AtlantEX OÜ
Privacy Policy
Website Privacy Policy and Client Data Protection Notice

1. General provisions

AtlantEX OÜ considers the protection of personal data not as a formal supplement to the service, but as part of the company's daily work. When a client registers, verifies their identity, submits an order, receives support, or enters into a transaction involving crypto-assets, the Company processes data. Such processing is related to the provision of crypto-asset services, client protection, performance of a contract, and compliance with legal requirements.

For AtlantEX OÜ, data processing is part of the operating model. The Company does not collect data "just in case" or use it for any purpose that is not clearly defined. Each core process must have a practical explanation: what data is needed, who is responsible for processing it, where the data is stored, to whom it is transferred, how long it remains in the system, and which records of processing are retained for later verification.

The Company adheres to the principles of lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, confidentiality, and accountability. These principles mean that data is used only to the extent necessary for a specific service, regulatory obligation, platform security, or the protection of the legitimate interests of the Company and the client.

2. Controller of personal data

AtlantEX OÜ is the controller of personal data in respect of processing for which it independently determines the purposes and means within the framework of its platform, customer service, AML/CFT, KYC and KYT checks, order processing, communications, and compliance with legal obligations.

If a separate service provider acts on behalf of AtlantEX OÜ, it is considered a data processor within the scope of the agreed task. If a bank, e-money institution, state authority, law enforcement agency, Financial Intelligence Unit (FIU), supervisory authority, or another organisation independently determines the purposes and means of processing, that organisation acts as an independent controller within the limits of its competence.

Name	AtlantEX OÜ
Registry code	14648093
Address	Masina 22, Tallinn, Estonia
E-mail for data questions, complaints, and the exercise of rights	complaints@atlant-ex.eu
Website	https://atlant-ex.eu

The address complaints@atlant-ex.eu is the single official channel for requests related to personal data, the exercise of data subject rights, complaints related to personal data protection, retention periods, data

rectification, restriction of processing, and requests for withdrawal of consent where processing is based on consent.

3. Scope

The Policy applies to website users, registered customers, potential customers, representatives of legal entities, beneficial owners, authorised persons, contact persons, applicants, persons contacting the support service, and other persons whose data is included in AtlantEX OÜ's processes in connection with checks, transactions, security, or compliance with legal obligations.

The Policy covers the processing of data when visiting the website, creating an account, verifying identity, verifying the source of funds or source of wealth, using the client portal, making transactions with EUR and crypto-assets, contacting support, reviewing complaints, conducting AML/CFT and KYT monitoring, investigating suspicious transactions, complying with the accompanying information rule, and communicating with banks, payment partners, regulators, and government authorities.

If the client acts on behalf of a company, AtlantEX OÜ processes the data of the representative and other related natural persons. This applies to the director, member of the management board, beneficial owner, person with signatory authority, contact person, actual user of the account, and person who submits documents or orders on behalf of the client.

4. What data is processed?

4.1. Identification data

Such data includes first and last name, personal identification number or date of birth, nationality, country of residence, address, document details, document photograph, video verification data, or other identification results if such a method is used in a particular process. This data is needed to understand who the customer is, who is acting on behalf of the customer, and whether that person has the right to use the service.

4.2. Contact information

The Company processes e-mail address, telephone number, postal address, language of communication, correspondence data, and contact history. This data is needed to communicate with the customer, send notifications, confirm actions, review inquiries, and provide information related to security, changes to terms and conditions, transaction status, or complaints.

4.3. Customer profile and business relationship data

As part of initial client due diligence and subsequent servicing of the client, AtlantEX OÜ processes data on the type of client, the purpose of the business relationship, the expected nature of transactions, the source of funds, the source of wealth, the economic rationale of transactions, the client's links to

jurisdictions, profession or field of activity, the ownership structure of the legal entity, beneficial owners, and persons controlling the client.

