MOL Nyrt. hereby informs those entering the premises about the following:

1. Rules of Conduct

MOL Nyrt. considers that anyone who enters the premises agrees, by implication, to be bound by the rules set out in this document.
On the premises, audio and/or video recordings may only be made in the pre-agreed manner and in possession of a prior written authorisation issued by MOL Nyrt.
MOL Nyrt. reserves the right to ban any person committing an offence or crime in any of its facilities from the premises owned by the company, and to refuse to enter into a legal relationship with such person.

It is prohibited to bring to MOL Nyrt.'s premises any firearms, ammunition, alcohol (except for representation purposes), drugs, hallucinogenic substances, knives or daggers with a blade exceeding 8 cm length (or any objects with a risk of jab or cut injuries), poisonous, explosive, radioactive or chemical materials or any objects particularly dangerous to public security.

2. Privacy notice concerning the operation of closed-circuit video surveillance cameras

Operator of the CCTV (video surveillance) system
Cameras are operated by MOL Nyrt. as controller.
Address: HU-1117 Budapest, District XI, Október huszonharmadika utca 18
Contact information of the data protection officer: dpo@mol.hu

Data processors
Civil Biztonsági Szolgálat Zrt., address:HU-1149, Budapest, Angol utca 77, data protection officer: Nikolett KORPONAI, e-mail: adatvedelem@civil.hu, Mobile: +36 30 423 7935

In Algyő: **Bon-Sec Vagyonvédelmi Kft., address:** HU-1111 Budapest, Bertalan Lajos utca 22, Telephone: +36 72 510 630, bonsec.hu

At your request, MOL shall provide you with information about the personal data processed by the processor engaged by or on behalf of MOL, the source of the data, the purposes, legal basis and duration of the processing, as well as the legal basis and recipient of data transfers.

Scope of the personal data processed
The CCTV (video surveillance) system captures and records images of persons entering the area monitored by the cameras and the act of these people. The CCTV system does not record sounds.

Management of recordings
MOL Nyrt. uses a CCTV system for the purpose of protecting human life and physical integrity, guarding hazardous substances, protecting trade, payment and banking secrets as well as protecting property. On a case-by-case basis, it may be necessary to use the recordings in a procedure conducted by the Ethics Committee operating at MOL Group in order to investigate fraud, abuses or other ethical breaches that infringe the rules laid down by MOL Group's Code of Ethics and Business Conduct and Code of Ethics for Business Partners. The Privacy Notice of the Ethics Committee is available at the following link: https://mol.hu/hu/molrol/etika-es-megfeleles/etika/.

Legal basis for the management of recordings
Surveillance by cameras is primarily subject to Sections 30-31 of Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators.
The legal basis for management of the recordings is the legitimate interest of the controller under Article 6(1)(f) of the EU General Data Protection Regulation ("GDPR"). The balancing test concerning MOL's legitimate interest can be downloaded from the mol.hu website, or upon request, the security service will provide it.

Duration and place of storage of recordings:
Where recordings are not used, the controller will store recordings for 3, 30 or 60 days of the date of recording as detailed in the table below.

Recordings extracted from the device can be accessed on an internal server located on an official, dedicated storage space of MOL Regional Security Hungary, which is accessible only with special privileges. The storage media on which recordings are stored are located in a secure room with limited access and furnished with an alarm. Access to the recordings is limited by an electronic access control system. Any access to the digital recorders is logged.

Cameras used to make video recordings:
Depending on the area monitored, closed-circuit cameras may be grouped as follows:

No.	Area monitored by the camera	Location	Duration of storage	Legal reference
1	Incoming and outgoing traffic	Filling station	3 days	Section 31(2) of Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereinafter referred to as "Security Services Act")
2	External area and associated servicing areas	Filling station	3 days	Section 31(2) of the Security Services Act
3	Cash register(s)	Filling station	30 days	Section 31(3)(c) of the Security Services Act
4	Shop area	Filling station	3 days	Section 31(2) of the Security Services Act
5	Shop entrance from the inside/outside	Filling station	3 days	Section 31(2) of the Security Services Act
6	Fuel dispensers	Filling station	30 days	Section 31(3)(d) of the Security Services Act
7	LPG dispenser	Filling station	30 days	Section 31(3)(d) of the Security Services Act
8	PB gas storage	Filling station	30 days	Section 31(3)(d) of the Security Services Act
9	Unloading installation	Filling station	30 days	Section 31(3)(d) of the Security Services Act

