

VOLTEUM PRIVACY NOTICE

Website and Services — Version 2.0, effective 1 October 2026 (replacing the Privacy Policy dated 25 October 2022)

1. WHO WE ARE

Volteum Korlátolt Felelősségű Társaság (“Volteum”, “we”) is a company registered in Hungary under company registration number 01-09-354596 (tax number 27335178-2-42), with its registered seat at 1064 Budapest, Vörösmarty u. 42. fszt. 5., Hungary. Privacy matters can be addressed to info@volteum.io. Volteum provides fleet electrification and fleet management software for electric and mixed vehicle fleets, namely Electric Fleet Planner (EFP) and Live Fleet Management (LFM, formerly Electric Fleet Operations) (together, the “Services”), and operates the websites volteum.io, volteum.hu and volteum.ie (together, the “Website”). The web applications through which the Services are accessed form part of the Services, not of the Website.

This Notice is provided under Articles 13 and 14 of Regulation (EU) 2016/679 (“GDPR”). It applies to visitors of the Website, persons who contact us or subscribe to our communications, representatives of our (prospective) customers and partners, job applicants and, to the extent described in Section 3, users of the Services. It does not cover the processing of our employees’ data, which is addressed in a separate employee privacy notice.

2. OUR TWO ROLES — CONTROLLER AND PROCESSOR

The role in which Volteum processes your data determines whom you should turn to when exercising your rights.

(a) Volteum as controller. For the Website, our marketing and sales activities, our contracts and invoicing, recruitment, and our own support and legal administration, Volteum determines the purposes and means of processing and acts as controller. These processing activities are described in Sections 4 and 5.

(b) Volteum as processor. When your organisation (typically your employer or fleet operator, or a leasing company) uses the Services, the fleet-related personal data processed through the platform — such as vehicle telematics, location, charging and driver-assignment data — is processed by Volteum as a processor on behalf of and on the documented instructions of that organisation, which is the controller. That processing is governed by the data processing agreement under Article 28 GDPR that we conclude with the controller; our standard version is published at www.volteum.io/legal/dpa. If you are a driver or fleet-team member and wish to exercise your data protection rights regarding fleet data, please contact your organisation as controller in the first instance. We will support it in responding, and if you contact us directly we will forward your request to it without undue delay.

The 2022 version of this document incorrectly described Volteum as a “data processor” generally. This Notice corrects the role descriptions.

3. PROCESSING THROUGH THE SERVICES (VOLTEUM AS PROCESSOR) — SUMMARY

On behalf of customer controllers, we process the following categories of personal data of drivers, fleet managers, dispatchers and other authorised users for the purpose of providing the Services — identity and contact data; organisational identifiers and vehicle assignment; authentication data (login ID, IP address, device identifiers); vehicle telematics and location data (GPS position, routes, mileage, trip logs) received from the customer’s telematics or OEM-connected data providers; charging session and energy consumption data; and driving and usage metrics where the customer’s data source provides them. No special categories of data are processed by default. Retention follows the customer’s configuration and the data processing agreement (the term of the agreement plus a deletion and return period).

Where your organisation configures it, we also send periodic service communications through the Services on its behalf, such as scheduled-maintenance reminders and charging-plan or status notifications. These are service messages sent on your organisation’s instructions and are not direct marketing. You can manage your notification preferences, and opt out of non-essential notifications, through the link included in each such message or in your account settings.

For the development and improvement of the Services, we additionally process certain fleet data for our own account as an independent controller, within the strict boundary described in Section 4 (“Product improvement and analytics”).

Our current sub-processors — including our EU cloud hosting provider (Google Cloud, EU regions), telematics and connected-vehicle data providers, and our e-mail delivery and error-monitoring providers — are listed at www.volteum.io/legal/subprocessors.

4. PROCESSING FOR OUR OWN PURPOSES (VOLTEUM AS CONTROLLER)

The table below describes each processing activity, the data concerned, the legal basis, the retention period and the recipients. Where we rely on legitimate interests (Article 6(1)(f) GDPR), we have carried out and documented a balancing test, a summary of which you may request at info@volteum.io.

