



aiMotive

LOGIN POLICY

aiMotive Ltd.

Effective from 05 July 2018

1. Introduction and the purpose and scope of this policy

The purpose of this policy is to set out the terms and conditions under which aiMotive Informatikai Korlátolt Felelősségű Társaság (hereinafter: “**aiMotive**”) as data controller may process personal information (hereinafter: “**Login data**”) in connection with the Insights section of its following website [aimotive.com; hereinafter: “**Section**”]. Personal information may be collected from individuals (the data subjects) using the internet to access documents, videos and other types of content provided by aiMotive and uploaded to the Section.

The access of the Section necessitates the processing of the personal data detailed in section 4 of this policy. This data processing falls under the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter: “**GDPR**”).

aiMotive is dedicated to protecting privacy and personal data and strives to put in place the necessary measures for this purpose. In order to ensure compliance with the underlying legal regulations and to eliminate, to a reasonable extent, potential negative consequences of the data processing, aiMotive hereby sets out the rules on the processing of the personal data by aiMotive, as well as the rights and remedies of individuals affected by aiMotive’s processing of their personal data in the course of accessing the Section. aiMotive shall publish this policy on its website and update it as applicable and when necessary (e.g. due to a change in aiMotive’s activities or in laws).

This policy covers the processing of personal data by aiMotive in connection with the Login data, including monitoring the user’s activity while accessing the Section. The terms of this policy shall be in addition to, not exclusive of or in substitution for the rights and remedies of individuals under the applicable mandatory legal regulations, especially the GDPR.

2. Legal basis of data processing

For the purposes set out in section 4 of this policy, aiMotive collects and processes the information (including personal data) as per section 6 of this policy from and about individuals and stores it in its files (which may include written, printed and electronic form).

The legal basis of the processing of Login data under this policy is the explicit and informed consent of the data subject given in line with Section 6 (1) a) of the GDPR.

3. Details of the data controller

The data controller in respect of personal data handled under this policy is as follows:

Name: aiMotive Informatikai Korlátolt Felelősségű Társaság

Seat: 1025 Budapest, Szépvölgyi út 22.

Company reg. no.: 01-09-208015

Tax no.: 25316663-2-41

Telephone no.: +36-1-770-7234

website: <https://aimotive.com>

e-mail: info@aimotive.com

Primary Contact: Head of Legal Department

Data Protection Officer: David Végh

4. Categories of processed personal data, purpose and legal basis of data processing, data retention period

Categories of personal data concerned	Purpose of data processing	Legal basis of data processing	Period for which the personal data is stored
Name and e-mail address of the data subject, data shared by the user's LinkedIn or Microsoft account.	Registration to Section and sending e-mails, messages and newsletters for direct marketing purposes, in particular advertisements, brochures, information on events and other activities related to the operation of aiMotive. The content of the aforementioned materials is dependent on the activity of the data subject while accessing the Section.	Explicit and informed consent of the data subject	Login data provided may be stored by aiMotive until the data subject withdraws his/her consent by unsubscribing or withdrawal notice. If the purpose of the data processing ceases, the data will be erased without delay.

aiMotive highlights that the consent to the data processing is voluntary, however the processing of the above personal data is necessary in order for the data subject to be able to access the Section. Failure to provide consent results in no detrimental consequence to the data subject, but the content of the Section will not be accessible in this case.

Recipients or categories of recipients of the personal data

See section 9.

Processing of special categories of personal data

The data controller does not process any special categories of personal data in the course of this process.

Data of the data subject obtained from other sources

You can access the Section by using your LinkedIn or Microsoft account. Therefore, certain information shared by the account you use to access the Section (see section 7) will be available to us. In line with the principle of purpose limitation we will only use the information that is absolutely necessary to ensure that you have access to the Section and its content.

5. Persons with access to personal data

Login data processed by aiMotive under this policy may be accessed by the following persons at aiMotive (as applicable from time to time), on a need-to-know basis:

- IT department; technical implementation, troubleshooting, monitoring
- Commercial Team; technical implementation, user support, monitor content and usage statistics
 - Chief Commercial Officer
 - Head of Business Development
 - Business Development Managers
 - Head of Marketing and Communications
 - Marketing Managers

6. User tracking, marketing contact and profiling

The informed and explicit consent of the user extends to the tracking of downloads they complete while accessing the Section and use this data to provide a personalized marketing experience. This tracking forms and integral part of the data processing specified in section 4.

We will use the tracking results to provide users with custom-tailored e-mails, messages and newsletters and other information the content of which will be based on their previous downloads. The impact of this on users is that they will only receive the content that is deemed relevant to them on the basis of their downloads. aiMotive employees may reach out directly to users based on their interests with further information, business opportunities and offers.

