

Privacy Policy

Document	Privacy Policy
Version	2.0
Effective from	9 October 2026
Previous version	1.0 of 6 May 2026
Controller	ML Consulting MB, legal entity code 306991112, Vilnius, Republic of Lithuania
Privacy contact	support@mlconsulting.lt
Scope	The website mlconsulting.lt, enquiries, professional services, and the iOS applications published by ML Consulting MB

Contents

1. About this Policy
 2. Who we are
 3. Scope
 4. Our role: controller or processor
 5. Personal data we process
 6. Where we obtain personal data
 7. Purposes and legal bases
 8. Confidentiality in professional engagements
 9. Artificial intelligence and automated processing
 10. Recipients of personal data
 11. International data transfers
 12. How long we keep personal data
 13. Security
 14. Personal-data breaches
 15. Your rights
 16. Regional notices
 17. Children
 18. Cookies and similar technologies
 19. Communications and direct marketing
 20. Application-specific notices
 21. Changes to this Policy
- Version history

1. About this Policy

This Privacy Policy explains how ML Consulting MB processes personal data when you visit mlconsulting.lt, contact us, engage us for professional services, or use one of the iOS applications we publish. It is written to meet Articles 13 and 14 of Regulation (EU) 2016/679, the General Data Protection Regulation (the "GDPR"), and the Law on Legal Protection of Personal Data of the Republic of Lithuania.

Version 2.0 extends the Policy to our professional services — regulatory compliance advisory, compliance automation, and software and application development — and to the personal data we handle for clients. The provisions on our iOS applications continue to apply in substance as in version 1.0.

Where an application or an engagement involves processing that goes beyond this Policy, an application-specific privacy notice (section 20) or a data processing agreement with the client (section 4.2) applies in addition.

2. Who we are

ML Consulting MB ("ML Consulting", "we", "us", "our") is the controller of the processing described in this Policy, except where section 4 says that we act as a processor.

- **Legal form.** *Mažoji bendrija* (small partnership) governed by the law of the Republic of Lithuania.
- **Legal entity code.** 306991112 (Centre of Registers of the Republic of Lithuania).
- **Seat.** Vilnius, Republic of Lithuania.
- **Website.** <https://mlconsulting.lt>
- **Privacy contact.** support@mlconsulting.lt, for all data-protection enquiries and requests.
- **General enquiries.** mantvydas@mlconsulting.lt

We have not designated a Data Protection Officer because our processing does not meet the criteria in Article 37(1) GDPR. If that changes, we will appoint one and publish the contact details in this Policy.

Our lead supervisory authority is the State Data Protection Inspectorate of the Republic of Lithuania (*Valstybinė duomenų apsaugos inspekcija*, "VDAI"), L. Sapiegos g. 17, LT-10312 Vilnius, telephone +370 5 271 2804, email ada@ada.lt, website vdai.lrv.lt.

3. Scope

This Policy applies to:

- the website mlconsulting.lt, including its contact and support forms;
- enquiries, consultations and correspondence with prospective clients;
- the professional services we provide to clients: regulatory compliance advisory, compliance automation, and software and application development (the "Professional Services");
- every iOS application we publish on the Apple App Store, unless the application carries its own privacy notice that expressly displaces this Policy; and
- direct-marketing communications, where we send them.

Where Apple, Google, a payment provider or a client's own service provider processes personal data on its own account, it acts as a separate controller and its own privacy policy applies.

4. Our role: controller or processor

4.1 When we are the controller

We decide the purposes and means of processing, and this Policy applies in full, for:

- the operation and security of the website;
- enquiries, consultations and correspondence;
- the management of our relationships with prospective clients, clients and suppliers, including engagement letters, conflict-of-interest checks, invoicing and our engagement records;
- accounts, telemetry, support and billing for our applications; and
- direct marketing.

4.2 When we process data for clients

In many engagements a client gives us access to documents, systems or data sets that contain personal data — for example customer due-diligence files, beneficial-ownership records, transaction and alert data, complaint records, staff lists or contracts — so that we can review them, test controls, or build and operate an automation solution.