4.4. Transaction and payment data

The Company processes data about the Client's orders, amounts, currencies, crypto-assets, networks, wallet addresses, transaction identifier (TXID), transaction time, processing statuses, fees, applied limits, internal transaction IDs, bank payment details, IBAN, payment descriptions, refunds, rejections, blocks, cancellations, and other information necessary for the execution of the transaction and the subsequent verification of its progress.

4.5. AML/CFT, sanctions and risk data

Within the framework of anti-money laundering, counter-terrorist financing, and sanctions compliance requirements, AtlantEX OÜ processes the results of KYC, KYB, sanctions checks, politically exposed person checks, adverse media checks, blockchain analysis, transaction monitoring, risk assessment, alerts, internal notes, escalation records, enhanced due diligence decisions, requests for additional documents, and the results of checks of explanations provided.

4.6. Technical and security data

When using the Website and the Platform, the IP address, login date and time, device and browser data, session identifiers, technical logs, authorisation events, login attempts, changes to settings, account activities, system errors, and data related to the prevention of unauthorised access, fraud, abuse, and technical incidents are processed.

4.7. Communication, complaints, and support data

When the Client writes to the Company, calls, submits a complaint, or sends documents, AtlantEX OÜ processes the content of the inquiry, attachments, correspondence history, data of the person making the inquiry, date of receipt, measures taken, the Company's response, and internal records necessary to verify the circumstances. Such data is important not only for responding to the customer, but also for later confirming how the Company handled the matter.

4.8. Data from public and external sources

In certain cases, the Company uses data from public registers, sanctions lists, commercial databases, commercial registers, judicial or administrative sources, blockchain analytics service providers, KYC and KYT service providers, and other legitimate sources. Such data is used to verify identity, authority, ownership structure, sanctions risks, source of funds, links to higher risk, and the reliability of the information provided.

4.9. Special categories of personal data

AtlantEX OÜ does not seek to collect special categories of personal data. However, such data may be inadvertently included in documents submitted by the client, such as a bank statement, an explanation of the source of funds, a court document, or other supporting material. In such cases, the Company limits the use of this data to the purpose for which the document was submitted or for which it must be reviewed under law.

5. Purposes of processing

Personal data is not used for the purpose of collecting information for its own sake, but for the performance of specific tasks. The main purposes of processing are related to the provision of services, platform security, performance of the contract, compliance with AML/CFT, sanctions, the accompanying information rule and other legal obligations, and the protection of the rights of AtlantEX OÜ, customers, and third parties.

The data is needed to open an account, verify the client, accept orders, execute transactions, keep internal records, confirm transaction status, process refunds, record fees, and provide the client with information about their transactions. It is also used to answer questions, verify the applicant's identity, restore access, review complaints, send legally relevant notices, and document the processing of requests.

The Company retains and uses data for accounting, internal control, external audit, reporting, responding to regulatory inquiries, evidencing the performance of a contract, defending against unfounded claims, and filing claims where necessary to protect the legitimate interests of AtlantEX OÜ.

In the case of regulated crypto-asset services, processing also ensures the traceability of transactions, the ability to subsequently reconstruct the client's order, confirmation of transaction status, compliance with the accompanying information rule, and the preparation of evidence for internal control, the auditor, a bank, a partner e-money institution, or a competent authority.

6. Legal bases

The legal basis for processing depends on the specific situation. AtlantEX OÜ does not use one universal basis for all data. For each category of processing, the basis that corresponds to the actual purpose applies.

Legal basis	When it applies
Performance of the contract	When the data is required for registration, client verification, granting access to the platform, processing an order, executing a transaction, maintaining an account, or responding to a request related to the service.
Legal obligation	Where processing is required under AML/CFT, sanctions, tax and accounting requirements, the

Legal basis	When it applies
	accompanying information rule, reporting, regulatory recordkeeping, law enforcement requests, or another mandatory legal requirement.
Legitimate interest	When the data is needed for security, fraud prevention, log keeping, protection of rights, internal control, service improvement, incident investigation, or preparation of a legal position. Before using this basis, the Company assesses the balance of interests.
Consent	When consent is required by law, such as for optional cookies, marketing messages, or other voluntary actions. Consent may be withdrawn, but withdrawal does not affect the lawfulness of processing carried out before withdrawal.

