Airpelago Services - Privacy Policy

Reg. No.: 559062-8177

Töpelsgatan 5A, 416 55, Gothenburg, Sweden

Updated: 2026-04-22

Summary Notice

This Summary gives you a quick overview of how Airpelago AB processes personal data in connection with our websites, mobile applications and other digital services (the "Services"). Full details are set out in Sections 1–18 below.

Who is responsible? Airpelago AB, Swedish org. no. 559062-8177, Töpelsgatan 5A, 416 55 Gothenburg. Data protection enquiries: privacy@airpelago.com. (Section 2)

Why do we process your data? To provide the Services, keep them secure, improve them, communicate with you, send marketing (on a legitimate-interest/opt-out basis for business contacts and on consent for private individuals) and comply with legal obligations. (Sections 3–4)

Where is it processed? Exclusively within the EU/EEA. (Section 7)

What are your main rights? Access, rectification, erasure, restriction, portability, objection (including an absolute right to object to direct marketing) and withdrawal of consent. (Section 9)

Drone-based inspection: when Airpelago carries out drone-based inspection of power lines and energy infrastructure on behalf of a client, Airpelago acts as data processor, not controller. See our separate *Privacy Policy for Drone-Based Inspection - Supplement to Airpelago AB - Privacy Policy 2026*.

1. Introduction and legal framework

This Privacy Policy describes how Airpelago AB, Swedish corporate registration number 559062-8177, with its registered address at Töpelsgatan 5A, 416 55, Gothenburg, Sweden (“we”, “our”, or “us”) collects, processes, stores, and shares personal data when you use our websites, mobile applications, and other digital services (collectively, the “Services”).

This policy is provided in accordance with the transparency requirements set out in Articles 12, 13, and 14 of the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") and, where applicable, the UK GDPR as retained in UK law by the European Union (Withdrawal) Act 2018 (together, "data protection law"). The GDPR is supplemented in Sweden by Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (the "Swedish Data Protection Act") and Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning (the "Swedish Data Protection Ordinance"). In the United Kingdom, the UK GDPR is supplemented by the Data Protection Act 2018.

We process your personal data in accordance with the fundamental principles set out in Article 5 GDPR. This means that personal data is processed lawfully, fairly, and in a transparent manner; collected for specified, explicit, and legitimate purposes; limited to what is necessary in relation to those purposes; kept accurate and up to date; retained only for as long as necessary; and processed with appropriate security. We are responsible for, and are able to demonstrate compliance with, these principles (the principle of accountability).

Airpelago AB is the data controller for the processing of your personal data as described in this policy. Where we process personal data on behalf of another party, we act as a data processor under a data processing agreement with the relevant data controller.

2. Data controller and contact details

Data controller: Airpelago AB, Reg. No. 559062-8177

Address: Töpelsgatan 5A, 416 55, Gothenburg, Sweden

Data protection enquiries: privacy@airpelago.com

Website: www.airpelago.com

3. Personal data we collect

3.1 Information you provide to us

We collect personal data that you voluntarily provide to us, for example when you create an account, subscribe to a newsletter, participate in a survey, request a product demonstration, or otherwise interact with the Services. This may include:

- Full name
- Email address
- Postal address
- Phone number
- Company name and role
- Any other information you choose to provide, such as feedback or support queries

3.2 Information we collect automatically

When you use the Services, we automatically collect certain technical information about your device and usage, including:

- IP address (which may indicate approximate geographic location)
- Device identifiers and type
- Browser type, version, and language settings
- Operating system
- Referral source (the website or link you arrived from)
- Pages viewed, navigation paths, and interactions within the Services
- Date, time, duration, and frequency of visits

This information is collected through cookies and similar technologies (see Section 5).

3.3 Information from third parties

We may receive personal data from third-party sources and combine it with information we collect directly. Such sources may include:

- Social media platforms (e.g. LinkedIn) if you interact with our presence on those platforms or use social login features
- Business partners or customers who provide your contact details in connection with a service engagement

- Publicly available sources, such as company websites or business registries

Where we receive personal data from third-party sources, we inform you about the source at the time of first communication or within one month, in accordance with Article 14 GDPR.

