Privacy Policy

Last updated: 01.09.2023

Please read this privacy policy ("**Policy**") carefully to understand our policies and practices regarding your personal data and how we will treat it. This privacy policy will explain how DEX GlobalPay UAB (hereinafter referred to as „**Company**", „**we**", „**us**") processes personal data and how we apply data protection principles.

SCOPE OF THIS POLICY

This Policy applies to our relations with customers, including any potential customers, or any other person using or wishing to use any of our services, or addressing us with any request or claim, submitting any kind of document, visiting our web page or contacting us through remote means of communications, including post, e-mail or phone (hereinafter referred to as "you"). This Policy thus covers both our online and offline data collection activities, including personal data that we collect through our various channels such as websites, apps, third party networks or events. Certain parts of this Policy, where explicitly stated, apply to Trusted Contact Person (hereinafter referred to as „TCP") as well.

To the extent that you are a customer or user of our services, this Policy applies together with any Terms and Conditions and other contractual documents, including but not limited to any agreements we may have with you.

Our products and services are not available to children

Our products and services (and our websites) are not directed to persons under the age of 18, and we do not knowingly collect personal information from children. If we learn that we have inadvertently gathered personal information from a child, we will take legally permissible measures to remove that information from our records. The Company will require the user to close his or her account and will not allow the use of our products and services. If you are a parent or guardian of a child, and you become aware that a child has provided personal information to us, please contact us at legal@dex-gp.com and you may request to exercise your applicable access, rectification, cancellation, and/or objection rights.

You have the right to refuse providing you personal data to us, but in this case we may not be able to provide you with our services. The establishment and legality of the contractual relationship between you and us is dependent on the provision of the data requested by us. You must provide to us those of your personal data are necessary for commencement and execution of a contractual-based business relationship between us and for the performance of both parties' contractual obligations.

During the course of our contractual relationship you are obliged to provide us with certain personal data, as we are compelled by applicable AML/CTF legislation and regulations to know our customer. If you fail to provide us with the requested data, the commencement or the continuation of our business relationship will not be possible.

We treat any and all personal data we process (including data of TCP) as strictly confidential, and use them in compliance with applicable data protection laws. We endeavor to maintain the highest standards of confidentiality and to respect the privacy of our customers and associated persons and other individuals whose personal information we collect and process. Our commitment to privacy includes being transparent about the nature and extent of that processing and the rights that may be available to you with respect thereto.

This Policy will help you understand the following topics:

1. What data we collect and where we obtain them from

Our Company collects the following personal data:

I. Information you provide to us - when you or a person authorised by you contact or cooperate with us or our authorised persons, for example, submit your personal data during the process of creating an account or use our services or requests any information or submit an application for examination of a particular issue or request, send us an e-mail, text or other electronic message,

• **Personal identification information** (full name, date of birth, nationality, gender)

• **Supplemental identification information** (utility bills (for your billing address), photographs and/or videos, government-issued identity document, e.g. passport, driver's license, or state identification card, employment information (e.g. company name), information on political exposure, proof of residency, including visa information)

• **Personal contact information** (address, country of residence, email address, phone number, social network details)

• **Financial information and other transaction-related data** (bank account number, payment card primary account number, trading and investment experience, expectations regarding monthly trade amount, tax identification number, income/net assets/wealth verification statements , source of funds, information about the transactions, such as the name of the sender, the name of the recipient, the amount, currency preferences, payment method, date, and/or timestamp)

• **Calls to our call center** (Communications with our call center can be recorded or listened into, in accordance with applicable laws, for local operational needs (e.g. for quality or

training purposes). Payment card details are not recorded. Where required by law, you will be informed about such recording at the beginning of your call.

• **Electronic identification information** (Biometric information generated based on photos or videos you provide in order for us to verify your identity)

• **Wallet information** (When you use certain services crypto wallet, and connect it to your account you have with us, we collect your wallet address and information related to services you use)

Please note that Personal identification information, Personal contact information and Supplemental identification information are collected also in relation to directors, employees, beneficial owners of the customer that is a legal entity.