If the Client fails to provide the information required by the Agreement or by law, AtlantEX OÜ will not be able to open an account, continue providing services, execute the transaction, or will be required to limit certain actions until the required information is obtained.

Consent is not used as the legal basis for processing that is mandatory under law. In particular, AML, KYC and KYT checks, sanctions check, processing of accompanying information in accordance with the applicable rule, mandatory recordkeeping, and regulatory reporting are conducted on the basis of a legal obligation or another applicable legal basis, not on the basis of the client's voluntary consent.

7. AML/CFT and regulatory requirements

AtlantEX OÜ operates in the field of crypto-asset services, where requirements for identification, monitoring, and data retention are higher than in a regular online service. The Company must understand who the customer is, who stands behind a legal entity, where the funds come from, what the expected nature of the transactions is, and whether a transaction is related to money laundering, terrorist financing, sanctions, fraud, or another unlawful risk.

Within the framework of AML/CFT and sanctions processes, the Company has the right to request additional information and documents. These may include data on the source of funds, bank statements, contracts, proof of income, data on the sale of assets, corporate documents, company structure, an explanation of the economic purpose of the transaction, confirmation of the wallet address, information about the counterparty, or other material necessary for reasonable verification.

If the client does not respond to the request, provides incomplete or contradictory information, refuses to explain the source of funds, or the transaction appears disproportionate to the client's declared profile, AtlantEX OÜ has the right to postpone, limit, or refuse the transaction within the limits of law and the Terms of Service. In certain cases, the Company does not have the right to disclose all reasons

for the restriction to the customer if such disclosure is prohibited by AML/CFT rules or would create a risk of tipping-off.

AML/CFT, KYC and KYT data is not used to build a commercial profile of the client, but to comply with law, manage risks, and protect the platform. Internal risk conclusions are documented in a way that allows a subsequent audit to understand which facts were considered, which issue required escalation, and why a particular decision was made.

8. Automated processing and risk assessment

AtlantEX OÜ uses technical tools to verify data, identify matches on sanctions lists, analyse blockchain transactions, assess transaction risk, detect unusual transactions, and protect accounts. Such tools help detect risk more quickly, but must not replace reasonable assessment where a human decision is required.

Risk assessment means that individual characteristics of a transaction or client may increase or decrease the level of risk. For example, jurisdictions, client type, ownership structure, transaction history, source of funds, links to higher-risk addresses, results of sanctions check, and other characteristics are relevant. A technical signal does not always constitute a breach. It means that the Company must review the situation more thoroughly.

If an automated system generates a signal, further processing depends on the nature of the risk. The transaction may be referred for manual review, a request for documents may be sent to the customer, or the transaction may be suspended, rejected, or escalated to the responsible employee. AtlantEX OÜ does not base its policy on fully automated decisions that, without human involvement, produce significant legal effects for the client where applicable law requires human involvement.

Automatic alerts are used as part of risk-based control and are not considered final confirmation of a breach. The final decision is based on an assessment of the available facts, the context of the transaction, the applicable rules, internal procedures and, where applicable, MLRO or Compliance review.

9. Data sources

Most of the data comes from the customer: through the registration form, client portal, documents, correspondence, payment orders, support inquiries, and explanations that the customer provides during checks.

Another part of the data is generated by the platform itself. This includes login logs, technical events, activity history, transaction statuses, internal IDs, monitoring records, reconciliation results, support records, and other traces showing what happened to the account or transaction.

Data also comes from external sources: banks and partner e-money institutions, KYC and KYT service providers, blockchain analysis service providers, sanctions and PEP databases, business verification

services, public registers, state authorities, law enforcement agencies, courts, notaries, auditors, consultants, and other persons where there is a legitimate purpose for obtaining the data.