4. Purposes and legal basis for processing

Under Article 6 GDPR, every processing activity must have a lawful basis. We have set out below the specific purposes for which we process your personal data, together with the applicable legal basis and, where we rely on legitimate interest, the specific interest pursued.

Purpose	Legal basis (GDPR Art. 6)	Specified interest / detail	Categories of data
Providing the Services (account management, delivering functionality, customer support)	**Legitimate interest (Art. 6(1)(f))**	Our legitimate interest in providing the Services (account management, delivering functionality, customer support) to our business customers and their contact persons. Airpelago's customers are typically companies (B2B), so contractual performance under Art. 6(1)(b) does not apply to the individual contact persons; processing their data is nevertheless necessary in practice to operate the customer relationship.	Name, email, account data, support correspondence
Service-related communications (e.g. downtime notices, security alerts, changes to terms)	**Legitimate interest (Art. 6(1)(f))**	Our legitimate interest in sending operational notices (e.g. downtime alerts, security advisories and material changes to terms) that are essential to the proper, secure use of the Services by our B2B customers and their contact persons. These	Name, email, account data

		messages are not promotional and cannot be opted out of while you continue to use the Services.	
Analysing usage to improve the Services and user experience	**Legitimate interest (Art. 6(1)(f))**	Our interest in understanding, at an aggregated level, how the Services are used - for example, which features are most used, where users encounter errors, and how long common workflows take - so that we can fix bugs, improve usability and prioritise product development. Analyses are run on anonymised or pseudonymised data and do not involve individual profiling or decisions affecting you.	Anonymised/pseudonymised usage data, device info, IP address
Follow-up communications (e.g. satisfaction surveys, product tips)	**Legitimate interest (Art. 6(1)(f))**	Our interest in maintaining the customer relationship and helping you use the Services effectively, for example by sending short post-onboarding satisfaction surveys, targeted product tips following adoption of a new feature, and reminders about training or webinars relevant to your use case. You may opt out at any time via the unsubscribe link or by contacting us.	Name, email, usage data
Newsletters and marketing communications	**B2B: Legitimate interest (Art. 6(1)(f)); B2C: Consent (Art. 6(1)(a))**	For business contact persons acting in a professional capacity (B2B), our legitimate interest in marketing	Name, email

		our services to existing and prospective business customers, consistent with Section 20 of the Swedish Marketing Act (marknadsföringslagen (2008:486)) on an opt-out basis. Each message includes a working unsubscribe link. For natural persons in a private capacity (B2C), marketing is only sent on the basis of prior explicit consent, which you may withdraw at any time.	
Compliance with legal obligations (e.g. bookkeeping, tax, regulatory reporting)	**Legal obligation (Art. 6(1)(c))**	Required under the Swedish Bookkeeping Act (1999:1078), the Swedish Tax Procedures Act, and other applicable legislation.	Transaction data, invoicing data, correspondence where legally required
Security and protection of the Services (e.g. fraud prevention, access logging)	**Legitimate interest (Art. 6(1)(f))**	Our interest in protecting our systems, users and third parties from unauthorised access, misuse and security threats - for example by maintaining access logs for audit trails, detecting brute-force login attempts and unusual traffic patterns, blocking known-malicious IP ranges and investigating suspected security incidents.	IP address, access logs, device identifiers

Where we rely on legitimate interest as a legal basis, we have carried out a balancing test to ensure that our interests are not overridden by your rights and freedoms. You may request a copy of our legitimate interest assessments by contacting us.

Where we rely on consent, you have the right to withdraw your consent at any time (see Section 9). Withdrawal does not affect the lawfulness of processing carried out prior to the withdrawal.

5. Cookies and tracking technologies

We use cookies and similar technologies on our website. Cookies are small text files stored on your device. We use the following categories of cookies:

Strictly necessary cookies

These cookies are essential for the website to function (e.g. session management, security). They cannot be disabled. Legal basis: Legitimate interest (Art. 6(1)(f)), as the website cannot operate without them.

