

PRIVACY POLICY

This Privacy Policy ("**Policy**") sets out the main principles governing the processing of personal data of the visitors of the website of the crowdfunding platform "ROIX", operated by UAB ROIX (the "**Company**" or "**we**"), clients (investors, project owners), their representatives, beneficial owners, and persons who have provided collateral ("**You**").

The data controller of your personal data is: **UAB ROIX**, legal entity code: 305328324, registered office address: Naugarduko g. 3-401, Vilnius, Lithuania.

This Policy is prepared in accordance with:

- a. General Data Protection Regulation ("**GDPR**");
- b. Law on the Legal Protection of Personal Data of the Republic of Lithuania;
- c. Law on Electronic Communications of the Republic of Lithuania; and
- d. other applicable legal acts related to the Company's activities, including crowdfunding services, as well as the guidelines and recommendations of supervisory authorities.

If you have any questions regarding the protection of your personal data or the provisions of this Policy, please contact the Company at: info@roix.lt.

When processing your personal data, the Company adheres to the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, and accuracy. The Company also implements security measures and procedures aimed at protecting your personal data from unauthorized access, disclosure, loss, alteration, destruction, or other unlawful processing.

1. DEFINITIONS

- 1.1. In this Policy, capitalized terms shall have the meanings set out below, unless the context requires otherwise:
 - 1.1.1. Personal Data – any information that can be used directly or indirectly to identify a natural person, as well as any information relating to an identified natural person;
 - 1.1.2. Data Subject – a natural person who is a visitor of the Company's website www.roix.lt (the "**Website**"), a client of the Company, a sender of inquiries to the Company, or another person associated with the Company's activities and/or provided services;
 - 1.1.3. Processing – any operation performed on Personal Data, including but not limited to collection, recording, systematization, storage, modification, access, use, etc.
- 1.2. Other terms used in this Policy shall be interpreted as defined in the GDPR, other applicable legislation, and the Company's internal regulations.

2. PURPOSES, LEGAL BASES AND CATEGORIES OF PROCESSED PERSONAL DATA

- 2.1. The Company processes your Personal Data for the purposes and to the extent specified below:

Purpose of Data Processing	Legal Basis	Scope of Data Processing
1. Remote identity verification	Your consent	Name, surname, personal identification number, date of birth, nationality, identity document details and copies, photograph, biometric data (such as facial image ("selfie") and video recording), permanent residence

		permit data, phone number, email address, residential address, registered address or correspondence address.
2. Ongoing monitoring of business relationships	Legal obligation	Data required for the implementation of anti-money laundering and counter-terrorist financing measures, including the identification of the purpose of the business relationship and whether the client is a politically exposed person, information on the origin of funds, transaction counterparties and business activity, participation in legal entities, data on management and beneficial owners, representatives' contact details, IP address, login location, etc.
3. Creditworthiness assessment	Legal obligation, contract performance	Data required for us to fulfil the requirements set out in the Crowdfunding Regulation and the contract, which: a) are accessible in the systems: JAR, JADIS, JANGIS, TAAR, Mortgage Register, Creditinfo, public info, NTR; b) are provided by the client: contact details, audited financial statements of the legal entity for the last three years, projected cash flows, business plan, forecasted financial statements, information on collateral (real estate appraisal, cost estimates, permits, projects, proofs of payment, etc.), if needed, information proving cash flows, account statements, social insurance (Sodra) statements, data on criminal convictions and offences.
4. Reliability assessment	Legal obligation	Reliability assessment Legal obligation Data on criminal convictions and offences; data confirming whether the evaluated person fulfils credit obligations; data on whether there have been civil claims, administrative or criminal proceedings, investments or assumed risks and loans that may have a significant impact on the person's financial reliability; data on whether the project owner is listed in the criminal record register, as well as data verified in other reliable databases lawfully accessible to the Company. The processing of this data is based on the automatic creditworthiness assessment formula approved by the Bank of Lithuania.

