Balancing test concerning the processing of personal data through the operation of access control systems

1. <u>Legitimate interest</u> of the controller or of a third party:

- Interest of the controller:

The controller has a legitimate interest in the protection of persons and property and the confidential treatment of banking secrets, business information and personal data in its facilities. To pursue this interest, access control systems are in place, which are administered electronically and/or in paper form.

- Demonstration of the legitimacy of the interest:

The legitimacy of the processing activity can be established, since it does not conflict with any laws. Legitimacy is also supported by the fact that, pursuant to Section 31(1) of Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators, an electronic access control system may be operated on the basis of a relevant services agreement, provided that only authorised people are allowed to access to or stay in the protected area by law or based on the instructions given by the person/entity entitled to occupy the property.

In addition to the foregoing, data processing helps the controller to comply with the following statutory provisions.
Pursuant to Article 24(1) of the EU General Data Protection Regulation (hereinafter referred to as "GDPR"), taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and demonstrate that personal data are being processed in compliance with the GDPR. Such technical and organisational measures include regulation and restriction of physical access to business information and personal data, and to this end, proper identification of the staff of MOL contractors. Furthermore, under the GDPR, the controller shall ensure, in line with the "principle of data minimisation", that only those individuals may have access to personal data and confidential information that absolutely need them in order to perform their job duties.
Pursuant to Section 1(1) of Act LIV of 2018 on the Protection of Business Secrets, "business secret shall mean any fact, information or other data, or any compilation thereof, which is related to the business activity concerned and is secret – i.e. not generally known by the public, either as a whole or as a combination of its components, or not easily accessible to persons carrying out the economic activity concerned –, and therefore has a monetary value, and the holder of the secret exercises due care in order to keep it secret."
Under Subsections (1) and (2) of Section 11 of the Labour Code, "Employers shall be allowed to monitor the behaviour of employees only to the extent pertaining to the employment relationship. The monitoring conducted by the employer, and the means and methods used, may not violate human dignity. The personal life of employees may not be monitored. Employers shall inform their employees in advance concerning the technical means used for the monitoring of employees."

- The legitimate interest is sufficiently specific:

The legitimate interest is sufficiently specific, because vague and ambiguous language is avoided. Having regard to the circumstances, the most precise possible definition is provided. This is also proven by the fact that the controller has restricted the protection of persons and property and the confidential treatment of banking secrets, business information and personal data to its own facilities. Consequently, it would not be possible to provide a more precise and specific definition of the legitimate interest.

- The legitimate interest is real and present:

Given that a high number of external visitors actually and continuously visit the controller's premises, passenger traffic is considered to be exceptionally high in the controller's facilities, and thus uncontrolled access to these facilities would pose a major security risk. The above-mentioned data processing activity can thus effectively and immediately reduce the security risk posed by the high number of entries.

Balancing test concerning the processing of personal data through the operation of access control systems

- Interest of third parties and of society in relation to data processing:

Under Section M) of The Fundamental Law of Hungary ("*Magyarország Alaptörvénye*"), the country's economy is based on value-added work and the freedom to conduct a business. A pre-condition for the proper functioning of society is that enterprises can protect their business interests. In addition, some of the objects operated by the controller are considered as "national critical infrastructure components". National critical infrastructure component means an infrastructure component, designated pursuant to Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Infrastructures and Facilities, the disruption or destruction of which would have a significant impact on Hungary due to the lack of continuous fulfilment of vital societal functions. Thus, it is clearly demonstrated that the processing also serves social interests. The protection of persons and property is an interest of the whole of society, and, in the wider sense, is related to the efficient detection of crimes and to public security. The processing is also serves the protection of human life and physical integrity which can also be deemed as a social goal.

Based on the foregoing, a legitimate interest exists, and now therefore the question of necessity can be assessed.

2. <u>Necessity</u> of data processing

- **An explicit and clear demonstration of why data processing is absolutely necessary and adequate to achieve the interest:**

To achieve the legitimate interest, it is essential to control access to the facilities, since the risks to persons and property can be minimised by controlling access, so that only authorised people can gain access to the premises in a controlled manner. The use of access control systems for controlling entries and exits and the related technical solutions provide safeguards that ensure the precise identification of persons entering the premises. As a result, only authorised people can access the controller's facilities or any parts thereof.
Therefore, it can be concluded that the processing is absolutely necessary and suitable for the protection and security of persons and property located in the controller's facilities and the protection of its corporate data.

- **An assessment of whether alternative and, from the viewpoint of the individuals, less restrictive ways are available to achieve the same interest:**

No alternative and less restrictive means are currently available on the market to register and manage access authorisations and to verify the identity of people entering the premises. From the viewpoint of individuals, a less restrictive solution would be if the controller stored less personal data concerning them; however, this is not possible because only the data strictly necessary for the precise identification of the data subjects, and thus for the operation of the access control system, are processed. Both the personal data stored in the IT system and those on ID badges/access cards are necessary for the proper functioning of the access control system, and therefore the scope of the personal data processed cannot be reduced. Consequently, each of the above-mentioned data processing activities is limited to the scope of data absolutely necessary to achieve the above-identified legitimate interest in the least restrictive manner. Consequently, it can be concluded that no alternative and, from the viewpoint of the individuals, less restrictive ways are available to the controller achieve the same interest.

