

Privacy Notice

Your personal data

What do we need?

UAB "Maneuver LT," legal entity registration number 304785124, registered at the address Žalgirio str. 92-510, LT-09303 Vilnius, Lithuania, is an electronic money institution that needs your personal data for the proper provision of high-quality services and ensuring of maintenance requirements. We are the Controller of your data transmitted to us and collect the data such as:

- Identity Data – Name, surname, date of birth, Tax ID, address, ID documents information (number, date of issue and expiry, etc.) and other;
- Verification Data – Your picture, picture of your ID document, video and audio recordings;
- Transaction information – Information on your transactions made with a Genome account or payment card;
- Cookie information.

Why do we need this?

The Data is collected for Genome to provide services to you and ensure maintenance requirements. For the purposes of registration and recording of the customers, conclusion, administration, and performance of a contract, customer notification, protection and control of the assets held by us, and provision of high-quality services, we will collect only the data required for implementation of

the afore-mentioned objectives from you and will not collect from you personal data which is not necessary for the services or other legal purposes.

What do we do with this?

The legal grounds for the processing of data are Article 6(1)(b) (processing necessary for the performance of a contract), Article 6(1)(c) (processing necessary for compliance with a legal obligation), Article 6(1)(f) (processing is necessary for the purposes of the legitimate interest, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of personal data, and Article 6(1)(a) (your consent) of the EU General Data Protection Regulation. You are entitled to withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

In pursuance of ensuring the smooth functioning of the Genome, we must be provided access to your data.

How long will we store your data?

- Customer identification data and verification data – 8 (eight) years after termination of the contract relations;
- Business correspondence with the customer – 5 (five) years after termination of the contract relations;
- History of transactions and related documents confirming the transaction – 8 (eight) years after the execution or completion of the transaction.

What else would we like to do with your data?

We would also like to use your e-mail and your wallet ID to send news and proposals. Your e-mail can be transferred to our partner, who provides us with e-mail marketing platform services. However, you could refuse the sending of

newsletters at any time by clicking on the Unsubscribe link in the e-mails sent by us or logging in to your personal account via Genome Mobile App > Profile icon > Notifications > Marketing communication > disable respective toggle. When you disable the marketing communication toggle, you will no longer receive the above-mentioned content.

If you consent that we processed your e-mail for the purposes of direct marketing, you are kindly requested to mark your consent to processing of your personal data for the purposes of direct marketing at the moment of registration or log in to your personal account via Genome Mobile App > Profile icon > Notifications > Marketing communication > turn on respective toggle.

What are your rights?

Data subject rights are rights which data subjects have in relation to their personal data. Data subject rights are determined by the relevant legal jurisdiction applicable to the specific circumstances or each data subject.

Data subjects' rights include, for example (depending on your jurisdiction and applicable law), the right to receive a confirmation whether or not we process your personal data; the right to access your personal data and receive a copy of the personal data that we hold; the right to rectification of your personal data; the right to erasure of your personal data; the right to restrict processing of your personal data; the right to object to processing of your personal data; the right to data portability; the right to complain to a supervisory authority; and the right to withdraw consent to processing of personal data.

If you decide to exercise them, you can make a request by contacting the Company by e-mail: dpo@genome.eu. Kindly be informed that a "Data Subjects Request Form" is stored in the Company's internal network and is presented to Data Subjects who have expressed such a request. If you wish to make a

complaint for processing of your data by us, you may contact the data protection officer who will investigate the issue by e-mail dpo@genome.eu.

If you are not satisfied with our answer or believe that we process your personal data not in accordance with the legal requirements, you may lodge a complaint to the State Data Protection Inspectorate of the Republic of Lithuania (<https://vdai.lrv.lt/en/>) by e-mail ada@ada.lt or to the national Data Protection Agency (DPA) in the country of your residence.

For more information, please read our Privacy Notice below.

Effective day April 17, 2024

1. Introduction

1. UAB "Maneuver LT," acting under the "Genome" trademark, is a private liability company established and operating under Lithuanian law, legal entity code 304785124, and having an electronic money institution license #32 issued by the Bank of Lithuania on 29.03.2018. Genome's place of business is at Žalgirio str. 92-510, LT-09303 Vilnius, Lithuania. Genome is an electronic money institution that is considered a Data Controller for the purposes of this Privacy Notice.

2. For the purposes of this Privacy Notice, any references to "Genome," "we," "our," or "us" shall refer to UAB "Maneuver LT."



„Maneuver LT“ UAB
Reg N: 304785124
VAT: LT100011709919

3. Our contacts:

Data Protection Officer: dpo@genome.eu

Customer support service: support@genome.eu

Submit a form on our website to [contact us](#).

4. Genome respects the privacy of its customers, business partners, their officers, and other representatives, as well as visitors of the Genome's website who may choose to provide personal data to us.

5. The current Privacy Notice depicts your privacy rights in terms of gathering, use, storing, sharing, and protecting your personal data.

6. Please read this Privacy Notice carefully before registering, accessing, or using Genome products and/or services.

7. You should read and understand this Privacy Notice because it constitutes the core of our obligations to you when you visit Genome website and access Genome products or services or when you act on behalf of your organization and

provide your personal data to us.

8. You acknowledge that you have carefully read and understood this Privacy Notice by registering, accessing, or using Genome products and services.

2. Definitions

1. Terms used in this Privacy Notice shall have the following meaning:

1.1. "**Genome Services**" means the supply of Genome Wallet, issuance and redemption of e-money, execution of transactions, currency conversion, issuance and processing of Genome Card, providing access to Genome User Portal, where you can top-up your Genome Wallet, make and receive transactions, proceed with currency exchange, withdraw funds from our system, etc., as well as any other related services or products that we provide or make available to you.

1.2. "**Genome Wallet**" means a web-based multicurrency personal or business e-money account inside Genome opened and maintained by us in your name or in the name of any other natural or legal person.

1.3. "**Genome Card**" means physical or virtual debit Visa classic or business card

issued by Genome.

1.4. "Genome User Portal" means portal inside our system

(<https://my.genome.eu/>) therefrom you can use your Genome Wallet and obtain Genome Services.

1.5. "Our System" means internet-based software, API, and other software and technologies allowing to access Genome Wallet and obtain Genome Services;

1.6. "Genome Site" means /, including all its content and subdomains (e.g., <https://my.genome.eu/>; <https://blog.genome.eu/>, etc.).

1.7. "Genome Mobile App" means a mobile version of Our System which will be available to you upon downloading from App Store or Google Play and installing on iOS or Android system.

1.8. "You", "your", "yours" refers to any customer of Genome Site, Genome Wallet, and Genome Services. For the purpose of clarity, if you are acting on behalf of your organization that uses Genome products or services, this Privacy Notice shall apply to you as the officer or other representative of such organization.

1.9. “GDPR” means General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.10. “Data/Personal Data” shall mean any information relating to an identified or identifiable natural person (Data Subject’); an identifiable natural person is one who can be identified, directly or indirectly, 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 natural person.

1.11. “Recipient” shall mean a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

1.12. “Data Subject” shall mean a customer or any other person whose Personal Data is processed by the Data Controller.

1.13. “Processing” shall mean any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as

collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, blocking, erasure or destruction;

1.14. "Processor" shall mean a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller.

1.15. "Controller" shall mean a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; For the Processing of Personal Data described in this Policy, Genome is the Data Controller.

1.16. "Policy" shall mean this Privacy Notice.

1.17. For the purposes of this Policy, other terms correspond to the terms used in the GDPR, the Republic of Lithuania Law on Legal Protection of Personal data (hereinafter referred to as the "**LLPPD**"), and the Republic of Lithuania Law on Electronic Communications (hereinafter referred to as the "**LEC**").

