DATA MANAGEMENT AND DATA PROTECTION POLICY

Korax Gépgyár Kft. (Private Limited Company)
(headquarters: Hungary, 2300 Ráckeve, Sillingi road 30.)

Effective: May 25, 2018

I. The purpose of the Regulations

1. The purpose of these regulations is to ensure that **Korax Gépgyár Kft. (Private Limited Company)** (headquarters: 2300 Ráckeve, Sillingi road 30., company registration number: 13-09-070241) - hereinafter: the Company - as the Data Controller of its clients and employees and the visitors of its websites and social media pages - hereinafter collectively: data subject(s) - protects their legal interests and rights and the security of data management is given.
2. In view of the above, the purpose of these regulations is to ensure that the Data Controller complies in all respects with the provisions of the applicable legislation regarding data protection, so in particular, but not exclusively:

   - CXII of 2011 on the right to information self-determination and freedom of information. law,

   - Regulation (EU) 2016/679 of the European Parliament and of the Council,

   - CVIII of 2001 on certain issues of electronic commercial services and services related to the information society. law,

   - XLVII of 2008 on the prohibition of unfair commercial practices towards consumers. law,

   - CXXXIII of 2005 on the rules for the protection of persons and assets, as well as private investigative activities. law,

   - XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activities. law,

   - Act I of 2012 on the Labor Code (Mt.),

   - XCIII of 1993 on labor protection. law,

   - Act C of 2000 on accounting,

   - CL of 2017 on the taxation system. law,

   - LXXV of 2010 on simplified employment. law,

   - Act V of 2013 on the Civil Code,

   - CXVII of 1995 on personal income tax. provisions of the law.
3. The Data Controller hereby informs the data subjects that, while respecting the personal rights of the data subjects, it acts in accordance with the following regulations - hereinafter: Regulations - and its provisions during its data management.
4. The version of the Regulations in force at all times is available in electronic form on Company's websites - www.korax.hu; www.koraxsolar.com; www.korax-group.com - while it is available on paper at the place of actual data management (2300 Ráckeve, Sillingi út 30).
5. These Regulations are related to the internal regulations of the Data Controller and must be interpreted together with them.

6. The Data Controller reserves the right to change the Regulations due to changes in the legal background and alignment with other internal regulations.

II. Scope of the Regulations

1. Time scope: These regulations are effective from May 25, 2018 until further notice or withdrawal.
2. Personal scope covers:
    a. the Data Controller,
    b. Employees,
    c. the persons whose data is included in the data management covered by these Regulations, and
    d. the persons whose rights or legitimate interests are affected by the data management.

3. Therefore, the Data Controller primarily manages the data of natural entities who are its Partners, and the representatives, contacts of non-natural entity Partners, possibly other employee data and the data of its colleagues.

4. The material scope of the regulation covers:

    The scope of these Regulations covers all data processing involving personal data carried out by the Data Controller, regardless of whether it is done electronically and/or on paper. In the case of paper-based data management, the Data Controller also introduces and operates a document management policy that is formally separate from these regulations, which supplements the general provisions of these Regulations and which is covered by the scope of these Regulations, and is therefore considered an annex to these Regulations.

III. Concept definitions

1. **Data subject:** any natural entity identified or - directly or indirectly - identified on the basis of personal data, e.g. co-worker, natural entity applying for a job offer, natural entity using the Data Controller's services.

2. **Personal data:** any information relating to an identified or identifiable natural entity (i.e. the data subject); a natural entity can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural entity can be identified.

3. **Special data:** all data belonging to special categories of personal data, i.e. personal data referring to racial or ethnic origin, political opinion, religious or worldview beliefs or trade union membership, as well as genetic data, biometric data aimed at unique identification of natural entities, health data and personal data concerning the sex life or sexual orientation of natural entities.

4. **Data file:** the totality of the data managed in a register.

5. **Consent:** the voluntary and decisive declaration of the data subject's will, which is based on adequate information, and with which he gives his unequivocal consent to the processing of his personal data - in full or covering certain operations.
6. **Data controller:** a natural or legal entity or an organisation without legal personality who, independently or jointly with others, determines the purpose of data management, makes and implements decisions regarding data management (including the device used), or implements them with the data processor it has commissioned . Pursuant to these Regulations, the Data Controller is the IV. person specified in chapter

7. **Data management:** regardless of the procedure used, any operation performed on the data or the set of operations, including, in particular, collection, recording, recording, organisation, storage, change, use, query, transmission, disclosure, coordination or connection, locking, deletion and destruction, and preventing further use of the data, taking photographs, audio or video recordings, and recording physical characteristics suitable for identifying the person.

8. **Restriction of data management:** marking of stored personal data for the purpose of limiting their future processing.

9. **Profiling:** any form of automated processing of personal data in which personal data is used to evaluate certain personal characteristics of a natural entity, in particular characteristics related to work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement used to analyse or predict.

10. **Pseudonymization:** the processing of personal data in a way that, without the use of additional information, it is no longer possible to establish which specific natural entity the personal data refers to, provided that such additional information is stored separately and technical and organisational measures are taken to ensure that this personal data cannot be linked to identified or identifiable natural entities.

11. **Data transmission:** making the data available to a specific third party.

12. **Data processing:** the performance of technical tasks related to data management operations, regardless of the method and tool used to perform the operations, as well as the place of application, provided that the technical task is performed on the data. E.g. performing accounting tasks.

13. **Data deletion:** making data unrecognisable in such a way that their recovery is no longer possible.

14. **Data blocking:** providing the data with an identification mark for the purpose of limiting its further processing permanently or for a specified period of time.

15. **Data destruction:** complete physical destruction of the data carrier containing the data. E.g. shredding documents, destroying hard drives.

16. **Registry system:** a file of personal data divided in any way - centralised, decentralised or according to functional or geographical aspects - which is accessible based on specific criteria.

17. **Third party:** a natural or legal entity, or an organisation without legal personality, who is or is not the same as the data subject, the data controller or the data processor, or the persons who have been authorised to process personal data under the direct control of the data controller or data processor.

18. **Data protection incident:** a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to personal data transmitted, stored or otherwise handled.

19. **Partner:** legal entities that use the Data Controller's services on the basis of a contract and/or facilitate the performance of the Data Controller's services (implementation assistants), economic companies without legal personality, to which the Data Controller - after the data subject's consent - transmits or may transmit personal data, or which They carry out or can carry out data storage, processing, related IT and other safe data management activities for the data controller;

20. **Employee:** a natural entity in an employment, employment or other legal relationship with the Data Controller, who is entrusted with the task of providing and performing the services of the Data Controller or the Data Controller's partner and who comes into contact or may come into contact with personal data in the course of their data management or data processing tasks, and whose activities the Data Controller fully undertakes responsibility for the personnel of those involved and third parties. E.g. employee, temporary worker.

21. **Data controller:** the Employee from whom the data was generated and/or who has access rights to the data, and/or to whom the data was forwarded by another data controller or a third party, and/or to whom the data came into their possession in any other way.

22. **Website:** the https://www.korax.hu and koraxsolar.com and www.korax-group.com portals and all their subpages, operated by the Data Controller.

23. **Social page:** the online platform maintained by the Data Controller. For example: www.facebook.com/koraxkft

IV. The Data Controller

1. Based on these Regulations, the Data Controller:
   1.1.
   Name: Korax Gépgyár Kft. (Private Limited Company)
   Headquarters: 2300 Ráckeve, Sillingi út 30..,
   Company registration number: 13-09-070241
   Tax number: 12050844-2-13
   The address of the actual data management: 2300 Ráckeve, Sillingi út 30..,
   Internet contact: https://www.korax.hu
   Telephone number: +36/24 485 402
   Email: pbox@korax.hu
   Independently represented by: Managing Director Tamás Szöllősi

   1.2. Employee: in relation to whose activities Korax Gépgyár Kft. (Private Limited Company) assumes full responsibility towards third parties.

2. The data protection organisation of the Data Controller

   2.1. The management of the Data Controller in relation to data protection, data management and information security is provided by the Data Controller's executive (hereinafter: Data Manager).

   2.2. The management of the Data Controller coordinates data protection regulations, regularly checks data management and data protection, authorises Employees to access IT applications necessary for the performance of their duties, and performs other tasks specified by other regulations and legislation.

   2.3. At the Data Controller the following job groups exist on the date when these Regulations are coming into effect:

   - Production
   - Planning
   - Sale
   - Finance
   - Administration
   - Human resource
   - Administration
   - Marketing, business development

   2.4. Employer rights over employees are exercised by the management of the Data Controller.

   2.5. Management of the Data Controller:

   a. determines the access rights of data controllers;
   b. coordinates the activities of data controllers related to data protection and data management;

c. takes care of the replacement order of data controllers;
d. ensures the order of data management and data protection.
e. is obliged to support and monitor subordinates' participation in training, to check knowledge of training materials,
f. is obliged to provide information to assigned Employees and other stakeholders,
g. are obliged to take the necessary measures in the event of a data protection or data security incident.
h. is responsible for complying with the regulations and enforcing them with subordinate Employees, ensuring the inviolability of personal data handled by subordinate Employees.

