Privacy Policy

Effective Date: 2026 April 22

1. General Information

This Privacy Policy is issued by UAB Etapay, a private limited liability company incorporated under the laws of the Republic of Lithuania, with its legal entity code 304932396 and registered office at S. Moniuškos g. 27-4, Vilnius, Lithuania ("Etapay", "we", or "us"). For the purposes of the General Data Protection Regulation (EU) 2016/679 ("GDPR"), Etapay acts as the data controller when processing your personal data in connection with the services and activities described in this policy.

Etapay is established and operates within the European Union. Therefore, our personal data processing activities are carried out in accordance with applicable EU and Lithuanian data protection laws. If you are located outside the EU/EEA, please note that local data privacy regulations may differ from those in the EU, and we do not guarantee compliance with non-EU laws unless explicitly stated.

Etapay has appointed a Data Protection Officer (DPO). If you have any questions about this Privacy Policy or the processing of your personal data, you may contact our Data Protection Officer by email at: dpo@eta-pay.com.

2. How we use your personal data?

This Privacy Policy outlines how Etapay processes personal data in connection with various activities, services, and interactions. To provide a clear overview, we have structured the key data processing activities by purpose, type of personal data involved, applicable legal basis under the GDPR, and respective data retention periods. The processing activities described apply to different categories of data subjects, including job applicants, clients, business partners, platform users, researchers, landowners, and whistleblowers. Each activity is conducted in accordance with the principles of lawfulness, fairness, transparency, data minimization, and purpose limitation.

3. What are the legal bases for processing your personal data?

We process your personal data as described in this Privacy Policy based on the following legal grounds:

- the performance, conclusion, amendment, or administration of a service contract (Article 6(1)(b) of the GDPR);
- compliance with our legal obligations and regulatory requirements (Article 6(1)(c) of the GDPR);

- the pursuit of our or third parties' legitimate interests (Article 6(1)(f) of the GDPR);
- your consent (Article 6(1)(a).

In certain cases, the same personal data may be processed under more than one of the above legal bases.

Detailed information about the purposes and legal bases for processing your personal data is provided in the tables in Section 16 of this Privacy Policy.

4. How long do we retain your personal data?

We process and retain your personal data only for as long as necessary to achieve the purposes for which it is processed, or as required by applicable law. Detailed information about the potential purposes of processing your personal data and the corresponding retention periods is provided in Section 16 of this Privacy Policy.

Once the specified data processing or retention period expires, we will delete or securely and irreversibly anonymize your personal data as soon as reasonably possible within a justifiable time frame.

A longer retention and/or processing period than stated in this Privacy Policy may apply only in the following cases:

- the data is necessary for proper debt or damage management (e.g., if you fail to meet your financial and/or property obligations or cause harm to us or others);
- to resolve a dispute or complaint in order to protect our or third parties' legitimate interests;
- to enable us to defend against existing or potential claims, demands, or legal actions and to enforce its rights;
- there are reasonable suspicions of violations or unlawful activity that are or may be subject to investigation;
- to ensure the restriction of access to the services in cases where the agreement between us has been terminated due to serious violations;
- the data is needed to ensure the security, integrity, and resilience of information systems (e.g., upon detection of suspicious activity in the Account, Mobile App, Website, etc.);
- other legal grounds for retention exist under applicable law.

5. For what purposes and what personal data do we collect?

We collect and process only the personal data that is sufficient and necessary to achieve the defined purposes. The purposes of processing your personal data, along with the list of personal data collected, are described in detail in the tables provided in Section 16 of this Privacy Policy.

5.1. Clients Data Processing

We process personal data of our clients in order to provide, operate, and maintain our financial services. This includes opening and administering accounts, executing and receiving payments, and ensuring accurate accounting and reconciliation of transactions.

As part of delivering these services, we collect and use information necessary to identify clients, manage their accounts, and process transactions. This may include information related to account activity, payment details, and communications. We also maintain internal records to ensure the proper functioning of our systems and services.

To comply with applicable regulatory requirements, we carry out customer identity verification procedures and perform screening against anti-money laundering (AML) and sanctions lists. We also monitor transactions on an ongoing basis to detect unusual or suspicious activity and ensure compliance with financial crime prevention obligations.

Additionally, we process certain data to prevent fraud and manage risk. This may involve analyzing behavioral patterns, device and technical information, and system activity to protect our services, clients, and the integrity of transactions.

