PRIVACY POLICY AND DATA PROCESSING NOTICE OF MERTCONTROL HUNGARY KFT TO DATA SUBJECTS

June 2019

CONTENTS

CHAPTER I – GENERAL PROVISIONS

1. Purpose of the Policy

The purpose of this Policy is to determine those internal rules and to establish those measures that secure that the processing performed by Mertcontrol Hungary Kft, acting as controller, is in compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter as: GDPR or the Regulation) and Act CXII of 2011 on the Information Self-determination Right and the Freedom of Information (hereinafter as: Information Act).

2. Controller's name:

2.1. COMPANY NAME:	Mertcontrol Hungary Kft.
2.2. REGISTERED OFFICE:	2144 Kerepes, Szabadság út 13.
2.3. BUSINESS ESTABLISHMENT:	-
2.3. COMPANY REGISTRATION NUMBER:	13-09-155469
2.4. TAX NUMBER:	12178249-2-13
2.5. WEBSITE:	www.mertcontrol.com
2.6. E-MAIL:	info@mertcontrol.com
2.7. PHONE:	06-1-455-4010
2.8. NAME OF THE REPRESENTATIVE:	Csongor Kállay
2.9. NAME OF THE DATA PROTECTION OFFICER:	-
2.10. ADDRESS:	-
TELEPHONE NUMBER:	-
2.11. E-MAIL:	-

(hereinafter as: Company or Controller)

3. Scope of the Policy

3.1. The scope of this Policy shall include the processing by the Company of

personal data of natural persons.

3.2. For the purposes of this Policy, private entrepreneur, private company and licensed small-scale farmer clients shall be considered as natural persons.

3.3. The Policy does not cover the processing of personal data which concern legal persons, including the name and the form of the legal person and the contact details of the legal person. (Article 14 of the GDPR)

3.4. This Policy has to be interpreted in line with the data protection legislation effective as of 1 June 2019.

4. Definitions

For the purposes of this Policy, the definitions specified in Article 4 of the Regulation shall be applied. Accordingly, we hereby highlight the following key terms and definitions:

1. **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;
4. **'pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational

measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

5. ‘**filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

6. **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

7. ‘**processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

8. **‘recipient’** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with EU or Member State law shall not be regarded as recipients; the processing of such data by those public authorities must be in compliance with the applicable data protection rules in line with the purposes of the processing;

9. **‘third party’** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

10. **‘consent of the data subject’** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

11. **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

CHAPTER II – ENSURING LAWFULNESS OF PROCESSING

1. Processing based on the data subject’s consent

1.1. Any other statement or conduct which clearly indicates in the given context the data subject's acceptance of the proposed processing of his or her personal data shall also qualify as consent. Silence or inactivity should not therefore constitute consent.

1.2. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

1.3. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

1.4. The Company may not make the conclusion or performance of a contract conditional on the granting of a consent to the processing of such personal data that are not necessary for performance of the contract.

1.5. It shall be as easy to withdraw as to give consent.

1.6. If the personal data have been collected based on the data subject’s consent, the controller shall be entitled to process the collected data for the purpose of compliance with a legal obligation imposed on the controller, even without any further separate consent – unless otherwise stipulated by law – and even after the data subject withdrew his/her consent.

2. Processing based on performance of a legal obligation

2.1. In case the data is processed based on a legal obligation, the underlying piece of legislation shall be applied in terms of the scope of data to be processed, the purpose of data processing, the data retention period and the recipients.

2.2. The processing based on compliance with a legal obligation shall be

independent from the data subject's consent since processing is required by law. In this case, it must be communicated to the data subject prior to commencement of the data processing that the processing is mandatory, furthermore the data subject must be informed (prior to commencement of the data processing) in a clear and detailed manner about all facts related to processing of his/her data, in particular about the purpose and legal basis of data processing, the person(s) entitled to perform processing and the technical tasks of processing, the duration of processing, whether the controller manages the personal data of the data subject in order to perform a legal obligation of the controller and also about the group of persons that can access the data. The information shall also cover the rights of and remedies available to the data subject regarding the processing. In the case of mandatory data processing, this communication may also be fulfilled by disclosure of a reference to the legal provisions containing the above information.

3. General Data Processing Notice of the Company

3.1. This Policy contains the general data processing notice of the Company in a consolidated version and it is required to be made available at the Company's registered office.

3.2. Additionally, the different categories of data subjects (such as employees or job applicants, upon recording of their data) must be informed directly as well about the fact of data processing and the rights of the data subjects.

3.3. The Company shall be obliged to ensure the exercising of the data subject's rights in the course of each and every data processing actions executed by the Company.

CHAPTER III – PROCESSING RELATED TO THE EMPLOYMENT RELATIONSHIP

1. Employment and personnel records

1.1. Only such data can be requested from the employees and be registered and only such occupational medical aptitude tests can be carried out that are necessary to establish, maintain or terminate the employment relationship or to secure the social and welfare benefits, provided that these do not violate the employee's moral rights.

1.2. The below data of the employee shall be processed by the Company under the legal title of performance of a contract, for the purpose of establishing, performing or terminating the employment relationship:

1. name
2. name at birth
3. date of birth
4. mother's name
5. address
6. nationality
7. tax identification number
8. Social Security Number
9. pensioner ID number (if the employee is a pensioner)
10. phone number
11. e-mail
12. number of the ID card
13. number of the official card verifying the address
14. bank account number
15. online identifier (if any)
16. start and end date of employment
17. post of employment
18. copy of the certificate verifying education, qualification
19. photograph
20. CV

21. amount of the salary, data related to salary payment and other benefits
22. any debt to be deducted from the employee's salary based on a final and enforceable resolution or pursuant to a legal regulation or his/her written consent, as well as the entitlement thereto
23. evaluation of the employee's work
24. way and reasons of termination of the employment relationship
25. depending on the given post of employment (due to protection of the employer’s significant financial interest, secret protected by law, or other specifically defined interests protected by law) the presentation of the certificate of no criminal record
26. summary of the occupational aptitude tests
27. if the employee is member of a private pension fund or voluntary mutual insurance fund, the name of the fund, its ID number and the employee’s membership number
28. passport number in case of foreign workers; designation and number of the document verifying his/her eligibility for employment
29. data recorded in the records about the employee’s accidents
30. data required for the use of welfare services, commercial accommodation
31. data recorded by the camera and access control system and positioning systems applied by the Executive Office for security and property protection purposes.

