Meat-Land 65 Kft.

Headquarters: 2030 Érd, Sarkcsillag utca 1.

Web: www.meatland65.hu

Data Protection Regulation

Effective as of 25/05/2018

Contents

In order for the registry of the internal data management processes and to secure the rights of the persons concerned, Meat-Land 65 Kft. (hereinafter: Company or Data Controller) creates the following Data Protection and Data Safety Regulation (hereinafter: Regulation).

Data Controller title:	Meat-Land 65 Kft.
Data Controller office:	2030 Érd, Sarkcsillag utca 1.
Data Controller e-contact:	06 23 800 100
Data Controller representative:	István Orosz manager

Data protection officer: Zsófia Gergely
E-mail address: dataprotection@meatland65.hu
Phone number: 06 30 480 64 63

These regulations need to be determined in accordance with the other regulations of the Company. In case any contradictions arise regarding the protection of personal data between the requirements of these regulations and the requirements of any other regulation coming to effect before these regulations coming to effect, the current regulations are normative.

Abbreviation used in this regulation:

Infotv.	The 2011. CXII. law on the right to self-determination of information and freedom of information
Mt.	The 2012. I. law on the employment code
Mvt.	1993. XCIII. law on work safety
Ptk.	2013. V. law on the civil code
Sztv.	2000. C. law on accounting
Szvtv.	2005. CXXXIII. law on private security- and private detective activities
GDPR or Regulation	2016/679 regulation of the European Parliament (EU) and the Committee
NAIH or Authority	National Data Protection and Freedom of Information Authority

1. Regulation aim and validity

By creating the current regulation, the Company wishes to provide the realization of the right to notification determined in chapter 12. of the GDPR. 12.

The aim of this regulation is to provide sufficient notification regarding the data processed by the Company or its appointed data controller, their source, the aim of data management, its legal basis, its duration, the name, address and activity related to data management of the data controller related to data management, and the legal basis and addressee of the data transmission - in case of transmission of personal data of the concerned person -.

With the regulation, the Company wishes to provide the lawful order of the registry operations, the effectiveness of the legislative principles of data protection and the requirements of data safety, to prevent unlawful access to- and unlawful alteration and publishing of data.

The scope of the regulation extends to every process conducted by every organization unit of the Company, during which the management of personal data is realized as determined by point 1. of chapter 4. of the GDPR.

The regulation's validity period comes into effect from May 25th, 2018. Terms

- **Concerned:** any natural person defined, registered based on personal data or - directly or indirectly - identifiable.
- **Personal data**: any information regarding identified or identifiable natural ("concerned") person; a natural person is identifiable if he or she is identifiable directly or indirectly, especially based on any identification, for example name, serial number, location data, online identification or a natural person's identifiability regarding his or her physiological, genetic, intellectual, economic, cultural or social factors regarding identification.
- **Special data:**
  - data regarding racial heritage, nationality, political opinion or affiliation, faith or other philosophical beliefs, advocacy organization membership, sexual activity,
  - personal data regarding health status, harmful habits, and criminal personal data.
- **Criminal personal data:** data created related to information during or after criminal activity or relevant to the criminal procedure regarding the conduct of the criminal procedure or data created by the authorized bodies and the criminal procedure organization, or data regarding criminal history.
- **Consent of the concerned:** univocal, clear declaration of the concerned based on suitable notification, with which he or she expresses his or her consent of the data management regarding him or her according to the relevant declaration.
- **Objection:** declaration of the concerned, with which he or she expresses discontent regarding the management of his or her data and requests the termination of the data management and the deletion of the managed data.
- **Data controller:** natural or legal person, public authority, agency or any other authority determining the aims and means of personal data management, either individually or in collaboration with others; if the aims and means of data management is determined by Union or member state law, the special factors regarding the appointment of the data controller may be determined by union or member state law as well.
- **Data management:** Automated or not-automated any operation or a set of operations performed on personal data or files, as in through collection, recording, classification, sectioning, storage, alteration or modification, query, inspection, utilization, notification transfer, distribution providing availability in any form, be it synchronization or coupling, restriction, deletion or termination.
- **Data transfer:** provision of the data to a determined third party.
- **Publishing:** provision of the data for universal access.
- **Data deletion:** rendering of data unusable in a method which it is no longer retrievable.
- **Data blocking:** providing the data with an identification marking for the purpose of the permanent or temporary restriction of further management of said data.
- **Data marking:** providing data with identification mark for distinction.
- **Data termination:** Complete physical termination of the data carrier containing the data.
- **Data processing:** Carrying out the technical tasks regarding data management operations, regardless from the method and tool utilized for the operations or from the area of application, depending on the technical task being carried out on the data.

- **Data processor:** natural or legal person, public authority, agency or any other body managing data on behalf of the data controller.
- **Data file:** collection of data managed in one registry.
- **EGT-state:** member state of the European Union and other states being members of the Agreement on the European Economic Area, and states which contain citizens with rights equivalent to citizens of states based on citizens of a state being a member of the agreement regarding the European Union and its members states as well as the European Economic Area.
- **Third country:** any non-EGT state.
- **Data protection incident:** damage to safety resulting in the accidental or unlawful termination, loss, modification, unlawful publishing or unauthorized access of transferred, stored or otherwise managed personal data.
- **Restriction of data management:** marking of stored personal data for future restriction on their management.
- **Pseudonymisation:** management of personal data with the result being the data not able to inform on a relevant definitive natural person without using further information depending on this information being stored separately and secured with technical, organizational measures to make this data unable to be connected to identified or identifiable persons.
- **Biometric data:** personal data of a natural person regarding his or her physical, physiological or behavioral characteristics acquired in a manner which enables or strengthens the individual identification of the natural person, i.e. a portrait or dactyloscopic data.
- **Recipient:** natural or legal person, public authority, agency or any other authority with which (either a person or organization) information is being disclosed with, regardless of it being third party. Those public authorities which can access personal data in accordance with the union or member state rights within the framework of a specific investigation are not considered as recipients; for the goals of the data management, the public authorities' management of the aforementioned data needs to be in accordance with the utilizable data protection regulations.
- **Health data:** personal data of a natural person regarding his or her physical or psychic health, including data regarding health services containing information on the person's health.
- **Third party:** natural or legal person, public authority, agency or any other authority which is not equivalent with the concerned, the data controller, the data processor or persons appointed to manage the personal data under the direct control of the data controller or the data processor.
- **Genetic data:** personal data regarding a natural person's inherited or gained genetic characteristics which contain special information regarding the person's physiology or health status, primarily from the analysis of biological sample taken from the aforementioned natural person.
- **Representative:** natural or legal person appointed in writing by the data controller or data processor with area of activity or home address within the Union, who/which represents the data controller or the data processor regarding the responsibilities determined by the Regulation.
- **Binding company regulations:** regulation regarding the protection of personal data, which is followed by data controllers or data processors with an activity area within a

member state of the Union, regarding the transfers of personal data by data controllers or data processors within the same company groups or within collaborating companies' same groups in one or more third country.

- **Registration system:** divided personal data by any factor - centralized, decentralized, according to function or geographical factors -, available based on the determined information.
- **Profiling:** any form of automated management of personal data, during which the personal data is used for the evaluation of certain personal characteristics of a given natural person, especially regarding the analysis and prediction of performance at the workplace, economic status, health status, personal preferences, interests, reliability, behavior, place of residence or movement.
- **Relevant and justified objection:** objection submitted against the draft decision regarding the violation of the Regulation or whether the measure planned regarding the data controller or data processor is in accordance with the Regulation; the objection needs to contain the significance of the risks affecting the concerned person's basic rights and freedoms and in given cases the free flow of personal information within the Union by the draft decision.
- **Activity center:**
    - Place of central management within the Union in case of a data controller with activity areas in more than one member state, however, if the decisions on the aims and tools of personal data management are made on a different activity area of the data controller within the Union and the latter activity area bears the jurisdiction of executing the aforementioned decisions, the activity area making the aforementioned decisions is regarded as the activity center;
    - Place of central management within the Union in case of a data controller with activity areas in more than one member state, or if the data controller does not have a place of central management within the Union, then it is the data controller's area of activity within the Union, where the main data management activities are conducted in accordance with the data controller's area of activity, if the determined responsibilities are relevant to the data controller according to the Regulation.
- **Company:** natural or legal person conducting economic activity, regardless from legal form, including partnerships conducting regular economic activity and associations.
- **Company group:** the monitoring company and the companies monitored by it.
- **Supervisory authority**: an independent authority body created by a member state according to chapter 51. of the GDPR.