Analytics cookies

These cookies help us understand how visitors interact with the website by collecting anonymised usage data (e.g. pages visited, time on site). We use Google Analytics for this purpose. Legal basis: Consent (Art. 6(1)(a)). You may accept or decline these cookies via our cookie banner when you first visit the website, and you may change your preferences at any time through the cookie settings link in the website footer.

Marketing cookies

If enabled, these cookies allow us and our advertising partners to deliver relevant advertisements and measure campaign effectiveness. Legal basis: Consent (Art. 6(1)(a)). These are only set with your explicit consent.

The cookies we use do not, on their own, directly identify you by name. Where analytics or marketing cookies are used, anonymised or pseudonymised usage data may be shared with our partners (e.g. Google), who may combine it with other data they hold about you. This sharing only occurs on the basis of your consent.

6. Sharing of personal data

We may share your personal data with the following categories of recipients, and only to the extent necessary for the stated purpose:

- **IT and hosting providers**

  We use third-party service providers for cloud hosting, IT infrastructure, and technical support. These providers act as data processors and process your data solely in accordance with our documented instructions and under a data processing agreement pursuant to Article 28 GDPR.

- **Analytics and communication providers**

  Providers of analytics, email delivery, and customer relationship management tools These providers act as data processors.

- **Professional advisors**

  Lawyers, accountants, and auditors, where necessary for the purposes of obtaining professional advice or complying with legal obligations.

- **Public authorities**

  Where we are required by law to disclose data, for example in response to a binding request from a court or law enforcement authority, or to comply with tax or regulatory obligations.

- **Corporate transactions**

  In connection with a merger, acquisition, reorganisation, or sale of all or part of our business, personal data may be transferred to the acquiring entity. In such cases, we will ensure that the acquiring entity is bound by appropriate data protection obligations and will notify affected data subjects before or promptly after such a transfer takes place.

We may share aggregated or fully anonymised statistical data that cannot reasonably be used to identify any individual. Such data is not personal data within the meaning of the GDPR.

7. Processing of personal data within the EU/EEA

All personal data is processed and stored exclusively within the EU/EEA. We do not transfer personal data to third countries outside the EU/EEA.

8. Retention and deletion of personal data

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable law. The specific retention periods we apply are as follows:

Category of data	Retention period	Basis for retention
Account data (name, email, settings)	Duration of the account + 90 days after deletion	Necessary for contract performance; grace period for account recovery
Customer support correspondence	24 months after case closure	Legitimate interest in resolving follow-up issues and improving support quality
Accounting and financial records	7 years from the end of the financial year	Legal obligation: Swedish Bookkeeping Act (1999:1078), Ch. 7 §2
Analytics / log data	13 months	Legitimate interest in understanding service usage; aligned with recommended guidance on analytics retention
Marketing consent records	Duration of consent + 12 months after withdrawal	Legitimate interest in demonstrating that consent was validly obtained (accountability)
Cookies (analytics)	See appendix A	Set only with consent; aligned with supervisory authority guidance

When the applicable retention period expires, personal data is securely deleted or anonymised so that it can no longer be linked to you. We conduct periodic reviews of our data holdings to ensure compliance with these retention periods.

9. Your rights as a data subject

Under the GDPR, you have the following rights with respect to your personal data. These rights are not absolute; certain exceptions and conditions may apply as set out in the GDPR.

9.1 Right of access (Article 15)

You have the right to request confirmation of whether we process your personal data and, if so, to receive a copy of that data together with information about the purposes, categories of data, recipients, retention periods, and the source of the data. We will provide this information free of charge. If you make repeated or manifestly excessive requests, we may charge a reasonable fee or refuse the request.

9.2 Right to rectification (Article 16)

If any of your personal data held by us is inaccurate or incomplete, you have the right to have it corrected or supplemented. If you have an account with us, you may also update certain information directly through your account settings.

9.3 Right to erasure (Article 17)

You have the right to request deletion of your personal data where, for example, the data is no longer necessary for the purpose for which it was collected, you have withdrawn your consent (and no other legal basis applies), or the data has been unlawfully processed. This right does not apply where we are required to retain the data to comply with a legal obligation (e.g. accounting records under the Swedish Bookkeeping Act) or for the establishment, exercise, or defence of legal claims.

