

# DATA MANAGEMENT AND COOKIE POLICY

for customers, partners, job applicants, website visitors, and third parties

**Under the General Data Protection Regulation (GDPR) 2016/679 of the European Parliament and Council - concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data**

Aerisoul Metal & Energy Corp., as the Data Controller (hereinafter: Data Controller), informs the affected individuals in a concise and intelligible form through this policy about the personal data processing activities it carries out, the rights of the Data Subjects, and guarantees.

The Data Controller conducts its data processing activities in compliance with the General Data Protection Regulation of the European Parliament and Council No. 2016/679, known as GDPR, and the Hungarian Information Law (Act CXII of 2011), which fundamentally regulates the protection of natural persons concerning the processing of personal data and the free movement of such data.

The scope of this Policy extends to all processes of the Data Controller where personal data processing occurs. The temporal scope of the Policy lasts until its revocation. The Data Controller reserves the right to amend this Policy, with notifications about such changes made through publication on the website.

The purpose of the Regulation is to describe the internal rules and measures that ensure compliance (compliance) for the Data Controller, and it can also subsequently demonstrate (accountability) both to the data protection authority and the affected individuals.

This Notice applies to the data management by the Data Controller of personal data concerning natural persons involved in any capacity (client, partner, job applicant, third party), and provides information about this.

## I. Data Controller

Aerisoul Metal & Energy Corp.

Address: 93601 Šahy, Lesná 1863, Slovakia

Phone: +421 908 338 858

Email: oliver.arany@aerisoul.com

## II. General Concepts

a) **data subject:** any natural person who is identified or identifiable (the natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person);

b) **personal data:** any information relating to an identified or identifiable natural person (data subject) (such data considered particularly related to the data subject includes the data subject's

name, identifiers, and knowledge characteristic of one or more physical, physiological, mental, economic, cultural, or social identities, as well as conclusions drawn from the data concerning the data subject);

c) **special category data**: any data falling within the special categories of personal data, i.e., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying natural persons, data concerning health, and data concerning a natural person's sex life or sexual orientation;

d) **data controller**: the natural or legal person, or an organization without legal personality, which alone or jointly with others determines the purposes and means of the processing of personal data (including the means used);

e) **data processing**: any operation or set of operations performed on personal data, regardless of the procedure applied, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction;

f) **processor**: the natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller;

g) **data protection incident**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

h) **recipient**: the natural or legal person, public authority, agency, or another body to which the personal data are disclosed, regardless of whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing;

i) **third party**: a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

j) **data subject's consent**: a voluntary, specific, informed, and unambiguous expression of the data subject's will, by which the data subject, through a statement or an act unequivocally indicating agreement, consents to the processing of personal data relating to him or her.

## III. Data Controller's Data Processing Activities

### 3.1. Website Visit

Visiting Aerisoul Metal & Energy Corp. website does not require the provision of personal data for viewing publicly available information.

### 3.2. Contact Form

<b>Legal Basis for Data Processing:</b>	The data subject's voluntary and explicit consent (Article 6(1)(a) of the GDPR). Consent is given when filling out the contact form on Aerisoul Metal & Energy Corp. website, alongside the simultaneous electronic reading and acceptance of this policy.
<b>Scope of Data Subjects:</b>	All natural persons who submit the form on the website.
<b>Scope of Processed Data:</b>	Name, email address, subject of the message, message content.
<b>Purpose of Data Processing:</b>	The Data Controller conducts activities in the business areas published on the website. During a visit to the website, there is an opportunity to contact the Data Controller electronically and send a message. The message submitted by the user is processed, and contact is made based on the subject indicated. The Data Controller does not use the personal data of the Data Subject for purposes other than described.
<b>Duration of Data Processing:</b>	The Data Controller processes the personal data related to the form for 60 days after its receipt. The Data Controller responds substantively within 15 days of receiving the form, then sends a response to the Data Subject. If the user does not respond to the response sent by the Data Controller within 30 days, the Data Controller will verify this fact within 15 days and then delete the Data Subject's personal data. If the Data Subject withdraws consent before the 60th day, the duration of data processing extends from the granting to the withdrawal of consent. The Data Subject may withdraw consent at any time, free of charge, electronically or by post. Upon becoming aware, the Data Controller will arrange for the deletion of personal data within 15 days. If an automatic email returns after sending the response message stating that the email address is no longer accessible or is no longer used by the consenting Data Subject, the Data Controller will arrange to delete all personal data related to the email address within 15 days of becoming aware. The right to withdraw consent does not affect the lawfulness of processing based on consent before its withdrawal.