2.6. Under the direct management of the Data Controller, the Employees perform their duties in compliance with the obligations arising from the applicable laws, internal regulations and rules, instructions, job descriptions, and educational materials.

2.7. The Employee from whom the data was created and/or who has access rights to the data and/or to whom the data was forwarded by another data controller or third party and/or to whom the data came into his possession in any other way is considered a data controller in these Regulations Based on.

2.8. Data may only be deleted, corrected, blocked or destroyed by the data owner entitled to access, the representative of the Data Controller, or the Employee entrusted with this task, and only if all is convinced that the conditions are met and this is duly documented.

2.9. The Employee

a. must ensure that:
- the data and confidentiality provisions apply;
- process data only to the extent necessary for the performance of its task;
- the data must be available to other data controllers entitled to access to the extent necessary for the performance of their tasks;
- the data should not fall into the possession of unauthorised third parties. In order to ensure this, you must keep the data carrier documents under your direct supervision, or at the place of work, in a closed place inaccessible to unauthorised persons (in a locked drawer, cabinet);
- no one else can access the user ID and password of the devices he uses.

b. must:
- act with the utmost care when performing his duties;
- access the data of the electronic registration systems with your own user ID;
- perform a backup of the data it manages at regular intervals or have it done by the competent Employee;
- learn about and comply with the rules related to data management and data protection;
- participate in education related to data protection;
- inform the management of the Data Controller immediately in writing about inquiries related to external data management/data protection;
- immediately notify the management of the Data Controller after detecting a data protection incident;

- protect the personal data obtained.

c. responsible:
   - for complying with the regulations,
   - for the inviolability of the personal data it manages,
   - for violations resulting from his intentional or negligent conduct.

2.10. The Employee is entitled to request guidance and interpretation from the management of the Data Controller in matters related to data management and data protection.

2.11. In case of violation of the legal provisions on data management, data and privacy protection, as well as the provisions of the Data Protection and Data Management Regulations, other data protection or other internal regulations, job descriptions, employer instructions, data protection educational material, which are in force at all times, depending on the nature of the behaviour or omission, criminal law and/or or may be subject to civil and/or labor law liability.

2.12. Some of the Employee's tasks are contained in the relevant employment contract and job description, which may be supplemented with additional tasks by the Data Protection and Data Management Regulations, Organisational and Operational Regulations, job description, confidentiality agreement, and employer's instructions.

3. General tasks related to the enforcement of the data subject's rights, the procedure of the Data Controller

3.1. The Data Controller shall inform the data subject in writing without undue delay, within a maximum of 25 days (15 days in the case of a protest) of the receipt of the given request, of the steps taken in relation to the specified in the request, or of the factual or legal reason for not complying with the request, as well as the about the rights of the data subject and the legal remedies open to the data subject: the possibility of turning to the court and the National Data Protection and Freedom of Information.

3.2. In the event that the reason for the rejection of the request does not exist, the Data Controller shall notify in writing all the recipients of the data transfer to whom the data was previously forwarded or transferred for the purpose of data management, of the exercise of the rights contained in the request, if necessary. The notification may be omitted if, in view of the purpose of the data management, this does not harm the legitimate interests of the data subject, or if the information proves to be impossible or requires a disproportionately large effort. The above information tasks are carried out by the Employee entrusted with the task by the management of the Data Controller.

4. Data Controller's data protection training

4.1. The management of the Data Controller is obliged to hold documented data management and data protection training for Employees at least once a year.

4.2. The management of the Data Controller is obliged to provide the new employee with data management and data protection training in a documented manner.

V. Rights and remedies of the data subject

1. The Data Controller informs the data subjects that they can exercise their rights by sending a request to the e-mail address pbox@korax.hu or to the Data Controller's postal address (2300 Ráckeve, Sillingi út 30.), or they can also request information at these contacts.

2. The Data Controller examines and responds to the declaration as soon as possible, but within a maximum of 25 days, and takes the necessary steps based on the provisions of the declaration, the Regulations and legislation.

3. The right to information, or otherwise known as the "right of access" of the data subject: at the request of the data subject, the Data Controller provides information:
    - about the data and categories of personal data managed,
    - on the purpose of data management,
    - on the legal basis of data management,
    - on the duration of data management,
    - on the duration of data storage or, if this is not possible, on the criteria for determining this duration,
    - if the data were not collected from the data subject, information about their source,
    - where applicable, about automated decision-making, including profiling, as well as understandable information about the logic and the significance of such data management and the expected consequences for the data subject,
    - data processor data, if you have used a data processor,
    - about the circumstances, effects of the data protection incident and the measures taken to prevent it, and
    - in case of transmission of the data subject's personal data, the legal basis, purpose and recipient of the data transmission.

4. The information is free of charge if the information requester has not yet submitted an information request to the Data Controller for the same data set in the current year. In other cases, reimbursement may be established. The compensation already paid must be refunded if the data was handled unlawfully or the request for information led to a correction.

5. The Data Controller must refuse to provide information if, on the basis of a law, an international treaty or a provision of a binding legal act of the European Union, the Data Controller takes over personal data in such a way that the data controller who transmits the data indicates at the same time as the data transmission the limitation of the personal data subject's rights provided for in the said law, or the processing of the data other restrictions, the external and internal security of the state, such as national defence, national security, the prevention or prosecution of crimes, the security of the execution of sentences, and for the economic or financial interest of the state or local government, the significant economic or financial interest of the European Union, and the disciplinary and ethical offences related to the exercise of occupations, for the purpose of preventing and uncovering violations of labor law and labor protection obligations - including in all cases control and supervision - and also for the protection of the rights of the person concerned or others.

6. The Data Controller is obliged to notify the National Data Protection and Freedom of Information Authority of rejected information requests annually by January 31 of the following relevant year.
7. Right to rectification: The data subject has the right to have inaccurate personal data corrected without undue delay upon request by the Data Controller. Taking into account the purpose of the data management, the data subject is entitled to request the completion of incomplete personal data, including by means of a supplementary statement. If the personal data does not correspond to the reality, and the personal data corresponding to the reality is available to the Data Controller, the personal data will be obligatorily corrected by the Data Controller, even without the data subject's request.

8. The right to erasure, also known as the "right to be forgotten": The data subject has the right to have the data controller delete the personal data relating to him without undue delay at his request, and the data controller is obliged to delete the personal data relating to the data subject without undue delay , if it is not excluded by mandatory data management. In addition to the above case, the Data Controller must delete the data if:
   - the processing of the data is illegal;
   - the data is incomplete or incorrect - and this state cannot be legally remedied - provided that deletion is not precluded by law;
   - the purpose of data management has ceased, or the statutory period for data storage has expired;
   - it was ordered by the court or the Authority;
   - the personal data are no longer needed for the purpose for which they were collected or otherwise processed;
   - the data subject objects to data processing and there is no overriding legal reason for data processing;
   - the personal data must be deleted in order to fulfill the legal obligation prescribed by the law applicable to the Data Controller;
   - personal data was collected in connection with the provision of information society-related services offered directly to children, referred to in Article 8 (1) of Regulation EU 2016/679.

9. In the event that the Data Controller has made personal data public for some reason and is obliged to delete it pursuant to the above, it will take reasonable steps, including technical measures, taking into account the available technology and the costs of implementation, in order to inform the other parties handling the data. data controllers that the data subject has requested the deletion of the links to the personal data in question or the copy or duplicate of these personal data.

10. The data controller draws the attention of the data subjects to the limitations of the "right to be forgotten" arising from the EU regulation, which are as follows:
    - exercising the right to freedom of expression and information;
    - fulfillment of the obligation under the EU or Member State law applicable to the data controller requiring the processing of personal data, or the execution of a task carried out in the public interest or in the context of the exercise of public authority granted to the data controller;
    - public interest in the field of public health;
    - in accordance with Article 89 (1) of Regulation EU 2016/679 for the purpose of archiving in the public interest, for scientific and historical research purposes or for

statistical purposes, if the right to erasure would likely make this data management impossible or seriously jeopardize it; obsession

- submission, enforcement and defense of legal claims.

