DATA PROTECTION POLICY

TABLE OF CONTENTS

-	Appendix a other data controller on behalf of other service providers carried out by on the rules for the processing of personal data by a third party

I. CHAPTER 1 - GENERAL PROVISIONS

1. The purpose of these Rules is to

The purpose of this Policy is to establish the internal rules and measures to ensure that the Company, as a data controller, complies with the provisions of the EU Regulation 2016/679 (hereinafter: Regulation) and Act CXII of 2011 on the Right to Information Self-Determination and Freedom of Information (hereinafter: Infotv.).

2. NAME OF THE CONTROLLER:

2.1. COMPANY:	
2.2:	
2.3. ESTABLISHMENT:	
2.3. COMPANY REGISTRATION NUMBER:	
2.4:	
2.5. HONLAP:	
2.6. E-MAIL ADDRESS:	
2.7. TELEPHONE NUMBER:	
2.8. NAME OF REPRESENTATIVE:	
2.9. DATA PROTECTION OFFICER (IF ANY): NEVE:	
2.10. TITLE:	
PHONE:	
2.11. E-MAIL ADDRESS:	

(hereinafter referred to as the "Company" or "Controller")

3. THE IDENTITY OF THE DATA PROCESSORS:

3.1. Name of IT service provider data processor (if any)

2.1. COMPANY:	
2.2:	
2.3. ESTABLISHMENT:	
2.3. COMPANY REGISTRATION NUMBER:	
2.4:	
2.5. HONLAP:	
2.6. E-MAIL ADDRESS:	
2.7. TELEPHONE NUMBER:	
2.8. NAME OF REPRESENTATIVE:	
2.9. DATA PROTECTION OFFICER (IF ANY): NAME:	
2.10. TITLE:	
PHONE:	
2.11. E-MAIL ADDRESS:	

3.2. Name of the accounting, tax, payroll data processor (If this service is provided by an external service provider on behalf of the Data Controller.)

2.1. COMPANY:	
2.2:	
2.3. ESTABLISHMENT:	
2.3. COMPANY REGISTRATION NUMBER:	
2.4:	
2.5. HONLAP:	
2.6. E-MAIL ADDRESS:	
2.7. TELEPHONE NUMBER:	
2.8. NAME OF REPRESENTATIVE:	
2.9. DATA PROTECTION OFFICIAL (IF ANY): NAME:	
2.10. TITLE:	
PHONE:	
2.11. E-MAIL ADDRESS:	

3.3. Name of the data processor providing the data protection service (If this service is provided by an external service provider under the Data Controller's instructions.)

2.1. COMPANY:	
2.2:	
2.3. ESTABLISHMENT:	
2.3. COMPANY REGISTRATION NUMBER:	
2.4:	
2.5. HONLAP:	
2.6. E-MAIL ADDRESS:	
2.7. TELEPHONE NUMBER:	
2.8. NAME OF REPRESENTATIVE:	
2.9. DATA PROTECTION OFFICER (IF ANY): NAME:	
2.10. TITLE:	
PHONE:	
2.11. E-MAIL ADDRESS:	

3.4. POSTAI, COURIER SERVICE DUTIES NAME OF THE DATA PROCESSOR

2.1. COMPANY:	
2.2:	
2.3. ESTABLISHMENT:	
2.3. COMPANY REGISTRATION NUMBER:	
2.4:	
2.5. HONLAP:	
2.6. E-MAIL ADDRESS:	
2.7. TELEPHONE NUMBER:	
2.8. NAME OF REPRESENTATIVE:	

2.9. DATA PROTECTION OFFICER (IF ANY): NEVE:	
2.10. TITLE:	
PHONE:	
2.11. E-MAIL ADDRESS:	

3.5. Name of the intermediary processor - authorised to contract or mediate on behalf of the controller (if any)

2.1. COMPANY:	
2.2:	
2.3. ESTABLISHMENT:	
2.3. COMPANY REGISTRATION NUMBER:	
2.4:	
2.5. HONLAP:	
2.6. E-MAIL ADDRESS:	
2.7. TELEPHONE NUMBER:	
2.8. NAME OF REPRESENTATIVE:	
2.9. DATA PROTECTION OFFICER (IF ANY): NAME:	
2.10. TITLE:	
PHONE:	
2.11. E-MAIL ADDRESS:	