1.3. Sickness related data shall be processed by the employer only for purpose of fulfilment of a right or obligation determined in the Labour Code.

1.4. Recipients of personal data: head of the employer, the person exercising the employer’s rights, the Company’s employees and processors performing employment related tasks.

1.5. Personal data may be stored for 3 years following termination of the employment relationship.

1.6. The mandatory communication about the processing of the employee’s personal data and his/her moral rights – to be delivered to the employee upon conclusion of the employment contract – is contained in Annex 2.

2. Processing related to the employee's aptitude tests

2.1. Only such an aptitude test can be applied regarding the employee that is required by law in terms of the given employment relationship or which is necessary for exercising a right or performance of an obligation determined in a rule applicable to the employment relationship. Prior to the test, detailed information shall be provided to the employee – among others – about the skills and abilities the aptitude test intends to measure, and also about the tools and methods used for the test. If the execution of the test is required by law, the employee needs to be informed about the title and exact identification details of the concerned piece of legislation.

2.2. The employer shall have the right to request the employee to complete the test sheets aimed to measure his/her fitness and preparedness for work both prior to establishment and during the term of the employment relationship.

2.3. A larger group of employees can be requested to complete test sheets suitable for researching psychological or personality traits, only if it is clearly related to the employment relationship and its objective is to perform and organize work processes more efficiently, and provided that the data revealed during the analysis cannot be linked to individual employees, meaning that the data are processed anonymously.

2.4. Scope of personal data that can be processed: fact of fitness for the job (aptitude) and the conditions necessary for that.

2.5. Legal basis of processing: the employer's legitimate interest.

2.6. Purposes for which the personal data are processed: to establish, maintain the employment relationship, to fill in the position.

2.7. The recipients or categories of recipients of the personal data: the tested employees and the specialists performing the test can learn the results of the test. Only those pieces of information may be provided to the employer whether the tested person is fit for the given work or not, and what conditions need to be ensured for that purpose. However, the details of the test and its entire documentation shall not be disclosed to the employer.

2.8. Period of processing of the personal data: 3 years following termination of the employment relationship, except for the personal data related to the calculation of the pension. In the latter case the controller-employer shall keep the employment documents related to the employee's insurance relationship, containing information on the length of service or income to be taken into account in determining the pension, for 5 years after reaching the retirement age applicable to the employee. If the employer is dissolved or terminated without legal successor, it shall be obliged to report the place where the employment documents are kept to the competent pension insurance administration authority.

3. Processing of the data, applications, CVs of job applicants

3.1. Scope of personal data that can be processed: the natural person's name, place and date of birth, mother's name, address, qualification related data, photograph, phone number, e-mail, the employer's notes recorded about the applicant. Annex 4 shall be applied in terms of the applicant's declaration of consent to the data processing.

3.2. Purposes for which personal data are processed: assessment of the application, conclusion of the employment contract with the selected candidate. The data subject needs to be notified if the employer chose someone else for the concerned job.

3.3. Legal basis of processing: performance of a contract. Processing shall be deemed lawful if it is necessary in the context of a contract or the intention to enter into a contract, or if it is necessary in order to take steps at the request of the data subject prior to entering into the contract.

3.4. The recipients or categories of recipients of the personal data: the Company's executive entitled to exercise the employer's rights at the Company, employees in charge of HR tasks.

3.5. Data retention time of the personal data: it depends on the assessment of the application: if the application is deemed successful (when an employment status is established), the provisions applicable to the employee shall be applied: if the application is unsuccessful or withdrawn, the Controller shall

be obliged to erase the applicant's data permanently, within 5 days from the date when the application is declared unsuccessful or is withdrawn.

3.6. Only upon the data subject's explicit, clear and voluntary consent can the employer keep the applications, provided that the employer needs to keep these in order to achieve its data processing purpose in line with legislation. This consent shall have to be requested from the applicant after the job application procedure is closed.

4. Rules of inspection of the assets provided by the employer and legal consequences

4.1. The head of the employer or the person exercising the employer's rights shall have the right to inspect the assets and process the data.

4.2. It shall be guaranteed that the employee can be present during the inspection, unless the circumstances of the inspection preclude this.

4.3. Prior to the inspection, the employee must be informed of the interests of the employer giving rise to the inspection; who may perform the inspection on behalf of the employer, the rules according to which the inspection may take place (a gradual approach must be applied), what are the rules procedure, the rights and remedies they have regarding the inspection related data processing.

4.4. Gradual approach shall be applied in the course of the inspection. It must be established primarily from the title (heading) and subject matter data whether the concerned content is related to the employee's job-related tasks and not for personal purposes. Non-personal content can be reviewed by the employer without restriction.

4.5. If contrary to the provisions of this Policy, it is established that the employee used the asset for personal purposes, the employee must be instructed to delete any personal data immediately. In the absence of the employee or in the absence of their cooperation, the personal data will be deleted by the employer during the inspection. The employer shall have the right to enforce labour law sanctions against the employee on the grounds of use of the asset in violation of the policy or the employer's instructions.

4.6. The employee may exercise the rights determined in the Chapter of the employer's privacy policy dedicated to the data subject's rights in connection with the data processing applied in relation to the inspection of the asset.