In case the definitions of the prevailing data protection law (GDPR during the creation of the current regulation) differ from the definitions of this regulation, the definitions set by the law are the standard.

2. Rules of data management

Hence the self-determination of information is the basic right of every natural person set in the Fundamental law; data control may only be conducted during the procedures of the Company according to the regulations of the laws in effect.

Data management is only allowed with exercising the right or for fulfilling obligations. The use of personal data managed by the Company for individual gain is forbidden. Data control needs to adhere to the principle of purpose limitation at all times.

The company only controls data for a specific goal, for the sake of exercising the right and fulfilling obligation, as minimal a rate and duration as possible for reaching this goal. The data management needs to adhere to the goal at all times - and if the goal is terminated or if the control of data is unlawful, the data is deleted. Deletion is conducted by an actual data controller employee of the Company. The deletion may be checked by a person exercising an employer jurisdiction over the employer or the data protection officer. The name and contact data of the data protection officer can be found in annex. *1/a.*

The Company may only control personal data with the prior consent of the concerned - written consent in case of special personal data - or based on law or jurisdiction by law.

Prior to recording the data, Company always discloses the aim and legal basis of the data management with the concerned.

The employees conducting data management at the Company organizational units and the employees of organizations appointed by Company taking part in the data control or conducting some activity within it are all obligated to handle the given personal information as trade secret. The persons controlling or having access to the personal data are obligated to make a ***Confidentiality statement*** *(annex no. 2.).*

If the person bound by the regulation finds out that the data controlled by the Company is false, incomplete or untimely, he or she is obligated to correct it or initiate its correction at the college responsible for the data recording.

The data protection obligations relevant to natural or legal persons conducting data processing activity by appointment of Company, or organizations without legal personality are to be validated with the data processor in a management contract. The Company and the data controller enter into ***Data processing Contract,*** as required by the GDPR (annex no. 17.).

3. Company data protection system

The respective lead manager of the Company determines the organization of data protection, the tasks and jurisdiction regarding data protection and activity relevant to data protection - all in view of the peculiarities of the Company -, and appoints the person responsible for the monitoring of data management.

The managers of every relevant independent organizational unit are responsible for upholding the requirements set in the regulation.

During their work, the partners of the Company will take ample care to prevent access to personal data by unauthorized persons, furthermore, they ensure the storage and placement of personal data in a manner which prevents unauthorized persons' access, cognition, modification or, destruction of said data.

The monitoring of the Company data protection system is conducted by the leading manager through a personally appointed data protection officer.

The data protection officer needs to be appointed by his or her competency and his or her expert-level knowledge of data protection law and practice.

Company provides the necessary sources for the data protection officer and provides an environment in which he or she is not obligated to accept any instructions from anyone during his or her tasks being carried out; he or she cannot be fired or given penalties during the performance of his or her tasks. The data protection officer is organizationally responsible directly to the leading manager of the Company.

The data protection officer organizes, controls and checks the data protection and data safety system of the Company, with the direct supervision of the leading manager. The data protection officer is the employee of the Company. The employer's rights or the rights set in the contract are exercised by the leading manager of the Company.

Leading manager's tasks regarding data protection:
a) responsible for providing the necessary conditions for the exercise of the concerned person's rights determined by the GDPR;
b) responsible for providing personal, material and technical conditions for the protection of data managed by the Company;
c) obligated to cease any possible revealed flaws or infringing conditions during the check, to initiate and to carry out the procedure for determining personal responsibility;
d) monitors the activity of the data protection officer;
e) can order an inspection;
f) publishes the Company interior regulations regarding data protection.

Data protection officer's tasks regarding data protection:
a) provides help in securing the concerned person's rights;
b) issues an annual report for the leading manager on the completion of the Company data protection tasks with the deadline of January 15th;
c) has the right to check the compliance to the current regulation at given organizational units;
d) heads the data transfer registry;
e) monitors the law changes regarding data protection and information freedoms, based on these, he or she initiates the alteration of current regulation if justified;
f) contributes to the replies of the inquiries from NAIH to the Company and during inspection and data protection administrative procedures initiated by NAIH;
g) issues a request to the NAIH for general standpoint in case the emerged data protection question cannot be answered through means of legal definition;
h) provides information and professional advice regarding the completion of the obligations recommended in the Company data protection laws;
i) Checks the accordance to the data protection laws and the Company internal regulations, including the appointment of functions, the improvement of the persons' awareness participating in data management and their training, as well as the relevant audits;
j) by request he or she provides professional advice regarding the data protection impact assessment, and monitors the completion of the impact assessment;
k) complies with NAIH;

l) acts as a correspondence point for NAIH regarding data protection cases, and consults with the Authority regarding any other questions.

Data protection incident management

Data protection incident recognition and report

Every employee of the Company – including people employed in other jurisdictions as well - is obligated to immediately report any data protection incident occurring within the Company to the manager of his or her organizational unit as well as the data protection officer. The report contains the name, phone number, post, the organizational unit name of the notifying party as well as the topic of the incident, its brief description and the fact whether the incident affects the information system of the Company.

In case the data protection incident concerns the Company information system as well, the report needs to be sent to the appointed manager of the Information system division (hereinafter: IT manager) as well.

Following the arrival of the report to the data protection officer, the data protection officer immediately commences the inspection and evaluation of the data protection incident.

Data protection incident inspection, evaluation

The data protection officer - collaborating with the IT manager in case of an incident concerning the information system - inspects the report and requests further information on the incident from the notifying party, if necessary. By the notification of the data protection officer, the notifying party is obligated to provide: the time and location of the occurrence of the data protection incident, other conditions of the data protection incident, the scope and quantity of data affected by the data protection incident, the scope and number of persons concerned with the data protection incident, the possible effects of the data protection incident, the list of actions of the prevention of the data protection incident and easing its effects.

The notifying party completes the data provision to the data protection officer at least within 24 hours if not immediately.

In case the evaluation of the data protection incident requires inspection, the data protection officer may carry out the inspection in collaboration with the IT manager and other coworkers necessary for the inspection.

The inspection needs to include information on whether the data protection incident provides a high risk on the rights and obligations of the concerned, the type of risk and whether it is necessary to inform the concerned on the incident. If informing the concerned is not necessary, the reasons for that needs to be included in the inspection as well.

By the result of the inspection, the data protection officer makes a suggestion to the manager of the organizational unit concerned with the data protection incident on the necessary actions regarding the management of the incident.

The manager of the professional field - with the agreement of the IT manager, in case of data protection incident occurring in the information system - makes a decision regarding the suggestions given for further data control or processing to be realized.

The inspection needs to be completed in 72 hours from the report arriving to the data protection officer, and the leading manager of the Company is informed by the data protection officer.

Data protection incident registry

The data protection officer keeps records on the data protection incident.

The registry includes:

- the scope of concerned personal data,
- the scope and number of persons concerned with the data protection incident,
- the time of the data protection incident,
- the conditions and effects of the data protection incident,
- the actions for prevention and
- data required in other laws.

The data protection officer provides the precise management and actualization of data protection incident registry (annex no. 13.).

Reporting the data protection incident to the Authority

The data protection officer is obligated to report the data protection incident to the Authority immediately, but at least 72 hours from the occurrence of the incident, except if the incident is regarded as without risk to the rights and freedoms of natural persons. If the report is not made within the deadline, the data protection officer is obligated to justify the reason.

The authority report needs to include:

- The scope and approximate number of data concerned with the data protection incident,
- The scope and approximate number of persons concerned with the data protection incident,
- The nature and conditions of the data protection incident,
- name and address of the data protection officer,
- the possible consequences of the data protection incident and
- the measures taken for the repair and alleviation of the data protection incident.