4. Scope of the Rules

4.1. This Policy covers the processing of personal data relating to natural persons by the Company.
4.2. Customers, customers, customers and suppliers of self-employed persons, sole proprietors, sole proprietorships and self-employed farmers shall be considered natural persons for the purposes of these Rules.
4.3. It does not cover the processing of personal data relating to legal persons, including the name and form of the legal person and contact details of the legal person (GDPR (14))

5. Definitions

For the purposes of these Regulations, the definitions which shall apply are set out in Article 4 of the Regulation. The main definitions are highlighted accordingly:

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, 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, distribution or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. **"restriction of processing"** means the marking of stored personal data for the purpose of restricting their future processing;

4. **"profiling"** means any form of automated processing of personal data whereby personal data are used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict characteristics associated with that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. **"pseudonymisation"** means the processing of personal data in such a way that it is no longer possible to identify the natural person to whom the personal data relate without further information, provided that such further information is kept separately and technical and organisational measures are taken to ensure that no association with identified or identifiable natural persons is possible;

6. **"filing system"** means a set of personal data, structured in any way, whether centralised, decentralised or structured according to functional or geographical criteria, which is accessible on the basis of specified criteria;

7. **'controller'** means a natural or legal person, public authority, agency or any 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 the processing are determined by Union or Member State law, the controller or specific criteria for the designation of the controller may also be determined by Union or Member State law;

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

9. **"recipient"** means a natural or legal person, public authority, agency or any other body to whom or with which personal data is disclosed, whether or not a third party. Public authorities which may have access to personal data in the context of an individual investigation in accordance with Union or Member State law are not recipients; the processing of those data by those public authorities must comply with the applicable data protection rules in accordance with the purposes of the processing;

10. **"third party"**: a natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or the persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. **'consent of the data subject'** means a voluntary, specific, informed and unambiguous indication of the data subject's wishes by which the data subject

indicates, by a statement or by an unambiguous act of affirmation, that he or she gives his or her consent to the processing of personal data concerning him or her;

12. **"data breach"** means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

II. CHAPTER 4 - ENSURING LAWFULNESS OF PROCESSING

6. Processing based on the consent of the data subject

6.1. For processing based on consent, the data request form set out in **Annex 1 to** these **Rules** shall be used.
6.2. Consent is also deemed to be given if the data subject ticks a box when viewing the Company's website, makes the relevant technical settings when using information society services, or makes any other statement or takes any other action which, in the relevant context, clearly indicates the data subject's consent to the intended processing of his or her personal data. Silence, ticking a box or inaction therefore does not constitute consent.
6.3. Consent covers all processing activities carried out for the same purpose or purposes. Where processing is carried out for more than one purpose, consent shall be given for all the purposes for which the processing is carried out.
6.4. If the data subject gives his or her consent in a written statement that also relates to other matters - e.g. the conclusion of a sales or service contract - the request for consent must be presented in a way that is clearly distinguishable from those other matters, in a clear and easily accessible form, in clear and plain language. Any part of such a statement containing the consent of the data subject which is in breach of the Regulation shall not be binding.
6.5. The Company may not make the conclusion or performance of a contract conditional on the consent to the processing of personal data that are not necessary for the performance of the contract.
6.6. It should be possible to withdraw consent in the same simple way as it is given.
6.7. If the personal data have been collected with the consent of the data subject, the controller may process the collected data for the purpose of complying with a legal obligation to which the data subject is subject, unless otherwise provided by law, without further specific consent and even after the data subject's consent has been withdrawn.

7. Processing based on the performance of a legal obligation

7.1. In the case of data processing based on a legal obligation, the scope of the data to be processed, the purpose of the processing, the duration of data storage and the recipients are governed by the provisions of the underlying legislation.
7.2. The processing based on the performance of a legal obligation is independent of the consent of the data subject, since the processing is determined by law. The

the data subject must in this case be informed before the processing starts that the processing is mandatory and must be informed in a clear and detailed manner of all the facts relating to the processing of his or her data, in particular the purposes and legal basis of the processing, the identity of the controller and of the processor, the duration of the processing, the fact that the controller is processing the personal data of the data subject on the basis of a legal obligation to which the data subject is subject and the persons who may have access to the data. The information should also cover the rights and remedies of the data subject in relation to the processing. In the case of mandatory processing, the information may also be provided by making public a reference to the legal provisions containing the foregoing information.

8. The Company's General Data Processing Notice

8.1. The Company's general privacy policy **is set out in Annex 2 to** this Policy**, which shall be** published on the Company's website and made available at its registered office.
8.2. In addition, certain categories of data subjects - such as employees, contractors - should also be directly informed of the processing and of the data subject's rights at the time of collection.
8.3. The Company shall ensure the exercise of the rights of the data subject in all its processing.