3. Principles of personal data processing

1. We, as the Data Controller, ensure that we meet the following main data protection principles:

1.1. Personal Data shall be processed lawfully, fairly, and in a transparent manner in relation to the Data Subject (lawfulness, fairness, and transparency);

1.2. Personal Data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing of Personal Data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes (purpose limitation);

1.3. Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimization);

1.4. Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or

rectified without delay (accuracy);

1.5. Personal Data kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the Data Subject (storage limitation);

1.6. Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (integrity and confidentiality).

1.7. The Controller shall be responsible for and be able to demonstrate compliance with the principles set out herein above (accountability).

4. Legal basis for data processing

1. Genome processes customer data on the legal basis of:

1.1. Article 6 (1)(b) of General Data Protection Regulation. The necessity for the performance of a contract with the customer and to comply with our regulatory requirements when performing pre-contractual steps after the customer's request. The data is processed to open an account for the customer and to enable Genome to execute the customer's payments.

1.2. Article 6 (1)(c) of General Data Protection Regulation – Necessity for compliance with a legal obligation to which the Controller is subject. This legal basis is used by Genome when conducting KYC and other due-diligence procedures when opening an account for the customer as also after a business relationship has been established with the customer to execute the payments, conduct transaction monitoring, comply with reporting requirements and ongoing due-diligence requirements (Sanction screening and risk assessment).

1.3. Article 6 (1)(f) of General Data Protection Regulation – legitimate interest. The necessity of processing for the purposes of the legitimate interests of Genome, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, which require protection of personal data. In any cases, our interest is to conduct and manage our services to enable us to

provide the most secure experience.

1.4. Article 6 (1)(a) of General Data Protection Regulation – Your consent. This is applicable to Genome’s use of Cookies as well as your Contact information processing for contacting you regarding a new product or service offered by Genome.

5. Types of information, purposes and legal basis for personal data processing

1. The categories of personal data that we may collect:

1.1. about you when you open a personal Genome Wallet and use Genome Services for your private needs and

1.2. about your officers, shareholders, ultimate beneficiary owners, and other representatives when you are a business and open Genome Wallet or use Genome Services for and on behalf of your organization.

2. In order to provide you with Genome Services, Genome collects various types

of your Personal Data as mentioned above. Personal Data is collected and processed during 3 principal steps:

- 1). Registration;
- 2). Identity verification;
- 3). Use of Genome Services.

Processing of registration data

i. The registration process begins with an identifier, where you should choose the e-mail address or phone number that will be used for registration in our System. Also, you should create a strong, unique password. Submission of the herein-mentioned Personal Data is mandatory for your registration. To finalize your registration, we will send a one-time password to your verified e-mail address or phone number, which is used for two-factor (2FA) authentication in our System.

ii. After entering the verification code in our System, you can continue filing the Know Your Client (KYC) form to open the account and receive Services. For this purpose, we need to request more information in order to meet our Legal and

Regulatory Obligations. Therefore, proceeding with the account opening, you should provide us with your additional Personal Data, which includes data such as:

- First name;
- Last name;
- Date of birth;
- Information/confirmation about you, your immediate family members, and close associates of being or not being Politically Exposed Persons (PEP status);
- Registration address;
- Home address;
- Tax residency information (Country for tax residency; taxpayer identification number);
- Facial image;
- Video and audio recordings;
- Copy of identification document (i.e., copy of identity card, passport, or residence permit) and all data therein (e.g., photograph, personal identification number, document number expiry date, issued country, nationality, etc.);
- And any other information you provide us in order to prove your eligibility to use our services;

If you are a business and want to open a Genome Wallet or use Genome Services for and on behalf of your organization, we will collect this additional Data:

- evidence of beneficial ownership;
- business owner's citizenship country;
- business owner's address;
- business owner's tax information (country for tax residency; taxpayer identification number);
- evidence of source of funds;
- number of shares held;
- voting rights or share capital part;
- job title;

(ADDITIONALLY (only, if necessary, not submitted earlier or doubts arose about the submitted documents):

- a copy of the company director's passport.
- a copy of the company shareholder's passport.
- the director's personal utility bill.
- the shareholder's personal utility bill.

iii. Genome does not require information above that which is necessary for

fulfilling our Legal and Regulatory Obligations and will at all times ensure a minimalistic approach to data processing.

iv. Submission of Identity Verification Personal data is mandatory for an account to be opened and assigned.

v. In order to open the account, we need to know for what purpose our Services are necessary; therefore, during the process of opening your account, you must determine and indicate such activities. Such information is collected and processed in order to comply with Legal and Regulatory Obligations.

vi. Sometimes, we need to request more information to identify you or to meet Legal and Regulatory Obligations. On such occasions, you will be prompted to provide additional information.

vii. If you contact us, we will collect certain information you provide us voluntarily in relation or such features, such as your full name, your email, your phone number, your company (if applicable to you), the content of your message.

2.1. Personal Data collected by Genome in the registration step is used for the following purposes:

- Account opening;
- Client identification;
- Client risk assessment is mandatory under Legal and Regulatory Obligations.

viii. In order for us to provide you with our services and execute your payments, we must use the Data provided by you during the registration and verification process for the ongoing risk assessment.

ix. The main use of data is for the information checks against sanction lists and various databases or public resources that allow us to check possible adverse media on you:

- Genome is obliged by Legal and Regulatory Obligations to conduct such risk assessment during your verification process and on a continuous basis thereafter. This means that we can process your Data before or during the processing of your payments as well as on a scheduled interval basis;
- This assessment can be done either by us directly or by our Service providers;
- Genome can request from you additional data if during risk assessment new information is identified that under the applicable laws and regulations obliges Genome to perform enhanced due diligence.

Processing of identity verification data

x. In order to receive Genome Services, you must verify your identity. We verify you by the Personal Data you provide during registration, such as described above. However, such Personal Data must be confirmed; therefore, in addition, for verification purposes, we also rely on verification services managed and provided to us by our Service provider Onfido. Every time when you perform the identity verification process, you are informed that we use our partner Onfido for this purpose, and by clicking the button "Next," you agree that you will be redirected to Onfido's app page and give consent for processing your Personal Data, including biometric data.

xi. While exercising this verification step, you will be required to upload your ID document. You will undergo facial verification. For the above-mentioned purposes, we receive and rely on a certain confirmation from our partner, Onfido, that your identity has been verified. To learn more about this process, please see clause 6 of this Policy. Please note that under the applicable laws, Genome is obligated to collect and store all Data received during the client identification and verification process; therefore, scanned copies of ID documents, Data related to facial recognition, and other information will be stored by Genome in accordance with AML laws and Legal and Regulatory Obligations.

xii. Genome will request that further information be provided that will allow Genome to reasonably identify you and verify your identity. Genome reserves the right to contact you and request that you provide more information or approve that the provided information is up-to-date and valid.

xiii. Genome processes data gathered during client's verification in order to comply with regulatory and legal obligations as well as to ensure that clients are not attempting to create additional accounts or to commit fraudulent actions. Refusal to undergo ID and facial verification will terminate your account opening process.

Data processing using Genome Services data

xiv. While you are using our Services, we are collecting the following data:

- **Transaction Data** – transaction details (IBAN number, beneficiary details, date, time, amount, and currency which was used, purpose of payment, name, surname, IP address of sender and receiver), account number and/or credit card number, amount of transaction, income, location, documents confirming monetary operation or transaction or other documents having legal force related to the

performance of the monetary operations or conclusion of the transactions (e.g. invoices and/or contractual documentation (original documents)), any other data incoming or outgoing together with transaction.

- **Genome Card Data** – name, surname of the cardholder, telephone number, e-mail address, shipping address, PPAN (masked card number), card account number, transaction amounts, payment beneficiaries. Learn more about debit card granting, activation, processing, and execution of payment transactions by debit card here: [Genome Card Account Terms and Conditions](#), which is integrated in and shall be read in conjunction with this Privacy Notice.

