AITY CLOUD SRL

Privacy Policy

Version 1.2 · effective from 28 September 2026 · aity.tech/documents

DENUMIRE / ENTITY	AITY CLOUD SRL
CUI	39458128 (RO39458128)
NR. REG. COM.	J2018000824245
EUID	ROONRC.J2018000824245
CORESPONDENȚĂ / CORRESPONDENCE	Str. Heliade Între Vii nr. 35, cod 023382, Sector 2, București, România
CONTACT	office@aity.ro · support@aity.ro · aity.ro · aity.tech

(c) AITY CLOUD SRL

Table of contents

Privacy Policy 3
1. Sovereign hosting - our commitment 3
2. Our roles 3
3. What data we process, for what purposes, and on what grounds 3
4. Recipients and external sources 6
5. Transfers outside the EEA 7
6. Retention 8
7. Security 9
8. Your rights 9
9. Websites, cookies, and local storage 9
10. Minors 11
11. Changes 11
Version history 11

Privacy Policy

VERSION 1.2 · EFFECTIVE FROM 28 SEPTEMBER 2026 · AITY CLOUD SRL

Romanian version · Download PDF

This policy describes how **AITY CLOUD SRL**, a Romanian limited liability company, with its registered office at SACEL no. 1003, Săcel Village, Săcel Commune, Maramureș County, postal code 437290, Romania, tax ID 39458128 (VAT RO39458128), Trade Register J2018000824245, EUID ROONRC.J2018000824245, subscribed and paid-up share capital RON 5,000, correspondence address Str. Heliade Între Vii no. 35, postal code 023382, Sector 2, Bucharest, Romania, telephone +40735850896 (Monday-Friday, 09:00-18:00 Romanian time), e-mail office@aity.ro ("**aity**", "**we**"), processes personal data in connection with the websites, accounts, consoles, and **aity Platform** and **aity Cloud** services (the "**Services**"), in accordance with Regulation (EU) 2016/679 ("**GDPR**") and Romanian Law no. 190/2018.

Data protection contact: **office@aity.ro**. aity has not appointed a data protection officer; this address is the controller's contact point, not a DPO contact. The Romanian and English versions are both official; in case of divergence, the Romanian version prevails.

1. Sovereign hosting - our commitment

Customer Content stored at rest through the Services is kept in the European Economic Area, on infrastructure operated by aity or by EEA infrastructure partners contractually bound to comply with applicable security, confidentiality, and data protection requirements. The current list of sub-processors applicable to Customer Content is maintained in the DPA.

This commitment does not mean that messages are not transmitted to recipients selected by the Customer, that exports are not sent to the destination selected by the Customer, that data needed for accounts, authentication, payment, invoicing, domain registration, or support is not disclosed to the recipients described below, or that data cannot be disclosed to a competent authority where required by law. The inventory of providers, locations, remote access, and flows was reviewed on **16 August 2026**; the flows of the presentation websites, forms, newsletter, and advertising measurement were reviewed on **28 September 2026**.

2. Our roles

- **Controller**: for registration and authentication, account and organization data, tax and risk checks, conclusion and proof of the contract, invoicing and payment, consumption measurement, security, support, complaints, marketing, and website visits, in the situations described in this policy.
- **Processor**: for content stored or transmitted by Customers through the Services (messages, files, data from cloud instances), which we process exclusively on the Customer's instructions. This processing is governed by the Data Processing Agreement (DPA), which forms part of the contract with Business Customers. If you are an End User of an aity Customer (for example, you have a mailbox administered by your employer), the controller of your data is that Customer; address your GDPR rights requests to the Customer, and we will assist it under the DPA.
- **A Consumer's content**: when a Consumer uses the Services exclusively for personal or household activities and is not a controller subject to the GDPR, aity is the controller for the technical processing necessary to provide, secure, retrieve, and delete that content. We do not use it for advertising or commercial profiling.