### 3.3. Newsletter

<b>Legal Basis for Data Processing:</b>	The data subject's voluntary and explicit consent (Article 6(1)(a) of the GDPR). Consent is given when filling out the newsletter subscription form on the website, alongside the simultaneous electronic reading and acceptance of this policy.
<b>Scope of Data Subjects:</b>	All natural persons who submit the form on the website.
<b>Scope of Processed Data:</b>	Name, email address.
<b>Purpose of Data Processing:</b>	To send newsletters to the data subject. The newsletter is sent by the Data Controller for the purposes of promoting its own marketing activities, market research, informing about current information, promotions, direct marketing solicitations, preparing personalized offers, and maintaining contact, which may contain advertising.

<b>Duration of Data Processing:</b>	<p>Until the data subject withdraws consent, but no longer than 2 years from the last data update of the data subject. The Data Subject may withdraw consent at any time, free of charge, by clicking the "Unsubscribe" link found at the bottom of each newsletter, or by electronic or postal means. Upon becoming aware, the Data Controller will arrange for the deletion of personal data within 15 days.</p> <p>The right to withdraw consent does not affect the lawfulness of processing based on consent before its withdrawal.</p>
-------------------------------------	--

## IV. Cookie Policy

### What are cookies?

#### 4.1. General Information

A cookie is a text file placed on the visitor's device (typically a computer or mobile phone) by the web server when visiting a website. It stores information about the user, the operation of the website, or even the connection between the user and the web server. The web server often uses this information to enhance the user experience or provide services when the page is loaded.

Cookies are files created by websites you visit. By saving browsing data, they facilitate navigation. Our website uses cookies for the following purposes, and our company uses cookies to:

- Keep you logged in;
- Remember your site settings;
- Provide locally relevant content to you;
- Assist us in improving our website;
- Facilitate your navigation during the use of our website, allowing you to use its features more efficiently;
- Some cookies collect information about how you use our website to ensure a better user experience when you return to our site. This tracking also enables us to send messages about offers that may interest you;
- Cookies can also enable the placement of targeted advertisements on other websites.

#### 4.2. Basic Types of Cookies

##### 4.2.1. Cookies Essential for Website Operation

- User-input cookies: These session cookies are based on a session identifier (a random temporary identification number) and expire at the end of the session when the browser is closed. They ensure user data input during interactions with the service provider (e.g., filling out forms or clicking a button).
- Multimedia player session cookies: These cookies store technical data necessary for playing video or audio content (such as image quality, network connection speed, and buffering parameters) and expire when you exit the browser program.

- Social content sharing cookies: Enable users of social networks to share content they like with their friends. These cookies are deleted when the user logs out of the social networking platform or closes the browser.

#### 4.2.2. Cookies for „Convenience Services“

These cookies are not considered "strictly necessary" for the provision of services specifically requested by the user, so separate approval is needed for their use.

- **Social content sharing tracking cookies:** If members of social networks have approved "tracking" when logged in, such as for displaying behavior-based ads.
- **Proprietary analytics:** These are statistical tools that measure website traffic and use cookies. These tools estimate the number of unique visitors, identify the most frequently used keywords on search engines that lead to the website, and track certain web navigation issues. They serve exclusively for their own aggregated statistics to provide faster and more accurate service to visitors.

#### 4.2.3. Cookies Necessary for Performance Measurement

Management of analytical cookies (Google Analytics): This website uses Google Analytics, a service provided by Google Inc. ("Google"). Google Analytics (hereafter GA) uses "cookies" (see above), text files stored on the user's computer, to analyze user interactions created on the website. These cookies collect information about how the site is used, such as which pages were visited, where the user clicked, how many pages were accessed, the duration of each visit, and any errors encountered. While using GA services, the website operator does not collect personal data, does not store your name or address, and the collected data cannot identify you. These cookies cannot – and do not intend to – specifically identify visitors (even the IP address used is only partially recorded until you consent to the use of statistical cookies). The information about website use stored in "cookies" is transmitted and stored on Google's servers in the USA. This website has activated the anonymization of IP addresses, thus the user's IP address is shortened and anonymized by Google in the member states of the European Union or in other contracting states of the European Economic Area as early in the data collection process as possible.