<u>Based on the foregoing, the processing is necessary, and now therefore the aspects of proportionality can be assessed.</u>

3. <u>Proportionality</u> assessment

3.1. An assessment the nature of the interests

- Nature of the controller's legitimate interest:

The controller's legitimate interest, namely the protection of persons and property and the confidential treatment of banking secrets, corporate and business information, given its nature, is a socially and legally

recognised interest.

- Type of the controller's legitimate interest:

The employer has a fundamental interest in ensuring an appropriate level of security for persons and property in its facilities and in protecting business secrets and confidential information concerning the company. The absence of the data processing activities in question would significantly jeopardise the controller's fundamental economic and business interest in the protection of persons and property and information security. The importance of this legitimate interest is also highlighted by the fact that the controller intends to protect "national critical infrastructure components". This confirms the high level of social support enjoyed by the controller's legitimate interest. Consequently, the legitimate interest of the controller is of vital importance because it is essential and has great social significance.

- Interest of the data subjects:

The processing of personal data impacts the data subjects' right of informational self-determination, which is derived from the fundamental right of right to human dignity. The right to human dignity – together with the right to life – enjoys absolute, i.e. unlimited, protection. Based on the settled case-law of the Hungarian Constitutional Court, certain rights derived from the right to human dignity, such as the right to self-determination in this case – and within that, the right to exercise control over one's own personal data – may be limited to the necessary extent and in a proportionate manner.

- Nature of the data:

The data processed do not include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation; i.e. they do not contain any of the special categories of personal data as defined in Article 9 of the GDPR.
It should be noted, however, that the data processed include information relating to the movements and stays of the data subjects, which are considered to be of highly personal nature, and thus it is necessary to act with caution when processing them.

3.2. Data Processing Impact Assessment

- Favourable and unfavourable impacts of data processing on the data subjects:

Even though data subjects do not explicitly benefit from the data processing, it creates the fundamental conditions for staying safely at the controller's premises, and in addition, this specific data processing activity also serves the protection of data subjects and of their personal belongings. The processing may have an adverse effect on individuals, as they not necessarily want to be photographed. However, this adverse effect is mitigated by the fact that the controller, in the operation of its electronic or paper-based access control systems, does not intend to monitor data subjects, and the data stored may not be used for this purpose. This processing activity is not capable of triggering severe or extreme emotional reactions, such as anxiety or a sense of vulnerability, as it does not intrude so deeply in the private sphere of data subjects for this to happen. This is also corroborated by the fact that the use of such access control systems is a perfectly accepted practice. Accordingly, the processing does not seriously interfere with the rights of data subjects.

- Situation of the data subjects:

Data subjects are the visitors entering a specific facility of the controller.

- Situation of the controller:

MOL Nyrt. is a member of the Budapest-based MOL Group, which was 25,000 employees in 30 countries. MOL Group is one of the major corporate groups in Central and Eastern Europe. In the light of the foregoing, it can be concluded that the controller has a significant economic power.

- **Relationship between the data subjects and the controller:**

Depending on the purpose of the visit, the controller and the data subjects may have various kinds of relationships: it is also possible that there is no legal relationship between them, or their legal relationship is indirect.

Balancing test concerning the processing of personal data through the operation of access control systems

- **The impact of processing on the data subjects in the light of their relationship with the controller:**

The processing affects and/or restricts the data subjects' right to informational self-determination, and it is mostly carried out based on an unequal legal relationship. Sometimes there is no direct legal relationship between the controller and the data subjects, and therefore the processing has more limited repercussions on the data subjects.

- **Reasonable expectations of the data subjects:**

Data subjects should reasonably expect that the controller will process their personal data in the framework of the operation of an access control system to ensure the security of its facilities. This is especially true in the light of the fact that the controller informs the data subjects in advance of the existence of an access control system and that it intends to process personal data in order to operate that system.

- **Means of data processing:**

Implementing the principles of data minimisation and purpose limitation, processing is limited to the scope of data that is absolutely necessary to achieve the legitimate interest. Any data will only be accessed, recorded and stored in order to achieve the above legitimate interest. Therefore, the controller does not couple the personal data of data subjects with information obtained from other sources, nor does it carry out profiling or disclose personal data. This way, the impacts of data processing are foreseeable and predictable to the greatest possible extent.

- **Informing data subjects about the processing:**

At the start of the processing, the controller provides full, clear and comprehensible information to the data subjects about the scope of the personal data processed, the legal basis for processing, the means and duration of the processing, as well as the rights of the data subjects related to the processing. In addition, the Privacy Notice specifies in detail the scope of people authorised to access to personal data.

3.3. Other safeguards

- Storage of personal data for a limited period of time:

Personal data are processed for the shortest possible time, taking into account any applicable legislation and the various interests. 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.