II. Information collected automatically

• **App, browser and device data** (information about your device, unique device identifier or other device characteristics or identifiers operating system, your web address you came from or are going to, browser type, IP address, mobile network carrier, time zone or location)

• **Websites/communication and product usage information** (Information about what you view or click on while visiting our websites and Apps and how you use our services, information about how our services are performing when you use them)

• **Information from cookies, web beacons and similar technologies** (see our Cookie Policy for more information)

III. Information we obtain from third parties

• **Public database information** (We obtain information about you from public databases, such as the United Nations Sanctions List, List of financial sanctions of the European Union, Lists of financial sanctions published by the Office of Foreign Assets Control of Copyright 2023 – DEX GlobalPay UAB the U.S. Treasury Department and/or of the Republic of Lithuania, commercial registers. These information are used i.e. in the course of analysing your submitted application and implementing anti-money laundering and terrorist financing prevention requirements or sanctions requirements, know your customer requirements or implementing other legal obligations. These information include your name, address, email address, phone number, gender, national ID number and nationality/country of residence, date of birth, job role, public employment profile, listing on any sanctions lists maintained by public authorities, identities of directors, shareholders and ultimate beneficiary owners, their business ownership and control structure, information on political exposure, information on validity of identity documents)

• **Affiliates** (We may obtain information about you, such as Personal identification information, personal contact information, financial information and other transactionrelated data, website/communication and product usage information, from our Affiliates as a normal part of conducting business.)

• **Blockchain data** (We may analyze public blockchain data, including timestamps of transactions or events, transaction IDs, digital signatures, transaction amounts, and wallet addresses)

• **Information from analytics provider** (website usage, interactions, age group, and survey responses)

• **Information from our marketing and advertising partners** (We receive information such as your name and contact information from our marketing partners, including in some instances what marketing content you viewed or the actions you take on our websites)
• **Information from payment providers and credit reference agencies** (the banks you use to transfer money to us will provide us with your personal identification information, personal contact information as well as financial information and other transactionrelated information).
• **Third party social network information** (Any information that you share publicly on a third party social network or information that is part of your profile on a third party social network (such as Facebook or Twitter) and that you allow the third party social network to share with us. Examples include your basic account information (e.g. name, email address, gender, birthday, current city, profile picture, user ID, list of friends, etc.) and any other additional information or activities that you permit the third party social network to share. To learn more about how your information from a third party social network is obtained by us, or to opt-out of sharing such social network information, please visit the website of the relevant third party social network.)
• **Information about the Trusted Contact person** (we receive information about TCP such as name, surname, address, date of birth and relationship to the customer) from the Customers in case they wish to appoint TCP.
• **Information obtained from TCP** (we receive information from TCP about your current contact details, possible exploitation, your legal guardian, executor, trustee, or holder of a power of attorney, health status if there are concerns about your ability to make financial decisions)

Sensitive data

We request that you do not send us any sensitive data such as information related to racial or ethnic origin, political opinions, religious beliefs, health data, or genetic, criminal background or trade union membership information. If you do send us this information, then you are consenting to its processing in accordance with this Policy. To avoid processing of sensitive data, do not submit it.

2. Why and how will we use your personal data and on what legal grounds

Our Company collects and processes your personal data in the following circumstances (legal grounds):

• **with your consent**

You have the right to withdraw your consent at any time (note that this withdrawal will not affect our prior use of your data, based on your previously given consent).

Why we process your personal data	**Categories of personal data**
To enable device-based settings Collecting information that you allow us to receive through the device-based settings you enable (such as access to your GPS location, camera or photos) which we use to provide the features or services described when you enable the setting.	App, browser and device data
To send marketing communications, offers of products and services, and targeted advertising	Personal identification information; Supplemental identification information;