CHAPTER IV – CONTRACT RELATED PROCESSING

1. Client data

1.1. Under the legal title of performance of a contract, for purpose of conclusion, performance, termination of the contract and provision of contractual discounts, the Controller shall process the following data of the natural person with whom the Controller entered into contract: name, name at birth, date of birth, mother's name, address, tax identification number, tax number, entrepreneur or licensed small-scale farmer license number, ID card number, address, registered office, business establishment address, phone number, e-mail address, website address, bank account number. This data processing shall qualify as legitimate, even if it is necessary in order to take steps at the request of the data subject prior to entering into the contract. Recipients of personal data: the Controller's employees in charge of customer service duties, accounting, tax related tasks, and the Controller's data processors. Retention period of personal data: 5 years following termination of the contract (general civil law limitation period), or the special limitation period applied in terms of the specific legal relationship.

1.2. The legal basis of processing of the natural person contracting party's data provided under the contract for accounting and taxation purposes shall be the 'compliance with a legal obligation' and in this regard the data retention period shall be 8 years.

1.3. The personal data, address, e-mail, phone number and online identifier of the natural person (provided under the contract) signing the contract and acting on behalf of the legal person entering into contract with the Company shall be processed for the purposes of communication (liaising) and exercising of the contractual rights and obligations, and the legal basis of processing shall be 'legitimate interest'. Retention period of these data shall be 5 years following termination of the contract. When data are processed based on legitimate interest, the data subject shall have the priority right to object to the processing.

1.4. The name, phone number, e-mail address and online identifier of the natural person not signing the contract, but indicated as contact person in the contract concluded with the Company, shall be processed by the Company for purpose of communication (liaising) and exercising of the contractual rights and obligations, under the legal title of legitimate interest, taking into account that the contact person has an employment related legal relationship with the contracting party, hence this data processing does not adversely affect the data subject's rights. Contracting party declares that it has informed the concerned contact person about the data processing to be performed in relation to his/her contact person status. Retention period of these data shall be 5 years following termination of the contact person status.

1.5. Recipients of the personal data in terms of all data subjects: the Company's members involved in concluding and performing the contract, its contact persons, employees in charge of customer service duties, accounting, tax related tasks, and the Company's data processors.

1.6. The personal data may be handed over to the accounting firm (accountant) commissioned by the Company for taxation and accounting purposes, to the Hungarian Post (Magyar Posta Zrt) or to the employed courier service for the purpose of mailing and delivery and to the security service provider of the Company for the purpose of property protection.

1.7. Processing shall be deemed lawful if it is necessary in the context of a contract or the intention to enter into a contract, or if it is necessary in order to take steps at the request of the data subject prior to entering into the contract, therefore even the personal data collected within the framework of contract offers/proposals can be processed under the legal title of 'performance of a contract', in line with the provisions of this Section. The Company shall be obliged to notify the party submitting the offer/proposal or the recipient of the offer/proposal about this, upon submitting or receiving an offer/proposal.

1.8. The data processing provisions and communication to be applied in the contracts to be concluded by the Company shall be contained in the individual contract and the Annexes attached thereto. It shall be a duty and

obligation of the Company's employee to ensure that the data processing provisions are incorporated into the contract.

CHAPTER V – PROCESSING BASED ON LEGAL OBLIGATIONS

1. Processing carried out for the purpose of performance of tax and accounting obligations

1.1. Under the legal title of ‘compliance with a legal obligation’, the Company shall process the data (as defined by law) of the natural persons doing business with the Company as suppliers, for the purpose of fulfilling its tax and accounting obligations. The processed data based on Articles 169 and 202 of Act CXXVII of 2017 on the value added tax, in particular: tax number, name, address, tax status; based on Article 167 of Act C of 2000 on Accounting: name, address, name of the person or organization ordering the economic transaction, signatures of the authorizing officer and the person verifying execution of the order, as well as – depending on the organization – the signature of the inspector; in documents of inventory movement and cash receipts, the signature of the recipient, and the signature of the payer in counter-receipts, based on Act CXVII of 1995 on Personal Income Tax: the entrepreneur’s license number, licensed small-scale farmer license number, tax identification number.

1.2. Personal data may be stored for 8 years following termination of the legal relationship underlying the legal basis.

1.3. Recipients of the personal data: the Company’s processor in charge of taxation, accounting, payroll accounting, and social security tasks.

2. Processing by the paying agent

2.1. Under the legal title of ‘compliance with a legal obligation’, the Company shall process the personal data (as defined by tax laws) of those data subjects – employees, their family members, workers, other recipients of benefits – regarding whom the Company acts as a paying agent (payer) within the meaning of Article 7(31) of Act CL of 2017 on the Rules of Taxation (hereinafter as: Act on the Rules of Taxation), for purpose fulfilling its tax and payroll tax obligations (determination of taxes and advance taxes,

payroll taxes, payroll accounting, social security and pension related administrative tasks). The scope of the processed data is determined by Article 50 of the Act on the Rules of Taxation, and shall include, in particular, the following: personal identification data of the natural person (including his/her previous names and titles, too), gender, nationality, the tax identification number and social security number of the natural person. If the tax laws impose legal sanctions regarding this, the Company may process the employee's health data (Article 40 of the Personal Income Tax Act) and trade union membership data (Article 47(2)(b) of the Personal Income Tax Act) for the purpose of performance of tax and payroll tax obligations (payroll accounting, social security administration).

2.2. Personal data may be stored for 8 years following termination of the legal relationship underlying the legal basis.

2.3. Recipients of the personal data: the Company's processor in charge of taxation, accounting, payroll accounting, and social security tasks.

3. Processing of documents of lasting value as per the National Archives Act

3.1. Under the legal title of compliance with its legal obligation, the Company shall process its records qualifying as documents of lasting value as per Act LXVI of 1995 on public records, public archives, and the protection of private archives (the National Archives Act) for the purpose of keeping the Company's archive records of lasting value in good and usable condition for future generations. Data retention time: the period lasting until delivery to the public archives.