10	Safe deposit box	Filling station	3 days	Section 31(2) of the Security Services Act
11	Car wash	Filling station	3 days	Section 31(2) of the Security Services Act
12	Offices	Filling station/Office building/Operational area	3 days	Section 31(2) of the Security Services Act
13	Reception facility	Office building/Operational area	3 days	Section 31(2) of the Security Services Act
14	Perimeter detection camera	Office building/Operational area	3*/30**/60*** days	* ** ***
15	Monitored passage way	Office building/Operational area	3*/30**/60*** days	* ** ***
16	Public space	Office building/Operational area	no recording takes place	---
17	Internal area	Office building/Operational area	3 days	Section 31(2) of the Security Services Act

* 3 days in an office environment as there are no technology or hazardous materials there – Section 31(2) of the Security Services Act

** In the production area, we mainly protect our technology and/or hazardous or explosive materials, and therefore recordings are stored for 30 days – Section 31(3)(d) of the Security Services Act

*** For cameras supervised by armed security guards, the storage period is 60 days – Act CLIX of 1997 on Armed Security Guards and Environmental Protection and Rural Guards.

A CCTV map sketch has been created for each object which represents the approximate locations of and areas monitored by the cameras. The CCTV map is available at each object's security services.

MOL personnel having access to the recordings

Group Security Manager, Group Operations Manager, Anti-Fraud and Investigations Manager, Anti-Fraud Expert, Regional Security MOL: Director, Operations Manager, Investigations Manager, Senior Investigations Expert, Security Investigations Expert, Regional Security Manager, Regional Security Coordinator, Technical Security Manager, Information Security Expert, Senior Security Expert, Security Expert, MOL Security Centre Operator

Use of recordings:

Recordings are accessed, i.e. data processing tasks are performed, at 6 user levels:

1. **MOL Regional Security employee as administrator** – he or she is responsible for operation of the system and maintenance of an appropriate level of protection. He or she sets the access privileges and authorises activities involving the modification of data, which no other person is entitled to carry out.

2. **Civil Zrt.'s maintenance technician** –Performs the necessary tasks at the physical location in the case of system malfunctions or changes. He or she has no right to modify the data, e.g. to delete recordings, to stop the recording or to start a new recording. He or she may perform tasks involving the modification of data by obtaining a special temporary privilege from the administrator. Once the task is completed, the administrator shall check the system and close it again. Upon MOL's instruction, the maintenance technician, as data processor, shall be entitled to extract recordings locally.

3. **MOL Regional Security's Security Managers and employees** – they are allowed to access live images by local and remote access and to view or save recordings. They are not allowed to change the settings.

4. **Armed security guard employees of Civil Zrt.** – they are only allowed to access live images and view recordings locally in order to fulfil their job duties. They are not allowed to change the settings or to extract recordings.

5. **The personnel of Civil Zrt.** (or of Bon-Sec Kft. in the Algyő region), being employees of the company engaged by MOL Nyrt. to provide property protection services, are allowed to view live images or review the recorded footage on the premises, while the personnel of the Security Centre are allowed to view live images, review the recorded footage or extract recordings by remote access.

6 **Investigators of MOL Nyrt.** or employees working in investigations manager positions are allowed to view live images by remote access, and to retrieve or extract recordings.

In cases where MOL Nyrt. initiates an ethics inquiry, members of the Ethics Committee will have access to the personal data required to conduct the procedure.

3. Entry into the object

Scope of data processed
For access control systems administered electronically: first and last name of the individual entering the premises, company name, purpose of the visit, name of the person receiving them, vehicle license plate number, badge/card number, signature, movement data

For access control systems administered in paper form: first and last name of the individual entering the premises, badge/card number, signature, name of the person receiving them, place and time of entry

Purpose of data processing
Operation of an access control system administered electronically or in paper form

Description of the processing activity
After identification by means of a photo ID document, the security service staff will record the following data: where the system is administered electronically, the first and last name of the individual entering the premises, the company they come from, purpose of the visit and the name of the person receiving them will be recorded in the electronic system; where the system is administered in paper form, the name of the visitor, number of the ID badge/access card received, signature, the name of the person receiving them and the place and time of entry. Visitors confirm with their signature that they have familiarised themselves with the Privacy Notice and received a badge (access card).