- **Contact Information** – name, surname, postal address including correspondence address for delivery of Genome Card, e-mail address and/or telephone number, information/documents provided by the person applying to us, as a case may be.

- **Message content** – if you include a message with your payments or you send a message through the chat box available on the Genome Site or Genome Mobile App, the content of that message is stored by us; however, if you write messages outside of our working hours, the robot will communicate with you using artificial intelligence and the content of the messages will be stored by our Service provider.

- **Messaging history**, including but not limited to, claims and complaints made by you is processed due to the performance of obligations regarding provision of

Services.

- **Cookies** – The Genome Site and Genome Mobile App uses cookies. Learn more about cookies and other similar technologies that we use from our [Cookie Policy](#), which is integrated into and shall be read in conjunction with this Privacy Notice.

xv. Genome processes Personal Data collected while using Services on the following legal basis:

- Conclusion and performance of contractual arrangements and obligations between Genome and the Client; and
- Pursuance of legitimate interests of Genome, as controller and manager of Genome Site and Genome Mobile App;
- For compliance with a Legal and Regulatory Obligation.

xvi. In providing the Personal data of any individual other than yourself to us during the use of our Services, you agree that you have obtained consent from such an individual to disclose their Personal Data for collection and use. By providing such Personal Data to us, you bear all the responsibility towards such an individual if you have not received proper consent for such provision, and you undertake to indemnify us for any liability which may appear due to unlawful provision and/or disclosure of Personal Data.

Other types, purposes, and legal basis for the use of Personal Data:

Affiliates' Data

We collect data about participants of Genome loyalty programs (affiliates), such information includes your name, surname, IBAN / account number, payment details (date, amount, currency of the transaction).

We process the Affiliates' Data when you want to apply to the Genome loyalty program. We use this data to sign a contract with you and/or your organization, including [Affiliate terms and conditions](#).

Unverified persons' Data

We may collect data about you depending on what you provide us during the KYC procedure. Such information may include your name, surname, date of birth, address, tax information, etc.

We process this data to provide services properly and legally and to prevent possible money laundering and/or terrorist financing. We use this data based on

your consent, however, if your verification was rejected by us for important reasons, in such cases we process the data received from you in accordance with the legal and regulatory obligation.

Merchant's Clients' Data

We collect data about your clients (natural persons) when you are a business and use payment collection services under [Genome Merchant Terms of Service](#); such information includes your clients' name, surname, transaction details (date, amount, currency of the transaction), account number or card data (PAN number, cardholder name, service code, expiry date), phone number, device details (device type, operating system, IP addresses, imprecise location, etc.), email address.

We process this data to provide payment services to you when you are a business and use Genome payment collection services in order to fulfill transactions between you, as a merchant, and your clients. We use this data to sign a contract with you and/or your organization, including [Merchant Terms of Service](#).

Customer Support Data



„Maneuver LT“ UAB
Reg N: 304785124
VAT: LT100011709919

We collect data about persons calling the Genome support team; such information includes telephone conversation recording and metadata of telephone conversation records: user's telephone number, date and start time of the conversation and duration of the conversation. We may also collect your contact information, content, and history of communication.

We process this data to maintain and administer business relations with our clients and potential clients, customer service and quality assurance of services provided. The legal basis for it is your consent.

Scheduling events

We collect data about participants interested in joining events organized by Genome or other collaborating organizers in which Genome is involved. This information includes your first name and surname, company name, and industry.

We process this data to schedule a meeting with you if you would like to meet us at specific events. The legal basis for it is your consent.

Direct marketing

We process your email address and client wallet ID. For more information about Direct marketing, please see Clause 15, “Direct Marketing”.

We process this data to inform Genome clients about our similar goods or services and / or about services provided by our business partners or other third parties or in order to make assessments about your opinion on different issues in relation to our business partners or other third parties. The legal basis for it is your consent.

Data on debts

In cases when you inappropriately use our services and have a debt, we collect data about the basis of the debt; such information may include your name, surname, national identification number, address, date of birth, amount of the debt, date of incurring the debt, time limit, date of payment, email address, phone number, and other data related to the circumstances in which the debt arose.

We process this data to manage and collect debts, submit claims, demands, and lawsuits.

The legal basis for it is to fulfill our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of

the Data Subject, which require the protection of Personal Data.

Feedback and other information you provide us

We will process your information in case you have provided us with feedback or other information about you for various reasons, including for support, review and promotional and marketing purposes (i.e., public marketing campaigns such as via social media, online channels, etc.). Such information may include photos of you (e.g., for publicly publishing to promote your business or Genome, based on your prior consent), free text such as your feedback to our Service or product, etc.

We use this information to learn from your feedback and use the information for marketing purposes (as detailed), as well as to enhance our services, develop new products, and learn more about the customer's experience.

The legal basis for it is to fulfill our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, which require the protection of Personal Data. And in certain cases where it will be required (e.g., using your image) – based on your consent.

Job Candidates

When applying for a job and throughout the application and recruitment process, we will collect and process your Personal Data. Such Data includes contact information (name, surname, email address, phone number), CV information (data on qualifications, professional skills, education, professional (work) experience), information on language skills, information technology skills, other competencies, diplomas, certificates, training, written recommendations and data contained therein, other personal data provided by the candidate voluntarily (submission of data is not necessary, the candidate submits data voluntarily).

If a candidate is running for the position of manager, deputy manager, member of the management body, or person responsible for the management of electronic money issuance activities (Article 16 (2d) of the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania), the following additional information shall be collected:

- Data on the candidate's criminal record / non-criminal record*;
- Data of impeccable reputation* and other information according to the questionnaire of a member of the management body and/or key function holder of the financial market participant supervised by the Bank of Lithuania;

- Identity code;
- Copy of identity document

*The Company collects and processes the personal data of special categories of candidates only if and to the extent necessary for the selection for a specific job position and to the extent permitted by applicable law.

We will use this data in order to assess your skills, qualifications and consider your application and candidacy for the position you have applied for. As well as communicating with you regarding the recruitment processes and carrying out the recruitment of the Genome staff. In addition, we may use this data to comply with any legal or regulatory requirements.

The legal basis for it is your consent. Each time you apply for a vacant job position through the Genome Site, you voluntarily confirm that you have reviewed and agreed to our [rules for the processing of candidates' Personal Data](#). Such confirmation is mandatory.

Sometimes, the legal basis can be a legal obligation. For example, if a candidate is running for the position of manager, deputy manager, member of the management body, or person responsible for the management of electronic money issuance

activities.

Technical information

That information is automatically recorded when you visit the Genome Site, landing page, log in to the Genome User Portal, open the mobile app, or use the Genome Wallet or Genome Services, such as your IP address, device approximate location, type of device, operating system, other device identification data, user agent, referrer URL.

We process this data to protect your Genome Wallet and to take our Services safety, i.e. for security and fraud prevention.

The legal basis for it is to fulfill our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data and / or to fulfill the Legal and Regulatory Obligations applicable to us.

Cookies

When you visit the Genome Site, a small cookie file might be placed on your

computer or mobile device.

For the purpose of clarity, only necessary cookies used to ensure proper operation of the Genome Site are always active. To install analytical and/or marketing cookies on your device we will ask for your explicit consent.

Cookies allow us to collect and process data on users' behavior on Genome Site and technical information on their devices (e.g. device's IP address (processed during the session and stored in a de-identified form), device screen size, device type (unique device identifiers), browser information, geographic location (country only), preferred language etc.).

We process this data to ensure stable operation of our Site, to adapt its content to your needs, to improve features of Genome Site, and to manage advertising campaigns based on the interests of our audience.

We analyze data from cookies and use it to improve the quality of our services, track your activities with Genome, and keep your account safe.