We may send commercial communications and/or newsletters, and may offer services via e-mail, mobile, inapp, and push notifications or by sms.	Personal contact information; Financial information and other transaction – related data; Websites/communication and product usage information; Information from our marketing and advertising partners; App, browser and device data
Personalisation We use your personal data (i) to analyse your preferences and habits, (ii) to anticipate your needs based on our analysis of your profile, (iii) to improve and personalise your experience on our websites and apps; (iv) to ensure that content from our websites/apps is optimised for you and for your computer or device; (v) to provide you with targeted advertising and content. We also show you specific content or promotions that are tailored to your interests.	Personal identification information; Personal contact information; Financial information and other transaction – related data; Websites/communication and product usage information; Information from our marketing and advertising partners; App, browser and device data
Protection of customers against financial exploitation We use personal data of TCP to protect our customers of age 65 + against their elder abuse and misusing (often illegally) elderly people's finances, assets, or possessions.	Information about the Trusted Contact Person, Information obtained from TCP

• where there is a **contractual obligation** (a contract between the Company and you)

Note that we will need to terminate your account if we cannot process your personal information for such purposes.

Why we process your personal data	**Categories of personal data**
To set up and maintain your account We need your personal data to provide you with our services, including payment processing, and to allow you to create a customer account.	Personal identification Information, Supplemental Identification Information, Personal contact information, Financial Information and other transaction-related data
To conclude and execute the contract / provide our services and ensure the execution of the transaction We need your personal data to provide you with our Services, enter into a contractual relationship, clarify and verify information on the submitted application or to find out other additional information that promotes the progress of execution of the transaction.	Personal identification information; Supplemental identification information; Personal contact information; Financial information and other transaction – related data; Electronic identification information; Wallet information; Blockchain data; Website/communication and product usage information; Public database information; App, browser and device data
To provide customer support We need your personal data to respond to your request for support in the Apps, via the webites	Personal identification information; Supplemental identification information; Personal contact information; Financial information and other transaction – related

or by email and to respond to your inquiries, including providing telephone-based customer support, chat message support, and social support.	data; Website/communication and product usage information
To send you communication related to services and contractual relationship We need your personal data to send you legal, administrative or account-related communications about our services, which can include security updates or transaction-related information, through email, telephone, or in-product/push notifications. You may not opt-out of receiving critical service communications, such as emails or mobile notifications sent for legal or security purposes.	Personal identification information; Personal contact information; Financial information and other transaction – related data; Website/communication and product usage information
To ensure and foster the safety, security and integrity of our services We need your personal data to verify accounts and related activity, to make sure you do not violate the contract and if you do, to address such violation, investigate suspicious activity, detect, prevent and combat harmful or unlawful behaviour, detect fraudulent behaviour and to maintain the integrity of our services.	Personal identification information; Supplemental identification information; Personal contact information; Financial information and other transaction – related data; Website/communication and product usage information

• to meet a **legal obligation** (arising from EU or national legislation)

Note that if you do not provide the personal data required by law, we will have to close your account and terminate the Agreement.

Why we process your personal data	**Categories of personal data**
To check and verify your identity We need your personal data to fulfil our legal obligation to properly identify or verify your identity, including electronic identification, and comply with other specific anti-money laundering or sanctions laws.	Personal identification information; Supplemental identification information; Personal contact information, Electronic identification information
To ascertain we can provide you certain regulated products We need your personal data because certain products we may offer are suitable only for those clients who are legally eligible to use them and we may be required to carry out additional checks to ensure your suitability.	Personal identification information; Supplemental identification information; Personal contact information; Financial information and other transaction – related data
To comply with other legal and regulatory obligations	Personal identification information; Supplemental identification information; Personal contact information; Financial

We need your personal data because we may access, read, preserve, and disclose information when we believe it is reasonably necessary to comply with law (i.e. tax law, Anti-money laundering law, privacy law), legal obligations, regulations, law enforcement, governmental, and other legal requests, court orders, or for disclosure to tax authorities.	information and other transaction – related data; Wallet Information, Blockchain Data; Electronic identification information; App, browser and device data; Website/communication and product usage information; call recordings to our call center; Information obtained from TCP; information provided by the customer about TCP

• for our **legitimate interests** (or others)

We can process your personal data for our legitimate interests only after having checked that your fundamental rights and freedoms aren't seriously impacted. If your rights override our interests, then processing cannot be carried out based on legitimate interest.