In those cases the client is the controller and we are its processor. We process the data only on the client's documented instructions, under a data processing agreement that meets Article 28 GDPR. If your personal data is contained in a client's materials, please contact that organisation first; we will pass on any request we receive without undue delay.

4.3 Business workspaces in our applications

Where a business customer (the "workspace owner") uses one of our applications to manage information about its employees, contractors, customers, counterparties or other individuals, the workspace owner is the controller of that data and we act as its processor under a written Data Processing Addendum that meets Article 28 GDPR. The workspace owner is responsible for informing the individuals concerned and for having a lawful basis for the processing.

5. Personal data we process

5.1 Website visitors

When you visit the website, our hosting provider's servers process the technical data needed to deliver and protect it: IP address, date and time of the request, the page requested, browser and device type, and the referring page. We do not use analytics, advertising or profiling tools. Fonts and other resources are served from our own server, so your browser does not connect to third-party content providers when you open the website.

5.2 Enquiries and contact forms

When you write to us or use a form on the website, we process your name, email address, organisation, the subject you select, your message and any information it contains, the page

from which you wrote and the date. To prevent abuse, we store a one-way cryptographic hash of your IP address with the enquiry and use it to limit repeated submissions; we do not store the IP address itself.

5.3 Prospective and existing clients

For our client relationships we process the business contact details of client representatives (name, job title, organisation, business email address and telephone number), correspondence and meeting notes, proposals, engagement letters and non-disclosure agreements, the information needed to check conflicts of interest and to verify the identity and ownership of a prospective client, and billing details (invoicing entity, address, company and VAT codes, invoice and payment records).

5.4 Personal data in client materials

Where we act as processor under section 4.2, client materials may contain identification and contact data of the client's customers, beneficial owners and representatives; account, transaction and alert data; complaint records; data about the client's staff and service providers; and contract data. In anti-money-laundering work they may also contain information about suspected or established criminal offences, which is subject to Article 10 GDPR.

We ask clients to share only what the engagement needs, to use pseudonymised or test data wherever the purpose allows, and to make available special categories of personal data or data subject to Article 10 GDPR only where they have a valid legal basis and have instructed us in writing.

5.5 Users of our applications

Depending on the application and the features you use, we process:

- **Account and authentication data.** Name, email address, account identifier, authentication method (Sign in with Apple, Sign in with Google, or email and password), Apple-issued relay address where you used "Hide My Email", organisation or workspace membership, role and permissions. Where password authentication is used, we store salted password hashes only, never plaintext passwords.
- **Device, technical and telemetry data.** IP address (typically truncated for analytics), device model and operating-system version, application version, language and time zone, pseudonymised interaction events, crash reports, performance traces and security-relevant events such as failed log-ins.
- **Communications and support data.** The content and metadata of emails, support requests, in-application help messages and other correspondence with us, including attachments you choose to send.
- **Billing and payment data (direct customers).** Invoicing entity name, registered address, VAT identifier, signatory contact, order-form record, payment status, bank-transfer reference and, where card payment is used, the last four digits of the card. We do not store full payment-card numbers.
- **Apple App Store transaction metadata.** The Apple-issued purchase identifier, subscription tier, entitlement state and renewal events. The purchase contract is concluded

between you and Apple; we do not receive your Apple Account password or payment details.

- **User content and operational records.** Information you enter, upload, import, generate or export through an application, including notes, attachments, photographs, documents, reports and workspace data.
- **Camera, photo and location data.** Where an application offers camera-based features, frames are processed in memory on your device and stills are saved only when you capture them. Where an application offers a location feature, location is captured only at the moment of an action you initiate; we do not track location continuously.
- **Notification preferences and tokens.** Notification settings and, where push notifications are used, the device push token processed by Apple Push Notification service.
- **Application-generated data.** Outputs of computational features, such as calculations, classifications, summaries and alerts, with model-version markers and timestamps.
- **AI-feature inputs and outputs.** Where an application offers an opt-in AI-assisted feature, the prompts, selected records and generated results associated with it (see section 9).