The legal basis for it is to fulfill our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of

the Data Subject, which require the protection of Personal Data as well as your consent.

Please be informed that in specific cases, other data not listed above but which relates to the provision of our services, or which you have provided to us, or which we have collected from third parties in the course of providing or identifying the possibility of providing services to you or your organization, may also be collected and/or processed. We will provide you with the due information of collecting and processing immediately after obtaining the personal data, but at the latest within 1 (one) month, having regard to the specific circumstances in which the personal data is processed.

Pay attention that your personal data is not used for any additional purposes not mentioned in this Privacy Notice, [Cookie Policy](#) or the contract between Genome and you or your organization.

What do we mean when we say:

Concluding a contract / Contract performance: processing your personal data where it is necessary for the performance of the contract to which you are a party or to take steps at your request before entering into such a contract.

We rely on the contract as a legal basis to process personal data submitted by you in case you are an individual, or you transfer to us the personal data of your officers, shareholders, ultimate beneficiary owners, or other representatives. Processing of your personal data is necessary to provide you with Genome Wallet and Genome Services. Please note that we cannot provide you or your organization with the requested services or products without processing the personal data listed above, including, for example, without carrying out the “know your client” procedure or business risk assessment.

Legal and Regulatory Obligations: These are the obligations to collect Personal Data to ensure our requirements as an electronic money institution. Such collection of Personal Data is required to perform anti-money laundering and funding of terrorism requirements and other fraud and crime prevention laws and regulations, ensure compliance with international sanctions, “know your clients” obligations, AEOI & CRS (Automatic Exchange of Information & Common Reporting Standard) requirements, CESOP (the Central Electronic System of Payment information) requirements, legally required registers. For GDPR purposes – the legal requirement is set forth in AML 4th Directive and Lithuanian Law on Money Laundering and Terrorist Financing.

Please note that in order for you and/or your organization to use Genome Wallet and Genome Services, you will need to provide us with the requested information to fulfill our Legal and Regulatory Obligations. Otherwise, we may not be able to provide Genome Services and products to you and your organization.

Legitimate Interest: our interest as a business is in conducting and managing our services to enable us to provide these to you and/or your organization and offer the most secure experience.

We process your personal data on the basis of our legitimate interests, provided that such processing shall not outweigh your rights and freedoms. We rely on this legal basis when we carry out procedures that are part of Genome Services or that are transparent, expectable, and/or stable business practices. For example, to:

- safeguard the prevention, investigation, and detection of payment fraud;
- ensure your authentication and access to Genome Wallet through the Genome Site and Genome Mobile App;
- ensure that the Genome Mobile App and Genome User Portal work well on users' devices (identify active devices and adapt to the needs/settings of the client);

- provide you with high-quality customer service;
- provide you with technical and administrative notifications;
- contact you or other officers and representatives of your organization regarding customer service and product/services information or to send notifications related to the verification process or updates about your account status. As our client, we may provide you with information on products and Services that we offer or a new promotion that we are running that is related to Genome Wallet or Genome Services. These communications may be via e-mail, SMS, or in-app messages, which can be viewed in the notification center. If you do not want to receive direct marketing messages from us, you can opt-out at any time by clicking the relevant button in the e-mail, or you can do it in Genome Mobile App > Profile icon> Notifications > Marketing communication > disable respective toggle. Please note that if you do not agree to receive these marketing messages offered by us, this will not apply to Personal Data provided to us as a result of the use of our Services;
- ensure that traffic is best routed so users do not experience extra delays (geolocation definitions for traffic analysis and forecasting);
- know where the traffic comes from;
- lawfully disclose personal data to a third party, provided we take all technical and legal measures to protect personal data.

We will also process your data on the basis of our legitimate interest, where the processing of Personal Data is strictly necessary and proportionate to the purposes of information security.

Please note that in most cases, if you do not provide the requested information, we will not be able to provide you and/or your organization with Genome Services and products, e.g., our support cannot reach you in case of issues with your payment transaction without collecting your contact details.

If we process your personal data based on our legitimate interests, as explained above, you can object to this processing under certain circumstances. In such cases, we will cease processing your information unless we have compelling legitimate grounds to continue processing or where it is needed for legal reasons.

Consent: we can request your consent for processing when we are required to do so by law or when we do not have another legal basis for processing your data.

Where we rely on your consent to process your personal data, you have the right to withdraw or decline consent at any time, as mentioned in this Policy. In addition, the form for Data Subjects' consent withdrawal request is stored in the Company's

internal network and is presented to Data Subjects who have expressed a request to withdraw their consent. You can make such a request by contacting the Company by e-mail: support@genome.eu or dpo@genome.eu. After contacting the Company at the specified e-mails, you will be sent a form for the Data Subject's request for withdrawal of consent. Also, you have the right to submit such a request even without following the form provided to you. However, in all cases, you must identify yourself and clearly express whether you want to withdraw your consent in full or only partially. If so, you must clearly state which categories of personal data the consent should remain. For more information about your rights, please see Article 17 of this Policy. Please note that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

We do not rely on consent in common cases because the right to withdraw consent can be used for fraudulent activity. This would jeopardize the financial stability of Genome and the reliability and integrity of Genome Services, thereby harming all legitimate parties in the payment process.

6. Facial Similarity Check and Known Faces Service

1. As mentioned above, in order to make your identity verification, we are using the solution of our service provider – Onfido, which has Regulatory certifications of ETSI Technical Standards, Electronic Identification, Authentication and Trust Services (eIDAS), UK Digital Identity and Attributes Trust Framework (UKDIATF) and Kommission für Jugendmedienschutz (KJM). Onfido has also implemented the securities standards of ISO 27001 and SOC 2 Type II. The Processor Onfido is located and acting in the United States of America, thereof the Data is transmitting over European Union boundaries. Such Data transmission is executed by providing high-quality Data security. Data Controller and Processor implement the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

2. To verify your identity, Onfido conducts a facial similarity check comparing the face displayed on the identity document provided by you with a facial image captured from a photo or video recorded by you to verify that they are the same while requiring you to undergo liveness detection. Onfido matches the facial image of the user from the photo or video with the face displayed on the identity document. The comparison is conducted in order for Genome to fulfill “know your client” procedures and to comply with AML / CFT and risk management obligations, making sure that the person displayed on the identity document and

the one registering in the Genome system is the same person. Onfido does not uniquely recognize the user within the scope of the facial similarity check.

3. For this purpose, Onfido processes the following personal data: photo or video of the user, the image of the face in the identity document, and all other data therein (personal identification number, document number expiry date, issued country, nationality, etc.), transcribed text data from the video clip (if applicable), and numerical biometric data.

4. Image(s) of your identity document and photo or video recorded by you in the course of verification, as well as the result of the facial similarity check (match or mismatch), are transferred to Genome. Your personal data is processed by us on the basis of the above-described legal obligations applicable to us. Genome retains your data for as long as it is necessary to carry out verification and for the period required by AML / CFT laws, in particular for the period of 8 (eight) years from the date of the end of business relations with the client. The storage terms of documents, data, and logs can be additionally extended for no longer than 2 (two) years when there is reasonable instruction from the competent authority.

5. In addition to the above, Onfido may also compare the face on an image or video against a database of biometric numerical identifiers of the faces from past

checks completed by Genome (“known faces service”). Onfido alerts Genome if there is a match. Your extracted biometric numerical identifier from the face on the image or video is included in the Onfido database and can be used for future comparison checks. Within the known faces service, your numerical biometric data is used for the purpose of uniquely identifying a natural person.

6. For this purpose, Onfido uses the following personal data of yours: image or video of the user’s face, Onfido user unique identifier, check status/outcome and related tracking information, and numerical biometric data.