All personal data is processed only to the extent necessary for these purposes and in accordance with applicable data protection laws.

5.2. Customer Support and Business Communication

Etapay processes personal data in connection with various forms of communication used to respond to inquiries, maintain professional relationships, and provide service-related or promotional information. These communications may occur through multiple channels, including:

- email correspondence initiated by the user or Etapay staff;
- phone calls (inbound or outbound, including call notes if relevant);
- online meeting tools (e.g., Zoom, Microsoft Teams, Google Meet);
- contact forms submitted through our website;
- in-person meetings or business events;
- social media messages or interactions.

The purpose of this processing is to ensure effective customer service, technical support, relationship management, follow-up communication, and to provide updates on products and services.

5.3. Direct marketing messages

Direct marketing to existing clients. Etapay may process your personal data for the purpose of sending direct marketing communications regarding products or services that are similar to those you have previously purchased or contracted for. This processing is based on our legitimate interest in maintaining and developing business relationships, in accordance with Article 6(1)(f) of the General Data Protection Regulation (GDPR) and applicable e-privacy laws.

You have the right to object to the use of your personal data for direct marketing purposes at any time and free of charge. If you do not wish to receive such communications, you may object by contacting us at dpo@eta-pay.com. To ensure your preference is respected before any marketing communication is sent, **we kindly ask you to express your objection within 10 calendar days from the conclusion of the contrac**t. After this period, we may begin sending you relevant marketing messages, always including a clear unsubscribe option in each message.

Direct marketing to potential clients. Etapay may process personal data of potential clients for direct marketing purposes in accordance with the GDPR and applicable e-privacy regulations. Such processing will be based on your consent. You can withdraw your consent at any time by using the unsubscribe link provided in our messages or by contacting us at email: dpo@eta-pay.com.

5.4. Event Organization Data Processing

We process personal data in connection with the organization and management of events, including conferences, webinars, workshops, and other related activities.

This processing includes collecting and using information necessary to register participants, communicate event details, manage attendance, and ensure the smooth delivery of the event. We may also process information related to participants' professional background and involvement in the event, such as their role as attendees, speakers, presenters, or partners.

During events, we may capture and use visual and audio materials, such as photographs, video recordings, or live streams, for documentation, communication, and promotional purposes.

Personal data may be shared with third parties involved in the organization and delivery of the event, such as event partners, co-organizers, sponsors, service providers (including event platforms, logistics, and catering providers), media partners, and financial institutions where necessary for payment processing. We may also use communication service providers to support event management and related communications.

5.5. Candidates Data Processing

Etapay processes candidate personal data as part of its recruitment process to ensure fair, transparent, and informed hiring decisions. **When you submit a job application**, we collect the personal information you provide, including your name, email address, phone number, CV or résumé, cover letter, LinkedIn profile (if

provided), responses to application questions, and any other information or documents you choose to include.

At a later stage of the recruitment process, Etapay may collect references about you from individuals representing your current or former employers. These references may include information about your job title, employment period, job responsibilities, performance, reasons for leaving (if applicable), and professional conduct. References from your current employer are obtained only with your explicit consent, as required under Article 6(1)(a) of the GDPR. In the case of references from former employers, the legal basis is Etapay's legitimate interest in making informed and responsible hiring decisions, under Article 6(1)(f) of the GDPR.

We also process the personal data of the referees themselves - typically supervisors or HR representatives - which may include their name, position, professional contact details, and the content of their reference. This processing is necessary to evaluate the suitability of the candidate and is based on Etapay's legitimate interest in ensuring a fair and robust recruitment process. All data collected through reference checks is used solely for recruitment purposes and retained for no more than four months after the recruitment process ends, unless retention is required for legal claims.

5.6. Use of Social Media Platforms

Etapay maintains official company pages on social media platforms such as LinkedIn to promote its brand. When you interact with Etapay via external platforms - by commenting, liking, sharing, or sending direct messages - we may process certain personal data that is visible through your public profile or provided voluntarily.

This may include your name, profile link, comment or message content, reactions (likes, shares), and any information you submit through participation in interactive content such as polls, Q&As, or giveaways. We process this data based on our legitimate interest (Article 6(1)(f) of the GDPR) in managing public engagement, responding to inquiries, and maintaining our online presence. Data is stored for up to 12 months from your last interaction unless the content remains public (e.g., comments), in which case it may remain accessible until you delete it or request removal.