5. Assessment of investment experience and knowledge	Legal obligation	Name, surname, age, education, data on income, savings, obligations, investment experience and investment objectives, and other related information.
6. Administration of crowdfunding transactions	Contract performance, legal obligation	Name, surname, registered address (in case of a legal entity – name, surname, personal identification number, email address, phone number of the manager or authorised person), phone number, email address, loan agreement number, date of conclusion of the agreement, termination date, date of debt recovery transfer and receipt, investment data, loan purpose, amount, loan repayment schedule, information on collateral, investment data and other related information.
7. Prevention of money laundering and terrorist financing	Legal obligation, Public interest	Name, surname, personal identification number, date of birth, registration address, residential address, nationality, email address, phone number, number of shares held by shareholders (beneficial owners), object of investment, planned investment amount, income, main source of funds, actual owner of the funds, documentation of accounts and/or agreements, correspondence on business relationships, documents and data confirming financial transactions or contracts or other legally valid documents and data related to the execution of financial transactions or conclusion of contracts, IP address, checks in public and reliable registers, other data received from the Data Subject or provided during the “Know Your Customer” procedure, data on political activity, etc.
8. Ensuring compliance with international sanctions	Legal obligation, Public interest	Name, surname, personal identification number, date of birth, registration address, residential address, nationality, email address, phone number, number of shares held by shareholders (beneficial owners), object of investment, planned investment amount, income, main source of funds, actual owner of the funds, documentation of accounts and/or agreements, correspondence on business relationships, documents and data confirming financial transactions or contracts or other legally valid documents and data related to the execution

		of financial transactions or conclusion of contracts, IP address, checks in public and reliable registers, other data received from the Data Subject or provided during the “Know Your Customer” procedure, data on political activity, inclusion in sanction lists, etc.
9. Contract conclusion and execution	Intention to take actions prior to contract conclusion and contract execution	<p>Name, surname, phone number, email address, identification and verification data and other data required for the provision of Company services and contract conclusion/execution.</p> <p>Please note that in certain cases we are entitled to process the personal data of your lawful heirs (copy of identity documents, inheritance documents, bank account number and other information related to inheritance).</p>
10. Improvement of service quality, including the examination of complaints and/or claims submitted by you	Legitimate interest, Legal obligation	Name, surname, phone number, email address, residential address, registered address or correspondence address, information on actions performed on the Website, related technical information, IP address used during internet connection, version of the operating system and parameters of the device you use to access content/services; session usage time and duration; search queries entered on the Website, letters, emails, live chat conversations and other forms of communication messages and their content, etc.
11. To prevent, limit and investigate any abuse, fraud, unauthorised use or service disruption or to assert, exercise and defend legal claims	Legal obligation, Legitimate interest	Name, surname, phone number, email address, residential address, registered address or correspondence address, letters, emails and other forms of communication messages and their content, identification data, data on owned property, transactions, loans, obligations, deposits made on the platform (Website), account from which the deposit was made, etc.
12. Responding to your inquiries	Your consent, Contract performance	Name, surname, phone number, email address, residential address, registered address or correspondence address, letters, emails, live chat conversations and other

		forms of communication messages and their content.
13. Processing of statistical data	Legal obligation	<p>Information about the project owner and the amount raised, aggregated information about investors and invested amount, broken down by the investors' tax residency, distinguishing between experienced and non-experienced investors, and other statistical information required by legal acts applicable to the Company's operations.</p> <p>The above data is processed without the ability to identify a specific Data Subject, i.e., the personal data is anonymised.</p>
14. Debt recovery and administration	Contract performance	Name, surname, personal identification number, date of birth, residential address, registered address or correspondence address, phone number, email address, amount of debt, duration of delay, payment date, data required to assess solvency, collateral and other information related to the debt.
15. Investor information	Legal obligation	Information about the project owner(s) and the crowdfunding project, management and contact details, all natural and legal persons responsible for the information provided in the key investment information document, in the case of natural persons, including the project owner's management, administrative or supervisory board members – name, surname and position of the natural person, valuation reports, etc.

3. PROCESSING OF PERSONAL DATA FOR DIRECT MARKETING PURPOSES

- 3.1. If you are our client, we may use your contact details for direct marketing purposes related to similar services, provided that you are offered a clear, free of charge and easily exercisable option to object or opt out from such use of your contact details for the purposes mentioned above, and provided you did not initially object to such use of data.
- 3.2. In all other cases, we may use your contact details for direct marketing purposes only after obtaining your prior consent..
- 3.3. We provide you with a clear, free of charge and easily exercisable option to withdraw the given consent at any time. Please be informed that you have the right at any time to opt out of receiving direct marketing messages from us by notifying us of your decision via email at info@roix.it or by using the unsubscribe link provided in the direct marketing message itself.

