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, Október huszonharmadika utca 18, website: www.mol.hu, e-mail: 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 Committee, the Group Ethics Officer and local Ethics Officers.
In ethics 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 ethical issues, any document prepared or made available in the course of ethics procedures shall be treated confidentially, unless otherwise provided for in this Notice.

The Rules of Procedure of MOL Group's Ethics Committee 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 CLXV of 2013 on Complaints and Public Interest Disclosures, 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 Committee, the Group Ethics Officer and local Ethics Officers.
In order to protect the personal data of people involved in ethical issues, 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 defence 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:
Whistleblowers can report regulatory non-compliance, raise ethical concerns or submit ethics related questions in two ways: 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/) or by telephone (+36 1 464-1725 (from an external line) or 21-725). When the form is submitted, an automatic e-mail is generated about the whistleblowing and is sent to 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. The Secretary of the Ethics Committee transcribes and keeps records of whistleblowing reports recorded as voicemail. MOL's ethical organisational unit decides on ethical issues or complaints, where necessary, after conducting an investigation of the issue or complaint and gathering evidence from persons and/or entities inside or outside the MOL Group. Throughout the process, the contact details of the whistleblower and the entire content of the report are only accessible to the organisational 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

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
Operating an ethical complaint reporting and whistleblowing system	**Article 6(1)(f) and Article 9(2)(b) and (g) of GDPR** (the processing is necessary to pursue the controller's legitimate interest). Legitimate interest: the prevention and detection of, and holding accountable the persons responsible for, irregularities that jeopardise the assets, business	1. Where the whistleblowing is not made anonymously: • Personal data (name, e-mail address, postal address, telephone number) of the whistleblower • Personal data of the person against whom the whistleblowing report was made and of any other data subject indicated in it as witness. • Content of the whistleblowing	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. Where action is taken based on the investigation, including action related to the initiation of legal proceedings or	MOL Group's and external persons and entities involved on an as-needed basis in the investigation of whistleblowing reports.	**Artificial Group Kft.** As a contractual partner of MOL Nyrt., Artificial Group Kft. is in charge of the operation of the www.molgroup.info website, and thus of the whistleblowing interface. **Greenroom Kft.** **Servergarden Kft.** As a contractual partner of MOL Nyrt., Greenroom Kft. is in charge of the operation of the www.mol.hu website. Servergarden Kft. is a contractual partner of Greenroom Kft. and operates the servers hosting the www.mol.hu website, and thus the whistleblowing interface,

	secrets, intellectual property or business reputation of the controllers as well as the creation of an adequate working environment that is based on respect and is free from fear and retaliation. (read more)	report; any other personal data provided in the description. 2. Where the whistleblowing is made anonymously: • Personal data of the person against whom the whistleblowing report was made and of any other data subject concerned by the whistleblowing. • Content of the whistleblowing report; any other personal and sensitive data provided in the description.	of a disciplinary measure against the whistleblower, any data relating to the whistleblowing may be processed in the employer's whistleblowing system at the latest until the definitive conclusion of the proceedings initiated based on a specific whistleblowing report.		as the sub-processor of Greenroom Kft. **MOL GBS IT Magyarország Kft.** The company is responsible for providing IT and hosting services closely related to the processing. The system sends an automatic notification to speakup@mol.hu; only the Ethics Officer and their deputy has access to this electronic mailbox.

Investigating and considering complaints and whistleblowing reports, taking corrective actions based on the outcome, and handling the consequences	**Article 6(1)(f) and Article 9(2)(b) and (g) of GDPR** (the processing is necessary to pursue the controller's legitimate interest). Legitimate interest: the prevention and detection of, and holding accountable the persons responsible for, irregularities that jeopardise the assets, business secrets, intellectual property or business reputation of the controllers as well as the creation of an adequate working	1. Where the whistleblowing is not made anonymously: • Personal data (name, e-mail address, postal address, telephone number) of the whistleblower • Personal data of the person against whom the whistleblowing report was made and of any other data subject indicated in it as witness. • Content of the whistleblowing report; any other personal data provided in the description. 2. Where the whistleblowing is made anonymously: • Personal data of the person against whom the	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. Where action is taken based on the investigation, including action related to the initiation of legal proceedings or of a disciplinary measure against the whistleblower, any data relating to the whistleblowing may be processed in the employer's	MOL Group's and external persons and entities involved on an as-needed basis in the investigation of whistleblowing reports.	**MOL GBS IT Magyarország Kft.** The company is responsible for providing IT and hosting services closely related to the processing.

	environment that is based on respect and is free from fear and retaliation.	whistleblowing report was made and of any other data subject concerned by the whistleblowing. • Content of the whistleblowing report; any other personal and sensitive data provided in the description.	whistleblowing system at the latest until the definitive conclusion of the proceedings initiated based on a specific whistleblowing report.		
Communicating with the whistleblower and the persons concerned by the whistleblowing report and/or third parties	**Article 6(1)(f) and Article 9(2)(b) and (g) of GDPR** (the processing is necessary to pursue the controller's legitimate interest). Legitimate interest: the prevention and detection of, and holding accountable the persons responsible for, irregularities	Where the whistleblowing is not made anonymously: • Personal data (name, e-mail address, postal address, telephone number) of the whistleblower • Personal data of the person against whom the whistleblowing report was made and of any other data subject indicated in it as witness.	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. Where action is taken based on the investigation, including action	MOL Group's and external persons and entities involved on an as-needed basis in the investigation of whistleblowing reports.	**MOL GBS IT Magyarország Kft.** The company is responsible for providing IT and hosting services closely related to the processing.