11. Right to limit and block data processing: The data subject has the right to have the Data Controller limit data processing upon request. If, based on the available information, it can be assumed that the deletion would harm the legitimate interests of the data subject, the data must be blocked. The personal data locked in this way can only be processed as long as the data management purpose that precluded the deletion of the personal data exists. If the data subject disputes the accuracy and correctness of the personal data, but the incorrectness or inaccuracy of the disputed personal data cannot be clearly established, the data will be blocked. In this case, the limitation applies to the period that allows the Data Controller to verify the accuracy of the personal data. The data must be blocked if the data processing is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use, or the Data Controller no longer needs the personal data for the purpose of data processing, but the data subject requires them to submit, enforce or defend legal claims, or the data subject objected to data processing; in this case, the restriction applies to the period until it is determined whether the Data Controller's legitimate reasons take precedence over the data subject's legitimate reasons. If data management is subject to restriction (blocking), such personal data, with the exception of storage, will only be processed with the consent of the data subject, or for the presentation, enforcement or defense of legal claims, or for the protection of the rights of another natural or legal person, or in the important public interest of the Union or a member state can be handled.

12. The data controller draws the attention of the data subjects to the fact that the data subject's right to rectification, erasure and blocking may be limited by law in the interests of the external and internal security of the state, such as national defense, national security, the prevention or prosecution of crimes, the security of the execution of sentences, as well as state or local government for economic or financial interest, for the significant economic or financial interest of the European Union, as well as for the purpose of preventing and uncovering disciplinary and ethical offences related to the exercise of occupations, violations of labor law and occupational health and safety obligations - including in all cases control and supervision - as well as the person concerned or others in order to protect your rights.

13. Without undue delay, within a maximum of 25 days from the receipt of the request, the data controller informs the data subject of the information specified in the request and/or corrects the data and/or deletes and/or restricts (locks) the data, or takes other steps in accordance with the request, if there is no reason to exclude it.

14. The Data Controller shall notify the data subject in writing of the rectification, deletion, restriction of data processing, as well as all those to whom the data was previously forwarded for the purpose of data processing. At the request of the data subject, the Data Controller informs about these recipients. The notification may be omitted if, in view of the purpose of the data management, this does not harm the legitimate interests of the data subject, or if the information proves to be impossible or requires a disproportionately large effort. The data controller is also obliged to notify the data subject in writing if the exercise of the data subject's rights cannot be carried out for some reason, and must specify the factual and legal reason, as well as the legal remedies open to the data subject: the

possibility of turning to the court and the National Data Protection and Freedom of Information.

15. The "right to data portability": The data subject has the right to receive the personal data concerning him/her provided to the Data Controller in a segmented, widely used, machine-readable format, and is also entitled to transmit this data to another data controller without this would be hindered by the data manager to whom the personal data was made available, if the data management is based on consent; and data management is automated. When exercising the right to data portability, the data subject is entitled to - if this is technically feasible - request the direct transmission of personal data between data controllers. The exercise of the right may not violate the right to erasure. The aforementioned right does not apply if the data processing is in the public interest or is necessary for the execution of a task performed in the context of the exercise of the public authorities granted to the data controller. The exercise of the right must not adversely affect the rights and freedoms of others.

16. The right to object: The data subject may object to the processing of their personal data, including profiling, if
    - the processing (transmission) of personal data is necessary only to assert the rights or legitimate interests of the Data Controller or the data recipient, except in the case of mandatory data processing;
    - personal data is used or forwarded for the purpose of direct business acquisition, public opinion polls or scientific research;
    - the exercise of the right to protest is otherwise permitted by law.

    The data subject can object to EU Regulation 2016/679, Article 21, Paragraph 3. against the processing of personal data for the purpose of obtaining direct business, in which case the personal data may no longer be processed for this purpose.
    If personal data is processed for scientific and historical research purposes or for statistical purposes, the data subject has the right to object to the processing of personal data concerning him for reasons related to his own situation, unless the data processing is necessary for the performance of a task carried out for reasons of public interest.

17. The Data Controller examines the objection as soon as possible, but no later than 25 days after the submission of the application, with the simultaneous suspension of data management, and informs the applicant of the result in writing. If the applicant's objection is well-founded, the Data Controller shall terminate the data management, including further data collection and transmission, and block the data, and shall notify all those to whom the personal data affected by the objection was previously transmitted of the objection and the measures taken based on it, and who are obliged to take measures to enforce the right to protest.

18. If the data subject does not agree with the Data Controller's decision, or if the Data Controller misses the mentioned deadline, he is entitled to appeal to the court within 30 days of its notification.

19. Your data subject's rights in relation to automated decision-making, including profiling: With automated data processing only, a decision based on the evaluation of the data subject's personal characteristics may only be made if the decision was made during the conclusion or performance of a contract, provided that it was initiated by the data subject

or is required by law possible, which also establishes measures to ensure the legitimate interests of the data subject.
In the case of a decision made with automated data processing, the data subject must be informed - at his request - about the method used and its essence, and the data subject must be given the opportunity to express his point of view.

20. Legal enforcement: The data subject can go to court in the event of a violation of his rights. The court acts out of sequence in the case. The Data Controller is obliged to prove that the data management complies with the provisions of the law.

21. In the event of a violation of your right to self-determination of information, you can file a report or complaint: National Data Protection and Freedom of Information Authority Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c Phone: +36 (1) 391-1400 Fax: +36 (1) 391-1410 www: http: //www.naih.hu e-mail: ugyfelszolgalat@naih.hu

22. With content that offends minors, incites hatred, and excludes them, and in the event of a violation of the rights of a deceased person or the violation of his or her reputation hateful, or exclusionary content, rectification, you can file a report or complaint: Nemzeti Média- és Hírközlési Hatóság 1015 Budapest, Ostrom u. 23-25. Mailing address: 1525. Pf. 75 Tel: (06 1) 457 7100 Fax: (06 1) 356 5520 E-mail: info@nmhh.hu

23. Legal rules on compensation and damages: In the event that the Data Controller violates the data subject's right to privacy by unlawfully handling the data subject's data or violating data security requirements, the data subject may demand damages from the Data Controller.

24. In the event that the Data Controller has used a data processor, the Data Controller is liable to the data subject for the damage caused by the data processor, and the Data Controller is also obliged to pay the data subject compensation in the event of a privacy violation caused by the data processor. The Data Controller is released from responsibility for the damage caused and from the obligation to pay compensation if it proves that the damage or the violation of the privacy rights of the data subject was caused by an unavoidable cause outside the scope of data management.

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

VI. Principles of data management

1. The provisions of these Regulations, as well as the practices of the Data Controller, may not conflict with data management principles. The Regulations introduce the following data management principles, which are mandatory and serve as guidelines for issues that are not discussed in the Regulations.

2. "Principle of purpose-boundness": Personal data can only be processed for a specific purpose, in order to exercise a right and fulfil an obligation. In all stages of data management, the purpose of data management must be met, the collection and management of data must be fair and legal.

3. "Legality, fair procedure and transparency" principle: Personal data must be handled legally and fairly, as well as transparently for the data subject.

4. "Proportionality, necessity" or "data economy" principle: Only personal data that is essential for the realisation of the purpose of data management and is suitable for achieving the purpose can be processed. Personal data can only be processed to the extent and for the time necessary to achieve the purpose. In accordance with all of this, the Data Controller only handles data that is absolutely necessary.

5. "Accuracy" principle: During data management, the accuracy, completeness and - if necessary in view of the purpose of the data management - up-to-dateness of the data must be ensured, as well as that the data subject can only be identified for the time necessary for the purpose of the data management.

6. "Limited storage" principle: Personal data must be stored in a form that allows the identification of the data subjects only for the time necessary to achieve the goals of personal data management; personal data may be stored for a longer period only if the personal data will be processed in accordance with Article 89 (1) of Regulation EU 2016/679 for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, the e in order to protect the rights and freedoms of the persons concerned, subject to the implementation of the appropriate technical and organisational measures.

7. "Integrity and confidentiality" principle: By applying appropriate security measures, in order to protect the personal data stored in the automated data files, the Data Manager ensures the prevention of accidental or unlawful destruction or accidental loss, as well as unlawful access, alteration or distribution.

8. "Accountability" principle: The Data Controller is responsible for compliance with the provisions set out in the above paragraphs and in the Regulations, and must be able to prove this compliance.

9. "Privacy by design" principle: a very conscious way of thinking about data protection, which, in a very short summary, means that when determining the method of data management, as well as during data management, the Data Controller implements appropriate technical and organisational measures - for example, pseudonymization - for the effective implementation of the above principles, the fulfillment of obligations, incorporation of legal guarantees, etc. with its purpose, and it does all this in a regulated and detailed manner. In practice, the way of thinking is facilitated by the education and data protection awareness of Employees, as well as the impact assessment, risk analysis, and interest assessment test used during the introduction and/or regular review of individual data management.

10. During data management, personal data will retain its quality as long as the relationship with the data subject can be restored. The relationship with the data subject can be restored if the data controller has the technical conditions necessary for restoration.

