

## PRIVACY NOTICE

Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation, hereinafter referred to as “**GDPR**”) and to Hungarian Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, MOL Nyrt. (hereinafter referred to as „**MOL**” or „**controller**”) provides you – as the data subject with regard to the processing carried out by MOL in connection with its whistleblowing system – with the following information.

Contact details of the controller: registered office: HU-1117 Budapest, District XI, Dombóvári street 28 , website: [www.mol.hu](http://www.mol.hu), e-mail: [info@mol.hu](mailto:info@mol.hu); telephone number: +36 1 209-0000

### **Purposes of the processing and principles of the ethics procedure:**

The primary purpose this Privacy Notice is to provide a description of the data processing activities carried out in connection with the procedures aimed to ensure that people adopt the particular courses of conduct as defined in MOL Group’s Code of Ethics and Business Conduct and in MOL Group’s Business Partner Code of Ethics, and a description of the data processing carried out when responding to ethical questions and investigating possible violations of the rules of conduct as well as during proceedings of the Ethics Council, the Group Ethics Officer and local Ethics Officers.

In procedures, each participant is required to act in compliance with the criteria of objectivity and impartiality, in accordance with the rules laid down in the Code of Ethics and Business Conduct and the Business Partner Code of Ethics, and adopt a course of conduct that is in line with the principles of good faith and fairness.

In order to protect the personal data of people involved in cases reported via the whistleblower channel, any document prepared or made available shall be treated confidentially, unless otherwise provided for in this Notice.

The Rules of Procedure of MOL Group’s Ethics Council lay down the roles and responsibilities of people involved in procedures aimed to ensure that people adopt the particular courses of conduct as defined in MOL Group’s Code of Ethics and Business Conduct and MOL Group’s Business Partner Code of Ethics – including those involved in whistleblowing management and whistleblower protection as defined in Hungarian Act XXV of 2023 about complaints, reports in the public interest, and rules related to reporting abuses in the section on whistleblowing systems operated by employers –, and also set out rules for responding to ethical issues, for investigating possible violations of the rules of conduct, and for the proceedings of the Ethics Council, the Group Ethics Officer and local Ethics Officers.

In order to protect the personal data of people involved, any document prepared or made available in the course of ethics procedures shall be treated confidentially, unless otherwise provided for in this Notice.

Any people involved in ethical issues (Members of the Ethics Committee, Group Ethics Officer, local Ethics Officer, other investigators, whistleblower, person who is the subject of a whistleblowing allegation, witness, experts, etc.) are required to treat all pertinent information confidentially. This shall not cover the right of defense and the right to clarification of the facts of the person who is the subject of a whistleblowing allegation; however, in exercising his or her rights, the person who is the subject of a whistleblowing allegation shall act in compliance with the laws, and among other things, respect personality rights and the right to informational self-determination.

**Description of the processing activity:**

Within the framework of the internal whistleblowing system, information regarding illegal or suspected illegal acts, or omissions, or other abuse can be reported.

Whistleblowers can report

by completing a form on the “Speak-Up!” website (<https://molgroup.info/en/about-mol-group/speak-up> or <https://mol.hu/hu/molrol/etika-es-megfeleles/speak-up/>).

When the form is submitted, an automatic e-mail is generated and sent to [speakup@molgroup.info](mailto:speakup@molgroup.info).

Whistleblowers have the option to submit their report anonymously. Where the non-anonymous option is chosen, after reviewing the whistleblowing report, MOL Group will notify the whistleblower of the decision and the outcome of the investigation. MOL’s Ethics Council decides on whistleblower reports, where necessary, after conducting an investigation of the issue or complaint and gathering evidence from persons and/or entities inside or outside of MOL Group. Throughout the process, the contact details of the whistleblower and the entire content of the report are only accessible to the organizational unit responsible for conducting investigations, and accordingly, the records of whistleblowing reports are protected by access control and stored separately from other systems of MOL.

Whistleblowing report and documents generated during the related investigations may include personal and special personal data relating to natural persons.