Purpose	Personal data	Legal basis	Retention	Recipients and processors
Operating and securing the Website (server logs)	IP address, timestamps, requested URL, browser and user agent, referrer	Legitimate interest (Article 6(1)(f)) in delivering and securing the Website	Server logs are kept for 30 days on a rolling basis, and longer only where needed to investigate a security incident	Vercel Inc. (website hosting and delivery, United States); Rackhost Zrt. (website hosting, Hungary); TinaCloud, operated by SSW (website content management, United States); Better Stack (uptime monitoring)
Cookies and web analytics	Cookie identifiers, device and usage data, consent records	Strictly necessary cookies are exempt from the consent requirement of Section 155(4) of Act C of 2003 on Electronic Communications, read in line with Article 5(3) of Directive 2002/58/EC, and rely on our legitimate interest (Article 6(1)(f)). All other cookies (analytics, advertising) are set only with your consent (Article 6(1)(a)), collected through the consent banner.	As set out in the cookie tables of the Cookie Notice; consent records are kept for 5 years	The providers named in the Cookie Notice; CookieYes (consent management platform)
Responding to contact, demo and “Talk to our experts” requests	Name, business e-mail and phone, company and role, content of the enquiry	Steps prior to entering into a contract (Article 6(1)(b)); for representatives of the enquiring organisation, legitimate interest (Article 6(1)(f)) in B2B business development	Duration of the dialogue plus 2 years after the last contact	Google Workspace; HubSpot and Attio (CRM)
Newsletter and electronic direct marketing	Name, e-mail address, subscription date and IP address,	Your consent (Article 6(1)(a) GDPR and Section 6 of Act XLVIII of 2008 on the Basic	Until you withdraw your consent; the consent register is	Brevo (Sendinblue SAS, France), newsletter platform

	consent record; interaction data only if separately disclosed	Requirements and Certain Restrictions of Commercial Advertising Activities). You may unsubscribe at any time through the link in every message.	kept for 5 years thereafter for accountability	
Customer contract administration and invoicing	Contact persons' name, position, business contact data, signatures, contractual correspondence; invoice data	Performance of contract (Article 6(1)(b)); for contact persons, legitimate interest (Article 6(1)(f)); for invoicing, legal obligation (Article 6(1)(c) and Section 169 of Act C of 2000 on Accounting)	Contract file until the end of the contract plus 5 years (general limitation period); invoices and accounting records for 8 years	Adoptimum Plus Kft. (bookkeeping); Google Workspace
B2B relationship (CRM) management	Business contact persons' name, role, company, contact data, interaction history	Legitimate interest (Article 6(1)(f)) in organised B2B sales and partner management. We send no e-mail marketing without consent.	Active relationship plus 2 years after the last meaningful contact	HubSpot and Attio (CRM); Google Workspace
Support requests relating to the Services	Requester's name, contact data, account reference, content of the request	Performance of contract (Article 6(1)(b)), or legitimate interest (Article 6(1)(f)) for representatives	Term of the customer agreement plus the deletion period; 2 years for non-customers	Google Workspace; Sentry (error diagnostics)
Product improvement and analytics (including machine-learning model development and statistical benchmarks)	Platform feature-usage events of authorised users; fleet telemetry (trip, charging and energy data) in anonymised and aggregated form or, where strictly necessary for model training, in pseudonymised form	Legitimate interest (Article 6(1)(f)), acting as independent controller within the boundary agreed with our customers in our data processing agreement. We use anonymised data wherever possible and pseudonymised data only where strictly necessary, with restricted access. We make no decision about any individual driver, create no driver-level scores or profiles, and disclose no identifiable data to any other customer. You may object at any time (Section 9).	Usage analytics for 24 months; pseudonymised development datasets for a maximum of 36 months, after which they are anonymised or erased; anonymised aggregates are no longer personal data	Google Cloud; Sentry

Security of the Services (authorised platform users)	Login ID, IP address, browser and device data, audit logs of user actions	Legitimate interest (Article 6(1)(f)) in operating the Services securely and preventing misuse, as described in clause A.6 of Schedule A to the Master Subscription Terms	Audit logs are kept for 12 months on a rolling basis, and longer only where needed to investigate a security incident	Google Cloud; Sentry
Recruitment (applications via the Website, e-mail or LinkedIn)	Name, contact data, CV and any information you include in your application	Steps prior to entering into a contract (Article 6(1)(b)); limited retention of unsuccessful applications on the basis of legitimate interest (Article 6(1)(f)) in defending equal-treatment claims; talent pool only with your consent	Until the position is filled. Unsuccessful applications are erased within 3 months, or kept for up to 1 year with your consent.	Hiring managers; Google Workspace, Notion. Where you apply through LinkedIn, LinkedIn Ireland Unlimited Company processes your data as an independent controller under its own privacy policy. A detailed applicant privacy notice is provided in the application process.
Social media pages (LinkedIn, Facebook, Instagram)	Your public profile data and interactions with our pages; aggregated page statistics	Legitimate interest (Article 6(1)(f)); for page insights we are joint controllers with the platform under its page-insights supplement	Governed by the platform; our own exports are kept for 2 years	Meta Platforms Ireland Limited; LinkedIn Ireland Unlimited Company
Legal claims and authority requests	Data relevant to the given claim or lawful request	Legitimate interest (Article 6(1)(f)); legal obligation (Article 6(1)(c)) where a statutory duty applies. Disclosures to authorities are limited to the scope of a lawful, specific request.	Limitation period of the claim (generally 5 years) or closure of the proceeding plus 1 year	Legal counsel; courts and authorities

5. COOKIES

Detailed information on the cookies and similar technologies used on the Website — including their names, providers, purposes and lifetimes, and how to give, refuse and withdraw consent — is set out in our Cookie Notice, available at www.volteum.io/cookie-policy and through the “Cookie settings” link in the Website footer. Non-essential cookies are set only with your prior consent, which you may withdraw at any time with effect for the future.