VII. Legality and purpose of data management

1. The data management of the Data Controller is legal if and to the extent that at least one of the following is fulfilled:
    a. the data subject has given his prior and voluntary consent to the processing of his personal data for one or more specific purposes;

    b. data management is necessary to fulfil the legal obligation of the data controller;

    c. the data processing is necessary for the fulfillment of a contract in which the data subject is one of the parties, or it is necessary for taking steps at the request of the data subject prior to the conclusion of the contract;

    d. data processing is necessary to protect the vital interests of the data subject or another natural person;

    e. data processing is in the public interest or is necessary for the execution of a task performed in the context of the exercise of public authority granted to the data controller;

    f. data processing is necessary to enforce the legitimate interests of the data controller or a third party, unless these interests are overridden by the interests or fundamental rights and freedoms of the data subject that require the protection of personal data, especially if the data subject is a child.

    g. Point f) does not apply to data management carried out by public authorities in the performance of their duties.

2. Based on the above, the general purposes of data management are therefore the following:
    a. Preparation, conclusion and execution of contracts concluded or to be concluded with a data controller, in particular:
        - recording, storing and managing data of the data subject for contacting and maintaining contact with them;
        - recording, storing and handling data of the data subject for the purpose of concluding a contract in this regard and proving the concluded contract;
        - handling data of the data subject in connection with the provision of rights arising from the contractual relationship and the fulfillment of obligations;
        - Management of other data files for the use of data management services;
        - forwarding the data of the data subject to the Partner, as long as it facilitates the unavoidable service to the data subject and the data subject has previously consented to it;
        - forwarding the Partner's data to other relevant parties;

    b) the fulfilment of the legal obligations of the data subject and the Controller, and the enforcement of their legitimate interests;

c) after the termination of the contract with the Data Controller, the exercise of the rights derived from the contract and the fulfilment of obligations, thus in particular the enforcement of claims based on the contract;

d) prevention, investigation and disclosure of abuses

e) in the case of a separate consent for this, the request by the Data Controller for the purpose of direct business acquisition and market research;

f) increasing the level of service that fits the Data Controller's profile, market research and survey of habits carried out for this purpose.

3. When defining individual data management activities, the data controller names the individual legal basis(es) and purpose of the data management.

VIII. Legal basis for data management: voluntary consent and mandatory data management

1. The main rule is that the legal basis for data management is the prior, voluntary consent of the data subject based on prior information from the Data Controller.

2. Prior consent is acceptable if all three of the following requirements are met:

   • volunteering
   • definiteness (unambiguity) and
   • awareness.

3. In the case of voluntary data provision by the data subject, the Data Controller processes the personal data with the consent of the data subject. Voluntary consent, as consent, should also be understood as the behaviour by which the data subject accepts by using the website that, in his view, all regulations related to the use of the website, including these Regulations, are automatically covered, or precisely the behaviour during which - in advance after information - the data subject enters and stays in the area monitored by the camera system operated by the Data Controller, if such a surveillance system is operated by the Data Controller.

4. It must clearly follow from the consent that the data subject consents to data management. If the data processing is based on the data subject's consent, in case of doubt, the Data Controller must prove that the data subject consented to the data processing operation.
5. If the data subject gives his consent in the context of a written statement that also applies to other matters, the request for consent must be presented in a way that is clearly distinguishable from these other matters, in an understandable and easily accessible form, with clear and simple language.

6. The data controller hereby informs the data subjects that the data subject has the right to withdraw their consent at any time.

7. Withdrawal of consent does not affect the legality of data processing based on consent prior to the withdrawal, so the withdrawal applies only to the future and has no retroactive effect.

8. If the data subject is unable to give his consent due to his incapacity or other unavoidable reasons, then to the extent necessary to protect his own or another person's vital interests, as well as to eliminate or prevent a direct threat to the life, physical integrity or property of the persons concerned, the data subject's personal data will be processed as long as there are obstacles to consent they are manageable

9. The data controller draws attention to the fact that the consent or subsequent approval of the legal representative of the minor concerned who has reached the age of 16 is not required for the validity of the legal declaration containing the consent of the affected minor. In the case of a child under the age of 16, the handling of the children's personal data is legal only if and to the extent that the consent was given or authorised by the person exercising parental supervision over the child.

10. The Data Controller - taking into account the available technology - makes reasonable efforts to verify in such cases that the consent was given or authorised by the exerciser of parental custody over the child.

11. CXII of 2011. on the basis of Section 6, Paragraph 5 of the Act, if the personal data has been recorded with the consent of the data subject, the Data Controller shall, unless otherwise provided by law, use the recorded data for the purpose of fulfilling the relevant legal obligation, or for the purpose of asserting its own or a third party's legitimate interest, if the enforcement of the interest is proportional to the limitation of the right to the protection of personal data, it can be processed without further separate consent, even after the consent of the data subject has been revoked. The Data Controller informs the data subject if his personal data is processed on this legal basis.

12. If the Data Controller provides a service electronically to those who are absent, usually in return for a fee, to which the user of the service, as a data subject, has individual access, then the creation of a contract for the provision of this service, definition and modification of its content, monitoring of its performance, invoicing of the resulting fees, and for the purpose of validating related claims, it can process the natural personal identification data and address necessary to identify the user.

13. If the processing of personal data is mandated by law, data processing is mandatory. The Data Controller informs the data subject in detail about this in these Regulations and other regulations, which are to be considered annexes to these Regulations and to be interpreted together with them.

14. It is mandatory to record and hand over the data to the competent first-level state tax and customs authority (electronically or on the form established for this purpose) in connection with the insurance relationship, according to Act XCII of 2003 on the taxation system. Act and Act LXXV of 2010 on simplified employment. based on the law, so for example in the case of an employment relationship, a simplified employment relationship and an assignment relationship. The legal obligations, the data to be recorded and transferred, and the procedure to be followed are contained in detail in these Regulations and the

aforementioned legislation, as well as in the information and announcements of the tax and customs authorities.

15. In the event of a data management complaint, the name and address of the person concerned as a consumer, the place, time and method of presenting the complaint, the content of the complaint, the list of presented documents, documents and other evidence, the Data Controller's position regarding the complaint, the person recording the report and - by telephone or with the exception of a verbal complaint communicated using other electronic communication services - the consumer's signature, in the case of a verbal complaint communicated by telephone or using other electronic communication services, in relation to the unique identification number of the complaint.

16. Data management is mandatory in accordance with Act XI of 1998. based on the law, if the conditions for identity verification or the conditions for reporting obligations are met.

IX. Duration of data management

1. However, the duration of data management is defined in the data management description for all data management activities on a voluntary basis. if it cannot be applied due to some error or deficiency, the following rules must be applied:
    - until the goal is achieved and your personal data is deleted, or
    - until your permission to process your data is revoked and thus your personal data is deleted,
    - until the execution of the decision of a court or authority regarding deletion, or in the absence of such provisions - and in the absence of a different provision of law -
    - it lasts until the expiration of the enforceability of the rights and obligations arising from the legal relationship in connection with which the Data Controller manages the personal data. The effective Civil Code According to § 6:22, the general limitation period is 5 years.

2. In case of mandatory data management, the relevant law or regulation establishes the duration of data management.

3. In the case of complaint handling, the mandatory data management in relation to the data is the CLV of 1997. Act 17/A § 7. based on 5 years.

4. In the case of revocation of the data processing permission of the data subject, request for deletion, deletion decision, the data controller shall delete the data within 1 working day from the date of receipt thereof.

X. Certain activities involved in data management and the scope of the data managed

A. General provisions regarding individual data management activities, use of services provided by the Data Controller

1. As a general rule, among the data management activities and services provided by the Data Controller, the processing of all data related to the data subject is based on voluntary consent, and the general purpose is to ensure the provision of the service and maintain contact. The personal data specified in this chapter - with the exceptions contained in the individual sub-clauses - will be kept by the Data Controller for the period of time in accordance with the main rules set out in these Regulations, and then deleted, either at the request of the data subject within 1 working day from the date of receipt of the request, or within 1 working day from the date of receipt of the revocation of the permission for the processing of the data subject's data. deletes them within a working day.

2. The above general rule is supplemented by the data management mandated by law, about which the Data Controller informs the data subjects during the definition of individual data management.

3. As a general rule:

    - with some services, it is possible to enter additional data that helps to fully understand the needs of the data subject, but these are not conditions for using the services provided by the Data Controller.
    - personal data provided during any data management activity is stored by the Data Controller in separate data files, separately from other data provided. Only authorised Employee(s) of the Data Controller can view these data files.
    - In the absence of prior consent of the data subject, the data manager will not forward or hand over the individual data or the data files as a whole to third parties, except for mandatory data transmission and data transfer based on legislation, and will take all security measures to ensure that the data cannot be accessed by unauthorised persons.
    - The person concerned can modify, delete and/or block data recorded and stored during any data management activity, as well as request detailed information about data management, by sending a request to the following e-mail address, if no other contact information is specified in the definition of the given data management activity: pbox@korax.hu
    - the provision by the data subject of the data to be provided during each data management activity is a condition for using the services provided by the Data Controller.