In the context of contests or giveaways organized on our social media channels, we may process additional information, such as your contact details and submission content, for the purpose of managing participation and awarding prizes. This processing is based on contract performance (Article 6(1)(b) GDPR), and data is retained for up to 6 months after the contest concludes unless a longer retention period is required for compliance or dispute resolution.

Please note that interactions on social media platforms are also subject to the privacy policies of the respective platform providers. We recommend reviewing their terms and settings to understand how your personal data is handled independently of Etapay.

5.7. Defense of Legal Claims

We process personal data where necessary to establish, exercise, or defend legal claims, as well as to manage disputes, investigations, and related proceedings.

This may include the use of information related to identification, financial and transactional activities, contractual relationships, communications, and any other data relevant to a particular legal matter. We may also process technical, electronic, and risk-related information where it is necessary to support legal assessments or investigations.

Such processing may involve data relating to clients, employees, partners, service providers, counterparties in disputes, as well as other individuals involved in a matter, such as witnesses or experts.

In the context of legal proceedings or dispute resolution, personal data may be shared with external legal advisors, law firms, courts, and other dispute resolution bodies. Where required, data may also be disclosed to opposing parties and their representatives through formal legal processes, as well as to law enforcement or supervisory authorities. In addition, we may engage auditors, consultants, or subject-matter experts to support the assessment or handling of a case.

5.8. Publicity of the Company's Activities

We process personal data for the purpose of communicating and promoting our activities, services, and events through various channels, including websites, social media, press releases, and other communication materials.

This may include the use of information necessary to identify individuals, facilitate communication, and present their involvement in our activities. We may also process visual and audio materials, such as photographs, video recordings, or interviews, as well as content created or shared in connection with our communications. In certain cases, this may include publicly available information from professional or social media profiles.

Personal data may relate to employees, clients, partners, service providers, event participants, and media representatives who are involved in or associated with our activities.

For these purposes, personal data may be shared with third parties involved in publicity and communication activities, such as media outlets and journalists, event organizers and co-hosts, partners and sponsors, social media platforms, and IT or design service providers supporting content creation and distribution.

5.9. Conclusion and Execution of Contracts with Partners and Service Providers

We process personal data in order to enter into, manage, and perform contracts with our partners, contractors, subcontractors, and service providers.

This includes collecting and using information necessary to identify relevant individuals, verify their authority to act on behalf of an organization, and establish and maintain professional relationships. We process personal data to communicate

effectively throughout the lifecycle of the contractual relationship, including during negotiations, onboarding, day-to-day cooperation, and termination.

Personal data is also used to prepare, review, and execute agreements, as well as to ensure the proper performance of contractual obligations. This involves managing service delivery, coordinating activities, monitoring performance, and maintaining records of interactions and decisions. We may process financial and billing-related information to administer payments, invoicing, and financial reconciliation associated with the contract.

In addition, we process correspondence and documentation exchanged in the course of the relationship, including emails, meeting records, and other communications, in order to ensure continuity, accountability, and proper administration of contractual arrangements.

Where necessary, we also use personal data to assess risks, ensure compliance with internal policies and external requirements, and to resolve any issues, disputes, or claims arising in connection with the contractual relationship.

6. Automated Decision-Making and Profiling

In the course of providing our services, we may use automated processing, including profiling, for the following purposes:

- Fraud prevention and risk management – we analyse behavioural patterns, device information, and transaction data to detect and prevent potentially fraudulent activity. This may result in automated alerts, temporary restrictions on account activity, or flagging of transactions for manual review.
- Anti-money laundering (AML) and sanctions screening – we use automated tools to screen customers against sanctions lists and to assign risk scores based on transaction patterns and other relevant data. This processing may affect the outcome of customer acceptance decisions or trigger enhanced due diligence measures.
- Customer acceptance and termination – based on the results of KYC verification, AML screening, and risk assessment, decisions may be made regarding the acceptance, continuation, or termination of a business relationship.

Where such automated processing produces legal effects or similarly significantly affects you, you have the right to:

- obtain human intervention in the decision-making process;
- express your point of view;
- contest the decision.

We do not make fully automated decisions based solely on automated processing, including profiling, that produce legal effects concerning you without appropriate safeguards, unless such processing is: (i) necessary for the performance of a contract;

(ii) authorised by applicable law; or (iii) based on your explicit consent, in accordance with Article 22 of the GDPR.