3. What data we process, for what purposes, and on what grounds

DATA CATEGORY	PURPOSE	LEGAL BASIS (GDPR)
Account and organization data: name, personal and work e-mail, telephone, identifier, avatar, roles, organization, projects, preferences; password hash, if local authentication is used	Account creation and administration, authentication, authorization, and security	article 6(1)(b) - contract; point (f) - security

DATA CATEGORY	PURPOSE	LEGAL BASIS (GDPR)
Data received from the selected identity provider (Google, Microsoft, or GitHub): identifier, name, e-mail, avatar, and technical authentication information	Federated authentication; the provider learns that sign-in to the Services was initiated	article 6(1)(b)
Onboarding and verification data: identity, address, tax ID, data from ANAF registers, tax status, and indicators such as active/inactive/deregistered	Preparing the contract, checking eligibility, preventing fraud, and human risk assessment	article 6(1)(b), (c), and (f)
Contract data and evidence of acceptance: Consumer/Business Customer status, representative capacity, versions, statements, date and time, IP, user-agent, and proof of e-mail delivery	Concluding and proving the contract, complying with information obligations, and defending rights	article 6(1)(b), (c), and (f)
Billing data: identity, address, tax ID/VAT, trade register, e-mail, telephone, IBAN/bank where applicable, invoices, consumption, and payments	Invoicing, accounting, RO e-Factura, calculation and collection of fees	article 6(1)(b) and (c)
Payment data: cardholder name, e-mail, IP, Customer identifier, amount, currency, description, 3-D Secure result, and recurring token/mandate reference	Initiating, confirming, reconciling, refunding, and securing payments through PayU	article 6(1)(b) and (f); PayU determines its own role for the transaction. The PAN and CVC are entered in PayU's secure frame and are not stored by aity
Data for optional services: contact and company data for domain registration; telephone and SMS notification content; Cloudflare token supplied by the Customer, zone name, and DNS records	Providing the function requested by the Customer through the registrar, Web2SMS, or DNS import	article 6(1)(b)
Technical data: IP, session, request and response code, user-agent, referrer where transmitted, authentication/security events, resource identifiers, audit, consumption, diagnostics, and availability	Providing and securing the Services, preventing abuse, diagnostics, metering, and defending rights	article 6(1)(b) and (f)
Requests sent through the forms of the aity.ro and aity.tech websites: name, e-mail, telephone, company, message, and the other completed fields, the form's page and language, and the associated Attribution, if any	Responding to the request, preparing the offer, and recording the request in aity's CRM, with internal notification of the team	article 6(1)(b) - steps taken at your request before entering into a contract; (f) - management of requests
Requests for free guides (for example, the NIS2 checklist): e-mail, name, company, and the other completed fields, the page, language, and associated Attribution	Sending the guide by e-mail and recording you as a contact person in aity's CRM. The request does not subscribe you to the newsletter	article 6(1)(b) for sending the guide; (f) for recording the request
Attribution: the random token in the website's links, UTM parameters, advertising platforms' click identifiers (for example `gclid`, `oppref`, `li_fat_id`), landing page, external referrer, and time of the first visit; if an aity Platform account is then registered or activated, the time of those events and the organization's number of users	Determining which campaign brought a request, a guide request, a subscription, a registration, or an activation, and reporting that result (a "Conversion") to the advertising platform that showed the ad	article 6(1)(f) - measuring the effectiveness of our own advertising; the e-mail hash and storage on your device only with consent, article 6(1)(a) and section 9
Correspondence, support, complaints, DSA notices, and vulnerability reports: contact data, content, and attachments	Response, remediation, legal obligations, security, and defending rights	article 6(1)(b), (c), and (f)

DATA CATEGORY	PURPOSE	LEGAL BASIS (GDPR)
A Consumer's content: messages, files, contacts, calendars, and cloud data selected by the Consumer	Providing, securing, exporting, and deleting Services for personal/ household use	article 6(1)(b), (c), and (f), depending on the purpose
Newsletter and our other commercial communications: e-mail, a name derived from the address, the list and its language, subscription status, and its dates	Sending the newsletter and the e-mail series you subscribed to, through Listmonk. A subscription becomes active only after you confirm it from the e-mail you receive (double opt-in) and can be cancelled from any message	article 6(1)(a), revocable at any time; for our own similar services, only under the conditions of article 12(2) of Romanian Law no. 506/2004, with a simple and free right to object

Legitimate interests. When we rely on article 6(1)(f) GDPR, we pursue the protection of the Services, network, Customers, and third parties against unauthorized access, fraud, abuse, and attacks; continuity, diagnostics, and incident resolution; management of correspondence, requests, and complaints; measuring the audience of our websites and the effectiveness of our own advertising; establishment, exercise, or defense of rights; and proof of the conclusion and content of the contract. You may request information about the balancing assessment and object under section 8.