Why we process your personal data	**Categories of personal data**
Personalisation We use your personal data (i) to analyse your preferences and habits, (ii) to anticipate your needs based on our analysis of your profile, (iii) to improve and personalise your experience on our websites and apps; (iv) to ensure that content from our websites/apps is optimised for you and for your computer or device; (v) to provide you with targeted advertising and content. We also show you specific content or promotions that are tailored to your interests. It is in our interest to understand how you interact with our services in order to customize and/or improve our products and services and enable accurate and reliable reporting.	Personal identification information; Personal contact information; Financial information and other transaction – related data; Websites/communication and product usage information; Information from our marketing and advertising partners; App, browser and device data
To send marketing communications, offers of products and services, and targeted advertising We may send commercial communications and/or newsletters, and may offer services via e-mail, mobile, inapp, and push notifications or by sms. It is in our interest to promote our products and services that you may be interested in.	Personal identification information; Personal contact information; Financial information and other transaction – related data; Websites/communication and product usage information; Information from our marketing and advertising partners; App, browser and device data
To preserve and share information with others, including law enforcement, civil litigants, and others who may issue legal requests We need our personal data to share your personal data in response to requests from third parties, such as civil litigants, law enforcement, and other government authorities, for example to assist authorities in the investigation of fraud; to promote the safety, security, and integrity of our service, network, our clients, employees,	Personal identification information; Personal contact information; Supplemental identification information; Wallet Information, Financial information and other transaction – related data; Websites/communication and product usage information ; Blockchain data; Calls to our call center; Public database information; Information from payment providers and credit reference agencies; Third party social network information; Information

property and the public; to respond to your requests or communications. It is in our interest and the interest of the general public to prevent and address fraud, unauthorized use of the services, or other harmful or illegal activity; to protect ourselves (including our rights, personnel and property or services), our clients or others, including as part of investigations or regulatory inquiries; to secure our platform and network, to verify accounts and activity, to combat harmful conduct, to detect, prevent and address fraud, abuse, spam and other bad experiences or to prevent death or imminent bodily harm.	obtained from TCP; information about TCP obtained from the Customer
To promote safety, security and integrity We need your personal data to log customer reports and patterns of suspicious behaviour to understand techniques being used by bad actors who may wish to interfere with our services; and to identify and investigate patterns of suspicious behavior or violations of our policies and terms. It is in our interest and the interests of our customers to secure our platform and network, to verify accounts and activity, to combat harmful conduct, to detect, prevent and address fraud, abuse, spam and other bad experiences.	Personal identification information; Supplemental identification information; Personal contact information; Financial information and other transaction – related data; Wallet Information, Blockchain Data; Electronic identification information; App, browser and device data; Website/communication and product usage information; Calls to our call center; Information from cookies, web beacons and similar technologies; Public database information; Information from payment providers and credit reference agencies; Third party social network information
To research and innovate We need your personal data to carry out surveys of your experience using the services to conduct and support research and innovation on topics related to our services. It is in our interest and our clients' interest to find out how our services are working for you and to improve our services through information obtained from these research surveys and interviews and to develop new products and services.	Personal identification information; Personal contact information; Financial information and other transaction – related data; Website/communication and product usage information; Information from analytics provider; Information from marketing and advertising parties
To enforce and defend our rights It is our interest to enforce and defend our rights including initiating legal claims, preparing our defence in litigation procedures, addressing legal or administrative proceedings, whether before a court or a statutory body, and to investigate or settle disputes or other issues.	Personal identification information; Supplemental identification information; Personal contact information; Financial information and other transaction – related data; Wallet Information, Blockchain Data; Electronic identification information; App, browser and device data; Website/communication and product usage information; Calls to our call center; Information from cookies, web beacons and similar technologies; Public database information;

	Information from payment providers and credit reference agencies; Third party social network information

The Company process personal data both manually and by automated means.