10. Transfer of data

AtlantEX OÜ transfers personal data only where this is necessary for the service, law, security, audit, control, protection of rights, or necessary communication with a service provider. Transfer does not mean selling data. The Company does not sell customers' personal data to advertising agencies.

Data may be transferred to KYC and KYT service providers, blockchain analysis providers, IT and hosting service providers, payment partners, banks and e-money institutions, auditors, accountants, legal advisors, customer support providers, security service providers, state authorities, the Financial Intelligence Unit (FIU), the Financial Supervision Authority, tax authorities, courts, bailiffs, and other recipients if the transfer is based on law or is necessary for the protection of rights.

If a service provider acts as a data processor, AtlantEX OÜ must have a contractual basis for processing with that data processor, specifying the subject matter and duration of processing, categories of data, security measures, conditions for sub-processing, confidentiality requirements, the procedure for returning or deleting data, and audit and control rights. In the case of essential service providers, the Company evaluates not only price and functionality, but also the service provider's ability to ensure security, resilience, access to evidence, and support in the event of regulatory requests.

In certain cases, AtlantEX OÜ is obliged to transfer data without the client's consent. This applies to AML/CFT notices, sanctions obligations, inquiries from competent authorities, court orders, tax requirements, and other mandatory requirements. If the law prohibits notifying the customer of a transfer or request, the Company complies with that prohibition.

The Company engages a limited number of external service providers who process personal data strictly on behalf of AtlantEX OÜ and within the limits of the data processing agreements entered into with them.

Such recipients include:

- banks and payment institutions through which customer settlements are made
- KYC service providers (identity verification) and KYT service providers (transaction analysis)
- IT providers and infrastructure service providers (hosting, servers, security)
- software providers ensuring the operation of the platform
- legal and compliance advisors in the context of compliance with regulatory obligations
- state authorities, including the Financial Intelligence Unit (FIU), the Financial Supervision Authority, and other authorities where there is a legal basis

AtlantEX OÜ does not transfer data to third parties for their own marketing purposes.
Each service provider undergoes a preliminary check. Its ability to ensure data protection, GDPR compliance, and the existence of appropriate organisational and technical security measures are assessed.

Responsibility for data processing remains with AtlantEX OÜ. The transfer of functions does not mean the transfer of responsibility.

The selection and monitoring of service providers take into account the nature of the service, access to personal data, access to logs and evidence, the existence of subcontractors, the location of processing, information security measures, incident reporting obligations, audit rights or the possibility of obtaining assurances, and support in the event of supervisory requests.

11. Accompanying information rule

Transfers of certain crypto-assets are subject to the requirements of the accompanying information rule. This means that certain information about the sender and the recipient must be transmitted together with, or in connection with, the transfer. These requirements aim to ensure the traceability of transfers, reduce the risk of money laundering and terrorist financing, and give service providers the ability to verify transactions before or after they are executed.

Depending on the type of transaction, jurisdiction, counterparty, and applicable rule, AtlantEX OÜ may process and transfer the name, account identifier, wallet address, customer information, recipient information, address, date and place of birth, personal identification number, or other information required by applicable rules. If mandatory information is missing, the transaction may be delayed, rejected, or referred for further verification.

The Client must understand that the accompanying information rule is not a voluntary function of the Service. If the law requires the transfer or receipt of certain data for the transfer of crypto-assets, AtlantEX OÜ must comply with that requirement. Refusal to submit the necessary data affects the possibility of executing the transaction.

Data may be transferred before, during, or after the execution of a transaction as required by applicable law, a technical protocol, the relevant service provider's procedure, or the requirements of a regulated counterparty. AtlantEX OÜ documents such transfers to the extent necessary for subsequent verification and proof of fulfilment of the obligation.

12. International transfers

AtlantEX OÜ is located in Estonia and operates within the legal framework of the European Union. However, certain service providers, technical infrastructure, verification services, or counterparties may be located outside the EEA or use subprocessors located outside the EEA.