Each application's privacy notice describes its processing in more detail.

5.6 Marketing data

Newsletter subscription status, communication preferences, opt-in and opt-out records and, where applicable, campaign source and email engagement.

5.7 Special categories of personal data

We do not seek to collect special categories of personal data within the meaning of Article 9 GDPR, and our applications are not designed for them. You must not upload such data to our applications unless it is strictly necessary for your lawful use and you have a valid basis under Article 9(2) GDPR; in a business workspace, the workspace owner is responsible for that basis. Section 5.4 applies to client materials.

In our iOS applications we do not collect the contents of your contacts, calendar or photo library beyond the images you actively capture, we do not use advertising identifiers (IDFA) or share data with advertising networks, and we do not use analytics, attribution or crash-reporting software development kits that are not disclosed in this Policy and in the application's App Privacy details.

6. Where we obtain personal data

- **From you**, when you browse the website, write to us, meet us, engage us, or create an account in and use one of our applications.
- **From the organisation you work for or represent**, when it engages us, introduces you as a contact or makes client materials available to us.
- **From public sources**, such as company registers, public registers of supervisory authorities, official publications and company websites, to verify the identity and ownership of a prospective client and to check for conflicts of interest before we accept an engagement.
- **Automatically**, when you use the website or our applications.

- **From third parties connected with our applications**, when Apple supplies the result of Sign in with Apple or App Store transaction metadata, when Google supplies the result of Sign in with Google, when a workspace administrator invites you, or when a payment provider confirms a payment.

7. Purposes and legal bases

We rely on the following legal bases under Article 6(1) GDPR.

Purpose	Personal data	Legal basis
Operate the website and protect it against misuse	Technical data; IP-address hash	Legitimate interests in providing a secure website (Art. 6(1)(f))
Answer enquiries and arrange consultations	Enquiry data	Steps taken at your request before entering into a contract (Art. 6(1)(b)); legitimate interests in responding to business enquiries (Art. 6(1)(f))
Assess a prospective engagement, including identity, ownership and conflict-of-interest checks	Client contact data; public-source data	Legitimate interests in accepting only engagements we can perform independently and lawfully (Art. 6(1)(f))
Perform Professional Services and manage the client relationship	Client contact data; correspondence; engagement records	Performance of a contract where you are our client (Art. 6(1)(b)); otherwise legitimate interests in performing our contract with your organisation (Art. 6(1)(f))
Process personal data in client materials on the client's instructions	Personal data in client materials	Processing on behalf of the client under Article 28 GDPR; the client, as controller, determines the legal basis
Invoicing, accounting and tax	Billing data	Compliance with a legal obligation under Lithuanian accounting and tax law (Art. 6(1)(c)); performance of a contract (Art. 6(1)(b))
Keep engagement records and establish, exercise or defend legal claims	Engagement records; correspondence	Legitimate interests in evidencing our work and protecting our legal position (Art. 6(1)(f))
Provide and operate our applications, including accounts, features, subscriptions and support	Application data in section 5.5	Performance of a contract (Art. 6(1)(b)); consent for device permissions, notifications and iCloud sync, given through iOS (Art. 6(1)(a))
Secure our applications and prevent fraud and abuse	Authentication, technical and security-event data	Legitimate interests in protecting our services (Art. 6(1)(f))

Purpose	Personal data	Legal basis
Improve our applications through privacy-respecting analytics	Pseudonymised telemetry; aggregated statistics	Legitimate interests (Art. 6(1)(f)); consent where required (Art. 6(1)(a))
Send service messages, such as security, billing and change notices	Contact data	Performance of a contract (Art. 6(1)(b))
Send direct-marketing communications	Contact and marketing data	Consent, or the existing-customer exception under Article 13(2) of Directive 2002/58/EC as implemented in Lithuanian law (Art. 6(1)(a); Art. 6(1)(f))
Respond to data-subject requests	Data relevant to the request	Compliance with a legal obligation (Art. 6(1)(c))
Comply with legal obligations and lawful requests from authorities	Data required by law	Compliance with a legal obligation (Art. 6(1)(c))

Where we rely on legitimate interests, we have assessed that our interests are not overridden by your interests, rights and freedoms. Where we rely on consent, you may withdraw it at any time, without affecting the lawfulness of processing before withdrawal, through iOS Settings, the relevant in-application setting, the unsubscribe link in a marketing email, or by writing to support@mlconsulting.lt.