Duration and place of storage of personal data:
Within 24 hours from the entry, personal data associated with use of the badge/card will be either deleted automatically, or deleted or destroyed manually.

Legal basis of data processing
Legitimate interest of the controller (Article 6(1)(f) of the EU General Data Protection Regulation, "GDPR") The „balancing test" concerning the legitimate interest is available at the security services of each object.

MOL personnel having access to personal data

Group Security Manager, Group Operations Manager, Anti-Fraud and Investigations Manager, Anti-Fraud Expert, Regional Security MOL: Director, Operations Manager, Investigations Manager, Senior Investigations Expert, Security Investigations Expert, Regional Security Manager, Technical Security Manager, Information Security Expert, Senior Security Expert, MOL Security Centre Operator

Use of personal data stored in the access control system

Personal data recorded in the system are accessed, i.e. data processing tasks are performed, at 6 user levels:

1. **MOL Regional Security's employee as administrator** – he or she is responsible for operation of the access control system's software. Configures access privileges. Specifies the rules for setting up an access control system and verifies compliance with these rules.

2. **Civil Zrt.'s Maintenance Technician** –he or she performs the necessary tasks at the physical location in the case of system malfunctions or changes.

3. **MOL Regional Security's Security Managers and employees** – they perform their duties in accordance with the access privileges assigned to these roles through the client-side application of a pre-installed program.

4. **The armed security guard employees of Civil Zrt.** – they perform their duties in line with the instructions of MOL, through a pre-installed client-side program, in accordance with their assigned access privileges.

5. **The employees of Civil Zrt. (or of Bon-Sec Kft. in Algyő)** – as employees of the company entrusted with property protection by MOL Nyrt., they perform their duties either in the Card Office or as security guards, in line with the instructions of MOL, through a pre-installed client-side program, in accordance with the access privileges assigned to these roles.

6 **MOL Nyrt.'s Inspectors** or employees working in Investigations Manager positions – they perform their duties in accordance with the access privileges assigned to these roles, through a pre-installed client-side program.

In cases where MOL Nyrt. initiates an ethics inquiry, members of the Ethics Committee will have access to the personal data required to conduct the procedure.

4. 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. 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 infrastructural 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.

For CCTV systems: The storage media on which recordings are stored are located in a secure room with limited access and furnished with an alarm. Access to the recordings is limited by an electronic access control system. Any access to the digital recorders is logged.

For access control systems: the central database is located in a physically protected room with limited access. Access to the database is limited. The control units of entry points are tamper-proof. The database is accessed at the user level, through the client of the access control system, to which access privileges are assigned by Regional Security's MOL Administrator.
The database may also be accessed directly, for administrative and maintenance purposes, by MOL IS, Regional Security's MOL Administrator and the employees of Seawing Kft. with appropriate access privileges.
The client-side application of the access control system may only be used by persons having appropriate access privileges, a valid badge, a user name and a password. Any operations executed in the access control system's database are logged. ID badge (access card) application forms and any documents containing information related to these applications are stored in the Card Office ("*Kártyairoda*") in a locked cabinet or room. Photographs required for badge/card applications are stored in the database of the access control system.

5. 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 15-22 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. The most important provisions are summarised below.

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. In case of automated decision-making or profiling the data subject must be informed in an understandable way about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Data controller provides you with the abovementioned information by making this privacy notice 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. At 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. MOL provides 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 MOL the erasure of personal data concerning you without undue delay and MOL shall have the obligation to erase personal data without undue delay where certain grounds apply or certain conditions are met. Among other grounds, MOL 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; 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; or if the personal data have been collected in relation to the offer of information society services.

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 abovementioned 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 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. MOL shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

Your legal remedies
The controller shall provide information on action taken on a request based on your abovementioned 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 MOL does not take action on your request, it 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 Hungarian National Authority for Data Protection and Freedom of Information (*Nemzeti Adatvédelmi és Információszabadság Hatóság*, 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 MOL 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 MOL 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 (in Hungarian: "*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.