Notification of the concerned on the data protection incident

If - as a result of the inspection - it was accessed that the data protection incident invokes a high-level risk to the rights and freedoms of natural persons and the concerned need to be notified, the data protection officer notifies the concerned immediately and he or she notifies the leading manager of the Company of this fact. The list of persons to be notified is contained by annex. 14.

The concerned do not need to be notified if:

- the Company conducted technical, organizational and protective measures regarding the concerned data which prevent unauthorized access to- or prevent the interpretability of the data.
- if the Company has made measures following the occurrence of the data protection incident which guarantee that the revealed data management risk is not realized.
- if the notification would require a disproportionate amount of effort. In that case, the concerned need to be notified through published information, which can be conducted in electronic form as well.

Periodical training

According to point 9. of this regulation, the data protection officer guarantees education regarding data protection incidents for the goal of raising awareness, during which he or she describes and evaluates the experiences of past data protection incidents or the dangers of data protection incidents, provides information on the decrease and prevention of risks and checks the available information..

Impact assessment

In case a new data management process - regarding its nature, scope, conditions, aims - is determined as high risk regarding the rights and freedoms of natural persons, the Company conducts an impact assessment prior to the data control regarding the fact how the data management process affects the protection of personal data. Similar data management processes with similar risks may be carried out within one impact assessment.

The impact assessment is carried out by the data protection officer according to the base regulation. In case it is not conducted by him or her, the Company is obligated to request the professional advice of the data protection officer.

The Company conducts the impact assessment regarding the set of criteria set in annex. number 15 of the Company's current regulation.

Following the completion of the impact assessment he or she guarantees the inspection of the impact assessment by necessity, but at least at the point of change in risk of the data management processes, during which he or she conducts the evaluation of risks once more. The inspection of the risks needs to be conducted at least every 3 years.

Regarding the management of personal data, risk evaluation is the obligation of the data controller as well, which consists of the following steps:

- identification of risks regarding the control of personal data,
- issuing a list of risks,
- determination of the potential main reasons and foreseeable negative impacts of certain risks and
- based on these, creating preventive and corrective risk management processes.

The sources of risks need to be reveal, within which the elements of preventive and corrective aim management as well as the resource management system needs to be determined, and the objective and subjective risk elements need to be divided.
During the evaluation, the entire risk assessment system needs to be devised, within which a complete risk potential and risk priority order is realized (not equivalent to the measure system). The process and results of the assessment needs to be set in writing.

The risk potential needs to be determined from the point of likelihood:
- low
- medium
- and high likelihood of occurrence,

and regarding significance
- low
- medium
- and high significance risks.

This definition forms the basis for the future method of risk assessment regarding both the preventive and corrective procedure. The completion of the risk assessment is the obligation of the data protection officer.

Prior consultation

In case the performed impact assessment shows a possibly high risk data management process, the Company initiates a consultation with the Authority prior to the commencement of the data management process.

During the initiation of the consultation, the Company attaches the following information:
- the completed impact research,
- name and contact of the data protection officer,
- the list of tasks of the data controller(s) and data processor(s) involved in the data management process,
- the aim and method of the data management and
- the measures and guarantees taken for the protection of the rights and freedoms of the concerned.

Balance of interests

According to the provisions of the GDPR, there is a possibility of data management without consent, if some legitimate interests make it possible, if the Data controller fulfills his or her obligations of notification. During the inspection of the legitimacy of data management, points a)-f) of chapter (1) of article 6. of the GDPR are the standards.

In case the legitimacy is reported according to point f) of chapter (1) of article 6. of the GDPR, the data management process will be legitimate if it is necessary for the data controller's or a third party's legitimate interests, except if the interests or fundamental rights and freedoms of the concerned require the protection of personal data is of higher priority than said interests.

For the legitimacy of the data management, Company conducts an interest assessment test, during which the necessity of the data management's aim, inspects the proportionate restriction of the rights and freedoms of the concerned and supports it suitably.

During the interest assessment test, the Company identifies its justifiable interests regarding data control, and the concerned person's interest and the relevant base law as the counter point of the assessment. The condition of the assessment of the contradictory rights and interests is always evaluated by the Company regarding the specific conditions of the given case. During the assessment, the Company regards the nature and sensitivity of especially the controlled or to-be-controlled data, its degree of publicity, the severity of the possible infringement etc.

As a part of the interest assessment test, the Company performs the inspection of necessity and proportion as well, under which the exclusions from the protection of personal data and the restrictions on the protection need to remain within the necessary degree. The nature and quantity of the managed data cannot exceed the necessary degree for the validation of the legitimate interests. The inspection of proportionality contains the evaluation of the connection between the goals and the selected tools. The selected tools cannot exceed the degree of necessity; however, the tools need to be appropriate for reaching the determined goal.

Based on the performance of the assessment, the Company determines whether the personal data is manageable.

The concerned receive notification on the test results, which clearly lists the reasons and legal interest for the restriction to be considered proportionate, and the reason for the Company managing the data without consent of the concerned, thus why the legitimate interest of the Company for data management is a priority over the interests and rights of the concerned. The Company informs the concerned on the data protection guarantees utilized regarding the lack of consent, and the possibility of objection against data management.

The result of the assessment between the conflicting interests and rights cannot be ordered without the Company enabling a different result regarding the specifics of the given case, thus the Company conducts a separate interest assessment test in every case.
Possible script, which the Company reserves the right to differ from:
1. step: prior to the planned data management, the Company inspects whether the management of the personal data is absolutely necessary for reaching its goal: are there alternative solutions which enable the realization of the goal without personal data management.
2. step: the Company defines its legitimate interest as accurately as possible.
3. step: the Company defines the aim of the data management, and which personal data and duration of the management thereof is necessary by legitimate interest.
4. step: the Company determines the possible interests of the concerned regarding the given data management (for example, angles which the concerned might bring up against data management).
5. step: the Company performs the assessment of its legitimate interests and the interests and fundamental rights of the concerned, and based on that, it determines the manageability of the personal data. The Company determines the reasons for restricting the concerned person's rights and expectation due to the Company's legitimate interest - which is the basis for the data management -.
6. step: the Company determines the guarantees which provide the necessity-proportionality of the data management (naturally, other forms of guarantee measures may be utilized).

The Company conducts the interest assessment regarding annex 16. of this regulation.

Photocopying identity cards

The Company – in accordance with NAIH – does not issue photocopies of identity cards. Photocopies of official documents are not suitable for the identification of natural persons; hence the presence of the individual is crucial for the identification based on official documents. The official document with picture reasonably possesses standard of proof only if based on that, the Company can be certain that the person on the official document and the person showing the official document are the same. A copy of an official document does not have the standard of proof to be a legitimate copy of a valid official document.

To retain the principles of data collection and data quality, the Company however many create a masked photocopy (or scanned image - collectively: photocopy). During photocopying, the Company leaves only those parts of the official documents suitable for photocopying (to be further readable) which contain data that the concerned is obligated to issue of him- or herself anyway. In this case, the photocopy is made for the purposes of data reconciliation. The photocopy is immediately and irreversibly deleted by the Company following the comparison of the masked official document-photocopies by a coworker appointed by the Company, or within 30 days following the creation of the photocopy.

4. Data safety regulations

Physical protection

For the sake of the managed written personal data's safety, the Company utilizes the following provisions:

- the data may only be looked into by authorized persons, no other access is allowed, they cannot be disclosed with others;
- the documents are placed in an area which is well-lockable, dry, and preferably equipped with fire-protection- and private security equipment;
- Only persons with suitable jurisdiction may access the documents under continuous active management;
- The coworker of the Company conducting data control may only leave the area of data management after sealing the entrusted data carriers or closes the office;
- The coworker of the Company conducting data control seals away the paper-based data carrier after finishing his or her work;
- in case the managed paper-based personal data are digitized, the digitally stored documents are handled by the Company utilizing the standard safety regulations regarding digitized documents.