3. Retention periods

The Company will process and retain your personal data for a period of time necessary to safeguard all the rights and obligations resulting from the relevant contract, and thereafter for a period for which the Company, as data controllers, is required to retain personal data under applicable laws, or for which you have granted to the Company your consent with such processing. In other cases, the period of processing is based on, and must be proportionate to, the purpose of the processing, or is stipulated by applicable data protection laws.

We process personal data, based on the purpose of their processing, for the periods specified below:

Purpose of the processing	**Retention period**
Performance of contract	for the duration of the contract and for 10 years from termination of the contract
Compliance with legal obligations	for the period stipulated by applicable legal regulation
Sending marketing communications and offers of services, products and targeted advertising	for the duration of the consent to the processing of personal data, or until revocation of the consent, or in accordance with separate legal regulations
Protection of our legitimate interests or legitimate interests of third parties	any applicable limitation period (i.e. any period during which a person could bring a legal claim against us), and an additional 2 months following the end of the applicable limitation period (so we are able to identify any personal data of a person who may bring a claim at the end of the applicable period). In addition, if any relevant legal claims are brought, we may continue to process your personal data for such additional time necessary in connection with that claim, unless separate laws require otherwise, or unless it is necessary in justified cases to retain data for a longer period in connection with a particular case
Processing requests sent by means of electronic forms	for the period necessary to process the relevant request

Once the periods above, each to the extent applicable, have concluded, we will either

- permanently delete or destroy the relevant personal data, or

- anonymise the relevant personal data.

Therefore, the right to access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

4. What are your data protection rights

We would like to make sure you are fully aware of all of your data protection rights. As a data subject, you (including TCP) have certain rights in connection with the processing of personal data, which result from applicable laws and which you may exercise at any time.

The right to access – You have the right to learn if your personal data is being processed, obtain disclosure regarding certain aspects of the processing (such as the purpose of the processing, source of the personal data or the categories of personal data concerned) and you have the right to request our Company for physical or electronic copy of your personal data. To protect your personal data, we might require proof of identity from you prior to disclosing such information. For any further copies requested by you, we may charge a reasonable fee based on administrative costs.

The right to rectification – You have the right to request that we correct any information you believe is inaccurate. You also have the right to request our Company to complete the information you believe is incomplete. You may inform us at any time that your personal details have changed. In some cases we will ask you to provide supporting document to prove it.

The right to erasure – You have the right to request that we erase your personal data, under certain conditions. You can use this Right to Erasure Request form.

The Company will erase your personal data if

• the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed,

• you withdraw consent on which the processing is based and there is no other legal ground for the processing,

• the personal data have been unlawfully processed,

• you object to the processing and there are no overriding legitimate grounds for the processing of your personal data or you object to the processing for marketing purposes,

• the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject, or

• the personal data have been collected in relation to the offer of information society services.

Please note that in certain circumstances, where erasure would adversely affect the freedom of expression, contradict a legal obligation, act against the public interest in the area of public health, act against the public interest in the area of scientific or historical research, or prohibit the establishment of a legal defense or exercise of other legal claims, we may not be able to erase the information you requested.

The right to restrict processing – You have the right to request that we restrict the processing of your personal data where one of the following applies:

• the accuracy of the personal data is contested by you, for a period enabling the Company to verify the accuracy of the personal data

• the processing is unlawful and you oppose the erasure of the personal data and requests the restriction of their use instead

• we no longer need the personal data for the purposes of the processing, but we are required by you for the establishment, exercise or defence of legal claims

• you have objected to processing pending the verification whether our legitimate grounds override your rights and legitimate interests.

The right to object to processing – If we are processing your data based on our (or a third party's) legitimate interest you have the right to object, on grounds relating to your particular situation, at any time to our processing of your personal data, whereupon the processing will be discontinued without undue delay, unless compelling legitimate grounds for the processing demonstrably exist which override the interests, rights and freedoms of you or for the establishment, exercise or defence of legal claims.