9.4 Right to restriction of processing (Article 18)

You have the right to request that we restrict the processing of your personal data in certain circumstances, for example while we verify the accuracy of your data following a rectification request, or where you have objected to processing based on legitimate interest and we are assessing whether our interests override yours. While processing is restricted, we will store the data but not otherwise process it without your consent.

9.5 Right to data portability (Article 20)

Where our processing is based on your consent or on a contract and is carried out by automated means, you have the right to receive the personal data you have provided to us in a structured, commonly used, and machine-readable format. We currently support export in CSV and JSON formats. You may transmit that data to another controller without hindrance from us.

9.6 Right to object (Article 21)

You have the right to object at any time to our processing of your personal data based on legitimate interest (Art. 6(1)(f)) - including an absolute right to object to processing for direct marketing. You have the right to object to processing that is based on our legitimate interest (Article 6(1)(f)). Upon receiving your objection, we will cease processing your data for that purpose unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or the processing is necessary for legal claims. Where we process your data for direct marketing purposes, you have an absolute right to object, and we will cease such processing without exception. To exercise your right to object, contact us at privacy@airpelago.com or use the unsubscribe link in any marketing message.

9.7 Right to withdraw consent

Where processing is based on your consent (e.g. marketing communications, analytics cookies), you have the right to withdraw your consent at any time. You can do so by contacting us, using the unsubscribe link in any marketing email, or adjusting your cookie preferences. Withdrawal does not affect the lawfulness of processing that took place before the withdrawal.

9.8 How to exercise your rights

To exercise any of the above rights, please contact us at privacy@airpelago.com. To protect your privacy, we may need to verify your identity before acting on your request. We will respond within 30 days. If your request is complex or we have received a high volume of requests, we may extend this period by up to 60 additional days, in which case we will inform you of the extension and the reasons within the initial 30-day period.

If you are not satisfied with our response, you have the right to lodge a complaint with the supervisory authority (see Section 18).

10. Security measures

We implement appropriate technical and organisational security measures to protect your personal data against unauthorised access, accidental or unlawful destruction, loss, alteration, or unauthorised disclosure, in accordance with Article 32 GDPR. These measures include, but are not limited to:

- Encryption of data in transit (TLS) and at rest
- Access controls, including role-based access and multi-factor authentication for systems containing personal data
- Regular security assessments and vulnerability testing
- Staff training on data protection and information security
- Incident response procedures for detecting, reporting, and investigating security incidents

We maintain ISO 27001 certification for our information security, demonstrating our adherence to high industry standards. We regularly review and update our security measures to reflect the state of the art and the nature, scope, context, and purposes of processing, as well as the risks to your rights and freedoms.

11. Personal data breaches

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten, IMY) without undue delay and, where feasible, within 72 hours of becoming aware of the breach, in accordance with Article 33 GDPR.

If the breach is likely to result in a high risk to your rights and freedoms (for example, if sensitive data has been exposed or if there is a risk of identity theft or financial loss), we will also notify you directly without undue delay, in accordance with Article 34 GDPR. The notification will describe the nature of the breach, the likely consequences, and the measures we have taken or propose to take.

12. Automated decision-making and profiling

We do not currently use any automated decision-making, including profiling, that produces legal effects concerning you or similarly significantly affects you within the meaning of Article 22 GDPR.

If this changes in the future, we will update this policy and, where required, obtain your explicit consent or ensure another exception under Article 22(2) applies before such processing commences.

13. Children

Our Services are not directed at children under the age of 16 (being the default age of digital consent under the GDPR, as applied in Sweden). We do not knowingly collect personal data from children under 16. If we become aware that we have inadvertently collected personal data from a child without appropriate parental consent, we will take steps to delete the data as soon as reasonably possible. If you believe a child has provided us with personal data, please contact us at privacy@airpelago.com.

14. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our processing activities, legal requirements, or guidance from supervisory authorities. The date of the most recent update is indicated at the top of this document.