In case the aim of managing the personal data stored on paper, the Company takes measures to terminate the paper. In this case, the Company appoints an employee responsible for the termination. The employee responsible for the termination compiles the document package to be terminated involving the relevant organizational unit. A three-member termination committee is present at the termination. Annex 21 needs to be filled out regarding the termination.

In case the data carrier of the personal data is not paper but some other physical tool, the termination of the said physical tool is conducted according to the standard of terminating paper-based documents.

Information protection

For the safety of the data stored on the computer or on the network, the Company utilizes the following measures and guarantee elements:

- the computers used during data control are the property of the Company, or possesses rights equivalent to ownership over them;
- the data on the computer may only be accessed with valid, personal, identifiable jurisdiction - at least a user name and password -, the Company takes measures in case of necessary password changes;
- the data stored on the network computer (hereinafter: server) may only be accessed by specifically appointed persons with suitable eligibility;
- for the safety of the data stored on the network, the Company protects the servers with a high availability infrastructure, prevents data loss with saves and archiving;
- Conducts daily saves from the active data of the data bases containing personal data, the save relates to the complete files of the central server and is performed on to the NAS storage;
- always takes measures to provide virus protection on the network controlling personal data;
- prevents unauthorized network access using the given information technology tools.

Server safety

The flow of data controlled by the Company is realized electronically with servers and stored physically with the help of data storages. The data storages and the servers are places to an area established for this specific task. Regarding this area, an employment base needs to be established with access authorization, which are authorized to access these tools and to the possible stored data. The authorization to enter into the server room needs to be requested by the employee separately, which needs to be evaluated by the IT manager - with the agreement of the data protection officer -.

Only persons determined and exhaustively listed according to annex 19. of this regulation can enter the area designated for operating the servers and reaching the server central connections.

For the physical protection of the servers stored on the area of personal data storage (in case of utilizing a server operating service as well), the server rooms, the Company applies or demands the following measures and guarantee elements:

- the server room is climatised and equipped with a fire alarm,
- Only persons with server room key using authorization (annex 18.) may possess a key or acquire the key from the manager of the key according to the server room key management regulations,
- the Data controller keeps a registry on the persons with key using authorization,
- those who are not the employees of the Company may not possess an independent key using authorization,

- the type of the managed keys can be permanent or occasional, in case of permanent key using authorization, the owner of the authorization may possess a dedicated key,
- The respective surveillance service of the Company keeps a record on the picking up and turning in of the keys by the persons with permanent and occasional key using authorization.
- in case a person without permission for using the key or a person who is not the employee of the Company has to enter the server room in order to fulfill his or her duties, a person with key using authorization is present with him or her in the server room at all times.

Access management

The aim of access management regulation is the precise traceability of the distributed access, their storage in documented form, and to have the activities of the persons with certain access and the data used by them be verifiable. The timeliness of these data considerably helps the Company to fulfill the expected and realizable safety level and to operate the information network according to law and professional standards.
The regulation extends to the information system of the electronic surveillance systems and their connecting tools as well.

The changes of authorizations within the information system (existing authorizations, distribution, modification, termination of new authorizations) need to be documented.

For the safety of the personal data, the Company applies the following authorization management provisions:

- Principles
  - The setting of new access and the change of access is conducted by the IT manager based on the owner of the authorization, to the written request of the data protection officer
  - During the determination of the authorizations, only the authorizations required to work conduct need to be distributed.
  - Persons conducting other work or persons not requiring the ownership of authorization should not get complete access or administrator authorizations.
  - Named users with administrator authorization need to be utilized for the administration of the system in all cases, if possible. The not named system administrator passwords need to be stored in an opening-proof manner, signed. Their usage may be permitted by the leading manager of the Data controller or in case of his or her absence his or her deputy - according to the substitution regulations -. The usage of not named user authorizations needs to be justified and documented.
  - External – maintenance or development – company employee cannot possess a permanently valid indefinite access.

Access management process

The IT manager needs to send a request in email to the data protection officer by request of the owner of the authorization for access request- or change

The IT manager keeps an internal record of the access management, which is annex 22. of the regulation.

Following the email, the IT manager and/or the appointed coworker sets the access, then sends a confirmation toward the person requesting.
In case of cessation of work- or other legal status of the access owner, the data protection officer is obligated to notify the IT manager in order to delete the so-far authorized person's authorization.
In case of the cessation of the authorization, the data protection officer sends the termination request by electronic means to the IT manager, who provides the deletion of the authorization. Following this, the IT manager or an appointed coworker sends a confirmation to the persons initiating the deletion.
In case of replacement, the data protection officer is obligated to conduct the initiation of the deletion, modification of old authorizations or the inclusion of new authorizations.
The profiles of the persons exiting the information system need to be suspended, and rendered disused. The deletion of user accounts can be conducted following the inspection of the systems if the deletion does not result in data-loss.

5. Built-in data protection

The so-called privacy by design is introduced, which enables the Company to regard the provisions of the GDPR before the actual commencement of data management - for example, at the project preparation stage -. The built-in data protection is the accumulation of the internal procedures of the Company, with which - regardless of external regulations as well - it makes measures to protect its private sector as well as possible.

The protection of the rights and freedoms to which the natural persons are entitled to regarding the management of their personal data demands the suitable technical and organizational measures which guarantee the completion of GDPR demands. The aforementioned measures include the minimization of personal data management, the early pseudonymisation of personal data, the transparency of the personal data's functions and management, and the fact that the concerned may monitor the data management and the Company is able to create and further develop safety elements. The data management needs to be transparent and user-friendly; the data protection needs to be proactive, and needs to include the complete term of the data, being part of its entire process.

Regarding the status of science and technology, the costs of realization, the nature, scope, conditions and aims of data management as well as the risks with changing probability and severity, the Company applies the following suitable technical and organizational measures both during the determination of the data management method and during the data management –

a) encryption of personal data;
b) guarantee of the constant confidential nature of the systems and services for the management of personal data, their integrity, availability and resilience;
c) in case of physical or technical incident the ability to reset the access to personal data in time;
d) a procedure for the periodical testing, assessment and evaluation of the technical and organizational measures guaranteeing the safety of data management

-, which aims to effectively realize the data protection principles on one hand - for example the effective realization of data minimization -, on the other hand to incorporate the warranties into to data management process necessary for the completion of the provisions stated in the GDPR and for protecting the rights of the concerned.

The Company conducts suitable technical and organizational measure to provide the fact that by definition, only those personal data gets to be controlled which are necessary for reaching the given data management goal. This obligation refers to the quantity of the collected personal data, the degree of their management, the period of their storage and their accessibility. These measures need to especially guarantee that by definition the personal data cannot be accessed by an undefined number of persons without the interference of the natural person.

The approved certification mechanisms according to article 42. of the GDPR 42. can be used as part of evidence to the Company fulfilling the aforementioned requirements.

The Company and the data processor takes measures to guarantee that the natural persons with access to the personal data acting under the control of the Company or the data processor will only manage the aforementioned data according to Company instructions, except if union or member state rights bind them to differ from said instructions.

In case of data transfer, in case of absence of an adequacy decision, the Company or the data processor takes measures to counter-balance the third country data protection defects through providing warranties for the concerned. The warranties guarantee the adherence to the data protection requirements, and they provide rights equivalent to authorizations of data management within the European Union, including the enforceability of the concerned person's rights and the possibility of effective remedies, within these, the face that the concerned may utilize effective administrative or judicial remedies and to seek compensation within the European Union or in a third country. The warrantees are especially relevant to the relevant general principles of personal data management as well as the adherence to the principles of built-in and default data protection.

6. Mobile device management

From the point of data protection regulation, the mobile device management is an important obligation for the technical and information technology provision of the important services for the Company's conduct of business as well as data protection, i.e. the confidentiality, indestructibility and the safety frame system of the data under the ownership of the Company.

An information investment needs to be made in the Company system guaranteeing mobile management services, which need to provide the following:

- enforcement of complex password usage
- remote check of device
- remote authorization or blocking of mailing system use

7. Education and training system

The safety awareness training for the information and non-information employees of the organization needs to be regarded as a highlighted area.