Attribution and Conversions. When you reach the website from an ad or a link with UTM parameters, aity's server creates an Attribution record with the data above, without IP address, user agent, or e-mail, and adds a random token identifying it to the page's links. A visit that merely comes from another website, without such parameters, creates no Attribution. The token contains no data about you, and without consent the website stores nothing related to Attribution on your device. If you then submit a form, request a guide, subscribe to the newsletter, or register and activate an aity Platform account, the result is linked to the Attribution, and aity's servers report it as a "Conversion" to the platform that showed the ad: Google, OpenAI, or LinkedIn. The Conversion contains the click identifier, the type and time of the result, and an event identifier. An activation is reported twice: to OpenAI when it happens, with the organization's number of users at that moment, and to Google and LinkedIn 7 days later, with the number of users on that date, at most 10, as the value. For guide requests and newsletter subscriptions, only if you accepted advertising cookies, the Conversion also contains the e-mail address as a SHA-256 hash, a fingerprint from which the address cannot be read but which the platform can compare with addresses it already knows. We do not send the IP address, user agent, name, or form content. Google also receives the consent signal: if you did not accept, the Conversion is reported to it marked as lacking your consent to the use of data for advertising purposes. You may object at any time under section 8.

Requirement to provide data. Mandatory fields, payment and billing data, and contractual evidence are necessary to conclude or perform the contract and to comply with legal obligations. Without them, we cannot create the Account, provide the Services, process the Order, or issue the invoice. Optional data and marketing may be refused without affecting the other Services.

Data obtained indirectly. We may receive authentication data from the selected provider; tax data from ANAF registers; your name, professional address, role, and contact details from the Customer that creates an account for you or designates you as a contact person; and data about you from a complaint, notice, or correspondence. Subject to article 14(5) GDPR, notice is given within a reasonable period, but no later than one month, at the first communication if that occurs earlier or, where disclosure is envisaged, no later than the first disclosure.

We do not request or intentionally process special categories of data in the controller activities described above. Customer Content and uncontrolled correspondence may contain such data; it is processed only in the applicable role and for the applicable purpose. We do not request a Romanian personal numerical code (CNP) in the ordinary flow. If the law or an optional service requires a national identification number, we provide in advance the purpose, basis, necessity, recipients, period, and safeguards required by Romanian Law no. 190/2018.

We do not make decisions based solely on automated processing that produce legal effects or similarly significantly affect a person. Systems may flag spam, fraud, tax status, or abuse, but any material restriction, suspension, or termination involves human review and may be challenged at office@aity.ro. PayU or the card issuer may carry out its own automated anti-fraud and 3-D Secure checks, as explained by the relevant controller.

4. Recipients and external sources

We do not sell or rent personal data. We disclose only the necessary data, as applicable, to the recipients below; the contracting entity and mechanism applicable to a provider are those indicated in its interface and current contract with aity.

RECIPIENT/ CATEGORY	DATA AND PURPOSE	GDPR ROLE	LOCATION AND TRANSFER
aity infrastructure and backup providers	Hosting, redundancy, and recovery for Customer Content and operational data	Processor/sub-processor	EEA; the current list is in the DPA
PayU	Payment and transaction data described above; authorization, anti-fraud, payment, refund	Functional role indicated by PayU, including independent controller for its own payment and compliance obligations	EEA; adequacy or article 46 GDPR safeguards apply to any subsequent access from a third country
SmartBill and **ANAF/RO e-Factura**	Tax data and invoices; issue, transmission, and statutory retention	SmartBill: processor for the functions provided; ANAF: authority/separate controller	Romania/EEA; no third-country transfer applies
Google, Microsoft, GitHub	Authentication request and selected identity data; the provider learns that sign-in to aity was initiated	Separate controller for the identity service	EEA and, depending on the provider, adequate countries or article 46 GDPR safeguards
Google reCAPTCHA	IP, browser, device, and interactions necessary to protect registration and public legal forms against abusive automation	Controller/processor under Google's terms	EEA and possible third countries on the basis of adequacy or article 46 GDPR
Realtime Register or the registrar identified in the Order	Registrant data necessary for the optional domain registration service	Separate controller or processor, depending on the registry and purpose	EEA; any exception is disclosed before the Order
Web2SMS or the identified messaging provider	Telephone number and text of the requested notification	Processor/separate controller, depending on the service	EEA; any onward transfer uses the applicable legal mechanism
Cloudflare, only for DNS import initiated by the Customer	Token presented for the import session, DNS zone, and records	Separate controller for the Customer's Cloudflare service	Under the Customer's contract with Cloudflare; adequacy or article 46 GDPR where applicable
Message recipients and their providers	Address, headers, body, and attachments selected by the sender	Controllers or processors for recipients	Location selected through the recipient's address; the Chapter V mechanism is assessed for flows to third countries
Operational alerting providers	Minimized incident metadata and contact data strictly necessary for alerting	Processor or separate controller, depending on the service	EEA or, where applicable, adequacy/ article 46 GDPR