B. Marketing-related data management

a. Presence and marketing on social media:

1. The data manager is available on the Facebook social portal and on other community sites (e.g. LinkedIn).

2. The use of social media sites, especially the Facebook page, and through it, contacting and maintaining contact with the Data Controller, and other operations allowed by the social media site, are based on voluntary consent.

3. The scope of those affected: Natural persons who voluntarily follow, share and like the social pages of the Data Controller, especially the page on the facebook.com social page or the content appearing on it.

4. Scope and purpose of processed data:

Affected public name	identification
Affected public photo	identification
Affected public e-mail address	contact
Social media message sent by the Affected	contact
Affected's evaluation	Quality improvement

5. The Data Controller only communicates with the data subjects via the social media site, and thus the purpose of the scope of the processed data becomes relevant when the data subject contacts the Data Controller via the social media site.

6. The purpose of the presence on social portals, especially Facebook, and related data management is to share, publish, and market the content on the website on social media. With the help of the social site, the person concerned can find out about the latest advertised jobs.

7. Based on the terms and conditions of the social media site, the data subject voluntarily consents to follow and like the content of the Data Controller.

8. The data subject can rate the Data Controller textually and numerically if the social site allows this.

9. The Data Controller also publishes pictures of various events, the Data Controller's services, etc. on its social media pages, especially on its Facebook page. The data controller can connect the Facebook page to other social media sites in accordance with the rules of the social media portal facebook.com, so publication on the Facebook page must also be understood as publication on such linked social media sites.

10. If it is not a mass recording or a recording of a public appearance (Ptk. 2:48.§), the Data Controller always asks for the written consent of the data subject before publishing the images.

11. The data subject can receive information about the data management of the given social site on the given social site.

12. Duration of data management: until deletion at the request of the data subject.

b. Website visit data::

1. The Data Controller's website may also contain links that point to pages that are not operated by the Data Controller and are only for the information of visitors. The Data Controller has no influence on the content and security of the websites operated by the partner companies, so it is not responsible for them. Please review the data management regulations and data protection declarations of the pages you visit before entering your data in any form on that page.

2. The data controller uses the following cookies:
    a. Absolutely necessary cookies: Such cookies are essential for the proper functioning of the website. Without accepting these cookies, the Data Controller cannot guarantee that the website will function as expected, nor that the user will have access to all the information the user is looking for. These cookies do not collect personal data from the data subject or data that can be used for marketing purposes.
    b. Functional cookies: These cookies ensure a consistent appearance of the website tailored to the needs of the data subject and remember the settings chosen by the data subject
    c. Targeted cookies: Targeted cookies ensure that the advertisements on the website are tailored to the interests of the person concerned.

3. The Data Controller places a set of code on the website (or any of its subpages), the purpose of which is to make the Data Controller's advertisement available to the user visiting the given website while browsing Google's websites and/or to the Data Controller or related to the Data Controller's services are searched for in the Google system. The code set does not collect, store or transmit personal data. More information on the use and operation of the code set can be found on http://support.google.com.

4. Based on all of this, the Data Controller does not use analytical systems to collect personal data.

5. The Data Controller draws the attention of users to the fact that most Internet browsers automatically accept cookies, but visitors have the option to delete them or refuse them automatically.

C. Operational data management

c. Request for information

1. The Data Controller allows the data subjects to request information from the Data Controller by entering their details detailed below.

2. The request for information is based on voluntary consent.

3. Scope of stakeholders: All natural persons who contact the Data Controller and request information from the Data Controller in addition to providing their personal data.

4. Scope and purpose of processed data:

Name	identification
Address	contact
Phone number	contact
e-mail address	contact
Text of message	Required to answer

5. The purpose of data management is to provide appropriate information for the data subject and maintain contact.

6. The activity and process involved in data management is as follows: The data subject can negotiate with the Data Controller about the Data Controller's services and/or other related issues through or in a way that is available to him or her provided by the Data Controller. Data provided via the website will be sent to the data controller by e-mail. The Data Controller will answer the data subject's question and deliver it to him - in the same way as the request for information was received, if the data subject does not provide otherwise. In accordance with the purpose of the data management, the data subject voluntarily consents to the fact that, if he provided his contact information during the request for information, the Data Controller may contact him to clarify the question or to answer it for him.

7. Duration of data management: until the goal is achieved. In the event that the provision of information has any legal effect, the Data Controller processes the data until the end of the applicable statute of limitations.

D. Data management related to the establishment and maintenance of an employment relationship

1. The Data Controller keeps wage and employment records of its Employees and temporary, temporary workers, which is used for payroll, social security and statistical data provision, as well as CXVII of 1995. based on the law, it is used in connection with the assessment of employer's tax. The personnel register is data management for documenting the facts relating to the employment relationship or other legal relationship aimed at employment (e.g. an assignment carried out as an independent activity, a business, etc.). The data of the personnel register can be used to establish facts related to the employment relationship of Employees and to provide statistical data. The personnel register contains the data of all Employees of the Data Controller.

2. Based on the regulations in force, the data controller is obliged to collect data and transfer data to the tax authority in the event of an insurance legal relationship, such as the establishment of an employment relationship, simplified employment or a contract of employment.

3. The establishment of the legal relationship is based on voluntary consent, but data management is mandatory according to CL 2017 on the taxation system. § 50 and Annex No. 1 of the Act, as well as Act LXXV of 2010 on simplified employment. §§ 3 and 11 of the Act, Act I of 2012 on the Labor Code. § 10 and CXVII of 1995 on personal income tax. based on the provisions of the law.

4. The Data Controller reserves the right to contract with a third party for the performance of payroll tasks, who/which company processes the data as the Data Controller's data processor, without the specific consent of the Employees.

5. Regarding the management of Employees' data, an employee information sheet was prepared as an annex to the regulations, the purpose of which is to inform Employees in advance about data management.

6. The Data Controller makes the filling of the advertised positions subject to the presentation of a moral certificate only if, in the case of labor hire, the commissioning partner expressly requires it for the filling of the given position. Based on the above, the purpose of the official moral certificate as a legal institution is, among other things, for the employee to prove his moral suitability to the employer in relation to the given job. The employer may ask the person concerned to do so before the establishment of the employment relationship, during the hiring process, or even during the existence of the employment relationship, if the moral suitability is really essential for the performance of the given position. The official moral certificate provides the data security-related information necessary for the establishment of the employment relationship. The check of the clean moral certificate is carried out by the employee entrusted with HR tasks, who checks the validity of the moral certificate and its content. In order for the Data Controller to be able to prove that it examined the validity and content of the moral certificate during the recruitment process, it keeps the following data on file:

    - the date of issue of the moral certificate,
    - the document number of the moral certificate,
    - the identifier of the moral certificate application.

This data is not considered special personal data, however, the authenticity and content of the moral certificate can be checked based on this data. In this way, the Data Controller does not store certificates or copies thereof either during or in connection with any other legal relationship aimed at employment.

7. Scope of stakeholders: All natural persons who establish an employment relationship or other legal relationship with the Data Controller, in connection with which the Data Controller has a reporting obligation.

8. The scope of processed data in the case of an employment relationship:

ID card/passport number	Identification
ID card/passport validity	Identification
Nationatlity	Identification
Phone number	Contact
e-mail address	Contact
job role, job description	The determination of the tasks of the Employee on the basis of Mt
Management assignment	Task definition, responsibility
internship period, trial period, fixed-term employment relationship, regular working period	Working hours register
Place of residence	to determine travel expenses
the distance traveled to work	to determine travel expenses
fact of private pension membership, date of entry (year, month), bank name and code	Data report
Social security number (in the case of a retired employee)	Data report
occupational health certificate	necessary to conclude employment
certificates issued by the previous workplace, certificate of the insurance relationship and health insurance cover	necessary for data reporting, tax return preparation, registration of insurance legal relationship
in the case of non-full-time work, the nature of the legal relationship, the name and location of the employer, in the non-full-time workplace	Data report

average monthly working time completed, activity to be performed	
Addtitional leave, use of family tax allowances, for the purpose of requesting discounted travel card that considered tax-free, or tax-free school start support - all for Employee's relative not reached the age of 16 - those data as: place and date of birth, address, mother's name, social security number, tax id. Number, the fact of having a valid student ID	Necessary for additional leave, family tax allowance, family aid
Name of Employee	For the attendance sheet
Day	
Arrival	
Departure	
Signature	
Time period	