Safety aware conduct may prevent serious business damages and attacks.

The suitably established IT regulation, information safety provisions and data protection, data safety regulation are not enough in itself, the employees need to be informed through systematic education and training that the established regulation system and the IT tools in themselves do not guarantee the data- and information safety for the organization, they have to contribute to that by a responsible daily conduct.
The suitable training of employees have shown to have an effect of less safety incidents following the training, which is noticeable in the areas of damages resulting from direct data loss and possible data protection fines or in financial results.

The general data protection-information safety training order of the employees need to happen annually (can be attached to other systematic training, e.g. fire- and work safety) in a period of one hour. Information and non-information employees are both included.
Persons conducting information, especially administrative tasks require a separate training regimen. The goal of this is to shake out the persons under the training from their usual workflow and to reveal the current attack view of malicious attacks and hackers, to pin point the weak spots according to the current trends and to help them decide on the preferred solutions to prevent attacks and keep the risk level low during a perceived intrusion attempt.

8. Protecting the rights of the concerned

The concerned may request information regarding the management of his or her personal data, may request the correction of his or her personal data, and - except for the data controls ordered by law - the personal data's deletion, restriction on the highlighted contacts of the Company.

The concerned reserves the right to receive the personal data regarding him or her issued for the Data controller in an articulated, widely used, machine-readable form, as well as to transfer these data to another data controller.

The Company is obligated to move the request or objection to the competent lead manager of the organizational unit handling data management within three days from receipt.

The lead manager of the organizational unit with functions and responsibilities replies to the request of the concerned person regarding the management of his or her data within 25 - in case of objection, 15 - days from submission in articulated writing.

By request of the concerned, the data controller provides information on his or her data managed by the data controller or a data controller appointed by him, their source, the aim of the data management, its legitimacy, its duration, the name and address and activity of the data controller regarding data management, the circumstances and impact of the data protection incident and the measures taken for its prevention, and - in case of transferring the concerned person's personal data - the legitimacy of the data transfer and its addressee.

Information is free of charge according to base rule, if the person requesting information has not yet submitted an information request to the Data controller in the current year regarding the equivalent data set. In other cases, reimbursements can be set. The degree of reimbursement needs to be paid back in case the data was handled in an unlawful manner or if the information request leads to correction.

The data not equivalent to the truth are corrected by the lead manager of the managing organizational unit - in case the necessary data and proving public documents are available -, in cases stated in article 17. of the GDPR, he or she takes measures to delete the managed data.
The personal data needs to be deleted, if

a) the personal data is no longer necessary for the original goal or they were managed differently;
b) the concerned cancels his or her consent for the data management and the data management has no other legitimacy;
c) the concerned objects against the data management, and there is no legitimate priority reason for data management, or the concerned objects against the data management;
d) the personal data was managed unlawfully;
e) the personal data needs to be deleted for competing the legal obligation stated in union or member state law regarding the data controller;
f) the collection of personal data of children under the age of 16 was conducted with the offering of services in connection with information society;
g) if the Data controller has published the personal data and is no longer necessary for the original goal or they were managed differently, he or she is obligated to delete them, and takes the reasonable measures regarding the available technology and the costs of realization -, to inform the data controllers managing the data that the concerned has requested the deletion of the links pointing to the aforementioned personal data, the copies or duplicates of personal data.

The concerned may object against the management of his or her data, if

- the management or transfer of personal data is necessary only to the completion of the legal obligation of the Data controller or for the enforcement of the legitimate interest of the Data controller, data importer or a third party, except for obligatory data management;
- if the use or transfer of personal data is for the means of direct business-acquirement, public survey or scientific research; and
- in any other, legally defined case.

The Data controller inspects the objection as soon as possible, but within 15 days from the submission of the request the most, makes a decision regarding its legitimacy, and informs the applicant on his or her decision in writing.

If the Data controller states the legitimacy of the concerned person's objection, he or she terminates the data management - including further data acquisition- and transfer -, blocks the data, and notifies everyone on the objection and the resulting measures, who the data regarding the objection was sent to earlier, and who are obligated to act to enforce the right to objection.

If the concerned does not agree with the Data controller's decision, or if the Data controller misses the answering deadline, the concerned may turn to court - 30 days within the publishing of the decision or from the last day of the deadline -.
If the data importer does not receive the data for the enforcement of his or her rights due to the objection of the concerned, he or she may turn to court against the Data controller for the acquisition of data within 15 days of the notification. The Data controller may file a lawsuit against the concerned as well.

If the Data controller misses the notification, the data importer may request a clarification from the Data controller regarding the circumstances in connection with the failure of data transfer, to which the Data controller is obligated to provide information within 8 days following the request of the data importer. In case of clarification request, the data importer may turn to court against the Data controller from the submission of the data importer's request, but within 15 days from the deadline the latest. The Data controller may file a lawsuit against the concerned as well.

The Data controller may not delete the data of the concerned if the data management was ordered by law. However, the data may not be transferred to a data importer if the data controller agrees with the objection or the court has determined the legitimacy of the objection.

In case during the exercise of the concerned person's rights the assessment is not univocal, the lead manager of the organizational unit managing the data may request a stance from the data protection officer by sending the case files and the viewpoint regarding the case, who completes it within three days.

The Company pays for the damages caused by the unlawful management of the concerned person's personal data or by the infringement of data safety requirements to another party, or the grievance fees for personal infringement caused by it or by the data processor. The Data controller is exonerated from the responsibility of the caused damage and the payment obligation of the grievance fee if he or she proves that the damage or the personal rights infringement of the concerned was caused by an unavoidable reason outside the scope of data management. He or she does not pay for the damages if they are a result of the willful or severe obvious negligence of the aggrieved.

The concerned may exercise legal remedy or complaint at the National Data Protection and Information Freedoms Authority (1125 Budapest, Szilágyi Erzsébet fasor 22/C.), or at the competent court according to his or her address or place of residence.

9. Data management realized in the Company

Place of data management:
Primarily, the Company office, however, the data controller - within his or her scope of service - may differ from this by informing the concerned, according to the work processes.
Under the GDPR regulation system, the data controller controls the necessary quantity and type of data required to achieve the goal during the given data managements, according to the obligations state by the principles.

Registry numbers of the data controls:

With the utilization of the GDPR, the NAIH data management processes have been ceased, switched by the registry obligation of the data controller within his or her own organization.

Data processing, data transfer:
The addressees in connection with the given data controls and the addressees of the data transfers are contained by annex 1/a. of the regulation.

9.1. Data control regarding activity

Within the scope of services, the Company conducts its activity in the following areas:

During its commercial activity, the Company manages the data set necessary for the contractual contact in the client contact system regarding the persons in contact.

During commercial activity, management of personal data in private scope of interest - primarily through the contracting company partners - a small number of data control process identification occurs.
The regulation regarding the management of the data of employees partaking in the activity is detailed under the personal case data management point.

Commercial service area: The service is conducted almost exclusively with the completion of company partner contracts, the management of personal data regarding private persons only occurs in connection with design activities and transport.

The signing and completion of contract(s) the data of natural person employees, company representatives, collaborators and contacts are published and recorded. The personal data published in connection with the contract and informing the Company as an addressee are stored regarding trade, transport of goods and other services which involve the Company profile.

data control aim: following the completion of contracts, necessary identification and the inspection of the identified persons' holder's- and issuing rights.

scope of managed data: name, address, identifying personal data of contractual partners and designated eligible persons

legitimacy of data management: completion of point b) of chapter (1) of article 6. of GDPR, and point f) of chapter (1) of article 6. of GDPR, the validation of legitimate company interest
data storage deadline: 7 closed economic year following the termination of the service contract.

data storage method: electronically and on paper

9.2. Data management regarding outstanding amounts

The management of outstanding amounts occurring at the Company is conducted by an employee and a designated lawyer. The Company sends a payment notice - or in case of its failure, based on a general agency contract of the lawyer - to the concerned with outstanding amounts.

aim of data management: data management of the persons concerned with outstanding amount for dept management purposes

scope of managed data: name, address and phone number of person with outstanding amount

legitimacy of data management: the validation of legitimate company interest according to point f) of chapter (1) of article 6. of GDPR,
data storage deadline: settlement of outstanding balance or the forfeiture of the civil rights requests regarding the outstanding balance (5 years)

data storage method: electronically

In connection with the present data management, a data management brochure was issued in annex 3. of this regulation.