RECIPIENT/ CATEGORY	DATA AND PURPOSE	GDPR ROLE	LOCATION AND TRANSFER
Google (Google Ads)	The Google Ads tag, only after consent; the Conversions described in section 3, with the click identifier `gclid`, `gbraid`, or `wbraid`, the consent signal and, for guide requests and subscriptions, only with consent, the SHA-256 hash of the e-mail	Independent controller for the Google Ads tag and for Conversions based on the click identifier (Google Ads Controller-Controller Data Protection Terms); processor for Conversions based on e-mail, through enhanced conversions (Google Ads Data Processing Terms)	Google Ireland Limited; the transfer to Google LLC (USA) relies on the adequacy decision for the EU-US Data Privacy Framework, for certified entities, or on the standard contractual clauses in Google's terms
OpenAI (ChatGPT Ads)	The measurement pixel, only after consent; the Conversions described in section 3, with the click identifier `oppref`, the landing page and, for guide requests and subscriptions, only with consent, the SHA-256 hash of the e-mail	The role set by the OpenAI Conversion Terms and Ad Tools Data Processing Addendum: processor for the restricted processing defined there, independent controller otherwise	USA; the standard contractual clauses in the Ad Tools Data Processing Addendum or the applicable adequacy decision
LinkedIn (LinkedIn Ads), when we use it	The LinkedIn Insight Tag, only after consent; the Conversions described in section 3, with the click identifier `li_fat_id` and, for guide requests and subscriptions, only with consent, the SHA-256 hash of the e-mail	Processor for Marketing Solutions under the LinkedIn Data Processing Agreement; independent controller for LinkedIn's own purposes as described by LinkedIn	LinkedIn Ireland Unlimited Company; the transfer to LinkedIn Corporation (USA) relies on the standard contractual clauses in the LinkedIn Data Processing Agreement
Legal advisers, accountants, auditors, and insurers	Data necessary for the engagement, audit, or defense of rights	Separate controllers or processors, depending on their role	Generally EEA
Courts and public authorities	Data required by law, binding request, or defense of rights	Authorities/separate controllers	According to jurisdiction and applicable law

The CRM (Twenty), the newsletter service (Listmonk), traffic analytics (Plausible), and the e-mail service that sends internal notifications and guides run on aity's infrastructure in Bucharest; they are not external providers.

5. Transfers outside the EEA

When aity transmits or makes data available to a separate controller or processor in a third country, we use an adequacy decision or an appropriate safeguard under article 46 GDPR, together with the necessary assessment and supplementary measures. A copy or description of the safeguard may be requested at office@aity.ro. Transmission of e-mail to a recipient or provider in a third country on the Customer's instruction may make aity an exporter in its capacity as processor; the instruction does not remove the obligations of Chapter V GDPR. Google, OpenAI, and LinkedIn may process Conversions and the data collected through their tags in the USA, on the basis of the mechanisms stated in section 4.

6. Retention

We retain data only for as long as necessary for the purpose, then delete or anonymize it, except for statutory retention or isolation necessary for a specific investigation or dispute.