9. The scope of processed data in case of simple employment:

name, birth surname and name	data notification to tax authorities
tax ID number	data notification to tax authorities
address	data notification to tax authorities
place of birth	data notification to tax authorities
Date of birth	data notification to tax authorities
Mother's name	data notification to tax authorities
Social security number	data notification to tax authorities
nature of simplified work	data notification to tax authorities
Job title	data notification to tax authorities
date of commencement and termination of employment	data notification to tax authorities
in the case of casual work, the number of hours worked (per day)	data notification to tax authorities
Gross salary	data notification to tax authorities
Net salary	data notification to tax authorities
place of employment	data notification to tax authorities
Normal working hours	data notification to tax authorities
bank account number	Required to pay salary

10. The scope of processed data in the case of an assignment legal relationship:

name, birth surname and name	data notification to tax authorities
tax ID number	data notification to tax authorities
address	data notification to tax authorities
place of birth	data notification to tax authorities
Date of birth	data notification to tax authorities
Mother's name	data notification to tax authorities
Start of legal relationship	data notification to tax authorities
the number of the occupational FEOR	data notification to tax authorities
beginning, code, termination of the insurance relationship	data notification to tax authorities
duration of insurance suspension	data notification to tax authorities
Assignment fee (gross, net)	data notification to tax authorities
bank account number	payment of a assignment fee
place of employment	necessary for the fulfillment of the assignment

11. The purpose of data management is to fulfil the obligations according to the law, to establish, maintain and terminate the employment/mandatory legal relationship.

12. The above data can be accessed by the management of the Data Controller and the Employee entrusted with this task.

13. The data controller preserves and records the data during the existence of the enterprise, with the prohibition of discarding the labor, wage and social security records.

14. Activity and process involved in data management:

- Before the establishment of the employment relationship, the Data Controller informs the Data Subject that he has a statutory reporting obligation to the tax and customs authorities regarding the mandatory data, which the Data Subject acknowledges in writing.
- If the Data Subject does not take note of the fulfillment of the legal obligations, he does not contribute to them, and no employment relationship, simplified employment relationship or mandate relationship can be established with him.
- After becoming aware, the Data Subject, the future Employee, establishes an employment relationship, a simplified employment relationship, a mandate relationship with the Data Controller by concluding the relevant contract.
- In order to comply with its legal obligations, the data controller reports the mandatory data to the competent first-level state tax and customs authority electronically or on the form set up for this purpose, so it transfers the data.
- The Data Controller ensures that the data is managed only by those Employees whose data management is essential. If the management of this data is not necessary for the performance of the tasks of each Employee, they cannot be known by other Employees.
- The Data Controller is obliged to ensure that the Employee, especially if he is also a data controller, can familiarize himself with these Regulations, other relevant internal regulations, instructions, etc. no later than on his first day at work.
- If it is necessary to obtain a statement from the Employee in order to establish, maintain, or terminate the employment relationship, to prove related rights or to acknowledge obligations, then before obtaining the statement, the Data Controller draws the Employee's attention to the fact, legal basis, and purpose of data processing in relation to the data provided in the statement. In the event that the validity of the employee declaration requires the presentation of a document (identity card, student card), the Data Controller does not manage the data and/or image of the document in any way, but rather certifies the presentation of the document and its validity with the signature of the authorized Employee.
- In the event that the Employee provides the data of a third party (e.g. in connection with the use of additional leave, family tax allowance), he must declare in writing that he is authorized to provide the data of the third party.
- The Employee is obliged to notify the management of the Data Controller of any change in his/her data within 5 working days from the occurrence of the change, who will take care of transferring the change.

E. Data management related to medical fitness

1. 33/1998 on the medical examination and opinion of occupational, professional and personal hygiene suitability. (VI.24.) It is carried out on the basis of NM decree. In connection with the above, the Data Controller keeps records only to the extent necessary to achieve the goal, which contains special (health) personal data regarding the natural person.

2. The Data Controller has entered into a contract with a health care provider for the purpose of determining medical suitability, therefore it does not manage the detailed medical data of the Employee, but only the existence of suitability or the document related to the

decision on the future Employee's unfitness. If the employment relationship cannot be established due to the applicant's medical incapacity, the Data Controller will immediately delete the data of the person concerned.

3. The scope and purpose of the processed data:

Name of employee	Identification
job title	Identification
the date of the occupational aptitude test	it is necessary to verify that the test has taken place
suitable/unsuitable rating	Necessary for fulfilling the job and judging the eligibility

4. The above data can be accessed by the management of the Data Controller and the authorised Employee.

5. The data controller records the data for the entire duration of the company's existence.

6. The name of the healthcare provider contracted with the Data Controller is included in the annex to these Regulations.

F. Copy of identity card

1. In accordance with the NAIH's position, the Data Controller does not make photocopies of identity cards with a photo.

2. In order to maintain the principle of data recording and data quality, the Data Controller may make a masked photocopy or scanned image of the identification cards of the Employees who are newly entering or changing data. During the copying process, the Data Manager leaves only those parts of the ID card in a state suitable for copying, which data the Employee is required to provide about himself during his entry anyway. In this case, the purpose of copying is data reconciliation. The Data Manager will immediately and irrevocably delete or destroy the copy after the comparison of the data on the masked copies - by a designated Employee - but no later than 30 days after the copy has been completed.

3. The above data can be accessed by the management of the Data Controller and the authorized Employee.

G. Data management related to occupational accidents and occupational health and safety

1. The Data Controller collects and processes personal data from the data subjects in connection with occupational health and safety, as well as during possible work accidents and inspections.

2. In the event of work accidents, in addition to personal identifiers, personal health data is also recorded with a detailed description of the event.

3. Participation in periodic trainings and the data recorded there are confirmed by the participating Employees with their signatures. The Data Controller stores the documentation containing personal data related to education (name, job title, workplace), the documents of occupational health and safety inspections, and the reports of occupational accidents in a lockable cabinet in its file cabinet. The management of the Data Controller and the authorized Employee can access the data.

4. The purpose of data management is to investigate, report and register work accidents. The Data Controller, as an employer, has a legal obligation to perform these tasks.

5. The Data Controller handles data related to occupational accidents in accordance with Act XCIII of 1993 on occupational safety. Act XCIII of 1993 on labor protection. 5/1993 on the implementation of certain provisions of the Act. (XII.26.) MüM decree and LXXXIII of 1997 on compulsory health insurance benefits. Act and LXXXIII of 1997 on compulsory health insurance benefits. 217/1997 on the implementation of the law (XII.1.) is carried out on the basis of a government decree, i.e. these laws form the legal basis for data management.

6. The scope and purpose of the processed data:

suitability of other solutions	
Causes leading to the accident	
Data of those conducting the investigation	
time of work and firefighting training	ensuring occupational safety and legal obligations
the name of the Employee holding the work and firefighting instructor	ensuring occupational safety and legal obligations
starting date of employment	ensuring occupational safety and legal obligations
Birth name	data service, the recipient of care is obliged to notify the health insurance company of any facts or data that affect entitlement to care or the payment of care within 15 days
Place and date of birth	
Social Security number	
Address	
where, when and how the accident happened	
who caused the accident (name, address)	
in the event of a vehicle-related accident, details of the service maintenance and possible authority procedures	
name, time of the health care service that treated the injury	

7. The data controller will keep the data for 5 years from the end of the calendar year of the Employee's departure.

H. Data management related to the examination of fit for work

1. In the area of the Data Controller, the Employee may only stay and perform work in a condition suitable for safe work, in compliance with the instructions and regulations related to occupational safety. The Employee is obliged to cooperate with his colleagues and to perform his work in such a way that he does not endanger the physical integrity of others or himself.

2. Employees are prohibited from being under the influence of alcohol or other mind-altering substances in the entire territory of the Data Controller. Employees must not only be able to work when they report to work, but must maintain this condition until the end of their working hours.

3. The Data Controller may subject its Employees to a breathalyzer test, which may be initiated by the head of the relevant organizational unit, in the case of Employees under his supervision.

4. The head of the relevant organizational unit may initiate a breathalyzer test in case of suspicion at any time during working hours in compliance with the provisions of the Occupational Safety and Health Act.

5. In all cases, a report must be taken on the examination.

6. The purpose of data management is to ensure the maintenance of employees' working capacity and safe working conditions.

7. The scope and purpose of the processed data:

Name of employee	identification
Job title	identification
Date	necessary for determining working hours
the name of the Employee performing the inspection	identification
result (positive, negative,refuse)	proof of work capacity is required
The inspected employee's comment, if the result is disputed	proof of work capacity is required (deciding whether further examination is necessary)
The inspected employee's consent to perform blood test	proof of work capacity is required

8. The legal basis of data management:

   The Data Controller has a legal obligation to comply with Act XCIII of 1993 on labor protection. § 60 (1) and § 54 (7) b) of the Act, as well as § 11 (1) and § 52 (1) of Act I of 2012 on the Labor Code. a) to ensure the requirements of safe working, therefore you are obliged to make sure regularly whether the Employees comply with the provisions applicable to them.