The database tracks user interactions with the page through the use of cookies. The login cookie will store information on the login status of the user, and download link clicks will be paired with this login information. The compiled database is stored by aiMotive in its entirety and not shared with any third parties. For more information on the cookies we use please read the aiMotive Cookie Policy. For more information on the safety measures aiMotive takes to safeguard your data please see section 7a. of this policy.

7. Tools used to process collected data

aiMotive will use the tools specified below to collect and process the user data provided under this policy. More information on the types of data collected and how that data is collected is provided below in sections 7a and 7b respectively.

1. Internally developed user registry and tracking system (database)
2. Salesforce Customer Relationship Manager (CRM)

7a. Information collected and stored in the Internally Developed User Registry and Tracking System

The database is used to implement basic login functionality on the aiMotive website. User data is provided through OAuth authentication by LinkedIn or Microsoft accounts. The user is requested to confirm the data shared by these services. On completing OAuth authentication the user is presented and asked to review the data collected by aiMotive under this policy. This data includes:

- Full name
- E-mail address
- Current employment
- Location of current employment

The user is free to modify the data collected from the above-mentioned third-party services before submitting it to the aiMotive database.

aiMotive draws the user's attention to the fact that user downloads are actively monitored when logged in (e.g. if a user downloads a document one, the database is updated to reflect this). Members of our team will periodically review the downloads users have made to provide a tailored sales and marketing experience. Only interactions with downloads are monitored and all other statistical data is collected in bulk form by Google Analytics. For more information on the statistical data collected by aiMotive through Google Analytics please review our Cookie Policy.

7b. CRM

aiMotive uses the CRM tool to manage and track sales prospects and partner relations. User data is sent to the service automatically when the user submits their information through the review form.

The CRM is a third-party cloud service. User information stored therein falls under the Salesforce Privacy Policy which can be read here: www.salesforce.com/eu/company/privacy

Tracking data collected and stored in the database is not shared with the CRM and remains on aiMotive servers.

8. Rights of the data subject

The data subject may request from the data controller access to personal data concerning the data subject, rectification of inaccurate personal data, erasure of personal data, and in certain cases, restriction of processing. Additionally, the data subject is entitled to the right to data portability, to lodge a complaint with a supervisory authority and to an effective judicial remedy. In the case of profiling the data subject is entitled to the right to obtain human intervention on the part of the data controller and to express his/her point of view and contest the decision.

The data subject is also entitled to withdraw his/her consent at any time, which, however, does not affect the lawfulness of data processing performed based on consent before the withdrawal.

- ***Right to access***

The data subject is entitled to request information at any time about whether and how the data controller processes their personal data, including the purposes of data processing, the recipients to whom the data was disclosed or the source where the data controller received the data from, the envisaged period for which the personal data will be stored, the rights of the data subject concerning data processing, information concerning automated decision making, profiling, and information concerning related guarantees in the case of forwarding personal data to third countries or any international organization. When exercising the right to access the data subject is also entitled to request copies of the personal data undergoing processing; in the case of a request submitted electronically the data controller – in lieu of a request from the data subject that says otherwise – provides the requested information electronically (in .pdf, .xls or other similar format). If the right to access of the data subject has a detrimental effect on the rights and liberties, in this regard especially the business secrets or intellectual property of others, the data controller is entitled to refuse to comply with the request to the necessary and proportionate extent. If the data subject requests the above information in several copies or requests further copies later on, the data controller charges a reasonable fee, proportionate to the administrative costs of preparing the additional copies, which is HUF 200 per copy/page.

- ***Right to rectification***

At the request of the data subject the data controller corrects or completes personal data concerning the data subject. If any doubts arise concerning the corrected data, the data controller may request from the data subject the certification of the corrected data for the data controller appropriately,

primarily with documents. If the data controller disclosed the personal data of the data subject with this right to another person (e.g. the recipient as data processor), then the data controller shall immediately inform such persons after correcting the data, provided it is not impossible or it does not require a disproportionate effort from the data controller. At the request of the data subject the data controller informs them about such recipients.

- ***Right to erasure (“right to be forgotten”)***

If the data subject requests the erasure of any or all personal data of theirs, the data controller shall erase such data without undue delay if:

- the data controller does not need the personal data in question any more for the purpose such data was collected or otherwise processed for;
- it concerns data processing that was based on the consent of the data subject, but the data subject withdrew the consent and the data processing has no other legal basis;
- the data controller illegally processed the personal data, or
- the deletion of personal data is necessary for the performance of legal obligations.