	that jeopardise the assets, business secrets, intellectual property or business reputation of the controllers as well as the creation of an adequate working environment that is based on respect and is free from fear and retaliation.	• Content of the whistleblowing report; any other personal data provided in the description. 2. Where the whistleblowing is made anonymously: • Personal data of the person against whom the whistleblowing report was made and of any other data subject concerned by the whistleblowing. • Content of the whistleblowing report; any other personal and sensitive data provided in the description.	related to the initiation of legal proceedings or of a disciplinary measure against the whistleblower, any data relating to the whistleblowing may be processed in the employer's whistleblowing system at the latest until the definitive conclusion of the proceedings initiated based on a specific whistleblowing report.		

Contact person(s) of the controller(s):
MOL Nyrt. – Dr. Orsolya Füredi (Group Ethics Officer) e-mail: ofuredi@mol.hu

Contact information of the controller's Data Protection Officer:
MOL Nyrt. – 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 and Secretary of the Ethics Committee, Group Audit & Compliance 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.

Controllers belonging to the MOL Group are considered to be joint controllers, and in this context, they determine the purposes and framework of the data processing jointly, and have joint responsibility for the processing. Each controller has its own Privacy Notice.

Any companies outside the MOL Group are considered to be independent controllers.

Data may also be transferred to the competent authorities (National Authority for Data Protection and Freedom of Information, Tax and Customs Administration, Police etc.).

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. (Székhely: 1053 Veres Pálné utca 9. 1/2., +36 70 385 8249, https://www.artificialgroup.com) Fazekas Péter, +36 30 221 3207, peter@artificialgroup.com

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

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

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

Persons at the processor who are authorised 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 concerns an ethical problem associated with a MOL Group company established in a third country), to the required extent, personal data may be transferred to a third country.

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. Having regard to the foregoing, MOL Nyrt. and the given subsidiaries will conclude a model contract that ensures an adequate level of protection of personal data with regard to the transfers of data to a third country. 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:
The controller stores your personal data in a password protected and/or an encrypted database in order to ensure the secrecy, integrity and availability of your personal data in accordance with the IT security norms and standards. Throughout the process, the personal data processed are only accessible to the organisational 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.
Within the framework of risk-proportionate protection and measuring the classification of personal and business data, the controller ensures the protection of data at a network, an infrastructure and an application level (using firewalls, antivirus software, encryption mechanisms for storage and communication – encrypted data flow cannot be decrypted without knowing the decryption code due to the asymmetric coding –, as well as using content filtering and other technical and process solutions). Data security incidents are constantly monitored and handled. Only the authorised people, as specified in the Rules of Procedure of the Ethics Committee, shall have access to personal data.

Your data protection rights:
The GDPR sets out in detail your data protection rights and the available legal remedies, as well as the restrictions thereof (in particular Articles 5, 16, 17, 18, 19, 20, 21, 22, 77, 78, 79 and 82 of the GDPR). You can request information at any time about personal data processed concerning you, you can request the rectification or erasure of your personal data or the restriction of the processing, furthermore you can object to data processing based on a legitimate interest. You also have the right to data portability. The most important provisions are summarised below.

When exercising any right related to data processing, the exercise of rights can only take place as long as this does not violate the rights and freedoms of others, also including the fulfilment of the statutory obligation to investigate ethical and whistleblowing reports received through the employer's whistleblowing system as defined in Section 15 of Act CLXV of 2013 on Complaints and Public Interest Disclosures.

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 you 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 defence 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 defence 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 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 defence of legal claims.

How to exercise your rights:
The controller shall provide information on action taken on a request based on your above-mentioned rights without undue delay and in any event **within one month** of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform you of any such extension within one month of receipt of the request, together with the reasons for the delay. If the controller does not take action on your request, the controller shall inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the competent data protection supervisory authority (in Hungary: Nemzeti Adatvédelmi és Információszabadság Hatóság /National Authority for Data Protection and Freedom of Information/, abbreviated as “NAIH”) and seeking a judicial remedy. **Contact information of NAIH: HU-1125 Budapest Szilágyi Erzsébet fasor 22/C., Tel: +36 1 391 1400, Fax: +36-1-391-1410, e-mail: ugyfelszolgalat@naih.hu, website: http://naih.hu/**

In the event of an infringement of your rights, you may file for court action. The action falls within the jurisdiction of the general courts (“*törvényszék”*). Upon the data subject’s request, the action may be brought before the court that is competent based on the domicile or the place of residence of the data subject. The court may order the controller to provide information, to rectify, block or erase the data in question, to annul a decision adopted by means of automated data-processing, or to honour your right to object. The court may order publication of its judgment in a manner that the controller or any other controllers and the infringement committed by them can be clearly identified.

You may claim compensation for damages incurred in connection with unlawful processing of your data (including the failure to take data security measures) from the controller responsible for the damage. Where any controller violates your personality rights as a result of the unlawful processing of your data or by any breach of data security requirements, you shall be entitled to claim restitution (“*sérelemdíj*”) from the controller concerned. The controller may be exempted from liability, where it can prove that the damage was caused by or the violation of the personality rights of the data subject is attributable to inevitable reasons beyond its control.
No compensation shall be paid and no restitution may be claimed where the damage was caused by or the violation of personality rights is attributable to the intentional or grossly negligent conduct of the injured party.