3.2. Recipients of personal data: head of the Company, the Company's employee in charge of records management or archiving, associate of the public archives.

CHAPTER VI – DATA SECURITY MEASURES

1. Data security measures

1.1. During the Company's data processing actions performed for any and all purposes and legal bases, the Company is required to take all technical and organisational measures and implement the procedural rules that are needed to enforce the provisions laid down in the Regulation and the Information Act to ensure the protection of personal data.

1.2. The Controller shall apply the appropriate measures to prevent the accidental or unlawful destruction, loss, alteration, damaging, unauthorised disclosure of, or access to the data.

1.3. The personal data shall be classified and handled by the Company as confidential data. The Company shall impose an obligation of confidentiality to the employees regarding the processing of the personal data, to be incorporated into the individual employment contract. Access to the personal data shall be restricted by the Company by allocating different access levels.

1.4. The Company shall protect the IT systems with firewall and antivirus protection.

1.5. The electronic processing and record-keeping of data shall be performed by the Company through a computer program meeting the requirements of data security. The program shall secure that the data can be accessed only with purpose limitation, under controlled circumstances, only by persons who are required to access the data to fulfil their duties.

1.6. In the course of automated data processing of personal data the controller and the processor shall ensure by additional measures:

a) the prevention of unauthorised data input;

b) the prevention of the use of automated data-processing systems by unauthorised persons using data communication equipment;

c) the possibility to verify and establish if any personal data was or may be transferred or transmitted by means of a data transmission device

and to which entities;

d) the possibility to verify and establish which personal data were entered into the automated data processing systems, by whom and when;

e) the recoverability of the installed systems in the event of system failure and

f) the reporting of errors occurring in the course of automated data processing.

1.7. The Company shall provide for monitoring and controlling both incoming and outgoing electronic communication in order to protect personal data.

1.8. Sharing of personal data processed by the Company through the Internet shall be prohibited save for the exceptions specified by law or sectoral legal regulations.

1.9. Records under ongoing work or processing may only be accessed by the administrators in charge; documents containing personnel, payroll, HR and other personal data shall have to be kept locked up safely.

1.10. Proper physical protection of the data and the devices/carriers containing those data shall have to be ensured.

CHAPTER VII – HANDLING OF PERSONAL DATA BREACHES

1. Definition of personal data breach

1.1. Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.2. The most frequent reported breaches – among others – are as follows: losing a laptop or mobile phone, unsecure storage of personal data, unsecure transmission of data, unauthorised copying and transmission of customer and partner lists, server attacks, website hacking.

2. Handling and remedying of personal data breaches

2.1. It shall be the Controller's duty to prevent, handle personal data breaches and to observe the relevant provisions of law.

2.2. Access and attempted access to the IT systems shall have to be logged, and continuously analysed.

2.3. Should the Company's employees authorised to perform inspection or monitoring actions observe a personal data breach during their tasks, they shall be obliged to notify the head of the Company, without delay.

2.4. The Company's employees shall be obliged to report to the head of the Company or the person exercising the employer's rights if they observe a personal data breach or any signs indicating a personal data breach.

2.5. Personal data breaches can be reported to the Company's central e-mail address, phone number, where the employees, contract partners and data subjects can report the underlying events and security defects.

2.6. If a personal data breach is reported, the head of the Company shall examine the report without delay, and in the course of this examination, the breach must be identified, and the following must be examined and established:

a) the time and place of the personal data breach.

b) the description, circumstances and impacts of the breach.

c) the scope and number of the data compromised during the breach.
d) the persons affected by the compromised data.
e) the description of the measures made to remedy the personal data breach.
f) the description of the measures made to prevent, avert or mitigate the damages.

2.7. In the event of occurrence of a personal data breach, the affected systems, persons and data must be delimited and segregated and measures must be made to collect and keep the evidence proving the occurrence of the breach. Following this, restoration of the damages and lawful operation shall be commenced.

3. Register of personal data breaches

3.1. A register must be maintained regarding the personal data breaches, which shall contain the following:

a) the scope of personal data concerned,
b) the scope and number of persons affected by the personal data breach,
c) the time of the personal data breach,
d) the circumstances and impacts of the personal data breach,
e) the measures adopted to remedy the personal data breach,
f) other data required under the piece of legislation requiring the data processing.

3.2. The data pertaining to the personal data breaches included in the register shall be kept for the period of 5 years.

3.3. A sample for the personal data breach register is attached in Annex 3.

CHAPTER VIII – DATA PROTECTION REGISTERS

1. Data protection registers based on the Regulation

Controller shall maintain its data protection register required under the Regulation according to Annexes 1 and 3. The register shall contain, among others, the following parts:

- Register of the data processing activities
- Register of Personal Data Breaches

CHAPTER IX – RIGHTS OF THE DATA SUBJECT

1. Information about the rights of the data subject

1.1. Short summary of the data subject's rights:

1. Transparent information, communication and actions aimed to facilitate the exercising of the rights of the data subject
2. Right to receive prior information where personal data are collected from the data subject
3. Communication to the data subject and the information to be provided to them where personal data are not collected by the controller from the data subject
4. Right of access by the data subject
5. Right to rectification
6. Right to erasure (right to be forgotten)
7. Right to restriction of processing
8. Notification obligation regarding rectification or erasure of personal data or restriction of processing
9. Right to data portability

10. The right to object
11. Automated individual decision-making, including profiling
12. Restrictions
13. Communication of a personal data breach to the data subject
14. Right to lodge a complaint with a supervisory authority (right to remedy by the authority)
15. Right to an effective judicial remedy against a supervisory authority
16. Right to an effective judicial remedy against a controller or processor

1.2. The data subject's rights in detail:

1.2.1. Transparent information, communication and actions aimed to facilitate the exercising of the rights of the data subject

1.2.1.1. The controller shall provide any and all information and any and all communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to children. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

1.2.1.2. The controller shall facilitate the exercising of the data subject's rights.

1.2.1.3. The controller shall provide information to the data subject on the actions taken on the data subject's request made in terms of exercising of his/her rights, without undue delay and in any event within one month of receipt of the request. This deadline may be extended – subject to the conditions specified in the Regulation – with further two months, and the data subject shall have to be informed of such extension.