If the personal data under this right is disclosed by the data controller to another party (e.g. the recipient as for example data processor) then the data controller shall immediately inform such persons after the deletion, provided it is not impossible or it does not require a disproportionate amount of effort from the data controller. At the request of the data subject the data controller informs them about such recipients. The data controller is not always obliged to delete personal data, especially for example if the data processing is necessary for the establishment, exercising or defense of legal claims.

- ***Right to restriction of data processing***

The data subject can request the restriction of the processing of their personal data in the following cases:

- the data subject contests the accuracy of the personal data – in this case the restriction concerns the period enabling the data controller to check the accuracy of personal data;
- the data processing is unlawful but the data subject opposes the erasure of data, requesting the restriction of the usage of the same instead;
- the data controller does not need the personal data for data processing purposes any longer but the data subject needs the data for the establishment, exercise or defense of legal claims; or

The restriction of data processing means that the data controller does not process the personal data belonging under the scope of the restriction except for storage, or only processing such data to the extent the data subject consented to, and the data controller may process data necessary for the establishment, exercising or defense of legal claims or for the protection of the rights of other natural persons or legal entities or considering the important public interests of the European Union or any European Union member state even in lieu of such a consent. The data controller informs the data subject beforehand about releasing the limitation of the data processing. If personal data under this

right is disclosed to other persons (e.g. the recipient as for example data processor), the data controller shall immediately inform such persons about the restriction of data processing, provided it is not impossible or it does not require a disproportionate amount of effort from the data controller. At the request of the data subject the data controller informs them about such recipients.

- ***Right to data portability***

The data subject is entitled to request that the data controller hands over the personal data of the data subject provided to the data controller on the basis of consent or a contract, and processed by the data controller by automated means (e.g. by a computer system) to the data subject in a structured, commonly used and machine-readable format even for the purposes of transmitting such personal data to other data controllers or if it is technically feasible, the data controller, at the request of the data subject, transmits such personal data directly to another data controller as indicated by the data subject. In the case of such requests the data controller provides the requested data as a .pdf or .xls file or in other similar format. If the data subject's exercising of the right to data portability had adversely affected the rights and freedoms of others, the data controller is entitled to refuse to comply with the request of the data subject to the necessary extent. Measures taken in the scope of data portability do not mean the deletion of the data, only if, at the same time, the data subject submits a request to delete the personal data as well. Therefore, in lieu of such a request, the data controller stores such personal data as long as it has the purpose and the appropriate legal basis for the processing of those data, also considering the established retention periods.

- ***Right to lodge a complaint, right to an effective judicial remedy***

If the data subject considers that the processing of their personal data by the data controller infringes the provisions of the established data protection legal regulations, especially the GDPR, the data subject has the right to lodge a complaint with the competent data protection supervisory authority in the EU member state of his/her habitual residence, place of work or the place of the alleged infringement. In Hungary, this authority is the Hungarian National Authority for Data Protection and Freedom of Information ("**NAIH**"). Contact details of NAIH:

Website: <http://naih.hu/>
Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.
Mail address: 1530 Budapest, PO Box: 5.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

The data subject, regardless of his/her right to lodge a complaint, may also bring proceedings before a court for such infringement. The data subject is entitled to bring proceedings against the legally binding decision of the supervisory authority concerning the data subject as well. The data subject is entitled to effective judicial remedy if the supervisory authority does not handle the complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

9. Third party data processors

Login data may be transferred to companies within aiMotive's group (aiMotive Inc, having its business address at 1907 Colony Street Mountain View, CA, 94043 USA; Almotive GmbH, registered with the commercial register of the local court of Stuttgart under HRB 752689, having its business address at c/o Cormoran GmbH, Am Zirkus 2, 10117 Berlin) of companies. Login data is also shared with the above-mentioned third-party CRM. When the processing of Login data is carried out by a third-party processor, aiMotive takes the necessary contractual and organizational steps to ensure safe processing of the data.

10. Data Security

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorized purposes) of the personal data. Confidentiality means that only people who are authorized to use the personal data can access it. Integrity means that personal data should be accurate and suitable for the purpose for which it is processed. Availability means that authorized users should be able to access the personal data if they need it for authorized purposes.

Accordingly, aiMotive will ensure that appropriate measures are taken against unlawful or unauthorized processing of personal data, and against the accidental loss of, or damage to, personal data. These principles will be enforced by putting in place appropriate hardware and software-based security measures (including physical entry and system access control, locks, alarms, firewalls, etc.).

11. Miscellaneous

This policy takes effect on the day on which it is issued and remains in force until its withdrawal or replacement by aiMotive. aiMotive shall review this policy on a regular basis and align it with respect to the changed circumstances, as it deems appropriate.

12. Automated Decision Making, Profiling

No automated individual decision-making nor profiling is performed in the course of the data processing of the Data Controller concerning the Data Subject.

* * *