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

“Sensitive personal data” means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The detailed Rules of Procedure of MOL’s Ethics Committee are available at the following link:

[https://mol.hu/images/pdf/A\\_MOL\\_rol/Beszallitoi\\_kozpont/etikai\\_kodex/et\\_eljarasrend\\_20180720\\_hun.pdf](https://mol.hu/images/pdf/A_MOL_rol/Beszallitoi_kozpont/etikai_kodex/et_eljarasrend_20180720_hun.pdf)

Description and purpose of the data processing	Legal basis of the data processing	Scope and source of the processed personal data	Duration of the data processing	Recipient of data transfers	Processor and its processing activity
<b>Operating a whistleblowing system, investigations of complaints and reports, consequence management</b>	<b>In the case of a company employing at least 50 persons in the framework of a legal relationship aimed at employment, the data processing is in</b>	1. Where the whistleblowing is not made anonymously: <ul style="list-style-type: none"> <li>Personal data (name, e-mail address, postal address, telephone number) of the</li> </ul>	Where, based on the investigation, a report is unfounded or no further action is required, any data relating to the report should be erased within 60 days of the completion of the investigation.	A subsidiary belonging to MOL Group involved in the investigation of the report, as well as a whistleblower protection lawyer or other external persons and	<b>Artificial Group Kft.</b> As a contractual partner of MOL Plc., Artificial Group Kft. is in charge of the operation of the <a href="http://www.molgroup.info">www.molgroup.info</a> website, and thus of the whistleblowing interface.

	<p><b>order to fulfill legal obligation based on Article 6(1)(c) and Article 9(2) (g) of GDPR.</b></p> <p>The legal obligation is based on XXV of 2023 law on complaints, reports in the public interest, and rules related to reporting abuses (hereinafter: Whistleblower Act) Section 18 (1).</p> <p>In the case of a company that does not employ at least 50 people in the framework of a legal relationship aimed at employment, GDPR Article 6 (1) f) and Article 9, (2) points g) applies: the data processing is based on the legitimate interest of the data controller.</p>	<p>whistleblower</p> <ul style="list-style-type: none"> <li>Personal data of the person against whom the whistleblowing report was made and of any other data subject possessing relevant information regarding the case (for example witness).</li> <li>Content of the whistleblowing report; any other personal data provided in the description.</li> </ul> <p>2. Where the whistleblowing is made anonymously:</p> <ul style="list-style-type: none"> <li>Personal data of the person against whom the whistleblowing report was made and of any other data subject concerned by the whistleblowing.</li> <li>Content of the whistleblowing report; any other personal and sensitive data provided in the description.</li> </ul>	<p>If a measure is taken based on the investigation - including the initiation of a legal procedure or a labor law consequence against the Reporter - the data related to the report can be processed within the framework of the reporting system:</p> <ul style="list-style-type: none"> <li>for 3 years, in case of an employee, based on Section 286 (1) of the Hungarian Labor Code</li> <li>for 5 years, in other cases, based on the Hungarian Civil Code 6:22 Section (1).</li> </ul> <p>If a measure is taken based on the investigation - including the initiation of a legal procedure or a labor law consequence against the Reporter - the data related to the report may be processed within the framework of the reporting system until the final conclusion of the proceedings initiated on the basis of the report.</p>	<p>organizations.</p> <p>According to Section 6 (4) of Whistleblower Act: If it becomes obvious that the complainant or the whistleblower in the public interest has provided false data or information in bad faith and</p> <p>a) a circumstance indicating the commission of a crime or violation of regulations arises, the personal data must be transferred to the body or person authorized to conduct the procedure,</p> <p>b) it is reasonably probable that illegal damage or other rights violations to others was caused, the personal data must be transferred upon request to a body or person authorized to initiate or conduct the procedure.</p>	<p><b><u>KMAK Kelet-Magyarországi Adatközpont Szolgáltató Kft.</u></b></p> <p>A contractual partner of MOL Plc, in which role KMAK takes care of the operation of the website <a href="http://www.molgroup.info">www.molgroup.info</a>, including the whistleblower interface.</p> <p><b><u>Greenroom Kft. Servergarden Kft.</u></b></p> <p>As a contractual partner of MOL Plc., Greenroom Kft. is in charge of the operation of the <a href="http://www.mol.hu">www.mol.hu</a> website. Servergarden Kft. is a contractual partner of Greenroom Kft. and operates the servers hosting the <a href="http://www.mol.hu">www.mol.hu</a> website, and thus the whistleblowing interface, as the sub-processor of Greenroom Kft.</p> <p><b><u>MOL GBS IT Magyarország Kft. .</u></b></p> <p>The company is responsible for providing IT and hosting services closely related to the processing.</p> <p>The system sends an automatic notification to <a href="mailto:speakup@mol.hu">speakup@mol.hu</a>; only the Ethics Officer and their deputy has access to this electronic mailbox.</p>
--	--	---	--	--	---