1.2.1.4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and

seeking a judicial remedy.

1.2.1.5. The information and communication on the data subject's rights as well as the measures shall be ensured by the controller free of charge, however, a fee may be charged in the cases specified in the Regulation. The detailed rules are specified by Article 12 of the Regulation.

1.2.2. Right to receive prior information where personal data are collected from the data subject

1.2.2.1. The data subject shall be entitled to receive information about the processing related facts and information, prior to commencement of the processing. Within the framework of this, the data subject must be informed about the following:

a) name and contact details of the controller and its representative,
b) contact details of the data protection officer,
c) the purpose of the processing for which the personal data are intended as well as the legal basis for the processing,
d) if processing is based on enforcement of a legitimate interest, the legitimate interests of the controller or a third party,
e) the recipients to whom the personal data are transferred or the categories of recipients of the personal data, if any,
f) where applicable, the fact whether the controller intends to transfer the personal data to a third country or international organisation.

1.2.2.2. The controller shall provide the data subject with the following further information in order to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing

concerning the data subject or to object to processing as well as the right to data portability;

c) where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) the right to lodge a complaint with a supervisory authority;
e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

1.2.2.3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information. These detailed rules of the right to prior information are specified by Article 13 of the Regulation.

1.2.3. Communication to the data subject and the information to be provided to them where personal data are not collected by the controller from the data subject

1.2.3.1. The controller is required to notify the data subject about the facts and information specified in Section 2 above, furthermore about the categories of the data subject's personal data, and sources of the personal data and (if applicable) whether the data originate from publicly available sources, in the following manner: within one month after the personal data were obtained, at the latest, if the controller did not obtain the personal data from the data subject; at the time the data subject is contacted for the first time, at the latest, if the personal data are used for communication with the data subject; at the latest when the personal data are first disclosed, if a disclosure to another recipient is envisaged, too.

1.2.4. Right of access by the data subject

1.2.4.1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the related information mentioned in Sections 2-3 above shall be ensured to the data subject.

1.2.4.2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer pursuant to Article 46 of the Regulation.

1.2.4.3. The controller shall provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. The detailed rules of the data subject's right of access are specified by Article 15 of the Regulation.

1.2.5. Right to rectification

1.2.5.1. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

1.2.5.2. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. These rules are specified by Article 16 of the Regulation.

1.2.6. Right to erasure (right to be forgotten)

1.2.6.1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, if:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data have been collected in relation to the offer of information society services, offered directly to children.

1.2.6.2. The right to erasure may not be enforced if the processing is necessary

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation imposed by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for the fulfilment of public interest affecting the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e) for the establishment, exercise or defence of legal claims.

The detailed rules of the right to erasure are specified by Article 17 of the Regulation.

1.2.7. Right to restriction of processing

1.2.7.1. Where processing has been restricted, such personal data shall, with the

exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

1.2.7.2. The data subject shall have the right to obtain from the controller the restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
d) the data subject has objected to processing; in this event the restriction is pending the verification whether the legitimate grounds of the controller override those of the data subject.

1.2.7.3. The data subject shall have to be informed in advance about the lifting of the restriction of processing.

The respective rules are specified by Article 18 of the Regulation.

1.2.8. Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

These rules are specified by Article 19 of the Regulation.

1.2.9 Right to data portability

1.2.9.1. Subject to the conditions stipulated in the Regulation, the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a) processing is based on consent or a contract; and
b) processing is carried out by automated means.

1.2.9.2. The data subject can also request the personal data to be transferred directly by and between the controllers.

1.2.9.3. Exercising of the right to data portability may not violate Article 17 of the Regulation (Right to erasure (right to be forgotten)). The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This right shall not adversely affect the rights and freedoms of others. The detailed rules are specified by Article 20 of the Regulation.

1.2.10. The right to object

1.2.10.1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on public interest or performance of a task in the public interest (Article 6(1)(e)) or legitimate interest (Article 6(f)) including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights

and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

1.2.10.2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

1.2.10.3. At the latest at the time of the first communication with the data subject, the above rights shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

1.2.10.4. The data subject may exercise his or her right to object by automated means using technical specifications as well.

1.2.10.5. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

The respective rules are specified by Article 21 of the Regulation.

1.2.11. Restrictions

Union or Member State law to which the controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights (Articles 12 to 22 and Article 34, as well as Article 5 of the Regulation), when such a restriction respects the essence of the fundamental rights and freedoms.

The conditions of this restriction are specified by Article 23 of the Regulation.

1.2.12. Communication of a personal data breach to the data subject

1.2.12.1. When the personal data breach is likely to result in a high risk to the rights

and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The communication shall describe in clear and plain language the nature of the personal data breach and shall contain at least the following information:

a) the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

1.2.12.2. The communication to the data subject shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
c) the communication would require disproportionate efforts. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The further rules are specified by Article 34 of the Regulation.

1.2.13. Right to lodge a complaint with a supervisory authority (right to remedy by the authority)

The data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the Regulation. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint procedure, including also the possibility of a judicial remedy by the complainant at the regional court having competence according to his or her domicile or habitual residence.

The data subject can exercise his or her right to lodge a complaint through the following contact channels: Hungarian National Authority for Data Protection and Freedom of Information (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c., phone: +36 (1) 391-1400; fax: +36 (1) 391-1410, https://www.naih.hu, e-mail: ugyfelszolgalat@naih.hu).

These rules are specified by Article 77 of the Regulation.

1.2.14. Right to an effective judicial remedy against a supervisory authority

1.2.14.1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

1.2.14.2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged.