4. HOW DO WE OBTAIN YOUR PERSONAL DATA?

- 4.1. We process your personal data that:

- 4.1.1. you provide to us yourself;
- 4.1.2. are provided to us by our clients, for example, if you are their family member or you are a representative, employee, contractor, founder, shareholder, participant, owner, pledged asset owner, etc., of a legal entity client;
- 4.1.3. we receive from documents provided by clients, such as applications – forms, written explanations, payment documents, property valuation reports, purchase-sale and other contracts, insurance documents, court decisions, refinancing consents, etc.;
- 4.1.4. we obtain from external sources, such as:
 - 4.1.4.1. other financial institutions;
 - 4.1.4.2. supervisory and other public institutions or authorities, e.g., the Bank of Lithuania;
 - 4.1.4.3. from the State Enterprise Centre of Registers (e.g., the Population Register, the Register of Participants of Legal Entities (JADIS), the Register of Beneficial Owners (JANGIS), the Register of Legal Entities, etc.) and other registers;
 - 4.1.4.4. from persons administering joint debtor data files (e.g., UAB “Creditinfo Lietuva”);
 - 4.1.4.5. from law enforcement institutions;
 - 4.1.4.6. from natural or legal persons (notaries, bailiffs, attorneys, etc.) when they provide such data in accordance with contractual obligations or legal requirements;
- 4.1.5. we obtain while monitoring the use of our systems and services.
- 4.2. The Company may also verify publicly available information about you in order to verify the data you have submitted, the transactions being made, etc.
- 4.3. Please note that when you provide us with personal data, you are responsible for the accuracy, completeness, and relevance of such data. If inaccurate, false, or misleading personal data is provided, we have the right to delete such data or restrict access to our services, etc. If you provide personal data about other individuals (e.g., your relatives, employees, etc.), you are responsible for the accuracy, completeness, and relevance of such data, as well as for obtaining the consent of the data subject to have their data shared with us. It should be noted that in providing such data, we may ask you to confirm that you have the right to submit it. If such a person inquires about the receipt of their personal data, we will indicate you as the source of the data.

5. RETENTION PERIODS FOR PERSONAL DATA

- 5.1. We will retain your personal data for as long as they are necessary for the purposes for which they were collected and processed, but no longer than required by applicable laws and regulations. Upon the expiry of this period, personal data shall be deleted/destroyed in such a manner that they cannot be restored.
- 5.2. If the laws of the Republic of Lithuania or international legal acts do not establish a specific period for the retention of personal data, we shall determine such a period ourselves, taking into account the legitimate purpose of data retention, the legal basis, and the principles of personal data processing.
- 5.3. The main personal data retention periods are as follows:
 - 5.3.1. in the case of conclusion and performance of a contract, the contract shall be retained for 10 (ten) years after the expiration of the contract;

- 5.3.2. personal data of potential clients (who were offered services but did not conclude a contract) shall be retained for 2 (two) years from the date of the decision not to conclude the contract;
- 5.3.3. for the implementation of anti-money laundering and counter-terrorist financing requirements, copies of identity documents confirming the identity of the client, data of the beneficial owner, other data obtained during client identification, account and/or contract documentation shall be retained for 8 (eight) years from the end of the transactions or business relationship with the client. Correspondence related to business relationships shall be retained for 5 (five) years from the end of the transactions or business relationship with the client, either in paper format or electronic media. The retention periods may be extended for no more than 2 (two) additional years;
- 5.3.4. the retention period for personal data processed for direct marketing purposes is 3 (three) years from the date of receipt of the relevant data, unless you object to such processing before the end of the retention period. After the expiry of this period or if the data subject withdraws consent to data processing for direct marketing purposes prior to its expiry, we will cease processing your data. Upon expiry, we may ask you to renew your consent for direct marketing and/or provision of personalized offers;
- 5.3.5. data of project owners:
 - 5.3.5.1. documents forming the project file (contracts and other documents evidencing the existence of debt, their annexes, communication with the project owner and other documents related to the debt and its collateral, documents related to the implementation of the project, use of crowdfunding funds for their intended purpose, supporting expenditure documents, etc.) shall be retained for 10 (ten) years from the date of final and proper settlement;
 - 5.3.5.2. information, data, and documents collected (assessed) during the creditworthiness assessment of the project owner shall be retained for 10 (ten) years from the date of conclusion of the last financing transaction by the project owner;
 - 5.3.5.3. data on real estate pledged to secure obligations under the contracts shall be retained for 8 (eight) years from the date of conclusion of the last financing transaction by the project owner;
- 5.3.6. data from inquiries submitted to the Company by phone/email/other electronic or physical means and data of individuals submitting inquiries shall be retained for 2 (two) years from the date of the inquiry.
- 5.4. Please note that in certain cases, your personal data may be retained for longer:
 - 5.4.1. if necessary for us to defend against claims, demands, or lawsuits and to exercise our rights;
 - 5.4.2. if we have reasonable suspicions of unlawful activity under investigation;
 - 5.4.3. if personal data is required for proper resolution of a dispute or complaint;
 - 5.4.4. in other cases as provided for by law.