III. CHAPTER 2
EMPLOYMENT-RELATED DATA PROCESSING

9. Labour, personnel records

9.1. Employees may only be asked for and kept records of data and medical fitness for work examinations which are necessary for the establishment, maintenance and termination of employment and for the provision of social welfare benefits and which do not infringe their individual rights.
9.2. The Company processes the following data of the employee for the purposes of the establishment, performance or termination of the employment relationship for the performance of a contract:
1. Name
2. name at birth,,
3. date of birth,
4. mother's name,
5. your address,
6. your nationality,
7. tax identification number,
8. Social security number,
9. pensioner's permanent number (in the case of a retired worker),
10. phone number,
11. e-mail address,
12. identity card number,

13. the number of the official certificate of residence,
14. your bank account number,
15. online ID (if available)
16. the starting and finishing dates of your employment,
17. job title,
18. a copy of a document certifying your education and vocational training,
19. photo,
20. CV,
21. the amount of your salary, salary and other benefits,
22. the amount of the debt to be deducted from the employee's wages, or the right to deduct it, on the basis of a final decision or a legal provision or written consent,
23. an evaluation of the employee's work,
24. how and for what reasons the employment relationship is terminated,
25. a certificate of good character, depending on the job
26. a summary of the occupational aptitude tests,
27. in the case of membership of private pension funds and voluntary mutual insurance funds, the name of the fund, its identification number and the employee's membership number,
28. in the case of foreign workers, passport number; name and number of the document certifying entitlement to work,

Data recorded in the records of accidents involving 29 workers;

30. data necessary for the use of welfare services, commercial accommodation;
31. the camera and access control system used for security and asset protection purposes at the Company,

or data recorded by positioning systems.

9.3. The employer will process data relating to your illness and trade union membership only for the purposes of fulfilling a right or obligation under the Labour Code.

9.4. The recipients of the personal data are: the employer's manager, the person exercising the employer's authority, the Company's employees performing labour-related tasks and data processors.

9.5. Only personal data of employees in managerial positions may be transferred to the owners of the Company.

9.6. Duration of storage of personal data: 3 years after termination of employment.

9.7. The mandatory information on the processing of personal data and the employee's personal rights, which must be given to the employee at the time of the conclusion of the employment contract, is set out in **Annex 3.**

10. Data processing in connection with the assessment of the aptitude of employees

10.1. An employee may only be subjected to an aptitude test which is required by an employment rule or which is necessary for the exercise of a right or the performance of an obligation laid down in an employment rule. Prior to the examination, employees must be informed in detail, inter alia, of the skills and abilities to be assessed and the means and methods of assessment. If the examination is required by law, employees should be informed of the title of the law and the exact place where it is to be carried out. The website

information on data management in relation to aptitude tests is set out in **Annex 4.**

10.2. Employers can have employees complete the test forms for fitness for work and readiness for work both before the employment relationship is established and during the employment relationship.

10.3. In order to carry out and organise work processes more efficiently, a test form suitable for psychological or personality traits research can only be completed by a large group of employees in the interests of a more efficient work relationship if the data revealed during the analysis cannot be linked to individual employees, i.e. the data are processed anonymously.

10.4. The scope of the personal data processed: the fact of suitability for the job and the conditions required for this.

10.5. Legal basis for processing: legitimate interest of the employer.

10.6. The purpose of processing personal data is: to establish and maintain an employment relationship, to fill a position.

10.7. Recipients and categories of recipients of personal data: the results of the survey may be disclosed to the employees surveyed or to the professional carrying out the survey. The employer may only receive information on whether or not the person examined is fit for the job and on the conditions under which he or she is fit for the job. However, the employer cannot know the details of the examination or its full documentation.

10. .8. Duration of processing of personal data: 3 years after termination of employment.

11. Management of recruitment data, applications, CVs

11.1. The personal data that may be processed include: the name, date and place of birth, mother's name, address, qualifications, photograph, telephone number, e-mail address, employer's record of the applicant (if any).

11.2. The purpose of the processing of personal data is: application, evaluation of the application, conclusion of an employment contract with the selected person. The data subject must be informed if the employer has not selected him/her for the job.

11.3. Legal basis for processing: performance of a contract. The processing is lawful if it is necessary in the context of a contract or the intention to conclude a contract (Preamble 44) if it is necessary for the purposes of taking steps at the request of the data subject prior to entering into a contract (Article 6(1)(b)).