9. The Data Controller's Employee entrusted with this task is entitled to check compliance with the rules.
10. Activity and process involved in data management:
    - At the initiative of the head of the organizational unit, the commissioned Employee may order an alcohol test for any Employee at any time. However, the control of the influence of alcohol must not involve the violation of the Employee's human dignity.
    - In all cases, the commissioned Employee will take minutes of the inspection.
    - In the event that the checked Employee does not accept the result, the company doctor or other health care provider may initiate a blood alcohol level check with a blood sample.
    - If the Employee to be inspected refuses to submit to the inspection, the authorized Employee shall immediately notify the exercise of the employer's authority. Refusal to check is automatically considered unfit for work.
11. The data can be accessed by the Employee entrusted with occupational health and safety tasks and the management of the Data Controller.
12. The data controller will keep the data for 5 years from the end of the calendar year of the Employee's departure.

I. Data management related to the control of Employees

1. The Data Controller may, if necessary, check the Employees regarding their behavior related to the employment relationship. The legal basis for the control is the legitimate interest of the Data Controller based on Paragraphs (1)-(2) of Section 11 of the Mt.

2. The Data Controller informs the Employees in advance about the use of the technical tools that are used to check it.

3. The Data Controller has carried out interest assessment tests in connection with the control of Employees, which form an annex to these Regulations.

4. If the circumstances of the inspection do not exclude the possibility of this, the Data Controller provides the opportunity for the data subject to be present during the inspection. In the case of all types of audits, the Data Controller informs the data subjects before the audit begins about the method and purpose of the audit, the employer's interest in the audit, who can perform the audit, the rights and remedies of the data subject and the course of the procedure.

5. As a general rule, the inspections are carried out by the management of the Data Controller and the Employee performing the duties of the system administrator.

6. Control of company assets:

   6.1. The Data Controller can provide Employees with a computer, e-mail address and Internet access for work purposes. The devices provided by the Data Controller can only be used for work purposes, therefore the Data Controller can check all data stored on the laptop. If the Employee stores his personal data for private purposes on the

devices provided for the purpose of work, the Data Controller, as an employer, may also apply employment law legal consequences against him. In this case, the Data Controller may also get to know these data during the inspection of the computer, if the data subject does not indicate the personal nature of this data during the inspection. If, during the check, the data subject indicates which data are of a private nature, the Data Controller will not check this data. The Employee may not object to this data management, since the storage of personal data on the Data Controller's devices, not for work purposes, is considered to be the data subject's consent to the data management. The Data Controller informs the Employees about this, as well as the fact of archiving and system administrator activities, in writing before handing over the devices. The data subject acknowledges that the Data Controller performs backups at specified intervals in relation to the data file on the company laptop, which data is archived for the period specified in the Data Management and Data Protection Regulations.

6.2. In the case of company mobile phones, there is a fixed amount available for each job, and if the amount is exceeded, the Employee must pay the amount above the limit, because it is automatically classified as a private call. The Data Controller reserves the right to request a complete call list for the given phone number, but in this case calls the data subject to make the called numbers unrecognizable on the document for private calls. The Data Controller does not process personal data in this context.

7. Verification of company e-mail addresses

7.1. At the same time as the employment relationship is established, the Data Controller informs the Employees that all e-mail addresses in which the Data Controller is listed as a name extension are the property of the Data Controller, and correspondence carried out at these addresses is considered to be correspondence for work purposes. The contents of received and sent e-mails are the property of the Data Controller. The Employee may not use company e-mail addresses for private purposes, if he violates this provision, the Data Controller, as an employer, may apply labor law legal consequences against him. The Data Controller is entitled to inspect the correspondence conducted at these addresses in connection with the fulfillment of the obligations related to the employment relationship defined in Section 11.1 of Mt. The Data Controller is entitled to back up correspondence at these addresses at specified intervals, in order to ensure the continuity and stability of the electronic mail system, which data is permanently deleted after the period specified in the Data Management and Privacy Policy.

7.2. If the Employee also stores personal data in his company e-mail address without an explicit reference, the Data Controller may learn this data during the verification of the e-mail address, if the data subject does not indicate the personal nature of this data during the verification. If, during the check, the data subject indicates which data are of a private nature, the Data Controller will not check this data. The Employee may not object to this data processing, as the storage of personal data not for work purposes, but at the e-mail address of the Data Controller, is considered to be the data subject's consent to data processing.

7.3. Adhering to the principle of gradation, the Data Controller checks only the e-mail address and the subject of the letter as a first step. The Data Controller will only check

the content of the letters if it can be assumed that any of the Employee's legitimate interests have been violated. The Data Controller strives for gradualism, therefore, even in case of suspicion, it only checks the content of emails that, based on their size or other characteristics, may be suitable for committing a legal violation, and even then only for a limited time interval.

7.4. The Data Controller, as an employer, repeatedly draws the attention of the Employees on a six-monthly basis that the mail system and the company laptop can only be used for work purposes, therefore, when using the e-mail account, they should not send letters for private purposes, or store personal data on the company laptop.

7.5. Upon termination of the employment relationship, the employer must immediately terminate the Employee's access to the e-mail address. You can check the existing e-mails and e-mails created in the name of the concerned Employee for 30 days from the termination of the employment relationship in view of the legitimate interest of the employer. In this case, the legal basis for data management is the legitimate interest of the Data Controller (proper reception and management of customer data). During the inspection, the Data Controller automatically informs the sender of the letter that the letter will be read by another person in the future, as well as who he can contact in the future if he is looking for the employer. If the private nature of the content becomes apparent, the Data Controller will not check it.

8. The control of Internet usage
   The use of the Internet during working hours is only permitted for work purposes.
   As a result of the above, the related data and browsing history are considered company data. During a possible data controller check, these data lose their personal data character, and the Data Subject's consent provides a legal basis for knowing and storing these data

9. The purpose of data management:
   In accordance with the Data Controller's legitimate business interests, ensuring the security and stability of the Data Controller's devices, systems and data.

10. The scope and purpose of the processed data:

e-mail addresses	contact
Phone numbers	contact
browsing data, cookies	secure internet use, data fraud prevention, virus protection
data stored on a company computer	Archiving of relevant data for the business process

11. Data storage deadline:
    1 year from the date of the inspection, but no later than the statute of limitations for claims related to the inspection.

J. Data management related to the use of the GPS navigation system

1. The data controller installed a GPS tracker in his owned vehicle, which he complies with CXII of 2011 during data management. Act, the GDPR, the provisions of Act I of 2012, as well as the NAIH's recommendation on the basic requirements of the electronic monitoring system used in the workplace, as well as the previous, published decision of the NAIH, the position of data protection working group No. 29.

2. The legal basis for data management is the legitimate interest of the Data Controller, i.e. the precise organization of individual work processes, and the value of the vehicle justifies this.

3. The data controller declares that the vehicle equipped with a GPS tracker cannot be used for private purposes.

4. The scope of those affected: The management of the Data Controller, as well as all employees who drive a vehicle equipped with a GPS tracker and are also present in the vehicle

5. The scope and purpose of the processed data:

vehicle number plate	Identification
vehicle coordinate identification	Identification

6. The purpose of data management is to protect the Data Controller's business interests, to facilitate the fulfillment of the road registration driving obligation, and to protect the assets of the motor vehicle.

7. The place of data storage: the office of the Data Controller's accountant, the exact address of which can be found in the list of Data Processors in the annex to these Regulations.

8. Data storage period: 7 days from recording, 8 years for accounting documents.

9. Duration of data management: 120 days from the date of recording, if the data is used in official or judicial proceedings, it will be kept until the final conclusion of the proceedings.

10. Method of data management: done electronically and automatically.

11. Data source: directly from the person concerned.

12. Data disclosure: will be disclosed to third parties, these persons have been named in the annex to these regulations.

13. Automated decision-making, profiling: does not take place in connection with data management.

K. Complaint handling

1. The Data Controller provides an opportunity for the data subject to communicate his or her complaint regarding the Data Controller's behavior, activities or omissions orally (in person, by phone) or in writing (e-mail, post).

2. Scope of stakeholders: All natural persons who wish to file a complaint against the Data Controller.

3. The purpose of data management is:

Identification of the person concerned and the complaint, as well as the recording of data resulting from legal obligations.