The transfer of personal data outside the European Economic Area is permitted only where a legal mechanism is in place. This may include an adequacy decision by the European Commission, standard contractual clauses, additional technical and organisational measures, a transfer risk assessment, or another safeguard recognised by applicable law.

Before making an international transfer, the Company must take into account the nature of the data, the purpose of the transfer, the recipient country, the role of the service provider, the existence of subprocessors, safeguards, the availability of evidence, and the ability to comply with the rights of the data subject. For AML/CFT, the accompanying information rule, and law enforcement cases, the transfer is also assessed against mandatory legal requirements.

The transfer of personal data outside the European Economic Area is permitted only if there is a legal basis and safeguards provided for in the GDPR.

Depending on the situation, the following may apply:

- the European Commission's adequacy decision
- standard contractual clauses (SCCs)
- additional safeguards, if necessary

No data transfer will be conducted without proper safeguards.

13. Retention periods

AtlantEX OÜ retains data for no longer than is necessary for the purpose of processing, a contract, law, protection of rights, or proof of fulfilment of an obligation. The retention period depends on the data category.

Data category	Indicative period and retention logic
AML/CFT, KYC and KYT data	Generally, at least 5 years after the end of the business relationship or after a one-off transaction, unless applicable AML law requires another period or an extension.
Transaction and accounting data	Retained for the periods necessary for accounting, tax obligations, audit, regulatory reporting, and protection of rights, for a minimum of 7 years.
Account and contract information	Retained for the duration of the customer relationship and after its termination within the limits of the statute of limitations, regulatory retention, or internal control.
Correspondence, complaints, and support	Retained for as long as necessary for responding, quality control, evidencing the review of the request or complaint, compliance with complaint handling requirements, and protection of rights.
Technical logs and security data	Retained for the period necessary for security, incident investigation, audit of activities, abuse detection, and event reconstruction.
Cookies and analytical data	Stored according to the cookie banner settings, technical necessity, and the periods indicated for

Data category	Indicative period and retention logic
	the relevant tool.

After the expiry of the retention period, data will be deleted, anonymised, or archived with limited access if complete deletion is temporarily not possible due to backups, technical limitations, disputes, an inquiry from an authority, or mandatory retention. Access to archived data must be restricted and may be used only for legitimate purposes.

14. Rights of the data subject

The data subject has the rights provided for in applicable personal data protection legislation. These rights are not absolute. In certain cases, AtlantEX OÜ is obliged to retain data, refuse deletion, restrict disclosure of information, or continue processing due to AML, sanctions, accounting, regulatory, judicial, or other mandatory requirements.

The data subject has the right to request access to data, rectification of inaccurate data, erasure of data where grounds exist, restriction of processing, data portability, objection to processing based on legitimate interest, and withdrawal of consent where processing is based on consent.

Requests related to personal data must be sent to complaints@atlant-ex.eu. The inquiry must indicate which right is being exercised and which data the request concerns. If the identity of the applicant is not clear, AtlantEX OÜ has the right to request additional confirmation to ensure that data is not disclosed to a third party.

AtlantEX OÜ will respond to inquiries within the time limits prescribed by applicable law. If the request is complex, concerns a large amount of data, or requires additional verification, the deadline may be extended as prescribed. The data subject also has the right to contact the Data Protection Inspectorate if they consider that their rights have been violated.

Before contacting the supervisory authority, the data subject has the right to contact AtlantEX OÜ directly at complaints@atlant-ex.eu so that the Company can verify the circumstances, correct the error, or give a reasoned response to the substance of the request.

15. Personal data breaches

A personal data breach is a situation where data is accidentally or unlawfully destroyed, lost, altered, disclosed, or made available to persons who should not have seen it. It may be a technical incident, an access error, sending a letter to the wrong recipient, account compromise, loss of media, system vulnerability, or another event.