Providing personal data is voluntary, except where it is needed to enter into or perform a contract (for example, invoicing details) or required by law; without it we may be unable to provide the service concerned.

8. Confidentiality in professional engagements

Client information is treated as confidential. Access is limited to the people working on the engagement, it is not used for any other client or purpose, and it is returned or deleted at the end of the engagement as agreed with the client. We sign non-disclosure agreements on request. We disclose client information to a regulator or other third party only with the client's agreement or where the law requires it.

9. Artificial intelligence and automated processing

9.1 In our professional work

We may use AI tools to support research, drafting, document review and the solutions we build. We use them only under business or API terms that do not permit the provider to use inputs and outputs to train its models, and we prefer providers that process data within the European Economic Area. We do not enter client personal data into an AI tool unless the client has agreed

to that tool in the engagement letter or data processing agreement. Every output is reviewed by a person before it is relied on or delivered.

9.2 In automation solutions built for clients

The automation solutions we build are designed so that the client's staff approve decisions. The client, as controller, decides the purposes, configuration and providers of each solution, which are recorded in the data processing agreement.

9.3 In our applications

Some applications offer optional AI-assisted features, such as drafting, summarisation, classification suggestions or text recognition. These features are off by default and opt-in, assistive only and never autonomous, never write legally significant or status-bearing values automatically, and let you review and override the output before it is used. Where a feature relies on a third-party model provider, the provider acts as our sub-processor under a written agreement that prohibits the use of inputs or outputs to train its models, and we minimise the data sent.

9.4 No solely automated decisions

We do not take decisions that produce legal effects concerning you or similarly significantly affect you based solely on automated processing within the meaning of Article 22 GDPR. Where automated logic informs a decision affecting you, a person is meaningfully involved in the outcome.

9.5 EU Artificial Intelligence Act

We design and operate our AI features and solutions to comply with Regulation (EU) 2024/1689, including AI-literacy measures for our own use (Article 4) and transparency obligations (Article 50) where they apply. None of our current AI features is, or is held out as, a high-risk AI system within the meaning of Annex III of that Regulation.

10. Recipients of personal data

We share personal data only with the recipients below and only as far as necessary for the purpose. We do not sell personal data and do not share it for cross-context behavioural advertising.

Recipient	Purpose	Role
Hostinger International Ltd	Hosting of the website and of enquiry records; sending of website notification emails; content-delivery and security services	Processor
Google Ireland Limited (Google Workspace)	Business email, calendar, video meetings and document storage	Processor
Providers of AI models and	Research, drafting and client	Processor or sub-processor

Recipient	Purpose	Role
workflow platforms	solutions, as described in section 9; providers used for client data are named in the data processing agreement	
Subcontractors	Assistance with an engagement, only with the client's prior written consent	Processor or sub-processor
Apple Inc. and Apple Distribution International Limited	App Store distribution, in-application purchases, Sign in with Apple and iCloud / CloudKit storage where used	Independent controller for App Store processing; sub-processor for iCloud / CloudKit storage
Google LLC and Google Ireland Limited	Sign in with Google, where you choose it	Independent controller
Service providers of our applications	Hosting, email delivery, monitoring, crash reporting and payments, as listed in each application's privacy notice	Processors or independent controllers
Professional advisers (lawyers, accountants, auditors, insurers)	Legal, tax, audit and insurance matters, on a need-to-know basis	Independent controllers bound by confidentiality
Courts, supervisory and tax authorities	Where required by law or a binding request, including the VDAI and the State Tax Inspectorate	Independent controllers
A successor to our business	In a merger, acquisition or sale of assets, subject to confidentiality and to this Policy	Independent controller after completion

Clients receive the list of sub-processors used for their engagement as part of the data processing agreement. The providers used by each application are listed in its privacy notice.