- Restricting access to data:

Personal data are made accessible strictly to those employees who need to know such data to be able to perform their job duties; the job titles of such employees are specified in the relevant Privacy Notice, which is made available to the data subjects. In addition, 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 client programs of the access control system are protected by access privileges, and are installed individually. Any operations executed in the access control system's database are logged.

- Other technical and organisational measures

Additionally, the controller stores personal data in a password protected and/or an encrypted database in order to ensure the secrecy, integrity and availability of the data in accordance with the applicable 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, anti-virus 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.

Balancing test concerning the processing of personal data through the operation of access control systems

4. Outcome and documentation of the balancing test

A legitimate interest exists
The controller's legitimate interest exists, as the lawfulness of the legitimate interest can be clearly established based on the detailed explanation above. Since it can be concluded on the basis of the foregoing that the legitimate interest is sufficiently concrete, real and present at the same time, it is correct now to assess the necessity of the processing.

The processing is necessary
To achieve the legitimate interest, it is necessary to control access to the controller's premises, since the risks to persons and property can be minimised by ensuring that only authorised people can gain access to the premises. Owing to the access control systems and technical solutions in place, the controller can ensure a high-level of access control by identifying the people entering its premises. Moreover, the controller only processes the minimum data needed to precisely identify people. Having regard to the fact that no alternative and less restrictive means are available on the market to register and manage access authorisations and to precisely verify the identity of people entering the premises, the controller is not able to achieve this specific interest in any other way. From the viewpoint of individuals, a less restrictive solution would be if the controller stored less personal data concerning them; however, this is not possible, either, because only the data that are strictly necessary for the precise identification of the data subjects, and thus for the operation of the access control system, are being processed. Consequently, it can be concluded that no alternative and, from the viewpoint of the individuals, less restrictive ways are available to the controller achieve the same interest.

Data processing imposes a proportionate limitation to the data subjects' rights

An assessment the nature of the interests
Although data processing affects the data subjects' right to informational self-determination in relation to their personal data, this right is not absolute and unlimited, and therefore it may be limited to the extent necessary and in a proportionate manner. Given that, based on the foregoing, it can be established that the processing is necessary, an assessment of proportionality is justified. The nature of the interest of data subjects shifts the balance of proportionality towards the impermissibility of data processing. However, the nature of the interest of the controller shifts the balance of proportionality towards the permissibility of data processing, for it is a legally and socially recognised interest. Given the nature of the interest of the controller and the key importance of the same, which is also underpinned by the expectations of society, the balance of proportionality is further shifted towards the permissibility of the data processing. This is further reinforced by the fact that no special categories of personal data are processed. However, the fact that the data processed include information relating to the movements and/or stays of the data subjects, which are considered to be of highly personal nature, shifts the balance of proportionality towards the primacy of the data subjects' rights.

Assessment of the impacts of data processing
The fact that data processing may have a negative emotional impact on the data subjects shifts the balance of proportionality towards the impermissibility of data processing; nevertheless, this is entirely offset by the fact that the data processing also serves the protection of the data subjects and that the controller does not use the processing to monitor the data subjects. This is further confirmed by the fact that the processing does not interfere with the individuals' private sphere to such an extent that would provoke a sense of vulnerability. The fact that the controller has a significant economic power and a dominant position, shifts the balance of proportionality towards the primacy of the data subjects' rights.

However, this is also offset by the fact that the processing does not catch individuals unawares. The fact that the controller provides detailed information about the circumstances and conditions of the processing prior to the beginning of the processing reduces the vulnerability of individuals to the smallest possible extent, and thereby shifts the balance of proportionality towards the permissibility of the data processing. Moreover, the permissibility of data processing is also supported by the fact that, due to the means used, the effects of the processing are entirely predictable.

Balancing test concerning the processing of personal data through the operation of access control systems

Other safeguards

The balance of proportionality is further shifted towards the permissibility of the data processing by the security measures implemented by the controller. The duration of the processing and access to the personal data processed are limited to what is absolutely necessary. The controller only processes personal data as long as this is absolutely necessary and permitted by the applicable legislation. Furthermore, the personal data concerned are made accessible strictly to those employees who need to know such data to be able to perform their job duties. In addition, the central database is located in a physically protected room with limited access, and the control units of entry points are tamper-proof. The client programs of the access control system are protected by access privileges, and are installed individually. Any operations executed in the access control system's database are logged. In addition to the above, the controller stores personal data in a password protected and/or an encrypted database, in accordance with the applicable IT security norms and standards. Databases are protected using firewalls, anti-virus software and encryption mechanisms (encrypted data flows cannot be decrypted without knowing the decryption code due to the asymmetric coding), as well as content filtering and other technical and process solutions. Data security incidents are constantly monitored and handled.

All these measures can actually and significantly ensure the appropriate the protection of personal data, and therefore shift the balance of proportionality towards the permissibility of data processing.

On the basis of the above, it can be concluded that the rights of data subjects do not override the legitimate interest of the controller and that the data processing constitutes a necessary and proportionate limitation to the data subjects' rights.