DATA	STANDARD RETENTION PERIOD
Account, organization, and federated identity data	For the term of the contract, then no more than 3 years; data strictly necessary for a legal obligation follows the applicable statutory period
Incomplete onboarding session	30 days from the last activity; data necessary to investigate an unreconciled payment is retained until resolution and no more than 3 years
Contractual evidence, consents, and acceptances	For the term of the contract plus 3 years; identity, capacity, versions, texts, date/time, IP, user-agent, and proof of confirmation are retained
Payment reference and recurring mandate	While the method is active and necessary for the contract; revoked/deleted within no more than 30 days after replacement or termination, with transaction records retained separately for the applicable period
Accounting documents and invoices	5 years, calculated from 1 July of the year following the financial year, under article 25 of Romanian Law no. 82/1991; annual financial statements and documents subject to special regimes are retained for the specific statutory period
ANAF response data	Technical cache approximately 10 minutes; risk indicator used for onboarding, for the term of the contract plus 3 years
Correspondence, support, and complaints	For the resolution period, then 3 years; a file relating to a dispute or incident is retained until its conclusion and expiry of the applicable period
Distributed application traces	14 days
Application and workload logs	31 days
Infrastructure and out-of-band access logs	Up to 90 days, depending on the system
Operational metrics	60 days; labels containing personal data are minimized
Detailed hourly aity Cloud consumption data	120 days, without affecting the invoice and tax aggregates retained for the statutory period
Customer Content	Retrieval Period of at least 30 days; deletion of primary data within no more than 30 days after that; backups are removed through rotation within no more than 45 days after deletion of the primary data
Requests sent through forms and guide requests, on the website and in the CRM	For the duration of the business relationship; if no contract follows, 24 months from the last interaction
Attribution kept on aity's server	120 days from the first visit, then automatic deletion
The `aity_attr` cookie	90 days on the device or until consent is withdrawn
Conversions, at Google, OpenAI, and LinkedIn	Under each platform's terms
Plausible statistics	No limit; they can no longer be linked to a person after the daily rotation of the random value described in section 9
Marketing data	Until consent is withdrawn or an objection is made. Unconfirmed subscriptions are deleted after 30 days. After unsubscription we keep the address, a name derived from it, the subscription status, and its dates only as a suppression list, so that we never write to that address again

7. Security

We apply measures proportionate to risk, including TLS for external connections and internal flows where appropriate, role-based and need-to-know access control, multi-factor authentication for administrative access, network segmentation, redundancy, backup, monitoring, logging, vulnerability management, and periodic testing of the effectiveness of the measures. We minimize data in logs and alerts. Details applicable to Customer Data are in the DPA. We manage personal data breaches under articles 33-34 GDPR; vulnerabilities may be reported to security@aity.ro.

8. Your rights

You have the rights of access, rectification, erasure, restriction, portability, and withdrawal of consent, without affecting the lawfulness of prior processing. Write to office@aity.ro; we respond within no more than one month, extendable by no more than two months for complex requests, under article 12 GDPR. If aity processes the data on behalf of a Customer, we forward the request to that Customer and assist it under the DPA.

Right to object. You may object at any time, on grounds relating to your particular situation, to processing based on legitimate interests; we will not continue unless we demonstrate compelling legitimate grounds or necessity for a legal claim. You may object unconditionally and free of charge to direct marketing, including related profiling, through office@aity.ro or the unsubscribe link. You may also object to Attribution and Conversions at office@aity.ro: we delete the associated Attribution and stop reporting results linked to it.

You may lodge a complaint with **ANSPDCP**, B-dul G-ral Gheorghe Magheru no. 28-30, Sector 1, postal code 010336, Bucharest, dataprotection.ro, and with the authority in the Member State of your habitual residence, place of work, or the alleged infringement. You may also bring proceedings before the competent court.

9. Websites, cookies, and local storage

When websites and consoles are accessed, the servers process the IP address, date and time, method and requested resource, response code, user-agent, and referrer, if transmitted, for technical delivery, security, and diagnostics, based on article 6(1)(f) GDPR. Logs of the applications and of the public gateway, which record every request, including those to the traffic analytics service, are retained for 31 days and are accessible only to authorized personnel and providers with operational or security duties.

We store or access information on your equipment without consent only where the operation is strictly necessary to transmit a communication or provide the requested Service, under Romanian Law no. 506/2004.