Google processes this information on behalf of the website operator to evaluate the visiting habits of users, compile reports on website usage frequency, and perform further services related to usage for the operator. Nevertheless, you can decide at any time to disable the analytical cookies that monitor anonymous browsing activities on the website.

Cookie storage can be prevented by setting the browser software accordingly. By clicking the link, you can get more information on how to disable specific cookies:

<https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=hu>

Visitors who do not want GA to report on their activities on this site can install the GA so-called opt-out browser extension. This add-on instructs GA not to send visit information to Google. If you want to disable GA web activity, visit the Google Analytics opt-out page and

install the add-on for your browser. For more information on installing and removing the add-on, refer to the help section of your browser!

Please note that the opt-out browser extension only runs on the browser and computer used for the download; after downloading, do not deactivate or delete the opt-out add-on, otherwise, your browser will reset itself and GA application will become operable again. Data collection through Google Analytics can also be prevented. In this case, an "Opt-Out-Cookie" will be placed on your computer to prevent the collection of future visit information.

#### 4.2.4. "Remarketing" Cookies

The website operator uses Google AdWords advertising services (known as remarketing cookies) to increase visitor numbers. These allow targeted advertisements to be displayed to visitors of the site if they have previously browsed this website while logged into their Gmail accounts. Google AdWords is Google's pay-per-click advertising system, which displays personalized advertisements to internet users based on their search and browsing habits.

Remarketing is a marketing procedure that enables us to display personalized advertisements to users who have visited our website, even after they have left our site, at a later time while browsing. The remarketing service is provided by Google partly through the cookies described above.

These cookies do not link to personal data. The display of advertisements is performed by Google AdWords based on your further browsing habits. If you do not wish to see such advertisements, you can disable them on the following page: Google Settings or Google Analytics opt-out.

Google's privacy statement can be viewed at the following link: <http://www.google.com/intl/hu/policies/privacy/>. The cookies used by Google Adwords can also be disabled in Google's ad settings manager according to the instructions found there. For more information: <https://support.google.com/ads/answer/2662850?hl=hu>

#### 4.3. Cookies Necessary for Website Function

<b>Legal Basis for Data Processing:</b>	The Data Subject's consent, the Data Controller's legitimate interest.
<b>Scope of Data Subjects:</b>	Website visitors.
<b>Scope of Processed Data:</b>	PHPSESSID, accept_cookies
<b>Purpose of Data Processing:</b>	To enable comfortable, personalized browsing by the user. Identification of the user, identification of each session, identification of devices used for access. Ensuring the proper functioning of the website.
<b>Duration of Data Processing:</b>	For session cookies, for the duration of the website visit. For usability-enhancing cookies, for 6 months or until the cookie is deleted.

#### 4.4. Cookies for Statistical Purposes

<b>Legal Basis for Data Processing:</b>	The Data Subject's consent.	
<b>Scope of Data Subjects:</b>	Website visitors.	
<b>Scope of Processed Data:</b>	_ga, _gid, _gat, gac_ <property-id>	
<b>Purpose of Data Processing:</b>	Collecting information about how the visitor uses the website.	
<b>Duration of Data Processing:</b>	_ga	Based on settings or by default, 2 years.
	_gid	Based on settings or by default, 24 hours.
	_gat	Based on settings or by default, 1 minute.
	_gac_ <property-id>	Based on settings or by default, 90 days.

#### 4.5. Cookies for Statistical and Advertising Purposes

<b>Legal Basis for Data Processing:</b>	The Data Subject's consent.	
<b>Scope of Data Subjects:</b>	Website visitors.	
<b>Scope of Processed Data:</b>	Google Adwords conversion code, Google Adwords remarketing code, Google Analytics remarketing function, Facebook conversion code, Facebook remarketing code.	
<b>Purpose of Data Processing:</b>	Displaying relevant advertisements, creating and storing identifiers.	
<b>Duration of Data Processing:</b>	Depending on the cookie, for 90 days, 18 months, or 2 years.	