1.2.14.3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

1.2.14.4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion

or decision to the court.

These rules are specified by Article 78 of the Regulation.

1.2.15. Right to an effective judicial remedy against a controller or processor

1.2.15.1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under the Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with the Regulation.

1.2.15.2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

These rules are specified by Article 79 of the Regulation.

CHAPTER X – CLOSING PROVISIONS

1. Establishment and amendment of the Policy

The owner of the Executive Office shall have the right to establish and amend the Policy.

2. Communication of the Policy

The provisions of this Policy shall be communicated to all employees (workers) of the Company, and the work-related (employment) contracts shall stipulate that compliance with and enforcement of this Policy is an essential job responsibility of all employees (workers).

Place and date:

CHAPTER XI – ANNEXES

Annex 1

Inquiry-related register

(data protection compliance)

No.	Time of inquiry/request	Data Subject's name	Subject of inquiry/request	Measure/action	Note

Annex 2

DATA PROCESSING NOTICE TO EMPLOYEES

Dear Employee,

Below we provide information to you about the data processing activities carried out by the Employer in relation to your employment relationship.

1. Legislation applicable in terms of the data processing

The following pieces of legislation shall be applicable in terms of the data processing:

> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter as: GDPR); and

> Act CXII of 2011 on the Information Self-determination Right and the Freedom of Information (hereinafter as: the “Information Act”).

> Act I of 2012 on the Labour Code (hereinafter as: “Labour Code”).

2. Key Definitions

Controller shall mean a natural person or legal entity which alone, or jointly with other entities, determines the purposes and means of the processing of personal data. For the purposes of this Data Processing Notice the controller (hereinafter as: “Employer” or “Controller”) shall be as follows:

- name: Mertcontrol Hungary Kft.

- registered office: 2144 Kerepes, Szabadság út 13.
- postal address: same
- e-mail: info@mertcontrol.com
- phone number: 455-4010

Data subject shall mean an identified or identifiable living natural person whose data are processed within the scope outlined in this Data Processing Notice. For the purposes of this Notice, data subject shall mean the employee. For the purposes of this Notice, the term ‘employee’ shall also include the casual workers employed pursuant to Article 201(1) of the Labour Code.

Personal data: any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3. Principles of Processing

The employees’ personal data shall be processed by the Controller only in accordance with the following principles. Processing shall have to be compliant with the listed principles in each stage of the processing.

a) purpose limitation: personal data can only be processed for specific, explicit and legitimate purposes and may not be processed in a manner that is incompatible with those purposes;
b) proportionality, necessity, data minimisation: only such data can be processed, that are relevant and limited to what is necessary in relation to the purposes for which they are processed;
c) lawfulness, fairness and transparency: data processing must be in compliance with the currently effective legislation and must serve a lawful purpose, furthermore the data must be processed in a fair manner, without violating the privacy and rights of the data subjects;
d) accuracy: data must be accurate and up to date, and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) storage limitation: personal data shall be stored in a form that allows for the identification of the data subjects only for the time required to achieve the purpose of personal data processing;
f) principle of integrity and confidentiality: personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
g) principle of accountability: the Controller shall be responsible for, and be able to demonstrate compliance with the principles of data processing.

Only such statement or data provision can be requested from the employee that do not violate his/her personality rights, and which are essential in terms of the establishment, performance or termination of the employment relationship. Only such an aptitude test can be applied regarding the employee that is required by law in terms of the given employment relationship or which is necessary for exercising a right or performance of an obligation determined in a rule applicable to the employment relationship.

The Employer may not disclose any fact, data, or opinion pertaining to the employee to any third party unless required by law or consented to by the employee.

The Employer shall be allowed to monitor the behaviour of employees only to the extent pertaining to the employment relationship. The Employer's monitoring and the means and methods used may not be at the expense of human dignity. The private life of employees may not be monitored/checked.

4. Data protection officer

The Controller shall not employ a data protection officer.

5. Scope of processed data

The following data can be processed by the Controller in the personal records of the data subject in relation to the employment relationship:

1. natural identification data of the employee: the surname and first name of the data subject, their surname and first name at birth, place of birth, date of birth, and the mother's surname and first name at birth;
2. address, habitual residence;
3. nationality:
4. Social Security Number;
5. Social security data:
6. tax identification number;
7. the employee's e-mail address;
8. his/her phone or mobile phone number;
9. his/her bank account number;
10. income certificate;
11. data pertaining to the previous workplace(s);
12. accident statement;
13. record on the workplace accident;
14. patient file, hospital certificate, outpatient medical record, general practitioner

certificate;

15. start and end date of employment;
16. post of employment;
17. education, qualification;
18. amount of his/her salary;
19. any debt to be deducted from the employee's wages on the basis of a final resolution or pursuant to a legal regulation, as well as the entitlement thereto;
20. the duration of the sick leave taken by the employee during the year when the employment relationship was terminated;
21. data related to the employee’s ordinary paid time-off days (annual leave);
22. other essential data of the employment contract concluded with the employee (such as: allowances ensured to the employee);
23. evaluation of the employee's work;
24. worktime register;
25. warning / detrimental legal sanctions;
26. resolution imposing an obligation to pay damages;
27. rights ensured to the employee based on his/her family circumstances (such as parental leave, maternity leave, etc.);
28. results of the occupational physician’s aptitude test;
29. way and reasons of termination of the employment relationship;
30. contents of the employee’s certificate of no criminal record;
31. information obtained by the controller in the course of inspection of the work activity or lawful inspection of the usage of the work equipment provided to the employee for work related purposes.

The Employer shall process only those specific data out of the above listed data that are relevant in terms of the employment relationship of the individual data subjects (e.g.: sick leave related data, if the employee used sick leave).

6. Sensitive data

Out of the data listed in Section 5, the following shall qualify as sensitive data

(provided that these are relevant in terms of the employee and that the Employer processes such sensitive data): data belonging to categories no. 12, 13, 14, 20, 27 and 28.