6. Activities of security guards (in Hungarian: "*személy- és vagyonőr*", literally meaning "personal and property protection guards") and armed security guards

Under Act CXXXIII of 2005, **security guards** (in charge of the protection of individuals and property) are entitled and obliged to:

1. ensure protection of the premises and of the people entering the premises, as well as of the assets, valuables and property of these people;
2. In the course of guarding a client's premises that are not considered as a public area, the security guard carrying out property protection tasks shall be entitled to:
    a) call on persons entering or present on the premises to prove their identity, communicate the purpose of their presence or prove their entitlement to be present there; where the other person refuses to do so or the information provided by them is manifestly false, to prohibit the entry or presence of the person concerned to or on the premises and call on such people to leave;
    b) call on persons entering or exiting the premises to show their baggage and/or transport/shipping documents;
    c) call on persons present on or exiting the premises to show their baggage, vehicle or cargo;
    d) call on offenders to cease their act;
    e) use an electronic property protection system;
    f) use a weapon and/or explosive detection devices to check people entering the premises and prohibit them from bringing onto the premises devices that are particularly dangerous to public security.
3. Security guards performing property protection tasks may also perform such tasks outside the guarded premises (facility), in the course of which they shall have the rights specified herein, except that electronic surveillance and monitoring systems may not be used in public areas.
4. When guarding money or valuables, transporting valuables, escorting shipments or carrying out transportation tasks, security guards performing property protection tasks shall be entitled to verify the identity of any person who is improperly preventing the transport or jeopardising the security of the guarded or transported valuables and to call on such persons to cease their act.
5. Where the conditions set out in Act CXXXIII of 2005 are met, security guards performing property protection tasks shall be entitled to call on the person affected by their intervention to prove their identity. If the person called on by the guard refuses to voluntarily and credibly prove their identity, the guard may request an authorised official to hold back the person concerned and verify their identity;
6. Security guards carrying out property protection tasks shall be entitled to call on persons caught in the act of committing a crime or an offence to cease their act, to prevent the continuation of the act, to capture the perpetrator and to take away from the perpetrator any objects that were used to commit the crime or offense in question or were obtained as a result of the same, and any means of attack. However, they shall immediately hand over the arrested person to the investigating authority competent to proceed in the case; where this is not possible, that authority shall be notified immediately. The same procedure shall apply to objects taken away from a person caught in the act of wrongdoing.
7. Security guards carrying out property protection tasks may use proportional physical restraint to:
    a) prevent an attack jeopardising the security of the guarded persons;
    b) prevent any unauthorised access to the protected premises or area and remove any unauthorised persons therefrom;
    c) remove from an event any person who is disturbing or endangering the event;

d) remove any person who is unlawfully hindering the transport of money or valuables or to prevent an attack threatening the security of a transport.

8. When on duty, security guards carrying out property protection tasks are allowed to carry chemical self-defence equipment (pepper spray), rubber baton, guard dog and, in conformity with the provisions of the applicable legislation, firearms. Such equipment may only be used in justified cases of self-defence or in absolute emergencies.
9. Security guards carrying out property protection tasks shall draw up a record of any intervention.
10. In cases where a security guard infringes any of your rights, you may lodge a complaint with MOL's customer service, as well as the competent consumer protection authority. You may file a claim for damages directly with the competent court. In the event of a criminal act, you may contact the Police or the Public Prosecutor's Office.

Where an **armed security guard** is on duty, under Act CLIX of 1997, the guard shall be entitled and obliged to:

1. ensure protection of the facility and of the people entering the premises, as well as of the assets, valuables and property of these people;
2. call on persons violating the security rules or jeopardising security to cease their act, and require them to prove their identity;
3. detain persons physically opposing to the measures or caught in the act of committing a crime or an offence in order to cease their act until the police arrive or take them to a police station;
4. take away from a person from whom the guard requested proof of identity, or a person detained or taken to the police any objects that were used to commit the crime or offence in question or were obtained as a result of the same, and any means of attack and to inspect the clothing and luggage of the person to this end.
5. in order to put an end to any act jeopardising security, by respecting the requirement of proportionality with regard to the person committing the given act:

   (a) coerce the person committing the given act (with the use of physical force) to act or to stop acting in a certain way, and/or use a muzzled service dog with or without a leash,

   (b) prevent the escape of a detained person by using handcuffs,

   (c) use a chemical or electrical discharge weapon, a rubber baton or a muzzled service dog with or without a leash to prevent an attack or break the person's resistance,

   (d) apply or use an unmuzzled and unleashed service dog or a firearm to counter an armed attack or an attack committed wearing arms against the functioning of the State or against any activities, facilities or shipments that are of key importance in supplying the population.
6. In any case, a record shall be drawn up of any intervention.