<p><b>Legal claims related to the complaint or report asserted by the data controller or the data subject.</b></p>	<p>GDPR Article 6 (1) point f) - data management is necessary to assert the legitimate interests of the data controller.          Legitimate interest: legal enforcement on the part of the data controller based on Article 17 (3) e) of the GDPR or successful defense in a possibly initiated legal dispute or official procedure (e.g. court proceedings initiated by the data subject, official or out-of-court proceedings, etc.).</p> <p>Upon individual request, additional information about the conducted interest assessment tests can be provided.</p>	<p>As defined above.</p>	<p>As defined above.</p>	<p>The recipients of the data transfer may be courts and authorities involved in the procedure.</p>	<p>As defined above.</p>
--	--	--------------------------	--------------------------	---	--------------------------

**Name, address, telephone number, website (where the data protection information is available) and e-mail address of data controller(s):**

MOL Plc headquarters: 1117 Budapest, Dombóvári út 28. XI., website: [www.mol.hu](http://www.mol.hu), contact: [info@mol.hu](mailto:info@mol.hu); telephone number: +36 (1) 209-0000

In case of subsidiaries other than the INA Group, MOL Plc performs the tasks related to the operation of the whistleblower system and the investigation of complaints and reports (in cooperation with local ethics officers).

In the event of a complaint or report concerning a subsidiary company other than INA Group, the relevant subsidiary company is considered a data controller in terms of its participation in the investigation and the legal consequences applied as a result of the investigation.

In these cases, the data controllers are considered joint data controllers, in the framework of which the purpose and framework of the data management are jointly determined, and they are jointly responsible for the data management. The data controllers have a common data protection information sheet.

Data may be transferred to courts and authorities (data protection authorities, tax authorities, police, etc.).  
Recipients outside of MOL Group are independent data controllers.

**Contact person(s) of the controller(s):**

MOL Plc – Dr. Petra Kunszt (Group Ethics Officer) e-mail: [pkunszt@mol.hu](mailto:pkunszt@mol.hu)

**Contact information of the controller's Data Protection Officer:**

MOL Plc – [dpo@mol.hu](mailto:dpo@mol.hu)

**Controller's personnel who are authorised to access the data:**

The Group Ethics Officer and the experts supporting him or her in whistleblowing management and investigations, Members of the Ethics Council, Group Strategic Operations and Corporate Development Director.

In the course of the management of a specific whistleblowing report and the related investigation, personal data may be transferred to a MOL Group company or a third party involved in the case, solely for the purposes of investigating and solving the case and only to the extent necessary to follow up on the legal consequences, while maintaining the safeguards (preservation of anonymity, strictly limited access to the details of the case within the individual companies, etc.) granted during the whistleblowing procedure. The recipients of such transfers of data are considered to be controllers.

**Name, registered office, telephone number and website (where the privacy notices are available) of the processors and of other recipients processing the data; name and contact details of the Data Protection Officers:**

**Artificial Group Kft.** (Registered office: 1053 Veres Pálné utca 9. 1/2., +36 70 385 8249, <https://www.artificialgroup.com>) Fazekas Péter, +36 30 221 3207, [peter@artificialgroup.com](mailto:peter@artificialgroup.com)

**KMAK Kelet-Magyarországi Adatközpont Szolgáltató Kft.** (Registered office: 5000 Szolnok, Szapáry street 20. 3. em. 6., +36 1 556 63 68, <https://www.kmak.hu>) <https://www.kmak.hu/adatvedelmi-es-adatkezelesi-tajekoztato>