7. How do we ensure the security of your personal data?

We process your personal data responsibly and securely, in accordance with our internal data protection policies and by applying appropriate technical and organizational measures to safeguard against unlawful processing, accidental loss, destruction, damage, alteration, disclosure, or any other unauthorized processing actions. Accordingly, we adhere to the following key data processing principles:

- We collect personal data only for specified and legitimate purposes.
- We process personal data fairly and only for its original purpose.
- We retain personal data only for as long as necessary to achieve the defined purposes or as required by law.
- Personal data is processed only by employees who are authorized and have official access.
- We process data using appropriate technical and organizational measures.
- Personal data is disclosed to third parties only when a legal basis exists.
- Where applicable, we notify the State Data Protection Inspectorate of any confirmed or suspected data security breaches.
- We conduct regular data protection training for our employees.
- We carry out periodic internal and/or external IT security audits.
- We continuously review, adapt, and improve our processes to ensure the safest possible handling of personal data collection, access, transmission, use, and other operations.
- We regularly monitor our systems for potential breaches or attacks; however, it is not possible to guarantee the absolute security of information transmitted via the internet or to completely prevent breaches, especially those that may occur due to your own carelessness or sharing of data with others. Therefore, please note that you bear personal responsibility and risk when submitting your personal data via internet connection, the Mobile App, or the Website. You also assume full responsibility for voluntarily disclosing your account information to others and/or for careless or negligent handling of personal data received directly from us.

8. About cookies

Etapay uses cookies and similar technologies on the Platform. You can find out more by visiting our Cookie Policy.

9. Who receives your information?

To deliver its services effectively, Etapay may share personal data with carefully selected third parties, acting either as data processors or, in certain cases, as independent data controllers. These recipients are engaged based on contractual necessity, legal obligation, or legitimate interest and fall into the following categories:

- **Cloud infrastructure providers** – who provide the hosting, storage, and computing infrastructure necessary for running Etapay services.
- **Customer relationship and marketing service providers** – used to manage customer communications, marketing campaigns, and support interactions.
- **Communication and meeting scheduling tools** – including, used to arrange and conduct product demos, support sessions, and business meetings.
- **Payment processing and subscription management providers** – who handle billing, invoicing, and subscription services related to Etapay's commercial offerings.
- **Technical diagnostics and analytics providers** – used for performance monitoring, bug tracking, and improving user experience.
- **Legal, financial, and compliance consultants** – including external legal counsel, auditors, and accounting firms, engaged to ensure compliance with applicable laws and fulfill legal or audit obligations.
- **Public authorities and regulators** – such as prudential supervisors, tax authorities, data protection authorities, or law enforcement, where disclosure is legally required under EU or national legislation.
- **Former or current employers and professional referees** – in the context of recruitment, we may collect reference information about candidates from individuals acting on behalf of their former or current employers (e.g., supervisors or HR representatives).
- **Referees and individuals designated by candidates** – where candidates provide the contact details of former or current employers for reference purposes, we may process the name, job title, professional opinion, and contact information (email, phone number) of the designated referee. This data is not collected directly from the referees themselves but is used to obtain information relevant to the candidate's suitability.

10. International Data Transfers

In the course of providing our services, your personal data may be transferred to, stored, or processed in countries outside the European Union / European Economic Area (EU/EEA), including the United States.

Where such transfers take place, we ensure that appropriate safeguards are in place to protect your personal data in accordance with Chapter V of the GDPR. Depending on the recipient and the country of destination, we rely on one or more of the following mechanisms:

- European Commission adequacy decisions (Article 45 GDPR) – where the destination country has been recognized as providing an adequate level of data protection;
- Standard Contractual Clauses (SCCs) approved by the European Commission (Article 46(2)(c) GDPR), supplemented by additional technical and organizational measures where necessary;
- Other appropriate safeguards as provided under Article 46 or derogations under Article 49 of the GDPR, where applicable.

You have the right to obtain a copy of the relevant safeguards by contacting us at dpo@eta-pay.com.

11. Links to third-party websites

We may provide hyperlinks to third-party websites as a convenience to you. We do not control third-party websites and are not responsible for the contents of any linked-to, third-party websites or any hyperlink in a linked-to website. We are not responsible for the privacy practices or the content of third-party websites.