9.3. Data management in connection with complaint resolution

The concerned person has the possibility to submit a complaint regarding the activity of the Company. The complaint may be submitted personally, through postal service, on the phone or through email.
The verbal complaint is immediately inspected by the Company, and remedies it if necessary. If the client does not agree with the complaint remedy, or if its immediate inspection is not possible, a record is created of the complaint, and a copy is handed to the client.

The record of the complaint contains the following:

a) name of the client;
b) client address, official office, and postal address if necessary;
c) location, time and method of the complaint proposal;
d) detailed description of the client's complaint, separately recording the objections within the complaint to have every objection within the client complaint inspected completely;
e) an account on the documents, writings and other evidence presented by the client;
f) The signatures of the person drawing up the record and the client (the latter is expected in case of personally given verbal complaint);
g) record location, date.

aim of data management: record of client complaints, management of complaints regarding commercial activity

scope of managed data: client name, client address/office, postal address, phone number, notification method, service regarding the complaint, complaint description, reason, requirement of the complainant, copies of necessary documents in the client's ownership for the support of the complaint, not in possession of the Company, other data necessary for the inspection and reply of the complaint
legitimacy of data management: consent of the concerned according to a) of (1) of article 6. of GDPR, and chapters (6)-(7) of par. 17/A of the 1997. CLV law on consumer protection

data storage deadline: The Company is obligated to retain the record of the complaint and the comply of the reply for 5 years, and to present it to the inspecting authorities by request [17/A. § (7) of the consumer protection law]

data storage method: electronic and paper

In connection with the present data management, a data management brochure was issued in annex 3. of this regulation.

9.4. Data management regarding the data of job applicants

Company application process

During the selection of applicants, the Company realizes the management of personal data.

Application may be sent to a position not advertised, in this case, the curriculum vitae are sent to the Company address hr@meatland65.hu.
The curriculum vitae of the applicants are stored by the Company electronically and on paper.

The Company HR coworker and the respective leading manager is responsible for the selection of the applicant, thus they are obligated to secure the rights of the concerned during the performance of tasks related to the present data management.

Mutual regulations regarding „arriving curriculum vitae" and workforce recruiting

The Company does not differentiate between the arrival method of curriculum vitae intended for job application (hereinafter: CV): paper-based and electronic CVs fall into the same evaluation.

According to base regulation, the Company stores the CVs for immediate and later utilization, and creates a database out of them for later vacant or available positions. The data entered into the database will be terminated 2 years later, hence after that amount of time the data will be no longer relevant for job application purposes.

Legitimacy is provided by the concerned person's consent according to a) of chapter (1) of article 6. of the GDPR regarding every CV revealed for the Company.

Consent to the data management can be cancelled, thus the concerned may cancel his or her consent according to this regulation.

Special regulations regarding the „arriving curriculum vitae"

In case of application to a non-advertised job position, the Company sends a reply to the applicant, in which it informs him or her on the data management, its legitimacy and the forms of objection against the data management. It is the annex no. 4/1. of the regulation entitled "Reply to the curriculum vitae recorded in the database".

Special regulations regarding workforce recruitment

The Company stores the CVs for later use, according to the base regulation. The CV and the personal data within are managed by the Company according to the regulation. The Company sends information regarding this fact. The text of the information is the annex no. 4/1 of the regulation.

Special regulations relevant to curriculum vitae arriving by means of recommendation

The company recognizes and regards the employment recommendation system. Any employee of the Company may recommend his or her acquaintance for a general or a designated position - in this case, the Company always has the employee make a statement (annex 4/3) on the fact that he or she possesses empowerment regarding the person concerned with the data and he or she

discloses it to the Company. This statement is kept until the storage deadline of the CV, and is terminated along with the data on the CV.

However, due to the fact that the Company can only presume the contribution of the concerned - even with a job application statement -; it always sends an information letter to the recommended person, in which it informs him or her on the data management, its legitimacy and the forms of objection against the data management. It is the annex no. 4/1. of the regulation entitled "Reply to the curriculum vitae recorded in the database".

Further management of the data of the concerned person selected based on the CV (i.e.: decision on suitability) is conducted for the purpose of establishing employment, the data management related to that is stated in point 11.5.

aim of data management: selection of a suitable future employee for a later establishment of employment, to fill in empty work positions
scope of managed data: name, date of birth, mother's name, address, training data, portrait, other data provided by the concerned, identification data of the recommending person, the success of background check
legitimacy of data management: concerned person's contribution according to a) of chapter (1) of article 6. of GDPR
data storage deadline: until the deletion request of the concerned, max. six months.
data storage method: on paper and electronically

9.5. Data management regarding employment

The aim of the data management regarding employment is the establishment, maintenance and termination of employment.

Photocopying Identification documents

The Company – in accordance with NAIH – does not issue photocopies of identity cards. Photocopies of official documents are not suitable for the identification of natural persons; hence the presence of the individual is crucial for the identification based on official documents. The official document with picture reasonably possesses standard of proof only if based on that, the Company can be certain that the person on the official document and the person showing the official document are the same. A copy of an official document does not have the standard of proof to be a legitimate copy of a valid official document.

To retain the principles of data collection and data quality, the Company however many create a masked photocopy (or scanned image - collectively: photocopy) of the newly entering- or data changing employees. During photocopying, the Company leaves only those parts of the official documents suitable for photocopying (to be further readable) which contain data that the concerned is obligated to issue of him- or herself anyway. In this case, the photocopy is made for the purposes of data reconciliation. The photocopy is immediately and irreversibly deleted by the Company following the comparison of the entry papers filled out by the employee and the data on the masked official document-photocopies by a coworker appointed by the Company, or within 30 days following the creation of the photocopy.

Health data management regarding medical fitness

The data relevant to medical fitness is not learned by the Company, and it does not manage the data of any concerned person in a manner which overextend the goal. For the decision of medical fitness, the Company decides on the given (future) employee's medical fitness based on the fitness results provided by the medical service for the purpose of deciding the person's medical fitness. The Company only manages the data which proves the medical fitness of the concerned.
In case the given concerned turns out to be unfit for employment during the signing of the employment contract, and due to this, the employment is not established or is terminated, the deadline and method of the data management is carried out accordingly as well.

Data controls regarding the maintenance and termination of employment

The Company keeps personnel-, salary- and employment record of the employees.

The Company stores the data of the accepted employers electronically and on paper as well. The data of the employees are recorded which are necessary for the establishment of employment.
The personnel registry is data management intended for the documentation of facts of employment and other position regarding employment (e.g. independent activity employment, venture etc.). The data of the personnel registry can be used for the determination of facts regarding the employment of the employee and for statistical data provision. The personnel registry contains the data of every employee of the Company.

The legitimacy of the data management of employees is the statutory authority (2012. I. law on the employment code).

Statements regarding data management in relation to employment

In case an acquirement of a statement from the employee is necessary for the establishment, maintenance, termination of employment and for the approval of the entitlements and obligations related to the employment is necessary, during the acquirement of the statement the Company always notifies the employee on the fact, legitimacy and goal of the data management related to the data provided on the statement.

In case the validity of the statement requires the presentation of an official document (national identity card, student card), the Company will not manage the data and/or photocopied or scanned image of the official document, rather it attests to the presentation of the official document and its validity with the signature of the eligible employee.

Employee training

The Company reserves the right to enter into a contractual agreement with a third party for the purpose of employee training. In case the training is mandatory by law in order to fill the position, the third party processes the data as the data processor of the Company, in case of every other training; the personal data is transferred to the third party with the consent of the employee.

Fringe benefits

The Company reserves the right to provide fringe benefits to the employees and to enter into a contractual agreement with a third party. In case the employee selects the services he or she wishes to utilize from the fringe benefit elements, the Company transfers the data necessary to the relevant services.