11.4. Recipients or categories of recipients of personal data: managers and employees performing labour-related tasks who are entitled to exercise rights as employers in the Company.

11.5. Duration of storage of personal data: until the application is processed. Personal data of unsuccessful applicants will be deleted. Data of candidates who withdraw their application or candidature will also be deleted.

11.6. The employer may retain applications only on the basis of the explicit, unambiguous and voluntary consent of the data subject, provided that the retention is necessary for the purposes of the processing in accordance with the law. Such consent shall be requested from candidates after the recruitment procedure has been completed.

12. Rules on the control and consequences of employer-provided equipment

12.1. The head of the employer or the person exercising the employer's rights is authorised to control and manage the data.
12.2. Where the circumstances of the inspection do not preclude this, it must be ensured that the worker is present during the inspection.
12.3. Prior to the inspection, the employee must be informed about the employer's interest in the inspection, who on the employer's side may carry out the inspection, - the rules according to which the inspection may take place (compliance with the principle of gradual approach) and the procedure to be followed, - the employee's rights and remedies in relation to the processing of data in connection with the inspection.
12.3. The principle of gradualness should be applied in the monitoring. In the first instance, the title and subject headings should be used to establish that the content is related to the employee's job function and is not personal. Non-personal content may be reviewed by the employer without restriction.
12.4. If, contrary to the provisions of this policy, it can be established that the employee has used the device for personal purposes, the employee must be requested to delete the personal data without delay. In case of absence or non-cooperation of the employee, the personal data shall be deleted by the employer upon verification. The employer may take legal action against the employee under labour law for using the device in violation of the policy or the employer's instructions.
12.5. The employee may exercise the rights set out in the data subject's rights chapter of the employer's data processing policy in relation to the processing of data involving the control of the device.

IV. CHAPTER 2
CONTRACT-RELATED DATA PROCESSING

13. Customer data: managing data of contracting partners, contacts - registering customers, suppliers

13.1. The Company shall process the name, birth name, date of birth, mother's name, address, tax identification number, tax number, entrepreneur's, farmer's or self-employed person's identity card number, personal identity card number of the natural person contracted with it as a buyer or supplier for the purpose of contract performance, contract conclusion, performance, termination, or granting of contract discounts, address, address of the registered office, address of the establishment, telephone number, e-mail address, website address, bank account number, customer number (customer number, order number), online identifier (list of customers, suppliers, frequent buyer lists), This processing is also considered lawful if the processing is necessary to take steps at the request of the data subject prior to the conclusion of the contract. Recipients of personal data: employees of the Company performing customer service tasks, employees performing accounting and tax tasks, and data processors. Duration of storage of personal data: 5 years after termination of the contract.
13.2. The legal basis for the processing of the data of the natural person contracting party provided in the contract for accounting and tax purposes is the fulfilment of a legal obligation, in this context the period of data storage is 8 years.

13.3. The Company shall process the personal data of the natural person acting on behalf of the legal person contracting with it - the person signing the contract - provided in the contract, as well as his/her address, e-mail address and telephone number, online identifier for the purpose of contact, exercising rights and obligations arising from the contract, and for the purpose of contact for legitimate interest. The storage period of these data is 5 years after the termination of the contract. In the case of processing based on legitimate interest, the data subject has the specific right to object to the processing.
13.4. The Company shall process the name, address, telephone number, e-mail address, online identifier of the natural person - not a signatory - indicated as a contact person in the contract concluded with it for the purpose of maintaining contact and exercising rights and obligations arising from the contract, for legitimate interest, taking into account that the contact person is in an employment relationship with the contracting party, so this processing does not adversely affect the rights of the data subject. The Contracting Party declares that it has informed the contact person concerned of the processing relating to his capacity as contact person. The storage period of this data shall be 5 years after the contact has been established.
13.5. For all data subjects, the recipients of the personal data are: the Company's manager, employees performing customer service tasks, contact persons, employees performing accounting and tax tasks, and data processors.
13.6. The personal data may be transferred for processing to the accounting office appointed by the company for tax purposes, to the Hungarian Postal Service or the appointed courier service for postal delivery purposes, and to the company's security agent for asset protection purposes.
13.7. The processing is lawful if it is necessary in the context of a contract or the intention to conclude a contract (Preamble 44) if it is necessary for the purposes of taking steps at the request of the data subject prior to the conclusion of the contract (Article 6(1)(b)). When making or receiving an offer, the Company is obliged to inform the offeror or the offeree of the offer.
13.8. The data processing clauses and information to be applied in the contracts to be concluded by the Company are set out in **Annex 5 to** this Policy. It is the responsibility and obligation of the Company's employees to ensure that these data processing clauses are included in the text of the contract.