7. The purposes of processing

The purposes of processing of personal data can be manifold; a particular data may be processed for several different reasons, so there are overlaps between the categories. The personal data listed in Section 5 shall be processed by the Employer for the following purposes:

- Identification of the data subject. The identification data of the natural person data subject (e.g.: name, place of birth, mother's name, etc.) are partly required to identify the employee and separate him/her from the other persons.
- Conclusion of the employment contract. Those personal data belong (also) to this category that are mandatory or voluntary content elements of the employment contract (based on the agreement of the parties), hence all those data which are required to identify the data subjects (see the previous Section) and which pertain to the concerned post of employment, salary and other conditions of the employment relationship.
- Performance of the employment contract. A substantial part of the above listed personal data are required (also) in order to ensure the cooperation between the parties and to fulfil the rights and obligations arising from the employment relationship. These data shall include, among others, the data related to the payment of the salary (amount and due data of the salary, bank account number, etc.) or the information related to the time sheet. In addition to these, the contact data of the employee (e-mail, phone number) shall also be required for purpose of performance of the employment contract.
- Exercising of the Employer's right of inspection. The Employer shall be entitled to monitor and inspect the employee's conduct related to the employment, within the scope specified by the Labour Code and the

practical application of law. The purpose of processing of the data listed in Section 5.31 is to exercise the right of inspection.

> Fulfilment of the tax and social security related obligations. The Controller shall be obliged to report certain personal data of the employees to the authorities in order to guarantee its compliance with the tax and payroll tax payment obligations. Therefore a certain part of the above listed personal data are processed by the Employer for that purpose as well.

8. Legal bases of processing

Just as the purpose of data processing, the authorisation for processing is based on several legal bases as well:

> Article 6(1)(b) of the GDPR: processing is necessary for the performance of a contract to which the data subject is party. A substantial part of the personal data listed above are processed by the Employer for purpose of performance of the employment contract, hence to exercise and perform the employment related rights and obligations.

> Article 6(1)(c) of the GDPR: processing is necessary for compliance with a legal obligation to which the controller is subject. The legal basis of processing of data required to be reported to the authorities and of the other data related to tax obligations is established by the laws on the personal income tax, the rules of taxation and the social security.

> Article 6(1)(f) of the GDPR: processing is necessary for enforcement of the controllers' legitimate interests. The legal basis of processing of the data created in relation to monitoring of the employee is the Controller's legitimate interest. It is in the Controller's fundamental interest to ensure that the services provided by the Office are of high quality. For that purpose it is essential to monitor and control the work of the employees. Prior to performing any specific monitoring/control activities, the Controller weighs the relative weight of the different interests as compared to each other, on a case-by-base basis (interest balancing test).

> Article 9(2)(b) of the GDPR: processing is necessary for the purposes of

carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. The legal basis of processing (if any) of the sensitive data listed in Section 6: to perform the statutory obligations of the employer related to accidents, incapacity to work, other health conditions. The legislation contain partly labour law (e.g.: protection against dismissal) and workplace safety (e.g.: facilitated post of employment) requirements and partly record-keeping, taxation and social security (e.g.: allowances, social security benefits) requirements or rights. The Controller needs to process certain sensitive data of the data subject in order to ensure its compliance with these requirements.

9. Data transfer

The Controller shall perform its employment relationship related payroll accounting, record keeping, official notification, etc. obligations by employing an external contractor to which the employees' personal data shall be transferred for that purpose. Hence, the accountant (payroll accountant) shall qualify as the Employer's processor. Contractor's particulars:

Name: Balkán Consult Kft.
Registered office: 1037 Budapest, Gyógyszergyár utca 61. 2. em. 7.

10. Scope of persons entitled to access the personal data

The Controller shall have access to the employees' personal data on behalf of the Controller. The processors can access the personal data within the scope and for the purpose specified in Section 9.

11. Data Security

The personal data shall be stored by the Employer partly on hard copy (paper), in files stored in locked up cabinets and partly in electronic form, on its own servers. The

Controller shall take all technical and organisational measures to guarantee the security of the personal data.

12. Rights of the data subject

12.1. Exercising of the Rights

The exercising of the below listed rights of the data subject may be reported by the employee to the Controller. Controller shall provide information to the data subject on the measures/actions taken upon request within thirty days of receipt of the request at the latest. That period may be extended by further thirty days where necessary, taking into account the complexity and number of the requests. The Controller shall inform the data subject about the extension of the deadline, together with the reasons for the delay, within thirty days of receipt of the request, if possible, and unless requested otherwise by the data subject, in an electronic form. If the Controller does not take action on the request of the data subject, the Controller shall inform the data subject within the above deadline of the reasons for not taking action and on the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

If the request filed by the data subject is clearly groundless or excessive, a reasonable fee may be charged by the Controller or may refuse to take action based regarding the request.

12.2. Access

The data subject may request access to his/her data from the Controller, including that the Controller should provide information regarding the following:

- which personal data are processed,
- what is the legal basis,
- for what processing purposes,
- what is the source of data,

- for how long are the data processed,
- to whom, when, under what legal basis was access provided to data subject's personal data, which personal data were involved, to whom these data were transferred.

If so requested by the data subject, the Controller shall provide a copy of the personal data undergoing processing to the data subject free of charge for the first occasion, and after that it may charge a reasonable fee based on the administrative costs.

12.3. Rectification

If the data subject can verify – by providing sufficient and reliable proof – the accuracy of the rectified data, the Controller shall perform the request within thirty days at the latest, and shall notify the data subject thereof through the provided contact details.

12.4 Erasure

The data subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controller shall have the obligation to erase personal data of the data subject without undue delay, where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing;
c) the personal data have been unlawfully processed;
d) the personal data have to be erased for compliance with a legal obligation.