Data provided by third parties regarding employment

The data of third parties regarding employment (for example rest leave, family tax allowances or the appointment of contact in case of incident) can be recorded and managed within the necessary time period.

In case the employee provides the data of a third party, he or she is obligated to acquire the consent of said third party for data management, with which the Company can prove that it has a jurisdiction to manage the data of the third party. The statement is contained in annex no. 6.

aim of data control: establishing, completing or termination of employment, acknowledgment of jurisdiction related to this, certification of obligations and the guarantee of the benefits related to employment

scope of managed data:

- name,
- birth name,
- birth location and date,
- nationality,
- mother's birth name,
- home address,
- place of residence (in case it differs from the home address),
- private pension fund
    - membership,
    - entering date (year, month, day),
    - bank name and code,
- tax number,
- social security number (TAJ number),
- retired prime number (in case of a retired employee),
- workbook copy (if available)
- dept statement,
- statement on the retention of data safety,
- current account number,
- first day of employment,
- insurance coverage type,
- number of weekly work hours,
- phone number,
- family status,

- a copy of an official document certifying qualification,
- medical certificate for employment,
- employment,
- proof of medical fitness,
- certificate of good conduct:
    - date issued,
    - serial number,
    - identification of application,
- following accounting, proof on the closing medical examination of the medical certification for employment,
- in case of employee with reduced work capacity, an expert's statement establishing the employee's reduced work capacity,
- in case of work conduct outside of main employment:
    - type of employment,
    - name and office of employer,
    - monthly general work time at the workplace outside of main employment,
    - activities to be performed,
- certification regarding previous employment:
    - certificate on insurance coverage and social security
    - employer's certification on the termination of employment
    - previous year tax base
- regarding the utilization of rest leave according to par. 120 of Mt.
    - photocopy of a document certifying reduction of work capacity issued by the rehabilitation expert body,
    - photocopy of an official document certifying eligibility for disability benefits,
    - photocopy of an official document certifying eligibility for personal allowance for blind persons,

utilization of rest leave, family tax allowances, request for tax-free beneficial travel certificate regarded as within the category of benefits in kind, or a request for tax-free school-starting benefit for the employee's

a) relative under the age of 16
b) relative or companion over the age of 16:
    - name, birth name,
    - birth place and date,
    - home address,
    - mother's name,
    - social security number (TAJ number),
    - tax number,
    - valid student card

legitimacy of data management: statutory authority, (1) and (3) of par. 10 of the 2012. I. law on employment code and the relevant provisions of tax- and social security laws

data storage deadline: the realization of the data management goal, according to base regulation

- termination of employment regarding eligibility and obligations in relation to employment
- until the deadlines set in the laws on pension payment in connection to eligibilities resulting from employment status

data management method: on paper and electronically

Regarding the management of employee data, an employment brochure was established as a part of annex 5. of this regulation; its aim is the preliminary informing of the employees on data management.

9.6. Data management regarding the inspection of the employees' technical tools

The employer may inspect the employees within the scope of their behavior in relation to their employment. The inspection is justified by sections (1)-(2) of par. 11. of the Mt.
The Company inspects its employees with the legal base provided in the Mt. The Company preliminary informs the employee on the utilization of technical tools intended for the inspection of the employee. This brochure is contained in annex 5.

Inspection of Company tools

The Company provides computers, computer and web programs, phone, email address and internet access to the employees in justifiable cases. The company informs the employees on the rules of utilization and the possibility of inspection with the employment brochure within annex 5. of the current regulation.

Hence the Company provides its own personal computers and laptops, mobile phones, company email addresses for work purposes, storing personal data on them is forbidden. In case the employee stores private personal data on these tools (e.g. family photos, phone books, private databases etc.) regardless of the prohibition, the Company may learn of these data as well during the inspection of the computer. The Company informs the employees in writing on this fact before the usage of the tools (as well as the archiving and administrative activity).

Inspection of Company email addresses

The employees of the Company acknowledge that every email address bearing the Company name as an extension (…@meatland65.hu) is the property of the Company and messaging conducted on these addresses constitute as work-related messaging. The content of the received and sent emails are Company property.

In case of justified legal base, the Company is entitled to look into the messaging conducted under these addresses. The Company is entitled to periodically save the messaging for safety purposes on the above-mentioned addresses, for the continuity and stability of the electronic messaging system.

It is forbidden to conduct any non-work related (private or otherwise) messaging on the company email addresses. In case the employee conducts private- or any other type of correspondence on his or her company email address (…@meatland65.hu)", and simultaneously stores his or her private personal data in the mailbox, the Company is entitled to learn of these data during the inspection of the email address..

Aside from these, according to base regulation, the employer is not entitled to learn of the content of private messages, even with entitlement from work position.

Inspection of internet usage

The above rules adhere to internet usage as well: the use of the internet is only permitted for company purposes within work hours. Due to this fact, the internet data constitute as company data.

Inspection

The Company may inspect every tool it owns, with regard to the step-by-step principle, and the guarantee of the employee's presence.
The Company informs the employee concerned with inspection on the fact of the inspection. The technical inspection is conducted by the administrator by performing occasional inspections; however, it can be requested by any employee of the Company if a process endangering the economic interests of the Company can be ascertained.

aim of data control: inspection of the employees according to (1) of par. 11. of the Mt. according to the legitimate business interests of the Company, especially the inspection of the computer, email address, phone use and internet access provided by the Company.

scope of managed data: stored data during inspection, especially private email addresses, private phone numbers, photos, private computer documents, internet histories, cookies, infringement during working hours, description of infringement

legitimacy of data control: (1) of par. 11 of 2012. I. law

deadline of data storage: 1 year from inspection and at the latest the expiry of the request for inspection

data management method: electronically and on paper

9.7. Work protection inspection of suitable work condition

The employment contract signed with the employer and a) of (1) of par. 52 of the Mt states that the employee is obligated to be present in suitable work condition for the location and time required by the employer.

According to the authorization in (3) of par. 2 of Mvt., the realization of work conduct which is not endangering health and safe regarding influence due to alcohol is determined by the following:

Based on (1) of par. 60 of the Mvt., the employee may only conduct work in a condition suitable for work, adhering to the rules and instructions regarding work safety and according to the work safety training. The employee is obligated to collaborate with his or her coworkers, and conduct work in a manner that is not endangering his/her or others' health and physical wellbeing.

The Company prohibits employees present at the workplace under the influence of alcohol and/or drugs on every stage of employment. This also relates to the case of the employee being present after his or her work hours with no work conduct purpose, hence a person under the influence of alcohol and/or drugs can endanger the safe work conduct of others. It is forbidden to enter into the

premises of the Company or into the work area (if it differs from the Company premises) under the influence of alcohol and/or drugs, it is forbidden to consume alcohol and/or drugs there, or to conduct work under the influence of alcohol and/or drugs.

Written relief from this rule can be provided by the leading manager under justifiable cases.

The lack of suitable work condition endangers the conditions of safe work conduct, which includes being under the influence of alcohol and/or drugs. Due to this, not only the employees need to be fit for work, but they are obligated to retain this condition until the expiry of his or her work hours.

During work conduct, the employee cannot endanger his or her or others' health and physical wellbeing.

Regarding its obligations stated by the safe working conditions, the Company is obligated to systematically ascertain that the employees adhere to the regulations regarding them. The regulations for inspecting the employment legislations are determined by the Mt., as well as the Mvt.

Mt. 11. § (1) *The employer may only inspect the employee regarding his or her conduct in the workplace. The employee's inspection and the tools and methods used therein cannot infringe upon dignity. The private life of an employee cannot be inspected.*

Mvt. 54. § (7) b) *For work conduct which does not endanger health and promotes safe working conditions, the employer is obligated to systematically ascertain that the working conditions are suitable for the requirements, and that the employees acknowledge and uphold the regulations related to them.*

Persons entitled for inspection - aside from the person liable for work safety - are the following:

- the leading manager,
- security service experts.