## V. Storage and Security of Data

The Data Controller takes all necessary security steps and organizational and technical measures to ensure the highest level of protection of personal data and to prevent unauthorized modification, destruction, and use of the data.

The Data Controller primarily manages personal data on a properly constructed and protected computer system. During the operation of the computer system, it ensures an appropriate level of information security attributes for the data stored, processed, and transmitted, such as:

- **Integrity:** the originality and immutability of the data are ensured;
- **Confidentiality:** only those authorized, and only to the extent of their authorization, can access the data;
- **Availability:** the data is accessible and available to the authorized persons within the expected availability timeframe. The necessary IT infrastructure is operational and available.

The Data Controller protects the managed data with a structured system of information security measures. The Data Controller designs and operates the system of protection measures and the protection levels of individual measures in proportion to the risks arising from the threats to the data being protected. The protective measures primarily aim to prevent accidental or intentional deletion,

unauthorized access, malicious and bad-faith publication, accidental exposure, data loss, and data destruction.

The Data Controller stores personal data on an integrated computer system. All personal data affected by data processing listed in this policy is stored in the databases of various software. The geographical, physical locations of these databases depend on the specific software and storage locations:

**Hosting Provider:**

Company name: Rackforest Zrt.,

address: Budapest, Victor Hugo u. 11-5. emelet, 1132

website: [www.rackforest.com](http://www.rackforest.com)

## **VI. Data transfer, data processing, and the circle of persons who have access to the data.**

The Data Controller does not use personal data for purposes other than those specified. Personal data is only transferred to third parties with the prior and informed consent of the Data Subject. This does not apply to potential mandatory data transfers required by law, which can only occur in exceptional cases. Before complying with any requests for data from authorities, the Data Controller examines the legal basis for the data transfer for each piece of data to ensure it is valid.

The Data Subject, based on Section 14 of the Info Law, may request information about the processing of their personal data, and may request the correction, deletion, or blocking of their personal data, or may object to the processing of their personal data as provided for in Section 21.

## **VII. Rights Related to Data Processing and Their Enforcement**

### **7.1. Right to Information and Access**

The Data Subject may request in writing from the Data Controller to be informed about:

- Which personal data of theirs is being processed,
- On what legal basis,
- For what purpose of data processing,
- From what sources,
- For how long,



- To whom, when, and under what legal basis the Data Controller has provided access to their personal data or to whom it has been transferred.

The Data Controller must fulfill the Data Subject's request within no more than 15 (fifteen) days, via an electronic or postal letter sent to the contact information provided by the Data Subject.

The Data Controller may ask the Data Subject to specify the content of the request prior to fulfilling it, to precisely indicate the requested information or data processing activities.

If the Data Subject's right of access, as mentioned in this section, adversely affects other people's rights and freedoms, such as business secrets or intellectual property of others, the Data Controller is entitled to deny fulfilling the Data Subject's request to a necessary and proportionate extent.

If the Data Subject requests multiple copies of the information, the Data Controller is entitled to charge a reasonable fee proportional to the administrative costs of making each additional copy.

If the Data Controller does not process the personal data specified by the Data Subject, it must inform the Data Subject in writing.

## **7.2. Right to Rectification**

The Data Subject may request in writing that the Data Controller rectify any of their personal data that is inaccurate, incorrect, or incomplete. In this case, the Data Controller must immediately, but no later than 5 (five) days, correct or complete the specified personal data or, if compatible with the purpose of data processing, supplement it with additional personal data provided by the Data Subject or a statement attached to the managed personal data. The Data Controller must notify the Data Subject of this via an electronic or postal letter sent to the contact information provided.

The Data Controller is exempt from the obligation to rectify if:

- Accurate, correct, and complete personal data are not available, and the Data Subject does not provide them,
- The authenticity of the personal data provided by the Data Subject cannot be conclusively established.

## **7.3. Right to Erasure**

The Data Subject may request the Data Controller in writing to erase their personal data. The Data Subject must submit the request for erasure in writing and specify which personal data they wish to have erased and for what reason.

The Data Controller must reject the erasure request if any law obligates the Data Controller to retain the personal data. If there is no such obligation, the Data Controller must fulfill the Data Subject's request within no more than 15 (fifteen) days and notify the Data Subject via an electronic or postal letter sent to the contact information provided.