If the above conditions are met, the Controller shall erase the data permanently and unrecoverably.

12.5 Data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transfer those data to another controller, or – if it is technically feasible – request direct transfer between the controllers, if the concerned processing action is based on the data subject's consent (Article 6 (1) a) of the GDPR) or if it affects sensitive data as per Article 9 (2) a) of the GDPR, or if it affects contractual legal basis within the meaning of Article 6 (1) b) of the GDPR.

12.6. Right to restriction of processing (right to block)

The data subject may request through the contact details provided to the Controller that the processing of his/her personal data be restricted (by clearly indicating the restricted nature of processing and by ensuring a processing separated from the other data), if:

- he/she contests the accuracy of his/her personal data (in this case the Controller shall restrict processing for the period until it checks the accuracy of the personal data);
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- the data subject has objected to processing (in this event the restriction is pending the verification whether the legitimate grounds of the controller override those of the data subject)

Where processing has been restricted, the restricted personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the

European Union or of a Member State.

12.7 Objection

The data subject shall have the right to object, on the grounds relating to his or her particular situation, at any time to the processing of his/her personal data based on Article 6 (f). In this case, the Employer shall no longer process the personal data unless the Employer demonstrates legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

13. Legal remedy

The data subject shall have the right to lodge a complaint to the supervisory authority regarding the processing executed by the Employer. Name and contact details of the supervisory authority:

Hungarian National Authority for Data Protection and Freedom of Information
address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C
phone: +36 1 391 1400
e-mail: ugyfelszolgalat@naih.hu
www.naih.hu

In addition, the data subject may refer the case to court in order to protect his/her data, and the court will address the case in an accelerated procedure. In such an event, the data subject may decide whether he/she files his/her legal action to the regional court having competence according to his/her domicile (permanent address) or according to his/her habitual residence (temporary address) or the registered office of the Controller. The data subject can look up the regional court having competence according to his/her domicile or habitual residence on the website at http://birosag.hu/ugyfelkapcsolati-portal/birosag-keresooldalon.

14. Amendment to the Data Processing Notice

The Controller reserves its right and obligation to amend this Data Processing Notice at any time, subject to the provisions of applicable legislation. The amended Data Processing Notice shall become effective as of its communication to the employees.

I have acknowledged the above information:

……

employee’s signature

Annex 3

Register of Personal Data Breaches

Name of the controller: Contact details of the controller: Name of the data protection officer:	
Purpose of data processing:	compliance with a legal obligation
Legal basis of data processing:	Article 33 of GDPR
The categories of data subjects:	the persons affected by the personal data breach
Categories of personal data:	the data affected by the personal data breach
Categories of recipients:	none
Data transfer to a third country	none
Deadline envisaged for data erasure:	transparency, accountability and lawfulness shall be verified on a continuous basis, but at least five years reckoned from occurrence of the personal data breach
Technical and organisational measures:	see in a separate Section

Annex 4

DATA PROCESSING NOTICE TO APPLICANTS

Dear Applicant,

By accepting this Data Processing Notice you consent that we keep your application (CV, letter of motivation) and contact you through the contact details provided by you, if and when a post of employment matching your qualifications or similar to the job now advertised becomes available at the Employer (Controller).

Below we provide to you detailed information about how we process your personal data based on your consent.

1. Scope of process personal data: identifying and other personal data provided in the CV and the letter of motivation.
2. Purpose of data processing: the Controller intends to retain the submitted job applications so that if new job offers are advertised by the Controller, it may contact the applicants (candidates) included in the database, organise meetings with them and (potentially) make a job offer to them.
3. Legal basis of processing: the data subject's consent (Article 6(1)(a) of the GDPR).
4. Data retention time: the retention time of the personal data depends on the assessment of the application: if the application is deemed successful (when an employment status is established), the provisions applicable to the employee shall be applied: if the application is unsuccessful or withdrawn, the Controller shall be obliged to erase the applicant's data permanently, within 5 days from the date when the application is declared unsuccessful or is withdrawn.
5. Persons entitled to access the data: the Controller and its current associate(s) in charge of HR matters.
6. Your rights: You can request the Controller at any time to provide to you written information about the scope of processed personal data and

furthermore about the legal basis, purpose, source and duration of processing by the Controller, and also about the persons/entities who were granted access to the personal data. If you so request, your personal data processed by us will be made available to you in a machine readable format, free of charge. Additionally, you may request the rectification or erasure of your personal data at any time if (a) you withdraw your consent to processing, (b) the personal data are no longer necessary, (c) the personal data were unlawfully processed, or (d) they are required to be erased for compliance with a legal obligation. You may lodge your request electronically or in a traditional letter sent to the above specified addresses. The Controller shall take action based on the request within maximum 30 days.

Please be informed that you may withdraw your consent to processing at any time, and in such case the Controller shall erase your application and personal data from its database permanently and unrecoverably.

7. Legal remedy: you have the right to lodge a complaint to the supervisory authority regarding the processing executed by the Controller. Name and contact details of the supervisory authority:

Hungarian National Authority for Data Protection and Freedom of Information
address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C
phone: +36 1 391 1400
e-mail: ugyfelszolgalat@naih.hu
www.naih.hu

In addition, the data subject may refer the case to court in order to protect his/her data, and the court will address the case in an accelerated procedure. In such an event, the data subject may decide whether he/she files his/her legal action to the regional court having competence according to his/her domicile (permanent address) or according to his/her habitual residence (temporary address) or the registered office of the Controller. The data subject can look up the regional court having competence

according to his/her domicile or habitual residence on the website at http://birosag.hu/ugyfelkapcsolati-portal/birosag-keresooldalon.

8. Amendment to the Data Processing Notice

The Controller reserves its right and obligation to amend this Data Processing Notice at any time, subject to the provisions of applicable legislation. The amended Data Processing Notice shall be effective as of its communication to the applicant.

I have acknowledged the above information:

…….

Applicant