V. CHAPTER 2
PROCESSING BASED ON A LEGAL OBLIGATION

14. Data processing for tax and accounting obligations

14.1. The Company processes the data of natural persons who have business relations with the Company as customers and suppliers for the purpose of fulfilling its legal obligations, tax and accounting obligations (accounting, taxation). A kezelt adatok az általános forgalmi adóról szóló 2017. évi CXXVII. tv. 169.§, és 202.§-a alapján különösen: adószám, név, cím, adózási státusz, a számvitelről szóló 2000. évi C. törvény 167.§-a alapján: név, cím, a gazdasági műveletet elrendelő személy vagy szervezet megjelölése, az utalványozó

and the signature of the person certifying the execution of the order and, depending on the organisation, of the auditor; the signature of the recipient on the stock movement vouchers and cash management vouchers, and of the payer on the counterfoils; on the basis of Act CXVII of 1995 on personal income tax: entrepreneur's identity card number, farmer's identity card number, tax identification number.

14.2. The period of storage of personal data is 8 years after the termination of the legal relationship giving rise to the legal basis.

14.3. Recipients of personal data: employees and data processors of the Company performing tax, accounting, payroll and social security functions.

15. Payer data processing

15.1. The Company processes the personal data of the data subjects - employees, their family members, employees, other beneficiaries - with whom it has a relationship as a paying agent (Act 2017:CL on the Order of Taxation (Art.) 7.§ 31.) for the purposes of fulfilling its legal obligations, tax and contribution obligations (tax, advance tax, contributions, payroll, social security, pension administration). The scope of the data processed is defined in Art. Article 50 of the Act defines the data processed, specifically highlighting the following: the natural person's natural person identification data (including previous name and title), gender, nationality, tax identification number, social security number (social security number). If the tax laws impose a legal consequence, the Company may process data relating to employees' membership of health (Section 40 of the Social Security Act) and trade unions (Section 47(2) b) of the Social Security Act) for the purposes of meeting tax and contribution obligations (payroll accounting, social security administration).

15.2. The period of storage of personal data is 8 years after the termination of the legal relationship giving rise to the legal basis.

15.3. Recipients of personal data: employees and data processors of the Company performing tax, payroll, social security (payroll) functions.

16. Data management of documents of lasting value under the Archives Act

16.1. The Company shall, in fulfilment of its legal obligation, manage its documents of permanent value pursuant to Act LXVI of 1995 on public records, public archives and the protection of private archival material (Archives Act), in order to ensure that the permanent part of the Company's archival material is preserved intact and in a usable condition for future generations. Duration of storage: until the transfer to the public archives.

16.2. The recipients of the personal data are: the head of the Company, the employees of the Company performing document management and archiving, the staff of the public archives.

VI. CHAPTER 2
DATA SECURITY MEASURES

17. Data security measures

17.1. The Company shall take the technical and organisational measures and establish the procedural rules necessary to enforce the Regulation and the Information Act in order to ensure the security of personal data for all purposes and for all lawful purposes.
17.2. The Data Controller shall take appropriate measures to protect the data against accidental or unlawful destruction, loss, alteration, damage, unauthorised disclosure or access.
17.3. The Company classifies and treats personal data as confidential. It imposes a confidentiality obligation on employees with regard to the processing of personal data, to which the clause in **Annex 6** applies. Access to personal data is restricted by the Company by setting levels of authorisation.
17.4. The Company protects its IT systems with firewalls and virus protection.
17.5. The Company's employees may connect their own computing, data storage and recording devices to the workplace computers.
17.6. The Company carries out electronic data processing and record-keeping by means of a computer program that meets the requirements of data security. The program ensures that access to the data is restricted to those persons who need it for the performance of their duties, under controlled conditions and for a specific purpose.
17.7. When personal data are processed automatically, the controller and the processor take additional measures to ensure:
a) prevent unauthorised data entry;
b) preventing the use of automated data processing systems by unauthorised persons using data transmission equipment;
c) the verifiability and ascertainability of the bodies to which personal data have been or may be transmitted using data transmission equipment;
d) the verifiability and ascertainability of which personal data have been entered into automated data processing systems, when and by whom;
e) the recoverability of the installed systems in the event of a failure, and
f) that errors in automated processing are reported.
17.8. The Company will ensure that incoming and outgoing electronic communications are monitored to protect personal data.
17.9. Sharing personal data processed by the Company on the Internet is prohibited!
17.10. Visiting file downloading, gaming, chat and sexual services sites at work and on Company equipment is strictly prohibited!
17.11. The use of unauthorised programs obtained from external sources or downloaded from external sources is prohibited!
17.12. Only the competent administrators have access to documents in the course of work or processing, and documents containing personnel, payroll, labour and other personal data must be kept securely locked.
17.13. Ensure adequate physical protection of the data and the devices and documents that carry them.