TECHNOLOGY	PROVIDER AND PURPOSE	INDICATIVE DURATION
oauth2-proxy/ Keycloak authentication and session cookies	aity; login, session, redirection, and CSRF security	Main session cookie: up to 10 hours; transient cookies: duration of login/session
Console local storage	aity; profile, organization, project, region, and functional state necessary for the interface	Until logout, deletion by the user, or expiry defined by the application
Drive application local storage	aity; maintaining the session and interface operation	Duration of the session or until deletion/logout, depending on the mechanism

TECHNOLOGY	PROVIDER AND PURPOSE	INDICATIVE DURATION
Consent choice (`consent`) and display theme (`theme`), local storage on aity.ro and aity.tech	aity; remembering the choice made in the consent bar and the light or dark theme	Until you clear them from the browser
`aity_attr`, first-party HttpOnly cookie, only after consent	aity; keeping the Attribution (UTM parameters, click identifiers, token, landing page, external referrer, first visit) across the website's pages, to link requests and registrations to the campaign that brought them	90 days
Google Ads tag (gtag.js), only after consent	Google; conversion measurement and advertising: cookies on the aity domain (`_gcl_au`, `_gcl_aw`, `_gcl_gb`, `_gcl_dc`) and Google cookies on Google domains	`_gcl_*`: 90 days; the others under Google's policy
LinkedIn Insight Tag, only after consent	LinkedIn; conversion measurement and advertising: cookies on the aity domain (`li_fat_id`, `li_gc`) and on linkedin.com (for example `bcookie`, `lidc`, `UserMatchHistory`, `AnalyticsSyncHistory`)	Under LinkedIn's policy
ChatGPT Ads measurement pixel, only after consent	OpenAI; measurement of conversions from ChatGPT ads: the `__oppref` and `__obref` cookies on the aity domain	`__oppref`: 30 days from the last update; `__obref`: 365 days
PayU secure frame	PayU; entry and authorization of the requested payment	Under the PayU policy displayed in the payment flow
Google reCAPTCHA v3	Google; protecting registration and public legal forms against abusive automation	Under the Google policy applicable to the security mechanism

Google reCAPTCHA v3 loads only on registration pages and the public withdrawal, switching, and illegal-content notice forms. If the mechanism is unavailable, the request may be submitted through the alternative channels shown on the form page.

Consent on the aity.ro and aity.tech websites. The consent bar appears while we use advertising tags. The Google Ads tag, the LinkedIn Insight Tag, the OpenAI pixel, and the `aity_attr` cookie load or are set only after you press "Accept". Refusing does not affect browsing, forms, or account creation. You can change your choice at any time from the "Cookie settings" link in the website footer; on withdrawal, the tags no longer load, and the `aity_attr` cookie and the tags' cookies on the aity domain are deleted. Cookies already set by Google or LinkedIn on their own domains are deleted from your browser settings.

Traffic analytics. On the aity.ro and aity.tech websites we use Plausible Community Edition, hosted by aity in its Bucharest data centre, without cookies and without storage on your device; it therefore does not ask for consent. To count unique visitors, Plausible computes an identifier from the IP address and user agent combined with a random value that is replaced and deleted every 24 hours; Plausible does not store the IP address, which appears only in the logs described at the beginning of this section. It records the page visited, referrer, UTM parameters, the country and, where applicable, the region or city inferred from the IP, device type, browser, operating system, and events such as clicks on the main buttons, form submissions, guide requests, and subscriptions. The purpose is understanding how the websites are used, under article 6(1)(f) GDPR; the statistics are not shared with third parties.

Static document pages do not use analytics or advertising. We do not currently use our own marketing or analytics cookies in the consoles. If we introduce a non-essential purpose, we first request specific, informed, freely given consent that is as easy to withdraw as to give; refusal does not affect functions that do not objectively depend on the refused technology.

10. Minors

The Services are intended for persons at least 18 years old; minors may use them only as End Users under a Customer's responsibility (for example, within an organization). We do not knowingly collect minors' data outside this context.

11. Changes

Material changes to the processing of Account holders' data are announced at least 30 days in advance, by e-mail to them and by publication on this page. Changes that describe new processing without changing the processing of Account holders' existing data apply from publication and are brought to Account holders' attention by an informational e-mail; previous versions remain available in the PDF archive. The effective date of the current version is shown in the header.

Version history

VERSION	DATE	CHANGES
1.2	28 September 2026	Presentation websites: forms, guides, newsletter, Plausible traffic analytics, Attribution and Conversions reported to Google, OpenAI, and LinkedIn, advertising cookies only with consent.
1.1	17 August 2026	Clarified reCAPTCHA v3 use for public legal forms.
1.0	15 August 2026	First published version.