6. ENSURING THE SECURITY OF PERSONAL DATA

- 6.1. In order to ensure the security of your personal data and to prevent unlawful or accidental destruction, alteration, disclosure, as well as any other unauthorized data processing, we implement various technical and organizational security measures aimed at achieving these objectives. These measures include various technical and software tools, additional agreements with engaged service providers, internal rules related to personal data protection, and other measures.

- 6.2. Transmission of information via electronic communication channels (e.g., email, mobile devices, etc.) may in certain cases be less secure due to reasons beyond the control of our chosen technical or organizational measures. Therefore, to ensure the security of your confidential personal data, we recommend that you refrain from submitting information to us through less secure and/or unsupported electronic systems.

7. RECIPIENTS OF PERSONAL DATA

- 7.1. The Company, in the course of conducting its activities, may engage certain data processors (service providers, e.g., companies providing data storage services, software development and maintenance services, debt management services, communication services, etc.). Certain of your Personal Data may be transferred to such parties; however, we ensure that your Personal Data is transferred only in those cases and to the extent necessary for the provision of their respective services.
- 7.2. Understanding our obligation to process your Personal Data in strict compliance with applicable requirements, we engage only such service providers who have implemented/undertake to implement appropriate technical and organizational security measures and ensure that such service providers comply with proper personal data protection, security, and confidentiality obligations set forth in a written agreement.
- 7.3. The recipients of your Personal Data may also include the following persons or institutions:
- 7.3.1. payment and other service providers and financial institutions whose services the Company uses in the course of its activities, e.g., UAB “BLUE EMI LT”;
 - 7.3.2. entities administering joint debtor data files (e.g., UAB “Creditinfo Lietuva”, UAB “Scorify”, etc.);
 - 7.3.3. state institutions and registers (Bank of Lithuania, Statistics Department, law enforcement authorities, etc.);
 - 7.3.4. courts, notaries, bailiffs;
 - 7.3.5. auditors, legal and financial advisors;
 - 7.3.6. if necessary – companies that would consider acquiring or acquire the Company’s business;
 - 7.3.7. other third parties related to the provision of the Company’s services and/or having a legal basis to receive such data.

8. DOES THE COMPANY TRANSFER YOUR PERSONAL DATA OUTSIDE THE EU/EEA?

- 8.1. The performance of the Company’s activities does not require transferring your Personal Data to recipients located outside the European Union (EU)/European Economic Area (EEA).
- 8.2. However, in exceptional cases, if it becomes necessary to transfer part of your data to a data recipient located outside the EU/EEA, we will take all necessary measures required by legal acts to ensure that your Personal Data remains appropriately protected.
- 8.3. Your Personal Data may be transferred outside the EEA only if one of the following conditions is met:
- 8.3.1. the data recipient has signed standard contractual clauses approved by the European Commission; or
 - 8.3.2. the data recipient is established in a country for which the European Commission has adopted an adequacy decision, i.e., the transfer of data to the recipient in such a country is equivalent to a transfer within the European Union; or
 - 8.3.3. pursuant to Article 49 of the GDPR, you have given your consent to such transfer of your Personal Data outside the EEA.

9. THIRD-PARTY WEBSITES

- 9.1. On our Website, we may provide links to or from partner, information source, or related party websites. Please note that the websites of other persons, which you may access by following links on our Website, have their own privacy policies, and we do not assume any responsibility for such privacy policies. Before providing any of your Personal Data on another website, you should familiarize yourself with the rules, privacy policy, and other relevant information published on that specific website.