Where we make material changes that affect how we process your personal data or your rights, we will notify you by email (to the address associated with your account) or by posting a prominent notice on our website at least 14 days before the changes take effect. We encourage you to review this policy periodically.

15. Special categories of personal data

We do not intentionally collect or process special categories of personal data as defined in Article 9 GDPR (such as data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation). If we become aware that we have inadvertently collected special category data, we will promptly delete it unless we have a valid legal basis for processing it.

16. Third-party links

Our Services may contain links to third-party websites, applications, or services that are not operated by us. We have no control over, and assume no responsibility for, the content, privacy policies, or practices of any third-party sites or services. We encourage you to review the privacy policy of every site you visit. This Privacy Policy applies only to our Services.

17. Right to lodge a complaint with a supervisory authority

If you consider that our processing of your personal data infringes the GDPR, you have the right, under Article 77 GDPR, to lodge a complaint with a supervisory authority, in particular in the EU/EEA Member State of your habitual residence, place of work, or place of the alleged infringement.

In Sweden, the competent supervisory authority is:

Integritetsskyddsmyndigheten (IMY)

The Swedish Authority for Privacy Protection

Address: Box 8114, 104 20 Stockholm, Sweden

Website: www.imy.se/en/

Email: imy@imy.se

We encourage you to contact us first so that we have the opportunity to address your concerns directly.

18. Contact us

If you have any questions about this Privacy Policy, our processing of your personal data, or wish to exercise any of your rights, you may contact us at:

Email: privacy@airpelago.com

Post: Airpelago AB, Att: Data Protection, Töpelsgatan 5A, 416 55 Göteborg

Appendix A - List of cookies and similar technologies

This Appendix lists the individual cookies and similar technologies that Airpelago currently uses on its websites and within the Services, as of the date of this policy. The table is maintained and updated when cookies are added, removed, or materially changed. Analytics and marketing cookies are only set where you have provided consent via the cookie banner; strictly necessary cookies are set on the basis of Article 6(1)(f) GDPR (legitimate interest), as the website cannot operate without them.

Cookie name	Category	Purpose	Duration	Provider / legal basis
airpelago_session	Strictly necessary	Maintains the user's authenticated session and links successive page requests to the same logged-in user.	Session	Airpelago / Art. 6(1)(f) GDPR
XSRF-TOKEN	Strictly necessary	Security token used to protect against cross-site request forgery (CSRF) attacks on forms and API requests.	Session	Airpelago / Art. 6(1)(f) GDPR
cookie_consent	Strictly necessary	Stores the user's cookie preferences (accept/decline per category) so that the banner is not shown again on every visit.	12 months	Airpelago / Art. 6(1)(f) GDPR
_ga	Analytics	Distinguishes unique users by assigning a randomly generated	24 months	Google LLC / Art. 6(1)(a) GDPR (consent)

		client identifier, used to produce aggregated site-usage statistics.		
_ga_<property-id>	Analytics	Persists session state for the specific Google Analytics 4 property and supports measurement of page views, events and engagement.	24 months	Google LLC / Art. 6(1)(a) GDPR (consent)
_gid	Analytics	Identifies a user across a short time window to distinguish unique visits for short-term analytics reporting.	24 hours	Google LLC / Art. 6(1)(a) GDPR (consent)
_gcl_au	Marketing	Used by Google Ads conversion tracking to measure how users interact with our ads and attribute conversions.	90 days	Google LLC / Art. 6(1)(a) GDPR (consent)
li_fat_id / bcookie	Marketing	Set by the LinkedIn Insight Tag to enable conversion tracking, retargeting and measurement of LinkedIn advertising campaigns.	Up to 12 months	LinkedIn Corporation / Art. 6(1)(a) GDPR (consent)

Note: Third-party cookies set by providers such as Google or LinkedIn are governed by those providers' own cookie and privacy policies. This appendix is reviewed and updated whenever we add, remove or materially change the cookies in use. You can withdraw or change your cookie consent at any time via the "Cookie settings" link in the website footer.