The right to object for direct marketing purposes - You may also object if we are processing your data for direct marketing purposes which includes profiling to the extent that it is related to such direct marketing without providing any justification and at any time. You can opt-out of receiving marketing communications from us through your account settings or by submitting a request via our contact channels. Where you objects to processing for direct marketing purposes, the personal data will no longer be processed for such purposes.

You may also object to any automated decisions or profiling taken and performed by us based on your personal data.

The right to data portability – You have the right to to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from us, where

• the processing is based on your consent or on a contract, and

• the processing is carried out by automated means to which the personal data have been provided.

The right to revoke consent to any of our data processing activities - Where the legal basis for processing of your personal information is your consent, you have the right to withdraw that consent at any time by contacting us using the details found under the 'How to contact us' section of this Policy. Where you have consented to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once your consent is withdrawn, the processing of your data will be halted, unless said processing is found on another legitimate basis, for example due to a legal obligation to keep your data.

Automated decision making and profiling - If we have made a decision about you based solely on an automated process (e.g. through automatic profiling) that produces legal effects concerning you or services or has another significant effect on you such as effects your ability to access our products, you can request not to be subject to such a decision. Such decision making is allowed if

• the decision is authorised by union or member state law to which we are subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests, or

• where necessary for the entering or performance of a contract between you and us, or

• when you have given your explicit consent.

Even if such decision making is allowed, you may ask for an explanation of the decision reached after such assessment and contest the decision and require human intervention. We may not be able to offer our products or services to you, if we agree to such a request (i.e. end our relationship with you). However, we do not use automatic decision-making or profiling when processing personal data.

The right to complain to competent data protection authorities - If you have unresolved concerns you also have the right to complain to competent data protection authorities. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes GDPR Regulation. https://vdai.lrv.lt/en/.

Should you wish to report a complaint or if you feel that we have not addressed your concern in a satisfactory manner, you may contact the Information the Director of the Lithuanian State Data Protection Inspectorate (https://vdai.lrv.lt/en/).

Email: ada@ada.lt

Address: L. Sapiegos str. 17 (Left-hand entrance) LT-10312 Vilnius

5. **How to exercise your rights**

Your rights (including rights of TCP) can be exercised by sending us an e-mail legal@dex-gp.com or writing to us at Žalgirio g. 88-101, 09301 Vilnius, Lithuania, attaching a copy of your ID or equivalent details (where requested by us and permitted by law). If the request is submitted by a person other than you, without providing evidence that the request is legitimately made on your behalf, the request will be rejected. Please note that any identification information provided to us will only be processed in accordance with, and to the extent permitted by applicable laws.

If you make a request, we have one month to respond to you. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We will inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where requests to exercise the above rights is repetitive or manifestly unfounded, the Company may either charge a reasonable fee for the exercise of the relevant right, or refuse to act on the request. If this is the case, you will be informed accordingly.

6. **Blockchain related notification**

Please note that public blockchains are distributed ledgers, intended to immutably record transactions across wide networks of computer systems. **When interacting with blockchains, we will likely not be able to prevent external parties from processing any personal data which has beenwritten onto blockchains. we do not have full control over the means and purposes of processing as much of this is done within the blockchains themselves and depending on the way the relevant blockchain is structured, may involve external parties processing your data.** This may affect your ability to exercise your rights such as your right to erasure (this being your 'right to be forgotten'), the right to rectification of your data or your rights to object or restrict processing, of your personal data. IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS.

7. **Cookies**

Please see our Cookie Policy to learn how you can manage your cookie settings and for detailed information on the cookies we use and the purposes for which we use them.

8. Security

We use reasonable physical, technical (such as encryption and pseudonymization) and organisational (such as internal policies, access control management, security incident response management and training of employees) measures to safeguard your personal information (including information of TCP) against loss, theft and unauthorized disclosure, access, use and modification, destruction or damage. We continuously develop our security processes and measures.

We also 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.

However, please note that the transmission of information via the internet is not completely secure and therefore we cannot guarantee the security of data sent to us electronically and the transmission of such data is entirely at your own risk. Where we have given you (or where you have chosen) a password so that you can access certain areas of our website, you are responsible for keeping this password confidential.