5A. NO AUTOMATED DECISION-MAKING; CHILDREN

We make no decision producing legal or similarly significant effects concerning you based solely on automated processing within the meaning of Article 22 GDPR, and we perform no such profiling. The outputs of the Services

are decision-support tools used by human operators of our customers. The Website and the Services are directed at professional users and are not intended for children, and we do not knowingly collect children's data through them (dependant data processed in our HR context is described in the employee privacy notice).

Nature of the provision of data. Where processing is based on a contract or pre-contractual steps (contact and demo requests, contract administration, invoicing, recruitment), providing the data is necessary for us to respond or to conclude and perform the contract, and without it we cannot process your request. Where processing is based on consent (newsletter, non-essential cookies), provision is entirely voluntary and refusal has no adverse consequence.

6. SOURCES OF DATA

We collect personal data primarily from you. In B2B contexts we may also receive your business contact data from your organisation or colleagues (for example when you are named as a contact person in a contract), and from public professional sources (company registers, your organisation's website, LinkedIn). For the product-improvement processing described in Section 4, fleet telemetry is received from our customers and from the telematics, connected-vehicle and charging data providers they designate. Where we receive data about you from such sources, this Notice serves as the information under Article 14 GDPR.

7. INTERNATIONAL TRANSFERS

We host the Services and customer data in the EU (Google Cloud, Belgian/Dutch regions). The Website is hosted by Vercel Inc. (United States) and Rackhost Zrt. (Hungary). Some of our providers process personal data outside the EEA, in particular in the United States (for example Vercel, our website hosting provider, and TinaCloud, our website content management system operated by SSW, as well as Sentry, GitHub, Slack, Notion and HubSpot) and, for certain telematics integrations, in the United States, the United Kingdom or Canada. Such transfers rely on an adequacy decision of the European Commission (United Kingdom, Canada, and the EU-US Data Privacy Framework where the provider is certified) or on the Standard Contractual Clauses of Commission Implementing Decision (EU) 2021/914, supplemented by transfer impact assessments and additional technical measures. SSW, which operates TinaCloud, is not certified under the EU-US Data Privacy Framework, so transfers to it take place under the Standard Contractual Clauses. You may request a copy of the applicable safeguards at info@volteum.io.

8. DATA SECURITY

We apply technical and organisational measures appropriate to the risk (Article 32 GDPR), including encryption in transit and at rest, role-based access control and multi-factor authentication, environment separation, logging and monitoring, vulnerability and dependency scanning, backups, and staff confidentiality and training. Details are set out in our internal security documentation and, for customers, in Annex 2 of the data processing agreement.

9. YOUR RIGHTS

Where Volteum is the controller, you have the right to access your personal data (Article 15), to rectification (Article 16), to erasure (Article 17), to restriction of processing (Article 18), to data portability (Article 20, for automated processing based on consent or contract), and to object to processing based on legitimate interests, including at any time and without giving reasons to processing for direct marketing (Article 21). Where processing is based on consent, you may withdraw it at any time without affecting the lawfulness of prior processing. We respond without undue delay and at the latest within one month, which may be extended by two further months for complex requests with reasons given (Article 12(3)). To exercise your rights, contact info@volteum.io or write to our registered seat. We may reasonably verify your identity. Exercising your rights is free of charge except in the cases of Article 12(5) GDPR.

For fleet data processed on behalf of a customer (Section 3), please address your request to the controller (your organisation). We will forward misdirected requests and assist the controller in responding, as required by our data processing agreement.

10. COMPLAINTS AND REMEDIES

You may lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH, 1055 Budapest, Falk Miksa u. 9–11., postal address 1363 Budapest, Pf. 9., phone +36 1 391 1400, e-mail

ugyfelszolgalat@naih.hu, www.naih.hu), or with the supervisory authority of the Member State of your habitual residence, place of work or the place of the alleged infringement (Article 77 GDPR). You may also bring proceedings before the courts (Article 79 GDPR). In Hungary, you may choose to bring the case before the regional court of your domicile or habitual residence.

11. CHANGES TO THIS NOTICE

We may update this Notice from time to time. The version in force is published at www.volteum.io/privacy, and material changes affecting you will be communicated through the Website or, where appropriate, directly. This version 2.0 replaces in full the Privacy Policy dated 25 October 2022 and the former product privacy policies of Electric Fleet Planner (version 1.1) and Electric Fleet Operations, which are withdrawn.