7. Learn more about facial biometric checks and authentication from the Onfido [Privacy Policy](#).

8. In the course of opening Genome Wallet at the stage of your identity verification, we will ask you to confirm your redirection to the Onfido app page to start the verification process and to give your consent for the processing of your personal, including biometric data by Onfido for the above-listed purposes.

9. You have the right to withdraw your consent at any time as described in Section 5, “Consent” of the Policy. However, please note that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its

withdrawal.

10. For the purpose of clarity, Genome does not have access to the Onfido database of biometric numerical identifiers of the faces. We do not create, store, use, or otherwise process your numerical biometric data.

11. For the avoidance of doubt, withdrawal of your consent shall not affect the retention period or processing by Genome of your personal data transferred to us by Onfido that is processed by Genome for compliance with the above-described legal obligations applicable to us.

12. If you do not feel comfortable with the Onfido identity verification method or have questions regarding its functionality, you may contact us by e-mail at support@genome.eu for further clarification.

13. Please note that if you are not satisfied with the results of the identity verification provided by Onfido, e.g., in the event your enrollment application/registration in the Genome system was rejected because of the unsuccessful verification process, you can contact our customer support service by e-mail support@genome.eu and ask to check your application.

7. Ways of obtaining your personal data

1. We obtain personal information from you when you provide it directly to us. For example, when becoming a new client or when you provide us information through direct communication (e.g., completing a form on the Genome Site, registration for our services), by setting up, accessing, and using the Genome Wallet and Genome Services (e.g., by making payment transactions or transactions with Genome Card) when you subscribe to our electronic publications (e.g., newsletters), etc.

2. If you are a beneficial owner, shareholder, representative, or employee of our corporate client, we are collecting your Personal data in order to fulfill Legal and Regulatory obligations. Your Personal data is provided to us by the representatives of the company where you hold a certain position. Personal data received under this clause is processed in accordance with the provisions of this Policy, and you have all the rights of the Data subject listed herein in this Policy and in the applicable laws.

3. We also collect personal information about you from third parties, mainly:

3.1. When it is provided to us by a third party that is connected to you and/or is

dealing with us, for example, business partners, sub-contractors, service providers, merchants, fraud prevention agencies, etc.;

3.2. Third-party sources, for example, registers held by governmental agencies or where we collect information about you to assist with “know your client” check-ups as part of our client acceptance procedures, such as sanctions list, politically exposed persons list, publicly available profile information, etc.;

3.3. From banks and/or other financial institutions in case the personal data is received while executing payment operations;

3.4. From publicly available sources – we may, for example, use sources (such as public websites, open government databases, or other data in the public domain) to help us maintain data accuracy, provide and enhance our Services;

3.5. From other entities which we collaborate with.

4. Information we collect about you from third parties mentioned above can include your Personal Data, Contact information, credit search information, information that helps us to verify your identity, or information relating to your payment transactions.

8. How we use your Data

1. The main goal of gathering and processing your Personal Data is to provide high-quality Services and deliver an effective, scalable, smooth, and personalized Genome experience. Hence, the personal data we collect might be used to:

- Ensure maximum Genome Wallet user experience;
- Process transactions and issue relevant notifications in the most comprehensive manner;
- Settle disputes, levy charges, and resolve occurring problems;
- Prevent clients from becoming subject to illegal activities and potential fraud;
- Improve quality of Services, solutions, and incentives Genome offers on a daily basis;
- Provide target-oriented Services based on your experience with the company;
- Being able to contact you in case of emergency via one of the means available;
- Make sure the information you provide is accurate in case discrepancies occur;
- Send personalized offers of Services and products in accordance with the rules as they are described in the “Direct marketing” parts of this Privacy Notice;
- Carry out regulatory checks and meet our obligations to our regulators;
- Prevent and detect fraud, money laundering, and other crimes (such as terrorist financing and offenses involving identity theft);

- Safeguard you from scams, fraud, and misuse of any private data you might share;
- Develop new services based on the collected information.

9. How we protect your Data

1. We warrant and represent that Genome has implemented the technical and organizational security measures and technological development to ensure an appropriate level of security of Personal Data. Your Data is protected by means of physical, technical, and administrative resources to lower the risks of loss, misuse, unauthorized entry, disclosure, or alteration by third parties. To keep your data safe, we apply:

- firewall and data encryption protection;
- physical authorization control system;
- surveillance facilities, video/CCTV monitor, alarm system;
- securing decentralized data processing equipment and personal computers;
- user identification and authentication procedures;
- tunneling, logging, and transport security;
- audit trails and documentation;
- backup procedures, and many more things.

2. Genome also carries out regular network vulnerabilities scans and penetration testing, especially after any significant changes or updates to the infrastructure and applications.

3. As Genome is PCI DSS V 3.2.1 certified, we maintain all required technology, methods, and business processes to protect cardholder data, and also use such technology and methods as regards the security of your personal data.

4. We monitor our systems 24×7 and our staff is always ready to respond to your notifications and queries within a short time.

5. We implement extensive security measures to ensure the security of your data and the data of your clients, officers, and other representatives of your organization transferred to or collected by us on your behalf; you shall maintain the confidentiality of your password and login from Genome Wallet. You are recommended to sign out of Genome Wallet when you have finished work with it. In any case, responsibility for any loss of passwords and misuse of Genome Wallet by third parties lies with you and/or your organization. Read more about it in Genome T&Cs.

6. Genome respects your privacy and your personal data and warrants that:

6.1. Your data will not be disclosed to any unauthorized third party;

6.2. We will use your data only as described in this Privacy Notice, [Cookie Policy](#), and the contract entered into between Genome and you or your organization;

6.3. We will maintain appropriate administrative, technical, and organizational measures to protect your personal data. For more information about our technical and operational security measures, please see Section 10, “Technical and organizational measures” of the Policy;

6.4. We will keep your data and any information provided by you in confidence;

6.5. We will notify you promptly of a personal data breach when it is likely to result in a high risk to your rights and freedoms;

6.6. We will respect and protect the personal data of the officers, shareholders, ultimate beneficiary owners, and other representatives of your organization when you are a business and open Genome Wallet for your organization, as well as the personal data of your clients when you use Genome payment collection services,

- where such data is transferred to us or collected by us on your behalf;

6.7. We will immediately inform you if, in our opinion, you infringe GDPR protection provisions. You shall ensure the security of the data you transfer to Genome. You assume full liability for failures to meet the GDPR in cases when it is envisaged by this Privacy Notice, GDPR, and/or the contract entered into between Genome and you or your organization.

6.8. We will assist you in ensuring compliance with the duties under GDPR;

6.9. We impose on our subcontractors, partners, and service providers the same data protection obligations as set out in the contract with you or your organization.

10. Technical and organizational measures

1. Measures of pseudonymization and encryption of personal data:

- Data stored in the database is fully encrypted;
- Data in transit is transferred by a secured protocol (HTTPS encryption).

2. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services:

- Genome is implementing strong authentication (2FA), multiple replicated sites for full redundancy, all security tools that are implemented are reviewed\updated regularly, and the information security is continuously improving\updating the security settings\policy.

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:

- Genome's infrastructure is located in geographically distributed AWS data centers, which comply with a number of leading industry standards for security and reliability. Backups and BCP/DRP procedures are implemented and regularly tested.

4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing:

- internal and external network vulnerability scans - quarterly or after each

significant change in infrastructure - until all critical, high, and medium vulnerabilities are eliminated;

- internal and external penetration tests - at least once at 6 months or after each significant change in infrastructure - until all critical, high, and medium vulnerabilities are eliminated.

5. Measures for user identification and authorization:

- Access to a DB (database) and production environment is limited to a small group of employees that are identified by strong authentication. Every access is approved by ISO and all actions are logged.

6. Measures for the protection of data during transmission:

- Data is transferred by encrypted range (HTTPS encryption).