4. The scope and purpose of the processed data:

name	identification
the identifier of the complaint	identification
the date of receipt of the complaint	identification
Phone number	contact
personal data provided in the conversation	identification
Correspondence address	contact
the complained activity/omission	investigation of the complaint
complaint	investigation of the complaint

5. The purpose of data management is to ensure that complaints are made and to maintain contact.

- Activity and process involved in data management:
- The data subject communicates his complaint to the Data Controller orally or in writing.
- If the data subject makes his complaint verbally, the Data Controller will record it.
- The Data Controller investigates and responds to complaints received within a reasonable time frame.

7. Data management period:

The Data Controller is subject to the CLV of 1997 on consumer protection. based on paragraph 17/A.§ (7) of the Act, the record of the complaint and the copy of the response are handled for five years.

L. Data management related to the licensing of private individuals' solar panels

1. The data controller initiates an authorization procedure with the electricity network provider.

2. Contacting, maintaining contact with the Data Controller and other operations permitted by the electricity network service provider are based on voluntary consent.

3. Scope of the affected parties: The natural persons with whom the Data Controller concludes a solar panel installation contract.

4. The scope and purpose of the processed data:

Data of the contracting party	
Name	Identification, contact
Phone number	Identification, contact
E-mail address	Identification, contact
Birth name	identification
Mother's birth name	identification
Place and date of birth	identification
Address /correspondence address	Identification, contact
tax identification number	identification
ID card type and number	identification
Data of the place of use, map number	Identification, contact
Measurement point POD identifier at the point of use	identification
User ID	identification
Contract number with network power supplier	identification
Consumption meter factory number	identification

5. The data controller communicates with the data subjects only in connection with the authorisation procedure of the electricity network provider.

6. Duration of data management: until deletion at the request of the data subject.

XI. Data processing, data transmission

1. As a general rule, the Data Controller does not use external data processors, it processes the data it handles itself.

2. In the event that the Data Controller entrusts a third party with accounting, payroll, storage/server services, system administrator or other data processing tasks, the data of this partner as a data processor will be specified in the annex to the Regulations.

3. In the event that the Data Controller uses a data processor, the following rules must be followed and observed:

    - The Data Controller is responsible for the legality of the instructions regarding data processing operations for the data processor.
    - The data processor is responsible for processing, changing, deleting, transmitting and disclosing personal data within the scope of its activities and within the framework defined by the Data Controller.

- The data processor may not use another data processor in the performance of its activities. If you use it, you must ensure full compliance with data protection regulations.
- The data processor may not make substantive decisions regarding data management, may only process the personal data it comes to know in accordance with the provisions of the Data Controller, may not perform data processing for its own purposes, and must store and preserve the personal data in accordance with the provisions of the Data Controller.
- After becoming aware of the data protection incident, the data processor shall notify the Data Controller without undue delay.
- The transmission of data, as well as the connection of the database managed by the Data Controller with another data controller, takes place only on the basis of the consent of the data subject or authorization by law.
- The data controller only forwards personal data if its legal basis is clear, its purpose is clear, and the person of the recipient of the data transmission is specified.
- In the case of data transmission subject to the data subject's consent, the data subject shall give his/her declaration in the knowledge of all data affected by the data transmission, the recipient and purpose of the data transmission, and the expected time of data processing.

4. Data may be forwarded within the Data Manager only if the recipient's data controller also has access rights to the data(s) to be forwarded. Before forwarding, the data controller is obliged to obtain information related to the access rights of the recipient data controller.

5. Data transmission to a third party other than the Data Controller:

   The Data Controller may transmit the data determined by the data subject to its contractual Partners if the Data Controller has named the Partner for the data subject, defined the expected data processing time and purpose and the data subject has consented to the data transmission before the data transmission.
   The Data Controller can also name the Partners by means of information, if it makes it available to those concerned.
   Data Management Partners are defined in the Annex to the Regulations. In accordance with the previous point, the Data Controller may only transmit to its Partners the data to which the data subject has previously consented.
   The Data Controller will do everything that is expected of him in order to enforce the principles of data protection and transmit the appropriate, but as little data as possible to his Partners.

   In addition to data transmissions based on legal authorization, the data controller may transmit data based on and within the scope of the data subject's authorization, therefore the transmission of other data to others and outside of the authorization is prohibited.

XII. Data security, storage of personal data, information security

1. Personal data can only be processed according to the purpose of the given data management.

2. The data controller ensures the security of the data. To this end, it takes the necessary technical and organizational measures with regard to the data files stored through IT tools.

3. The data controller ensures that the data security rules stipulated in the relevant legislation are enforced.

4. It takes care of the security of the data, takes the technical and organizational measures and develops the procedural rules that are necessary to enforce the governing legislation, data and privacy protection rules.

5. The data controller uses appropriate measures to protect the data against unauthorized access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, as well as against becoming inaccessible due to changes in the technology used.

6. The Data Controller can also ensure the enforcement of data security rules by means of regulations, instructions, and procedural rules that differ in content and form from these regulations.

7. The data controller is obliged to act in accordance with the rules specified in the relevant legislation, these Regulations and other regulations related to data protection and others, which ensure a high degree of data security.

8. In order to enforce the conditions of data security, the Data Controller ensures the appropriate preparation of the Employees concerned, if it employs an Employee.

9. When defining and applying measures for data security, the data controller takes into account the state of the art at all times and chooses from several possible data management solutions the one that ensures a higher level of protection of personal data, unless it would represent a disproportionate difficulty.

10. As part of its duties related to IT protection, the Data Controller ensures in particular:

    - About the measures ensuring protection against unauthorized access, including the protection of software and hardware devices, as well as physical protection (access protection, network protection);
    - About the measures that ensure the possibility of restoring data files, including regular backups and the separate, safe handling of copies (mirroring, backups);
    - Protection of data files against viruses (virus protection);
    - About the physical protection of data files and the devices that carry them, including protection against fire damage, water damage, lightning strikes, and other elemental damage, as well as the reparability of damage caused by such events (archiving, fire protection).

11. The Data Controller provides the IT environment used for the management of personal data during the provision of the service in such a way that:
    - connects the personal data provided by the data subject only and exclusively with the data and in the manner specified in these regulations.

- ensures that only employees of the Data Controller have access to personal data for whom this is absolutely necessary for the performance of their duties arising from their job duties.
- all changes to the data are made by indicating the date of the change.
- the incorrect data will be deleted within 24 hours based on the relevant request.
- the data is backed up.

12. The Data Controller provides the required level of protection during the processing of the data - especially their storage, correction, deletion - when requesting information or protesting.

13. Data transmission takes place with the consent of the data subject, without prejudice to his interests, confidentially, with the provision of a fully adequate IT system, and in compliance with the purpose, legal basis and principles of data management. The Data Controller will not forward the data subject's personal data or make them available to third parties without their consent, unless this is required by law.

14. The other data concerned, which cannot be linked directly or indirectly, and cannot be identified - hereafter anonymous - are not considered personal data.

15. The Data Controller keeps records of any data protection incidents, indicating the facts related to the data protection incident, its effects and the measures taken to remedy it. The Data Controller shall report any data protection incident to the National Data Protection and Freedom of Information Authority without delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident is likely to pose no risk to the rights and freedoms of natural persons looking at.

16. Data protection incident: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled; (Regulation, Article 4, 12)

17. The most frequently reported incidents can be, for example: loss of laptop or mobile phone, personal data is not secure; unsafe transmission of data, unauthorized copying and transmission of customer and customer partner lists, attacks against servers, website hacking.

18. The management of the Data Controller is responsible for preventing and managing data protection incidents and complying with the relevant legal regulations.

19. Accesses and access attempts must be logged on the IT systems and analyzed continuously.

20. If the employees of the Company who are entitled to control notice a data protection incident during the performance of their duties, they must immediately notify the management of the Data Controller.

21. The employees of the Data Controller are obliged to report to the management of the Data Controller if they detect a data protection incident or an event indicating such a data protection incident.

22. A data protection incident can be reported to the e-mail address pbox@korax.hu or to the Data Controller IV. on the phone number specified in chapter 1, on which employees, contractual partners, and stakeholders can report the underlying incidents and security weaknesses.

23. In the event of a data protection incident being reported, the management of the Data Controller - with the involvement of the IT and legal expert - will immediately investigate the report, during which the incident must be identified and it must be decided whether it is a real incident or a false alarm. It must be examined and determined:

- the time and place of the incident,
- description of the incident, circumstances, effects,
- the scope and number of data compromised during the incident,
- the range of persons affected by the compromised data,
- a description of the measures taken to prevent the incident,
- a description of the measures taken to prevent, eliminate and reduce the damage.

24. In the event of a data protection incident, the affected systems, persons, and data must be demarcated and separated, and evidence supporting the occurrence of the incident must be collected and preserved. After that, you can begin to repair the damage and restore legal operation.

25. Data protection incidents must be registered in accordance with the annex. Data relating to data protection incidents in the register must be kept for 5 years.