12. Your rights

In this section, we have summarised the rights that you have under data protection laws. Some of the rights are complex thus we only provide the main aspects of such rights. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

Your other principal rights under data protection law are the following: (i) the right to access data; (ii) the right to rectification (note that you may exercise most of this right by logging to your account here; (iii) the right to erasure of your personal data; (iv) the right to restrict processing of your personal data; (v) the right to object to processing of your personal data; (vi) the right to data portability; (vii) the right to complain to a supervisory authority; and (viii) the right to withdraw consent.

The right to access data. You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.

The right to rectification. You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

In some circumstances you have the **right to the erasure of your personal data**. Those circumstances include when: (i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (ii) you withdraw consent to consent-based processing and there are no other legal basis to process data; (iii) you object to the processing under certain rules of applicable data protection laws; (iv) the processing is for direct marketing purposes; or (v) the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. Such exclusions include when processing is necessary: (i) for exercising the right of freedom of expression and information; (ii) for compliance with our legal obligation; or (iii) for the establishment, exercise or defence of legal claims.

In some circumstances you have the **right to restrict the processing of your personal data**. Those circumstances are when: (i) you contest the accuracy of the personal data; (ii) processing is unlawful but you oppose erasure; (iii) we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and (iv) you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data, however we will only further process such data in any other way: (i) with your consent; (ii) for the establishment, exercise or defence of legal claims; (iii) for the protection of the rights of another person; or (iv) for reasons of important public interest.

You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

The **right to data portability**. To the extent that the legal basis for our processing of your personal data is: (i) consent; or (ii) performance of a contract or steps to be taken at your request prior to entering into a contract, necessary to enter into such, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

If you consider that our processing of your personal information infringes data protection laws, you have a legal **right to lodge a complaint** with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement. Our data processing is supervised by State Data Protection Inspectorate of the Republic of Lithuania, registered office at A. Juozapavičiaus St. 6, LT-09310, https://vdai.lrv.lt/

To the extent that the legal basis for our processing of your personal information is consent, you have **the right to withdraw that consent** at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

You may exercise any of the rights indicated herein by contacting us at dpo@eta-pay.com.

13. Updating your data

Please let us know if the personal information that we hold about you needs to be corrected or updated.

14. Changes to our Privacy Policy

We may amend this Privacy Policy at any time, in case of material changes, we may inform you about such via email.

15. Contact Information

We will use all reasonable efforts to answer any questions or resolve any concerns regarding your privacy promptly.

All comments, queries and requests relating to our use of your personal information are welcomed. If you would like to contact us at dpo@eta-pay.com.

16. Detailed information about your personal data processing

The tables below are structured to provide a clear overview of how Etapay processes personal data. Each entry specifies the purpose of processing, the categories of personal data involved, the applicable legal basis under the GDPR, and the corresponding data retention period.

PURPOSE	PERSONAL DATA	LEGAL BASIS	RETENTION PERIOD
CANDIDATES			
Candidate selection	Identification data, contact details, professional data, assessment data, communication data	Consent (Art. 6(1)(a))	4 months after the end of the selection process. If prior consent from the candidate is obtained, the data shall be retained for 2 years from the date of consent
Enriching candidate profiles with publicly available LinkedIn data	Identification data, contact details (if provided), LinkedIn public profile information (such as current and past job titles, employer names, education history, profile photo, skills, other publicly visible content)	Legitimate interest (Art. 6(1)(f) GDPR)	4 months after the end of the recruitment process

Collection of references from former employers	Identification data (name, surname, employment history, professional qualifications and skills, assessment data	Legitimate interest (Art. 6(1)(f) GDPR)	4 months after the end of the recruitment process
Collection of references from the current employer	Identification data (name, surname), employment history, professional qualifications and skills, assessment data	Consent (Art. 6(1)(a))	4 months after the end of the recruitment process
CLIENTS			
Opening a current account	Identification data, national ID number/date of birth, contact details	Contract performance (Art. 6(1)(b))	10 years after the end of the customer relationship
Current account administration	Account identifiers, account balance, account activity logs, communication data	Contract performance (Art. 6(1)(b))	10 years after termination of the account agreement
Customer identity verification (KYC)	ID document data, biometric-adjacent data (photo), nationality and residence data, beneficial ownership data, authorized representative data, company role and governance data, remote identification metadata, PEP and sanctions status data	Legal obligation (Art. 6(1)(c))	8 years after the end of the business relationship or occasional transaction
AML / sanctions screening	Screening and match result data, risk scoring and profiling data, transaction pattern data, PEP determination data, adverse media, screening data, match analysis and investigation notes	Legal obligation (Art. 6(1)(c))	8 years after the end of the business relationship