7. Measures for the protection of data during storage:

- Data in storage is encrypted, and the encryption keys are kept separately;
- Access to the DB is limited to a small group of employees;
- Every entry and action on the DB are logged and monitored.

8. Measures for ensuring physical security of locations at which personal data are processed:

- The office is located in a secure building (watchman 24/7), access to the building is limited only for employees from the building, and access to the office is only by the employee's personal RFID (every access is logged). There is CCTV 24/7 and an alarm system;
- We use AWS with multiple availability zones, which comply with a number of leading industry standards for security and reliability.

9. Measures for ensuring events logging:

- we have a centralized logging and monitoring system;
- Security logs are stored at a minimum for 1 year.

10. Measures for ensuring system configuration, including default configuration:

- We use a centralized version and configuration management system. Genome is performing a review of the system's configuration constantly and updating the

settings if needed.

11. Measures for internal IT and IT security governance and management:

- There is a formal information security policy that is updated annually.

12. Measures for certification/assurance of processes and products:

- Genome has a PCI-DSS V 3.2.1 certificate that complies with the requirements of the PCI DSS standard.

13. Measures for ensuring limited data retention:

- All data and information are stored and kept according to the regional law.

14. Measures for allowing data portability and ensuring erasure:

- The organization is aligned with the privacy laws (GDPR). Every request for data erasure is reviewed by the DPO and taken care of according to the GDPR.

11. How we share your Data

1. Genome warrants that it will not disclose your personal data to unauthorized third parties. Genome may share your data with Genome’s contractors, partners, and suppliers, who may use such information only for the limited purpose of providing services to you or your organization and who are obligated to keep the information confidential. For the purpose of clarity, Genome’s cooperation with its contractors, partners, and suppliers is based on the service agreements that contain a data protection section thereunder or separate data protection agreements, which they are required to be in compliance with the data collection and processing regulations.

2. When we process Personal Data on behalf of customers, vendors, or merchants, we share Personal Data collected in the framework of such services with the relevant customer, vendor, or merchant. If you made a purchase as a consumer of goods or services with a certain vendor using our Services, you should take into consideration that your Personal Data will be shared with the vendor from which you made the purchase.

3. In order to provide you with the Services and meet our Legal and Regulatory Obligations or requests, we use third-party services, and such third parties use your Personal Data in delivering their services to us. Therefore, we share the information we collect about you with our service providers (Data processors),

such as:

- Card schemes (such as Visa or MasterCard), banks, and payment service providers - to make you and/or your organization able to obtain payment collection services, bank transfers, and other payment services.
- Card issuing institutions. For the purpose of providing you with a card for you to use our Services. Visa international payment card association – to process and manage information about payment operations with Genome Card.
- Beneficiaries of transaction funds receive the information in payment statements together with the transaction funds.
- Cloud storage/servers' providers. We use their service in order to store your data safely and securely.
- Identification and verification services providers – in order to verify your identity.
- Suppliers of analytical services – to monitor, evaluate, and improve functionality and accessibility of Genome Wallet.
- IT service suppliers (e.g. disaster recovery services, website hosting, data and applications hosting, software application provision and maintenance) - to ensure uninterrupted operation of Genome Wallet.
- Communication service suppliers – to communicate with you, send news and proposals, and/or provide you with up-to-date information on the usage of Genome Wallet or Genome Services, e.g., by SMS or e-mails.

- Customer support services – to operate our payment services platform and provide administration and customer support.
- Debt collection and recovery agencies - to manage and collect debts, submit claims, demands, lawsuits, etc., on behalf of us.
- Correspondent banking institutions. This is to enable payment execution as per your instructions.
- Law enforcement agencies. For the purpose of crime prevention and investigation.
- Regulatory bodies. For the purpose to enable financial market oversight or in cases where the regulator has received your complaint or when data is necessary to prevent or investigate financial crime.
- Tax authorities. This is for the purpose of complying with common reporting standards and requirements for financial institutions.
- Auditors, accountants, and lawyers: In order to complete financial, technical, and legal audits of Genome operations, we need to share information about your account and your Personal Data as part of such an audit.
- Other service providers with which we have concluded service provision agreements or when such sharing is mandatory according to applicable law.
- Other entities that have a legitimate interest or the personal data may be shared with them under the contract which is concluded between Genome and you or your organization.

4. If you have any questions related to our service providers, please contact us via email: dpo@genome.eu.

5. You should also be aware that if you provide your consent to third-party cookies, this data will be transferred to respective service providers, as detailed in our [Cookie Policy](#).

6. We only use the services of those data processors, which ensure safeguards and utilize technical and organizational security measures equivalent to the ones required by the EU General Data Protection Regulation.

7. We may also disclose your Personal Data if we are under a duty to disclose or share your personal information in order to comply with any legal or regulatory obligation or request.

8. To ensure the payment process runs smoothly, some of your personal information may be shared with a company or entity you cooperate with inside Our system.

9. Genome warrants that it will disclose your Data and the Data of your clients,

officers, and other representatives your organization transferred to us or collected by us on your behalf as specified in this Privacy Notice, [Cookie Policy](#), and the contract entered into between Genome and you or your organization, as well as where there is a legal requirement for data transfer or disclosure.

12. How organizations/merchants share Data with us

1. When you are a business and transfer to us any Personal Data of the officers, shareholders, ultimate beneficiary owners, and other representatives of your organization, as well as when you use payment collection services under Genome Merchant Terms of Service and transfer to us Personal Data of your clients, you shall be obliged to obtain prior consent or have other legal grounds for the collection, retention, use, and processing of such Data, as well as for the data transfer to Genome.

13. Cross-border transfer

1. For the purpose of providing you with the Genome Wallet and Genome Services, we may engage third-party service providers outside the EU/EEA. In such a case, your personal data may be transferred and processed outside the EU/EEA,

including, without limitation, in the United Kingdom and USA.

2. Data protection laws of third countries may be different from the EU data protection laws and not guarantee an adequate level of security. However, we will take measures to ensure that any such transfers comply with applicable data protection laws and that personal data remains protected.

3. The transfer of personal data outside the EU/EEA may be considered as needed in such situations as e.g.:

3.1. for the clients' identity verification;

3.2. in order to conclude the agreement between you and Genome and/or in order to fulfill the obligations that are set under such an agreement;

3.3. in cases indicated in legal acts and regulations for the protection of our lawful interests, e.g., in order to file a lawsuit in court / other governmental bodies;

3.4. in order to fulfill legal requirements or in order to realize public interest.

4. When we transfer your Personal Data internationally, we put in place

safeguards in accordance with applicable laws and in accordance with this Privacy Notice, and we will ensure that it is protected and transferred in a consistent way with the legal requirements applicable to the Personal Data.

5. To ensure that your Personal Data is treated securely, we undertake to follow the Technical and Organizational measures as specified in Clause 10 and the measures below:

5.1. In case of adequacy decision: the country to which we send the personal data, a territory or one or more specified sectors within that third country or the international organization is approved by the European Commission as having an adequate level of protection (as stated in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en);

5.2. In the absence of an adequacy decision of the European Commission, Genome may transfer personal data to a third country or an international organization only if we have provided **appropriate safeguards** and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available, in particular:

a) the recipient has signed standard data protection clauses for the transfer of personal data to third countries, i.e., for international transfers, which are approved by the European Commission

(<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D0914>);

b) in case special permission has been obtained from a supervisory authority.

5.3. In the **absence of an adequacy decision of the European Commission** or in case there is **no possibility to use any appropriate safeguards** mentioned above, a transfer or a set of transfers of personal data to a third country or an international organization could take place only on one of the following conditions (GDPR Article 49):

5.3.1. the Data Subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

5.3.2. the transfer is necessary for the performance of a contract between the Data Subject and the controller or the implementation of pre-contractual measures taken at the Data Subject's request;

5.3.3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and another natural or legal person;

5.3.4. the transfer is necessary for the establishment, exercise, or defense of legal claims;

5.3.5. other cases stated in the GDPR Article 49 of applicable legislation.