9. Disclosure of personal data

We work with service providers, partners and other third parties to help us provide our services, and as a result we need to share certain information with these third parties (in any case within the scope necessary to achieve the purposes of the processing and on the basis of the relevant legal title for the processing of the personal data). In some case defined by legislation, we are authorised, or even obligated, to transfer certain personal data under applicable laws to criminal prosecution authorities or other public authorities.

We may share your data with the following categories of data recipients:

• Affiliates - Personal information (including TCP information) that we process and collect may be transferred between companies, services, and employees affiliated with us as a normal part of conducting business and offering our services to you

• Linked third party websites - When you use third-party services or websites that are linked through our services, the providers of those services or products may receive information about you that the Company, you, or others share with them.

• Third party companies using Personal Data for their own marketing purposes - Except in situations where you have given your consent, we do not license or sell your personal data to third party companies for their own marketing purposes. Their identity will be disclosed at the time your consent is sought.

• Service providers - We share your information with external service providers that we use to help us run our business (e.g. order fulfilment, payment processing, fraud detection and identity verification, website operation, market research companies, support services, promotions, website development, data analysis, CRC, debt collection, financial, accountant services, legal services etc.). Service providers, and their selected staff, are only allowed to access and use your personal data on our behalf for the specific tasks that they have been requested to carry out, based on our instructions, and are required to keep your personal data confidential and secure. We exercise due diligence to ensure that such

cooperation partners act in accordance with this Policy and safety requirements provided for clients in the laws and regulations.

• Supervisory and governmental authorities - We also share your personal data (including data of TCP) with regulators, tax authorities, law enforcement, government agencies, and industry partners to respond pursuant to applicable law or regulations, court orders, legal process or government requests; to comply with our reporting and information sharing obligations with industry partners, including other Virtual Asset Service Providers and regulatory authorities; to detect, investigate, prevent, or address fraud and other illegal activity or security and technical issues; and to protect the rights, property, and safety of our clients and us, or others, including to prevent death or imminent bodily harm.

• Business Transfers. We may engage in a merger, acquisition, bankruptcy, dissolution, reorganization, or similar transaction or proceeding that involves the transfer of the information described in this notice. In such transitions, customer information and information of TCP is typically one of the business assets that is transferred or acquired by a third party. In the unlikely event that we or substantially all our assets are acquired or enter a court proceeding, you acknowledge that such transfers may occur and that your personal information can continue to be used as set forth in this privacy notice.

10. Transfers to a third country

We may transfer your data and data of TCP to third countries (outside the European Economic Area - EEA). A transfer of data to third countries will take place i.e. if this will be necessary for the execution of your orders, or if so required by law or if you have given us your explicit consent.

In addition, data may be transferred to our affiliates, subsidiaries or processors in third countries or subcontractors of our processors in third countries. These are obliged to comply with European data protection and security standards. Information about this can be obtained from us.

If personal data is transferred to a country which has been found by the European Commission to have an essentially equivalent standard of data protection to the EEA, then we may rely on an „adequacy decision“ to transfer personal data. If that is not the case we (i) have put in place European Commission approved standard contractual clauses to protect your personal data (and you have a right to ask us for a copy of these clauses and/or (ii) will rely on your consent (where permitted by law).

Please also note that some of our products and services rely on blockchain technology. Interacting with a global decentralized public network means that any personal data written onto blockchains may be transferred and stored across the globe.

11. Privacy policies of other websites

The Company website may contain links to other websites. Our Policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

12. Changes to our privacy policy

Our Company keeps its privacy policy under regular review and may make changes to its Privacy policy from time to time. We place any updates on this web page. We encourage you (including TCP) to review this Policy whenever you access or use our website to stay informed about our information practices and the choices available to you. If you do not agree to the revised Policy, you should discontinue your use of this website and our services.

13. How to contact us

If you have any questions about our privacy policy please do not hesitate to contact us. Email us at: legal@dex-gp.com Call us: +37052144866 Or write to us at: Žalgirio g. 88-101, 09301 Vilnius, Lithuania.