Ongoing transaction monitoring (AML)	Transaction metadata, payer/payee details, amounts, monitoring indicators	Legal obligation (Art. 6(1)(c))	8 years from the execution of the transaction
Customer acceptance and termination decisions	Risk assessment and scoring data, AML/KYC findings and investigation data, customer acceptance/termination decision data, decision approval and audit trail data	Legal obligation (Art. 6(1)(c)), Legitimate interest (Art. 6(1)(f))	8 years after the end of the business relationship or the final decision
Direct payment initiation	Payment order details, IBAN payer/payee identifiers, timestamps, device/IP data	Contract performance (Art. 6(1)(b))	10 years
Direct payment receipt (incoming payments)	Sender data, transaction references, IBAN, timestamps	Contract performance (Art. 6(1)(b))	10 years
Payment accounting and reconciliation	Internal transaction IDs, settlement data, reconciliation status	Legal obligation (Art. 6(1)(c))	10 years
Fraud prevention and risk management (monitoring and risk assessment)	Behavioural and pattern data, device and browser data, network and system log data, authentication and access data customer identification data	Legitimate interest (Art. 6(1)(f))	10 years after the last relevant event

Fraud investigations, complaints and refunds	Transaction data, communication and correspondence data, investigation notes and findings, customer statements and complaint data, fraud evidence data	Legal obligation (Art. 6(1)(c)), Legitimate interest (Art. 6(1)(f))	10 years after the closure of the investigation or complaint
Fraud-related regulatory and law enforcement reporting	Identification data, transaction data, investigation findings, statistical data	Legal obligation (Art. 6(1)(c))	10 years after submission of reports
Technical system operation and cybersecurity	System logs, IP addresses, device identifiers, API logs	Legitimate interest (Art. 6(1)(f))	3 years
Business communication	Identification data, contact details, communication content, professional information related to correspondence, any additional information voluntarily provided in communication	Legitimate interest (Art. 6 (1) (f))	12 months from last interaction
Direct Marketing (existing clients)	Identification data, communication data	Legitimate interest (GDPR Art. 6(1)(f))	6 months after the last active use of the service
Direct Marketing (potential clients)	Identification data, communication data	Consent (GDPR Art. 6(1)(a))	3 years from the date of consent or until consent is withdrawn
SOCIAL NETWORKS			
Managing the company's page and responding to	Name, profile link, comment content, reactions, direct messages	Legitimate interest (Art. 6(1)(f))	12 months after last interaction

messages/comments			
Promoting brand visibility and posting marketing content	Name (if user interacts), public comments, likes, shares	Legitimate interest (Art. 6(1)(f))	As long as the content remains public or until request for removal
OTHER			
Defense of legal claims, including handling, investigation and documentation of whistle-blowing reports, internal misconduct allegations and related compliance matters, as required by applicable law	Personal identification data, financial and transactional data, contract and correspondence data, legal and dispute-related data, technical and electronic data, risk and compliance data, information relating to alleged misconduct, suspected violations, investigation findings and evidence, data identifying persons reporting breaches (where not reported anonymously), data identifying persons involved in the reported breach	Legitimate interests (Art. 6(1)(f))	10 years
Event organization	Identification data, contact details, professional data, participation data	Consent (Art. 6(1)(a))	1 year from the date the event takes place
Publicity of the company's activities	Identification data, contact details, visual and audio data, communication data, participation data, author data, social media account data, technical data	Consent (Art. 6(1)(a))	5 years from the date of publication or creation of the publicity material (e.g.,

			press release, photo, video)
Management of communication with clients, partners, members of management bodies, candidates and other third parties (except clients and potential clients)	Identification data, contact details, communication content, professional information related to correspondence, any additional information voluntarily provided in communication	Legitimate interests (Art. 6(1)(f))	3 years
Conclusion and execution of contracts with partners and service providers	Identification data, professional data, contact details, contract data, financial data, communication data, legal data	Contract performance (Art. 6(1)(b))	10 years