10. TOOLS USED BY THE COMPANY FOR IDENTITY VERIFICATION

- 10.1. To perform your identity verification and authentication, we use the services of our partner's service provider UAB "ONDATO". This service provider captures your facial photograph or video and your submitted identity document through a specialized website with a camera. More information about UAB "ONDATO" can be found in the company's [Privacy Policy](#).
- 10.2. The UAB "ONDATO" solution is used to compare the captured facial images or video with the presented identity document in order to comply with legal obligations (e.g., to implement the requirements of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other anti-fraud and crime prevention regulations) and to fulfill risk management obligations.
- 10.3. The facial similarity result (match or mismatch) will be stored only as long as necessary to perform the verification and for the retention period specified in legal acts related to the prevention of money laundering and terrorist financing.
- 10.4. Your facial similarity check is a one-time user authorization comparing facial photographs with each other based on data obtained during verification. Your facial template is not created, recorded, or stored. It is not possible to reconstruct the original data from the stored information.
- 10.5. When using UAB "ONDATO" services, Personal Data is used to identify your identity, as UAB "ONDATO" compares the person's facial image on the document with the image captured. This process allows us to more accurately determine your identity, and it is quicker and more convenient. If you are not satisfied with this identity verification method, you may contact us via email at info@roix.lt to arrange for an alternative identification method.

11. COOKIES USED BY THE COMPANY

- 11.1. Cookies are small text files that a website stores on your computer or mobile device when you visit the website. Cookies allow a website to recognize a user's device (e.g., when a user returns to the same website), and may also be used to track the user's behavior and habits online. The Company may use similar technologies such as web beacons, tags, scripts, pixels, local storage, etc. (hereinafter collectively referred to as "cookies" in this Policy). The information collected by cookies helps ensure more convenient browsing on the Website, allows us to provide offers, understand user behavior on the Website, analyze trends, and improve the Website.
- 11.2. The following types of cookies are used on the Website:
- 11.2.1. Necessary cookies. These cookies are essential for the Website to function properly. Without these mandatory cookies, the Website may not function as expected;
- 11.2.2. Analytical cookies. These cookies help us better understand Website visitors, thus allowing us to improve the content and fix possible errors. The Company uses "Google Analytics," a web analytics service that allows the analysis of Website usage. The data collected by "Google Analytics" is referred to as site metrics or analytics. "Google Analytics" is provided by Google Inc. ("Google"). It uses cookies to understand visitor behavior. Google collects statistics that allow us to better understand how users interact with the Website;
- 11.2.3. Advertising cookies. These cookies are used to display ads that are relevant and interesting to the user. They may also be used to measure the effectiveness of an advertising campaign.

11.3. Based on their duration, cookies are classified as session cookies (deleted when the user closes the browser) and persistent cookies (stored for a longer period). Cookies may also be categorized as first-party (placed by the Website itself) or third-party (e.g., advertising providers).

11.4. The following cookies are used on the Website:

Cookie Name	Description and Type	Creation Time	Expiration Time	Data Used
customer-info	Used to identify the source of investor referral. This code is used to track advertising campaigns.	When a referral/ad code is used.	1 year	The cookie stores the code indicating the page from which the user entered ROIX portals and assigns a randomly generated number to recognize unique visitors. It does not store any personal data.
viewed_cookie_policy	Used to store whether the user has accepted the use of cookies.	When the cookie is accepted.	11 months	No personal data is stored.
_ga	Calculates visitor, session, and campaign data and tracks site usage for analytics reporting.	When the page is opened.	2 years	The cookie stores information anonymously and assigns a randomly generated number to recognize unique visitors.
https://invest.roix.lt/	Used to improve user experience.	When ROIX portals are opened.	14 days	Stores application settings (page, language, etc.) to improve user experience.

				No personal data is stored.
--	--	--	--	-----------------------------

- 11.5. To control cookies used by us, you may adjust your cookie settings via the notification banner before starting to browse our Website. This banner allows you to manage all cookies placed on our Website. To update or change your cookie consent, click [here](#).
- 11.6. If you do not agree to have cookies stored on your computer or other device (when we ask for your consent), you can change your browser settings and disable all cookies or manage them individually:
- 11.6.1. cookie settings in „[Microsoft Edge](#)“ browser;
 - 11.6.2. cookie settings in „[Firefox](#)“ browser;
 - 11.6.3. cookie settings in „[Google Chrome](#)“ browser;
 - 11.6.4. cookie settings in „[Safari](#)“ browser.
- Note that this may slow down your browsing, limit the functionality of some websites, or block access to the Website.
- 11.7. More information on how to disable local storage in different browsers can be found here:
- 11.7.1. settings in „[Microsoft Edge](#)“ browser;
 - 11.7.2. settings in „[Firefox](#)“ browser;
 - 11.7.3. settings in „[Google Chrome](#)“ browser;
 - 11.7.4. settings in „[Safari](#)“ browser.
- 11.8. If you delete cookies, all settings controlled by these cookies will also be deleted, and you will need to recreate them the next time you visit our Website.