**Greenroom Kft.** (Registered office: HU-1125 Budapest, Felső Svábhegyi út 12, + 36-1-315-0996, [www.greenroom.hu](http://www.greenroom.hu)) András Békássy, + 36 30 646 6012, [bekassy.andras@greenroom.hu](mailto:bekassy.andras@greenroom.hu)

**Servergarden Kft.** (Registered office: HU-1023 Budapest, Lajos utca 28-32, +36 1 432 3133, [dpo@servergarden.hu](mailto:dpo@servergarden.hu), <https://www.servergarden.hu>)  
István Szekeres , +36-1-432 3133, [dpo@servergarden.hu](mailto:dpo@servergarden.hu)

**MOL GBS IT Magyarország Kft.**(HU-1117 Budapest, Budafoki út 79.)

**Persons at the processor who are authorized to access personal data:**

Staff engaged in server and system operation.

**Data transfers to third countries:**

Where necessary for handling a case (e.g. the whistleblowing report is associated with a MOL Group company established in a third country), to the required extent, personal data (for example: information necessary to clarify the facts, investigation documents, etc.) may be transferred to a third country.

According to Section 26 (5) of the Whistleblower Act: the transfer of data handled within the framework of the internal whistleblowing system to a third country or to an international organization may take place only in the case of a legal commitment made by the recipient of the transfer to comply with the reporting rules contained in this law and taking into account the regulations on the protection of personal data.

In view of the above, personal data are also processed by MOL Group companies established in countries outside the EU that do not ensure an adequate data protection level in their national law as defined by GDPR. In view of this commitment referred to in Section 26 (5) of the Whistleblower Act, MOL Plc and the respective subsidiary apply binding corporate rules (Binding Corporate Rules) for data transmission to third countries and enter into a model contract that ensures an adequate level of protection of personal data. In such a case, the controller shall comply at all times with the provisions of Chapter V of the EU General Data Protection Regulation (GDPR).

**Whether or not automated individual decision-making is carried out (including profiling):**

No automated decision-making takes place in the course of the processing.

**Data security measures:**

<b>Information security management system</b>	Ensuring the confidentiality, integrity and availability of organizational information by introducing policies, processes, process descriptions, organizational structures, software and hardware functions.
<b>Physical access</b>	Ensuring the protection of physical devices that contain data relating to MOL Group.
<b>Logical access</b>	Ensuring that only approved and authorized users have access to data used by MOL Group companies.
<b>Data access</b>	Ensuring that only persons authorized to use the systems have access to MOL Group company data.
<b>Data transmission / storage / destruction</b>	Ensuring that MOL Group corporate data cannot be forwarded, read, modified or deleted by unauthorized persons during data transmission or storage. In addition, the immediate deletion of MOL Group's corporate data must be ensured when the purpose of the processing ceases.
<b>Confidentiality and integrity</b>	Ensuring that during the processing of MOL Group's corporate data, the data is handled and updated in

	a confidential manner, as well as in order to preserve its integrity.
<b>Availability</b>	Ensuring that MOL Group's corporate data is protected from accidental destruction or loss, and in the event of these consequences, timely access to the relevant MOL Group's corporate data and its restoration.
<b>Data separation</b>	Ensuring that the data of MOL Group companies is handled separately from the data of other customers.
<b>Incident management</b>	In case of any violation of MOL Group's corporate data, the impact of the violation should be minimized and the owners of MOL Group's corporate data should be notified immediately.
<b>Audit</b>	Ensuring that the processor regularly tests, examines and evaluates the effectiveness of the technical and organizational measures outlined above.

**Right to information:**

Where the controller processes personal data concerning you, it must provide you information concerning the data relating to you – even without your special request to that effect – including the main characteristics of the data processing, such as the purpose, legal basis and duration of the processing, the name and address of the controller and its representative, the recipients of the personal data (in case of data transfer to third countries indicating also the appropriate or suitable safeguards), the legitimate interests of the controller and/or third parties in case of a data processing based on a legitimate interest, furthermore your data protection rights and your possibilities of seeking a legal remedy (including the right of lodging a complaint with the supervisory authority), where this information is not yet available to you. The controller provides you the abovementioned information by making this privacy notice available to you.