6. We may also transfer personal data to a third country by taking other measures provided by GDPR and this Policy if they ensure appropriate safeguards as indicated in applicable law.

7. In Genome, Data may normally be transferred to a third party with the consent of the Data Subject and/or for the purpose of performance of the contract only in the following cases:

(a) When the customer executes a payment order to a third party (the payment service provider of the beneficiary of payment gets the information of payment order according to legislation; however, Genome could not have any contractual relations to payment service providers);

(b) For the execution of the customer's payment order with the help of a third-party correspondent partner (payment orders to third parties may include some payment correspondents, to which the information of payment order is provided according to legislation; however, Genome could not have any contractual relations to payment service providers).

8. If you would like to understand more about how Genome transfers Personal Data internationally and your rights in connection therewith, please contact us at dpo@genome.eu.

14. How long we retain your data

1. Genome shall apply different periods of retention of Personal Data depending on the categories and purposes of processed Personal Data.

2. We may use your data for as long as reasonably necessary for the limited purpose of providing you with Genome Wallet and Genome Services and complying with Legal and Regulatory Obligations. The terms of retention of the personal data for the purposes of the processing of the personal data as defined in this Privacy Notice are the following:

2.1. Data processed for the conclusion of the contract or performance of identification and verification procedures prior to the conclusion of the contract (to get to know, identify, and verify our clients):

a) for a period of 8 (eight) years from the date of the end of business relations with the client. The storage terms of documents, data, and logs can be additionally extended for no longer than 2 (two) years when there is reasoned instruction from the competent authority.

2.1.1. The conclusion of the contract itself:

a) until the contract remains in force and up to 10 (ten) years after the contractual relationship with the client has ended;

2.2. Data processed for fulfillment of a contract concluded with you, including but not limited to the provision of services of issuance, distribution, and redemption of electronic money, provision of payment services, complaint resolution, and customer service (this purpose includes, among other things, the monitoring of customers and their transactions):

a) for a period of 8 (eight) years from the date of the end of business relations with the client. The storage terms of documents, data, and logs can be additionally extended for no longer than 2 (two) years when there is reasoned instruction of the competent authority;

2.3. Data processed for compliance with legal obligations (e.g., implementation of the obligations under the Law on Money Laundering and Terrorist Financing Prevention of the Republic of Lithuania and other fraud and crime prevention purposes, implementation of AEOI & CRS (Automatic Exchange of Information & Common Reporting Standard) requirements), CESOP (the Central Electronic System of Payment information) requirements and risk management obligations:

a) for a period of 8 (eight) years from the date of the end of business relations with the client. The storage terms of documents, data, and logs can be additionally extended for a maximum of 2 (two) years when there is a reasoned instruction from the competent authority.

b) for a period of 8 (eight) years from the date of the end of unsuccessful verification if the verification was rejected by Genome due to an important reason.

2.3.1. Results of investigations of complex or unusually large transactions and

unusual transaction structures:

a) for a period of 5 (five) years in paper format or on an electronic medium. The storage period may be extended additionally upon a reasoned instruction of a competent institution. Nevertheless, the extension cannot last longer than 2 (two) years;

2.4. Data processed for the execution of payment transactions:

a) for a period of 8 (eight) years from the date of execution of the monetary transaction or conclusion of the transaction. The storage period may be extended additionally upon a reasoned instruction of a competent institution. Nevertheless, the extension cannot last longer than 2 (two) years;

2.5. Data processed for debit card granting, activation, processing, and execution of payment transactions by debit card:

a) for a period of 8 (eight) years from the date of execution of the monetary transaction or conclusion of the transaction;

2.6. Data processed for providing an answer if you are not our client and contact

us:

2.6.1. through Genome Site or Genome Wallet:

a) for a period which is necessary for the fulfillment of the request and to maintain further cooperation, but no longer than 6 (six) months after the last day of communication, in case there are no legal requirements to keep the data longer;

2.6.2. through other communication measures:

a) for a period which is necessary for the fulfilment of the request and to maintain further cooperation, but no longer than 1 (one) year after the last day of communication, in case there are no legal requirements to keep the data longer.

2.7. Processing of written or electronic correspondence relating to the business relationship with our clients:

a) for a period of 5 (five) years from the date of termination of business relations with the client. The storage period may be extended additionally upon a reasoned instruction of a competent institution. Nevertheless, the extension cannot last longer than 2 (two) years;

2.8. Data processed for the maintenance and administration of business relations with our clients and potential clients, customer service, and quality assurance of services provided:

a) 1 (one) year or as long as consent remains in force / is not withdrawn, based on the earliest event; however, if it is a suspicious call, question, or request related to AML, this could be stored according to AML Law (for a period of 5 (five) years from the date of termination of business relations with the client);

2.9. Data processed for direct marketing in order to inform Genome clients about our similar goods or services and/or about services provided by our business partners or other third parties or in order to make assessments about your opinion on different issues in relation to our business partners or other third parties:

a) as long as consent remains in force / is not withdrawn, based on the earliest event;

2.10. Data processed for authentication, fraud prevention, security, settings, service improvement, and marketing (based on cookies):

a) Strictly necessary cookies are essential for the functionality of the Genome Site. These cookies are always active.

b) Analytical and marketing cookies: data is processed as long as consent remains in force / is not withdrawn. The website visitor can delete and disable cookies at any time using browser settings even if you already gave consent for data processing;

However, in all cases cookies retention varies based on the type of cookie and is detailed in our Cookie Policy.

2.11. Data processed for providing payment services to you when you are a business and use Genome payment collection services in order to fulfill transactions between you, as a merchant, and your clients:

a) for a period of 8 (eight) years from the date of execution of the monetary transaction or conclusion of the transaction;

2.12. Data processed for application of Genome loyalty program:

a) as established in the contract or the governing law, the general storage term of

the contract is 5 (five) years (after the end of the contract);

2.13. Data processed for debt management, representing Genome in courts and/or pre-trial dispute resolution institutions:

a) according to the deadline set by the institution resolving the dispute, up to 10 (ten) years. In the cases when the terms of data keeping are indicated in the legislative regulations, the legislative regulations are applied.

3. Your personal data might be stored longer in the following cases:

3.1. ongoing investigations from Member States' authorities if there is a chance records of personal data are needed by Genome to prove compliance with any legal requirements;

3.2. when it is necessary in order for us to defend ourselves against claims, demands, actions, or to exercise legal rights in cases of lawsuits or similar court proceedings recognized under local law;

3.3. your personal data is necessary for the proper resolution of a dispute/complaint;

3.4. there is a reasonable suspicion of an unlawful act that is being investigated by us and/or the competent authorities;

3.5. under any other statutory ground.

15. Direct Marketing

1. We want to make it clear how we use your personal data for marketing purposes.

2. We may use our existing clients' e-mail for the marketing of our similar goods or services unless you object to the use of your e-mail for the marketing of our similar goods and services. You are granted a clear, free of charge and easily realizable possibility to object or withdraw from such use of your contact details on the occasion of each message, or please log into your personal account via Genome Mobile App > Profile icon> Notifications > Marketing communication > disable respective toggle.

3. We may also provide the information to you as our client about our products or services by sending messages through Genome Mobile App. Such messages may

be viewed in the notification center, in case you do not choose the “opt-out” function in our application.

4. In other cases, we may use your Personal Data for the purpose of direct marketing, if you give us your prior consent regarding such use of Data or based on legitimate interest, it is necessary to inform you about updates of mandatory rules or policies, such as this Policy or our Terms of Use.

5. We are entitled to offer the services provided by our business partners or other third parties to you or make assessments about your opinion on different issues in relation to our business partners or other third parties on the basis of a prior consent.