12. RIGHTS OF DATA SUBJECTS

- 12.1. As a Data Subject, you have the following rights:
- 12.1.1. to access your Personal Data and how it is being processed. You have the right to receive confirmation as to whether we process your Personal Data, and if so, to access that data and related information;
 - 12.1.2. to request the correction of incorrect, inaccurate, or incomplete data. If you believe the information we hold about you is inaccurate or incorrect, you have the right to request that such information be changed, clarified, or corrected;
 - 12.1.3. to request the deletion of your Personal Data ("the right to be forgotten"). In certain circumstances specified by law (e.g., if data is processed unlawfully or if the legal basis for processing ceases to exist), you may request that we delete your Personal Data;
 - 12.1.4. to request the restriction of the processing of your Personal Data. In certain situations defined by law (e.g., if data is processed unlawfully), you may request that we restrict the processing of your data;
 - 12.1.5. to request data portability to another data controller or directly to you in a convenient format. In certain cases, you have the right to transfer the data we process based on your consent to another data controller using automated means;
 - 12.1.6. to object to the processing of your Personal Data when processed based on legitimate interest, except in cases where there are compelling legitimate grounds

for such processing or where it is necessary for the establishment, exercise, or defense of legal claims;

- 12.1.7. to withdraw your consent for the processing of your Personal Data. If your Personal Data is being processed based on your separate consent, you have the right to withdraw such consent at any time. In that case, we will stop processing such data.
- 12.2. Please submit your requests for the exercise of Data Subject rights to us in writing via email at: info@roix.it. A Data Subject may also submit requests via our website chat window or through our Facebook, Instagram, LinkedIn, and other platforms.
- 12.3. If you believe your Personal Data is being processed unlawfully or your rights related to data processing have been violated, we encourage you to contact us using the means described in Clause 12.2. Your request will be fulfilled or rejected with reasons within 30 (thirty) calendar days from the date of submission. This term may be extended for an additional 60 (sixty) calendar days with prior notice if the request involves a large amount of data. The response will be provided using the same method the request was received (see Clause 12.2), unless a more detailed investigation is required, in which case the response may be provided via email. After reviewing the request, we will inform you of the outcome and the actions we took to fulfill your request or provide information on further steps if the request was not granted.
- 12.4. Your request must meet the following minimum requirements:
 - 12.4.1. the request must be written, legible, and understandable (a written request may be submitted via any of the methods listed in Clause 12.2);
 - 12.4.2. the request must contain your full name and other contact details (email, phone number);
 - 12.4.3. the request must specify clearly which right you wish to exercise and to what extent;
 - 12.4.4. if the request is submitted through a representative, it must include the representative's name, surname, contact details, and a document proving the authorization.
- 12.5. If you submit your request orally, we have the right to ask you to provide it in writing and are obliged to inform you of all the acceptable submission methods and minimum requirements.
- 12.6. You also have the right to lodge a complaint with the [State Data Protection Inspectorate](#) if you believe your rights have been violated. However, before doing so, we strongly encourage you to contact us directly, as this allows us to find the most efficient and mutually satisfactory resolution.
- 12.7. Please note that the rights described above may be restricted in order to ensure the prevention, investigation, detection, or prosecution of criminal offenses, or the execution of criminal penalties, including the protection of public security and as specified under Article 23 of the GDPR.

13. FINAL PROVISIONS

- 13.1. The Company reserves the right to update this Policy. Therefore, we recommend regularly reviewing this Policy to stay informed of any changes.
- 13.2. When making updates, we will not reduce your rights under this Policy or applicable personal data protection laws. Upon updating the Policy, we commit to publishing the updated version on our Website. We also provide access to previous versions of the Policy on our Website.
- 13.3. Amendments and/or supplements to the Policy shall enter into force from the moment they are published on the Website.