11. International data transfers

We aim to keep personal data within the European Economic Area. Some providers, including Google and Apple, may process data outside it. Where personal data is transferred to a country without an adequacy decision under Article 45 GDPR, we rely on safeguards under Chapter V GDPR, in particular adequacy decisions including the EU-US Data Privacy Framework for

certified recipients, the European Commission's Standard Contractual Clauses, and supplementary technical measures such as encryption in transit and at rest.

12. How long we keep personal data

We keep personal data only for as long as necessary for the purpose for which it was collected or as required by law. Where several periods apply, the longest applies.

Personal data	Retention
Website server logs	For the short period set by our hosting provider's log rotation, for security and troubleshooting
Enquiries and contact-form records, including the IP-address hash	Up to 24 months after the last correspondence, unless the enquiry leads to an engagement
Client relationship and engagement records (engagement letters, correspondence, Deliverables)	For the duration of the engagement and up to 10 years after it ends, corresponding to the general limitation period under Article 1.125 of the Civil Code of the Republic of Lithuania
Personal data in client materials (as processor)	For the duration of the engagement; returned or deleted within 30 days after it ends, unless the data processing agreement provides otherwise or the law requires storage
Billing, accounting and tax records	Up to 10 years from the end of the relevant accounting period, in line with the Law on Financial Accounting and the Law on Tax Administration of the Republic of Lithuania
Application account and authentication data	For the life of the account; deleted or anonymised within 24 months of complete inactivity, save where statutory retention applies
On-device application data	On your device for as long as you keep it; removed by the operating system when the application is deleted
Application telemetry	Pseudonymised where feasible; identifiable data for up to 13 months; aggregated or anonymised data may be kept indefinitely
Application support correspondence	Up to 24 months after the matter is closed; longer where it concerns a complaint, dispute or legal claim, until resolved plus the applicable limitation period
Apple App Store transaction metadata	For the life of the entitlement plus the period needed for refunds, disputes and statutory accounting
Workspace data (as processor)	As set in the Data Processing Addendum: a 30-day export window after termination, followed by deletion or anonymisation within a further 60 days
Audit and security logs	Up to 24 months, or longer where needed for security or legal claims

Personal data	Retention
Back-ups	Standard rotation cycles, typically up to 30 days
Marketing data	Until you withdraw consent or unsubscribe; reviewed every 24 months

13. Security

We take appropriate technical and organisational measures under Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing. They include encrypted devices and connections, multi-factor authentication on our accounts, access to client systems only through accounts provided by the client with the minimum rights necessary, encrypted transfer of files, and separation of each client's materials.

14. Personal-data breaches

If we become aware of a personal-data breach that is likely to result in a risk to the rights and freedoms of natural persons, we notify the competent supervisory authority without undue delay and, where feasible, within 72 hours (Article 33 GDPR), and the affected individuals where the risk is high (Article 34 GDPR). Where we act as processor for a client or workspace owner, we notify that controller without undue delay (Article 33(2) GDPR).

If you suspect a security incident affecting your data, please write to support@mlconsulting.it without undue delay. Do not include passwords or other secrets in the email.

15. Your rights

Subject to the conditions in the GDPR, you have the following rights. They are not absolute and may be restricted by law.

- **Access (Article 15).** To confirm whether we process your personal data and obtain a copy.
- **Rectification (Article 16).** To have inaccurate data corrected and incomplete data completed.
- **Erasure (Article 17).** To have personal data erased where the conditions in Article 17 apply. Many of our applications also offer an in-application "Delete account" control.
- **Restriction (Article 18).** To restrict processing in the circumstances set out in Article 18.
- **Portability (Article 20).** To receive data you provided, processed by automated means on the basis of consent or contract, in a structured, commonly used and machine-readable format, and to have it transmitted to another controller where technically feasible.
- **Objection (Article 21).** To object to processing based on legitimate interests on grounds relating to your particular situation, and at any time to direct marketing.
- **Automated decisions (Article 22).** Not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects (see section 9.4).