AtlantEX OÜ evaluates each incident based on facts: what data is affected, how many people are affected by the event, whether a person can be identified, and whether there is a risk of financial loss, fraud, identity theft, breach of confidentiality, or other damage. The decision on further action must be based on evidence, logs, technical data, and risk assessment, not assumptions.

If a breach must be notified to the supervisory authority, the notification is made without undue delay and, where applicable, within 72 hours of the time when the Company became aware of the breach. If the breach creates a high risk to the rights and freedoms of a natural person, AtlantEX OÜ notifies the affected persons in accordance with the procedure prescribed by applicable law.

The Company documents incidents, actions taken, conclusions, deadlines, responsible persons, and remediation measures. This is necessary not only to comply with law, but also to prevent a similar incident from happening again.

16. Cookies and similar technologies

The website of AtlantEX OÜ uses cookies and similar technical tools for the operation of the website, session protection, storage of basic settings, and the correct functioning of the customer interface. Without strictly necessary cookies, the website or some Platform functions may not function properly.

Cookie categories:

- strictly necessary (ensure the functioning of the website and login to the account)
- functional (remember the data subject's settings)
- analytical (help to understand how websites are used)

Cookies are not used for aggressive profiling or the sale of data. The data subject can manage cookies through browser settings.

If analytical, advertising, or other optional cookies are used on the website, they are used only on the basis of consent where such consent is required by law. The data subject can change cookie settings through the tool on the website or through browser settings. Disabling some cookies may affect ease of use but must not deprive the data subject of access to mandatory information.

Cookies may not be used for hidden processing that is not related to the declared purpose. If AtlantEX OÜ changes the set of cookies, adds a new analytics tool, or changes the purpose of processing, the relevant information must be updated in the cookie notice or in this Policy.

Strictly necessary cookies are used for the technical operation of the website, security, sessions, and user interface. Optional cookies, including analytical cookies, are used only after obtaining the user's consent where such consent is required by the applicable ePrivacy and GDPR legal framework. The detailed settings and list of cookies used must be published separately in the cookie policy or in the cookie banner, if such a tool is used on the website.

17. Security

AtlantEX OÜ implements technical and organisational protection measures that are appropriate to the nature of the data and the risks of its activities. The Company works with financial and crypto-asset

transactions, so data security is related not only to the protection of personal data, but also to the protection of client assets, fraud prevention, platform resilience, and the quality of evidence.

Safeguards include access segregation, role-based access, activity logs, administrative rights controls, account protection, monitoring, backups, incident management, service provider control, confidentiality obligations for employees and contractors, restriction of access to data on a need-to-know basis, and internal procedures for processing inquiries, complaints, AML/CFT alerts, and technical events.

The Company must not claim to use a particular protection technology where it has not actually been implemented. Therefore, this Policy describes a general approach to security without giving the misleading impression that specific technical solutions exist. AtlantEX OÜ's internal policies determine specific measures, process owners, control evidence, escalation, and control procedures.

Even where protective measures are in place, absolute security is not guaranteed. The Company's task is to reduce risk, quickly identify events, document actions, limit damage, and eliminate the causes of an incident in a timely manner.

Specific safeguards are defined by internal security policies, ICT governance, access control, incident management, business continuity assurance, outsourcing oversight procedures, and operational resilience requirements. This Policy does not confirm the existence of separate technical solutions that are not verified by the actual infrastructure of AtlantEX OÜ.

18. Obligation to provide data

In several cases, the submission of data is a condition for the provision of the service. If AtlantEX OÜ needs to identify the client, verify the beneficial owner, understand the source of funds, comply with the accompanying information rule, check sanctions, or assess operational risk, the client is obliged to provide the necessary data and documents.

If data is not provided, is submitted with delay, contains inconsistencies, or does not confirm the declared facts, the Company may refuse registration, decline to open an account, restrict separate functions, suspend the transaction, terminate the business relationship, or take other measures prescribed by law and contract.

