their username and password already.

"**Data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**Data controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

"**Data minimisation**": The principle of "data minimisation" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose.

"**Data processor**" means a natural or legal person (other than an employee of the controller), public authority, agency or other body which processes personal data on behalf of the controller.

"**Personal data**" means any information that relates to an identified or identifiable living individual (e.g. name, address, email, etc). Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data (e.g. location data, IP data, ID number, etc). Personal data that has been de-identified, encrypted or **pseudonymised** but can be used to re-identify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

"**PEP**" (politically exposed person) means any of the following persons: (i) head of state, head of government, minister, deputy minister or state secretary, (ii) member of Parliament or member of a similar legislative body, (iii) member of the board of a political party, (iv) member of a Supreme Court, Constitutional Court or other high-level court that gives rulings against which, except in exceptional circumstances, no appeal is possible, (v) member of a court of audit or a board of directors of a central bank, (vi) ambassador, agent or senior officer of the armed forces, (vii) member of the management, supervisory or administrative bodies of a state-owned company, (viii) director, deputy director, member of the board of directors or person holding an equivalent position at an international organization, or (ix) any of their family members (child, sibling or parent) or their spouse or partner.

"**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.