6. In case you do not agree to receive these marketing messages offered by us, our business partners or third parties, this will not have any impact on the provision of services to you as our client.

7. We provide a clear, free-of-charge, and easily realizable possibility for you at any time not to give your consent or to withdraw your given consent for sending proposals put forward by us. We shall state in each notification sent by e-mail that you are entitled to object to the processing of personal data or refuse to receive

notifications from us. You shall be entitled to refuse to receive notifications from us by clicking on the respective link in each e-mail notification, or you can give or withdraw your consent at any time by logging into your personal account via Genome Mobile App > Profile icon> Notifications > Marketing communication > disable / turn on respective toggle.

16. Automated decision-making and profiling

1. In some cases, we may make automated decisions regarding you using your information. When you instruct us to make a payment from your account or to request payment into your account from a bank or other payment services provider, our systems (or systems provided to us by our suppliers) make an automated check for authorization, sanction check, and/or automated checks to detect an unusual transaction pattern or location of your transaction and help us to fight fraud.

2. Automated decisions can be made by our partner Onfido in the course of your identity verification or by our partner Covery AI Limited that provides us automate KYC/KYB/AML procedures. Learn more about Onfido practices from their Privacy Policy (“Automated Decision Making and Onfido Reports” section), more about

Covery AI Limited services you can read here (Products: KYC Automation) and more about their privacy please read here.

3. At the same time, such profiling can be made by our third-party service providers specified in the Cookie Policy thereto we may transfer your data if you provide your consent to third-party cookies. In such a case the data is processed for marketing and targeting purposes.

4. Please be informed that you can request a manual review of the accuracy of an automated decision in case you are not satisfied with it and you have the right not to be subject to a decision based solely on such automated processing.

17. Your rights as a Data Subject

1. When we act as a data controller, you have the following rights regarding the protection of your Personal Data:

1.1. you have the right to know about the processing of your personal data as well as to have access to your personal data and processing (right to get familiar with your personal data and how it is processed);

1.2. you can ask us to erase or delete all or some of your personal data (e.g., if it is no longer necessary to provide Genome Services to you). Please note that this right to erasure is not absolute. In certain cases where we need to store your personal data because of a contractual relationship or law, we cannot erase all of your personal data;

1.3. you can ask us to change, update, or fix your data in certain cases, particularly if it is inaccurate. You may do it yourself; simply log in to your Genome Wallet and change your profile settings at once. If the type of data you want to change or update is not visible or editable in your profile settings, you can contact us using the contact details provided in this Policy and request that appropriate corrections be made to your personal data. You can also close your account using Genome Wallet functionality and/or contact our customer support service. If your personal data was transferred to third-party data processors, they will be notified of any editing or deletion of your personal data;

1.4. you can ask us to obtain restrictions on processing all or some of your personal data (e.g., if you believe that we have no legal right to keep using it) or to limit our use of it (e.g., if you believe that your personal data is inaccurate or unlawfully held). It can also pertain to a situation where you object to processing that we base on a legitimate interest. In such case, we must verify if our grounds

override yours;

1.5. you can obtain a copy of your personal data we retain about you unless this adversely affects the rights and freedoms of others. You have the right to ask us to provide your information in an easily readable format to another company;

1.6. where we are processing your personal information based on legitimate interest, and you may object to this. However, we may be entitled to continue processing your information based on our legitimate interests or where this is relevant to legal claims. You also have the right to object to the usage of personal information for direct marketing purposes or automated decision-making;

1.7. you can ask to transfer your personal data to another data controller or provide it directly to you in a convenient format (NOTE: applicable to personal data which is provided by you and which is processed by automated means on the basis of consent or on the basis of conclusion and performance of the contract);

1.8. you have the right to withdraw your consent so that we stop that particular processing, when the processing is based on consent. Such consent withdrawal does not affect the lawfulness of processing based on consent before its withdrawal;

1.9. you have the right to appeal to the State Data Protection Inspectorate or the court if you do not agree with our answer to your request or claim.

1.10. other rights established in GDPR and legal acts.

2. To exercise any of the rights mentioned above, please reach out to our client support team via e-mail support@genome.eu. or contact our Data Protection Officer as indicated below. A "Data Subjects Request Form" is stored in the Company's internal network, which you will need to fill out and send together with proof of identity to our Data Protection Officer by e-mail: dpo@genome.eu.

3. Your requests shall be fulfilled, or fulfillment of your requests shall be refused by specifying the reasons for such refusal within 30 (thirty) calendar days from the date of submission of the request, meeting our internal rules and GDPR. The afore-mentioned time frame may be extended for 30 (thirty) calendar days by giving prior notice to you if the request is related to a great scope of personal data or other simultaneously examined requests. A response to you will be provided in a form of your choosing as the requester.

18. The right to lodge a complaint

1. Moreover, you have the right to submit a complaint to us if you reasonably believe that the processing of personal data related to you is performed in violation of the applicable legal requirements. You can submit a complaint by post or e-mail (dpo@genome.eu), specifying your name, surname, contact details, and relevant information, which would indicate why you reasonably believe that the processing of the data related to you is performed in violation of the applicable legal requirements. Upon receipt of a complaint from you, we confirm receipt of the complaint and indicate the time limit within which the reply will be submitted. In each case, the deadline for submitting a reply may vary as it directly depends on the extent and complexity of the complaint filed, but we will make the maximum effort to provide the response to you within the shortest possible time. We, after examining the complaint, report the results and actions taken to satisfy your complaint or provide relevant information on what further actions you may take if your complaint is not satisfied.

2. You can also address the State Data Protection Inspectorate by e-mail ada@ada.lt or to the national Data Protection Agency (DPA) in the country of your residence (you can find the list of other EU data protection authorities and their contact details at https://www.edpb.europa.eu/about-edpb/about-edpb/members_en) with a claim regarding the processing of your personal data if you believe that the personal

data is processed in a way that violates your rights and legitimate interests stipulated by applicable legislation. You may apply in accordance with the procedures for handling complaints that are established by the State Data Protection Inspectorate and which may be found at this link:

<https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas>.

19. Minors

1. Genome does not voluntarily collect, use, or disclose the personal data of minors according to the minimum age equivalent in the relevant jurisdiction. Genome Wallet and Genome Services are not designed to attract minors. If you are a minor, you **may not** submit any personal information to us, open Genome Wallet, or subscribe to Genome Services. If we become aware that we collected the personal information of a minor, we will take steps to delete the information as soon as possible and will ask third-party data processors thereto the data was transferred (if any) to erase the data immediately.

20. Data breaches

1. We assure you that we have all the necessary technologies and methods to prevent, detect, and investigate a personal data breach. In case of a data breach,

we will endeavor our best efforts to send a notification to inform you of the breach as soon as possible, when it is likely to result in a high risk to your rights and freedoms. If your personal data was transferred to third-party data processors, they would be notified of a data breach as well.

21. Data Protection Officer

1. If you are not satisfied with how Genome handles your personal data or wish to raise a complaint regarding the processing of your personal data, please contact our Data Protection Officer at dpo@genome.eu.

22. How may this Privacy Notice be changed

1. We can make amendments to this Privacy Notice at any time by means of publishing a revised edition on the Genome Site. You will be notified of any substantial changes. The revised version will be in effect immediately and will be noted by the updated date at the end of this Privacy Notice. You are entitled to terminate the contract with Genome if you do not agree with any changes. By continuing to use Genome Wallet and Genome Services, you accept the changes. Please review this Privacy Notice from time to time to stay updated on any



„Maneuver LT“ UAB
Reg N: 304785124
VAT: LT100011709919

changes.

This Privacy Notice was last modified on April 17, 2024

Previous versions

[Download version 0.1 \(28.09.2020\) →](#)

[Download version 0.2 \(17.11.2022\) →](#)