**Right of access:**

You have the right to obtain from the controller confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and certain information related to the data processing such as the purpose of the data processing, the categories of the personal data processed, the recipients of the personal data, the (scheduled) duration of the data processing, the data subject's data protection rights and possibilities of seeking a legal remedy (including the right of lodging a complaint with the supervisory authority), furthermore information on the source of the data, where they are collected from the data subject. Upon your request, the controller shall provide you with a copy of your personal data undergoing processing. For any further copies requested by you, the controller may charge a reasonable fee based on administrative costs. The right to obtain a copy shall not adversely affect the rights and freedoms of others. The controller gives you with information on the possibility, the procedure, the potential costs and other details of providing the copy after receiving your request.

**Right to rectification:**

You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

**Right to erasure:**

You have the right to obtain from the controller the erasure of personal data concerning you without undue delay and the controller shall have the obligation to erase personal data without undue delay where certain grounds apply or certain conditions are met. Among other grounds, the controller is obliged to

erase your personal data at your request if, for example, the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; if you withdraw your consent on which the processing is based, and where there is no other legal ground for the processing; if the personal data have been unlawfully processed; or if you object to the processing and there are no overriding legitimate grounds for the processing; or if the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

**Where the processing is based on your consent, consequence of the withdrawal of your consent:**

Please note that the withdrawal of your consent shall be without prejudice to any data processing carried out based on your consent prior to the date of such withdrawal.

**Right to restriction of processing:** You have the right to obtain from the controller restriction of processing where one of the following applies:

- a) the accuracy of the personal data is contested by you, for a period enabling the controller to verify the accuracy of the personal data;
- b) the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- c) the controller no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defense of legal claims;
- d) you have objected to processing, pending the verification whether the legitimate grounds of the controller override your legitimate grounds.

Where the processing has been restricted for any of the above-mentioned reasons, such personal data shall, with the exception of storage, only be processed with your consent 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 reasons of important public interest of the Union or of a Member State. You shall be informed by the controller before the restriction of processing is lifted.

**Right to data portability:**

You shall have the right to receive the personal data concerning you, which you have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- a) the processing is based on your consent or on the performance of a contract (to which you are a party); and b) the processing is carried out by automated means.

In exercising your right to data portability, you shall have the right to have your personal data transmitted directly from one controller to another, where technically feasible.

The right to data portability may not infringe the provisions governing the right to erasure, and may not adversely affect the rights and freedoms of others.

**Right to object:**

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on the legitimate interests of the controller, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

**How to exercise your rights:**



The data controller will inform you without undue delay, but in any case within one month of the receipt of the request, of the measures taken following the request regarding your rights listed above. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months. The data controller will inform you of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request. If the data controller does not take measures following your request, it will inform you without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that you can file a complaint with the competent data protection supervisory authority (in Hungary, the National Data Protection and Freedom of Information Authority ; "NAIH") and can exercise its right to judicial remedy. NAIH contact details (address: 1055 Budapest, Falk Miksa street 9-11., postal address: 1373 Budapest, Postbox 9., Tel: +36 1 391 1400, +36 (30) 683-5969 or +36 (30) 549- 6838 Fax: +36-1-391-1410, e-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu), website: <http://naih.hu/>).

If your rights are violated, you can go to court. The lawsuit falls within the jurisdiction of the court. According to the choice of the person concerned, the lawsuit can also be initiated before the court of the place of residence or residence of the person concerned. The court may oblige the data controller to provide information, to correct, restrict or delete the data, to annul the decision made by automated data processing, and to take into account your right to protest. The court may order the publication of its judgment in such a way that the data controller or any other data controller and the violation committed by it can be identified.

You can request compensation from the data controller responsible for damages incurred in connection with illegal data processing (including the failure to take data security measures). If the data controller violates your right to privacy by illegally handling your data or violating data security requirements, you can demand damages from the data controller. The data controller is exempt from liability if it proves that the damage or the violation of the data subject's right to privacy was caused by an unavoidable cause outside the scope of data management.

The damage does not have to be compensated and no compensation can be claimed if it resulted from the intentional or grossly negligent behavior of the injured party.