## **7.4. Right to Restriction**

The Data Subject may request in writing that the Data Controller restrict the processing of their personal data. The restriction lasts as long as the reasons specified by the Data Subject necessitate the storage of the data. For example, the Data Subject may request the restriction if they believe that

the Data Controller has unlawfully processed their personal data, but it is necessary for the Data Subject's personal data not to be erased for the duration of a legal or judicial procedure initiated by them. In this case, the Data Controller will continue to store the personal data until the authority or court acts upon it, after which the data will be erased, and the Data Subject will be notified via an electronic or postal letter sent to the contact information provided.

## **7.5. Right to Restriction of Processing**

The Data Subject may request in writing that the Data Controller restrict the processing of their personal data. During the period of restriction, the Data Controller, or a data processor acting on its instruction or authorization, may perform operations other than storage on the restricted personal data only if it is done for the purpose of enforcing the Data Subject's legitimate interests or as specified by law.

The Data Subject can request restriction of data processing when:

- The Data Subject contests the accuracy, correctness, or completeness of the personal data processed by the Data Controller or Data Processor, and the accuracy, correctness, or completeness of the personal data cannot be conclusively established (for the duration needed to clarify the existing doubts),
- Data erasure would be applicable, but based on a written statement from the Data Subject or information available to the Data Controller, it can be reasonably assumed that erasing the data would harm the Data Subject's legitimate interests (for the duration that the legitimate interest justifying the omission of deletion exists),
- Data erasure would be applicable, but the data must be retained as evidence during proceedings conducted by or involving a public authority (until the investigation or procedure is concluded).

In case of restriction, the personal data can only be processed, apart from storage, with the consent of the Data Subject or for the establishment, exercise, or defense of legal claims, or for the protection of the rights of another natural or legal person, or for important public interest of the Union or a Member State.

The Data Controller will inform the Data Subject in advance about the lifting of the restriction of data processing.

After fulfilling the request for enforcement of the Data Subject's right to restriction, the Data Controller must promptly inform those persons with whom the Data Subject's personal data have been shared, provided that this is not impossible or does not require disproportionate effort from the Data Controller. Upon the Data Subject's request, the Data Controller must inform them about these recipients.

## **7.6. Right to Remedy**

### **7.6.1. Dispute Resolution with the Data Controller**

The Data Subject can submit their objections and requests concerning the processing of their personal data to the Data Controller verbally by phone at the following number: +421 908 338 858, or in writing, either personally, through a representative, by post, or via the following email address: [oliver.arany@aerisoul.com](mailto:oliver.arany@aerisoul.com). Additional contact details of the Data Controller can be found in section I.

### **7.6.2. Right to Lodge a Complaint**

If the Data Subject is unable to satisfactorily resolve their objections, complaints, or requests with the Data Controller, or if they believe that their personal data has been processed in a way that infringes their rights, or there is an imminent risk of such infringement, they have the right to file a complaint with the National Authority for Data Protection and Freedom of Information.

**Contact details of the National Authority for Data Protection and Freedom of Information:**

Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c. Mailing address: 1530 Budapest, Pf. 5

Phone: +36(1)3911400

Fax: +36(1)3911410

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

Website: [naih.hu](http://naih.hu)

### **7.6.3. Right to Judicial Remedy (Right to Initiate Legal Proceedings)**

Independently of their right to lodge a complaint, the Data Subject has the right to go to court if the processing of their personal data violates their rights under the GDPR or the Info Act.

Legal proceedings against the Data Controller, who has a domestic place of business, can be initiated in Hungarian courts.

The Data Subject may initiate legal proceedings at the court of their residence. The contact details of the courts in Hungary can be found at: <http://birosag.hu/torvenyszekek>

## **VIII. Other Information**

### **8.1. Enforcement of Rights Related to Personal Data After the Death of the Data Subject**

Within five years after the death of the Data Subject, the rights that the deceased had in their lifetime can be exercised by a person authorized by the Data Subject through an administrative arrangement or a statement made to the Data Controller (in a public document or a private document of full probative value). If the Data Subject has not made such a statement, the rights that the deceased had in their lifetime can be exercised by a close relative of the Data Subject under the Civil Code within five years of the Data Subject's death (if there are several close relatives, the relative who first exercises this right is entitled to enforce these rights).