However, the inspection of alcoholic influence cannot infringe upon dignity even in accordance with the above - thus the person conducting the inspection cannot abuse his or her inspection rights, and cannot exercise it opposite its function, for example, if the inspection is conducted several times in one day or from the motivation of personal revenge; it is also unlawful to have an unauthorized person ordering and inspection.

Accurate method of inspection:

- the person responsible for work safety can order the alcoholic inspection regarding any employee, also as a spot check
- in case of suspicion, the direct work area manager of the concerned is obligated to initiate a procedure,
- the person authorized for inspection is entitled to order an inspection to the notification of any employee of the Company, if the employee states the reason for inspection and the person to be inspected, however, he or she is entitled to refuse the inspection if from the work circumstances he or she clearly deems it unnecessary,

- The inspection needs to be conducted without the infringement upon the personal rights of the employee and with the presence of two witnesses, with a breathalyzer or with an instrumental breathalyzer,
- the person conducting the inspection creates a record of the inspection, the contents of the record: the fact of the inspection, the conditions giving reason for the inspection (general work safety inspection, or suspicion of alcoholic influence), the inspected person, date of the inspection, result of the inspection, the declaration of intent of the inspected person regarding the result of the inspection (approval, rejection),
- the record needs to be certified by the signature of the inspected employee, the person conducting the inspection and the witnesses present,
- in case the employee does not accept the results, he or she may request the analysis of blood alcohol level at the company medical expert or other medical services by means of blood sampling,
- in case the inspected employee refuses to comply with the person conducting the inspection and does not partake in the inspection, the person conducting the inspection immediately notifies the person with employer's jurisdiction above the employer,
- refusal of the inspection results in an immediate unsuitability for work according to (1) of par. 60 of Mvt., hence he or she refuses the obligation to comply stated in the law.

In case the inspection is conducted by a security service professional due to suspicion, he or she is obligated to immediately notify the person responsible for work safety on the inspection and its results.

In case of the employee is found to be unfit to work (positive result or the infringement of the obligation to comply), the inspecting person immediately notifies the person with employer's jurisdiction or decision-making jurisdiction above the inspected person, who is obligated to absolve the employee from work.

aim of data control: inspection of suitable work condition for work safety purposes

scope of managed data: result of inspection, date, suitable work condition, data of person conducting the inspection, inspected employee data. If the inspected person questions the results, this fact, or in case of positive sample, or if he or she refuses the right of blood sampling.

legal basis of data management: (1) of par. 60 of the 1993. XCIII. law on work safety, and chapters (1) and (2) of par. 11 of the 2012 law on the employment code

data storage deadline: the deadline available for enforcing rights regarding rights and obligations originating from the event

data management method: on paper

A brochure has been made of the inspection process, which the employees ha recognized. It is annex no. 5 of the regulation.

9.8. Data management regarding electronic surveillance

With legal basis stated in par. 31 of the Szvtv. 31 and regarding provisions, the Company operates an electronic surveillance system at its main office. The cameras of the system are Company

property, the Company guarantees the safe storage of the records. The surveillance system is suitable for image capture.

Method and deadline of the deletion of recordings created by the electronic surveillance system

In case of unused, the record is deleted within 3, as in three days from the recording [Szvtv. 31. § (2)]. Usage is regarded as the use of the record as evidence in a court procedure or in other administrative procedures.

The Company provides the facts determined in Szvtv. at all times, as in if the recording affects anyone's right or rightful interest, he or she may request not to delete or terminate the data with his or her legitimate certificate within the determined deletion period of the recording (three work days). The Company data protection officer decides on the request as quickly as possible. This marked recording needs to be saved and provided to the data protection officer, who guarantees its suitable storage according to this regulation. By inquiry of the court or other authority, the recording needs to be submitted to the court or the authority immediately. In case an inquiry does not occur within thirty days from the cancellation of the termination, the record gets terminated.

Guarantee arrangements regarding electronic surveillance

Using the electronic surveillance system, the Company only interferes in the personal space of the concerned in a necessary degree.

The Company does not conduct electronic surveillance for the following reasons:

- to monitor the work intensity of an employee,
- to influence the work place behavior of the employees,
- in sensitive areas, especially in dressing rooms, showers, bathrooms,
- in areas where the employees take their brake between work hours, especially in recreational rooms or designated smoking areas,
- in public areas.

However, the Company may conduct electronic surveillance to check whether the employees uphold the orders regarding them for the sake of non-health risking and safe work conduct.

Informing the concerned

Brochures have been made regarding the data management to inform the concerned on the data management. The brochure is the 7. annex of the regulation. The brochure is placed at every entry point of the surveilled area.

Informing the employees of the Company

Brochures have been made regarding the data management to preliminary inform the employees on the data management. The text of the brochure is contained by annex 5. of the regulation.

Viewing of camera images

For the reason of the least amount of interference of the Company into the private space of the concerned, the recordings created with the electronic surveillance system can only be accessed by designated persons.

Only a person designated in this regulation is entitled to view the recordings within the Company organizational system.

Only the persons listed under annex 8. of the regulation possess surveillance rights during the electronic surveillance established by the Company. the Company retains the data for 5 years from the cancellation.

A record needs to be made from the inspections of the camera images, according to annex 9. of the regulation.

Lock of camera images

Only a person designated for the surveillance of data management established by the Company camera system or the data protection officer may order for the lock of the camera images.

The lock of camera images can be initiated by the following:

- a person with inspection rights at the Company, in case he or she notices circumstances which might endanger the designated goal with the electronic surveillance system,
- anyone, whose rights or rightful interest is concerned with the recording.

The request of the lock of the recording may only be initiated in writing to the person designated for the surveillance of data management established by the Company and simultaneously to the data protection officer.

Decision on the lock is made by the person designated for the surveillance of data management established by the Company (in agreement with the data protection officer) as quickly as possible.

The Company keeps a record of every lock of camera images, in which the date of inspection and lockage, the event which initiated the lock and the marking of further use needs to be set. The record regarding this is annex 10. of the regulation.

Persons with locking entitlement

The Company keeps a record on the persons entitled for locking. Part of the record is the name and work description of the person with locking entitlement, the submission date of the locking rights, and the cancellation date of the locking rights. The data is kept by the Company for 5 years following the cancellation. The registry of persons with locking rights is listed in annex 11. of the regulation.

aim of data control: protection of the object's safety and the Company financial assets, as well as the protection of the physical wellbeing and financial assets of persons present on the surveilled area
scope of managed data: portrait of the concerned, data acquirable with camera images (place of residence, time of residence)

legal basis of data management:

- consent of the concerned by suggestive behavior [Szvtv. 30. § (2)]
- in case of employees, rightful interest according to point f) of chapter (1) of article 6. of GDPR

data storage deadline:

- In case of not using the recording, it gets deleted 3, as in three days from the recording [Szvtv. 31. § (2)]
- in case the recording was requested for the Company to not be deleted with approved right or rightful interest, however, the inquiry did not occur, the recording gets deleted 30, as in thirty days from the request [Szvtv. 31. § (6)]

data storage method: electronically

9.9. Management of extraordinary security events

An extraordinary event is every event or circumstance significantly differing from the norm, which can lead to catastrophic consequences to the persons' lives, physical wellbeing or material goods in the object, or if there is a realistic chance of catastrophic consequences to occur, creating serious failures in the operation of the object.

Person/persons designated by the Company keep records of events relevant from a security standpoint. The following data needs to be included in the record: date of filling out the record, name, signature of the person keeping the record, name, signature, birth name, birthplace, birth date, mother's name, home address, place of residence of the inspected person, and the description of the event. These data are relative personal data, which can be changed to personal data regarding the GDPR.

aim of data control: inspection of extraordinary security events
scope of managed data: date of filling out the record, name, signature of the person keeping the record, name, signature, birth name, birthplace, birth date, mother's name, home address, place of residence of the inspected person, and the description of the event
legal basis of data management: enforcing company interest according to f) of chapter (1) of article 6. of GDPR
data storage deadline: inspection of the event, the deadline available for enforcing rights regarding rights and obligations originating from the event
data storage method: on paper