- **Withdrawal of consent (Article 7(3)).** To withdraw consent at any time, without affecting the lawfulness of earlier processing.
- **Complaint (Article 77).** To lodge a complaint with the VDAI or with the supervisory authority of the EU Member State where you live, work or where the alleged infringement took place. We would appreciate the opportunity to address your concern first.

To exercise your rights, write to support@mlconsulting.lt with "Privacy request" in the subject line. We respond without undue delay and in any event within one month of receipt; we may extend this by up to two further months for complex or numerous requests and will tell you why within the first month (Article 12(3) GDPR). We may need to verify your identity in a way proportionate to the request. Requests are free of charge unless manifestly unfounded or excessive (Article 12(5) GDPR).

Where we process your data as processor for a client or workspace owner, please contact that organisation first. If you cannot identify it, write to us and we will redirect your request without undue delay.

16. Regional notices

- **United Kingdom.** The UK General Data Protection Regulation and the Data Protection Act 2018 apply to processing within their scope. The rights in section 15 apply equivalently. The supervisory authority is the Information Commissioner's Office.
- **Switzerland.** The Federal Act on Data Protection applies to processing within its scope. The supervisory authority is the Federal Data Protection and Information Commissioner.
- **United States.** Residents of California and other US states with comprehensive privacy laws may have rights to know, delete and correct personal information and to opt out of its sale or sharing. We do not sell personal information or share it for cross-context behavioural advertising, and we will not discriminate against you for exercising your rights. Write to support@mlconsulting.lt to exercise them. On the website we honour the Global Privacy Control signal where technically feasible.

17. Children

Our website and Professional Services are intended for adults acting in a professional capacity. Our applications are not directed at children, and we do not knowingly collect personal data from children below the age of digital consent applicable in their country (in Lithuania, 14 years for information society services offered directly to a child). Some applications set a higher minimum age, reflected in their App Store age rating. If we learn that we have collected a child's personal data without the required authorisation, we delete it without undue delay. Parents and guardians may contact us at support@mlconsulting.lt.

18. Cookies and similar technologies

The website does not use analytics, advertising, profiling or marketing cookies and does not load content from third-party servers. Our hosting provider may set a strictly necessary security cookie to protect the website against automated attacks; such a cookie is exempt from consent under Article 5(3) of Directive 2002/58/EC and is not used to track you.

Our iOS applications use on-device storage — the application sandbox, the Keychain, SwiftData, UserDefaults and, where you enable it, a private iCloud / CloudKit container — to deliver their features. This storage is governed by this Policy and the application's privacy notice.

19. Communications and direct marketing

We send service messages, such as security alerts, billing notices and notices of material changes, as part of performing our contract with you; they are not marketing. We send marketing communications only with your consent, or to existing clients and customers about similar services under the existing-customer exception, always with a simple way to opt out. You can opt out at any time through the unsubscribe link, by writing to support@mlconsulting.lt or in your account settings where available.

20. Application-specific notices

Where an application has processing characteristics that go materially beyond this Policy, we publish an application-specific privacy notice that applies alongside this Policy and is linked from the application's App Store listing and from within the application. The App Privacy details on the App Store are kept consistent with this Policy and the application-specific notice.

21. Changes to this Policy

We may update this Policy, for example to reflect new services, regulatory developments or changes in our providers. The current version is always published at <https://mlconsulting.lt/privacy-policy>. Where a change is material and adversely affects your rights, we give reasonable advance notice — typically at least 30 days, unless a shorter period is required by law — by in-application notice and, where we have your email address, by email. Each version is dated and archived; the version in force at the time of the processing governs that processing.

Version history

- **Version 2.0, effective 9 October 2026.** Extended to the website's contact forms, enquiries, Professional Services and personal data processed for clients; recipients, retention periods, cookies and AI sections updated; the reference to a separate sub-processor web page was replaced by section 10; the age of digital consent in Lithuania was corrected to 14 years. The processing in our applications is unchanged.
- **Version 1.0, effective 6 May 2026.** Original portfolio-level policy for the website and iOS applications.