AtlantEX OÜ tries to request only data that is relevant to the check. At the same time, in a regulated field, more information is sometimes required than the customer expects in a normal commercial service. This is because the Company has independent responsibility to supervisory and AML authorities.

19. Policy changes

AtlantEX OÜ may update this Policy in the event of changes in legislation, service structure, service providers, data processing procedures, customer interface, regulatory requirements, cookie handling, accompanying information rule processes, or internal security procedures.

The new version will be published on the website together with the date of the update. If the change significantly affects the rights of the data subject or the nature of data processing, AtlantEX OÜ will inform the data subject in an appropriate way: via the website, client portal, e-mail, or another available means of communication.

The data subject should periodically check the current version of the Policy. However, amendments may not be used to retroactively extend processing without a legal basis. If consent is required for new processing, it will be requested separately.

20. Contacts

Questions related to the processing of personal data, exercise of user rights, specification of retention periods, correction of data, restriction of processing, withdrawal of consent, or filing a complaint related to personal data protection should be sent to complaints@atlant-ex.eu

In the inquiry, it is recommended to indicate the name, contact e-mail address, content of the inquiry, and the data to which the question relates. If the request is related to an account or transaction, the internal contact number, transaction date, or another identifier should be indicated to help find the information quickly. Private keys, passphrases, passwords, or other information that is not required for reviewing a personal data protection request must not be sent by e-mail.

E-mail	complaints@atlant-ex.eu
Website	https://atlant-ex.eu
Company	AtlantEX OÜ
Registered address	Masina 22, Tallinn, Estonia

21. Legal framework

This Policy has been prepared taking into account the legal requirements applicable to the processing of personal data and the activities of crypto-asset service providers in Estonia and the European Union. The specific set of requirements depends on the service, the status of the client, the nature of the transaction, and the applicable period.

Act/Source	**Role in this Policy**
Regulation (EU) 2016/679 / General Data Protection Regulation (GDPR)	General rules for the processing of personal data, rights of the data subject, obligations of the controller, security of processing, and notification of breaches.
Personal Data Protection Act	National rules and institutional framework for the protection of personal data in Estonia.
Money Laundering and Terrorist Financing Prevention Act (MLTFPA)	AML/CFT obligations, due diligence, data retention, risk-based approach, and communication with competent authorities.

Act/Source	Role in this Policy
Regulation (EU) 2023/1113	Information accompanying transfers of funds and certain crypto-assets, including the accompanying information rule.
Regulation (EU) 2023/1114 / Markets in Crypto-assets Regulation (MiCA)	The regulatory framework for crypto-asset service providers, including organisational, client, and operational requirements where they relate to data processing.
Regulation (EU) 2022/2554 / Digital Operational Resilience Regulation (DORA)	ICT risk, incident management, and digital operational resilience where these processes concern the security of personal data.

In the event of a conflict between this Policy and a mandatory legal provision, the mandatory legal provision shall prevail. The Policy must be updated in the event of changes in law, supervisory practice, or the actual data processing model of AtlantEX OÜ.

This Policy does not replace the internal procedures of AtlantEX OÜ. It explains the basic rules of data processing to the data subject, while detailed control measures, records, logs, escalation routes, evidentiary requirements, and responsible functions are defined in the Company's internal documents.

22. Final provision

AtlantEX OÜ must be able to explain data processing not only to the client, but also to the auditor, the bank, the supervisory authority, and the court. Therefore, this Policy follows a simple logic: data is collected for a specific purpose, used within the limits of that purpose, transferred only where there is a basis, protected by reasonable measures, and stored only for as long as necessary for the purposes of law, contract, or protection of rights.

This wording is intended for publication on the website and for use as an external document of AtlantEX OÜ. Prior to publication, the Company must verify that the actual service providers, cookie tools, customer journey, data retention schedule, communication channels, and internal procedures comply with this Policy. If actual practice differs, the practice or the policy text must first be corrected, and the document must then be published.