VII. CHAPTER 2
HANDLING DATA BREACHES

18. The concept of a personal data breach

18.1. Data breach:: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed; (Article 4.12 of the Regulation)
18.2. The most common incidents reported include: loss of laptop or mobile phone, unsecured storage of personal data (e.g. payment slips thrown in the trash); unsecured transmission of data, unauthorised copying and transmission of customer and partner lists, server attacks, website hacking.

19. Handling and remediation of data protection incidents

19.1. The prevention and handling of data protection incidents and compliance with the relevant legal requirements are the responsibility of the Company's management.
19.2. Accesses and access attempts on IT systems should be logged and analysed on an ongoing basis.
19.3. If employees of the Company who are authorised to carry out checks discover a data protection incident in the course of their duties, they must immediately notify the head of the Company.
19.4. Company employees are required to report to the Company's manager or the person exercising the employer's rights if they become aware of a data protection incident or an event that may indicate such an incident.
19.5. A data breach can be reported to the Company's central e-mail address, telephone number, where employees, contractors, data subjects can report the underlying events, security weaknesses.
19.6. In the event of a data breach notification, the Company's manager, with the involvement of the IT, finance and operations manager, shall immediately investigate the notification, identify the incident and decide whether it is a genuine incident or a false alarm. It should be investigated and determined:
a. the time and place of the incident,
b. a description of the incident, its circumstances, its effects,
c. the scope and quantity of data compromised in the incident,
d. the range of persons affected by the compromised data,
e. a description of the measures taken to deal with the incident,
f. a description of the measures taken to prevent, remedy or reduce the damage.
19.7. In the event of a data breach, the systems, people and data involved should be contained and segregated, and care should be taken to collect and preserve evidence that the breach occurred. Damage restoration and return to lawful operations can then begin.

20. Records of data protection incidents

20.1. Records of data protection incidents must be kept, including:
a) the scope of the personal data concerned,

b) the scope and number of data subjects affected by the data breach,
c) the date of the data breach,
d) the circumstances and effects of the data breach,
e) the measures taken to remedy the data breach,
f) other data specified in the legislation providing for the processing.

20.2. Data on data breaches in the register must be kept for 5 years.

20.3. A model for the data protection incident record is set out in **Annex 6.** worksheet.

VIII. CHAPTER 2
DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

21. Data protection impact assessment and prior consultation

21.1. Where a type of processing, in particular one using new technologies, is likely to present a high risk to the rights and freedoms of natural persons, taking into account its nature, scope, context and purposes, the controller shall carry out an impact assessment prior to the processing, in order to assess how the envisaged processing operations will affect the protection of personal data. Similar types of processing operations which present similar high risks may be assessed in the framework of a single impact assessment.

21.2. Where the data protection impact assessment concludes that the processing is likely to result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority before processing the personal data.

21.3. The detailed rules on data protection impact assessment and prior consultation are governed by the provisions of Articles 35-36 of the Regulation and the Infotv.

X.
DATA PROTECTION RECORDS

22. Data protection records under the Regulation

The Company's data protection records under the Regulation are set out in **Annex 6.** according to. This includes:

- Records of processing activities
- Records of data processing activities
- Records of data protection incidents

X. CHAPTER 2
THE RIGHTS OF THE PERSON CONCERNED

23. Information on the rights of t h e data subject

25.1. A brief summary of the data subject's rights:

1. Transparent information, communication and facilitation of the exercise of data subject rights
2. Right to prior information - when personal data are collected from the data subject
3. Information to the data subject and the information to be provided to him or her where the personal data have not been obtained by the controller from him or her
4. Right of access of the data subject
5. The right to rectification
6. Right to erasure ("right to be forgotten")
7. Right to restriction of processing
8. Obligation to notify the rectification or erasure of personal data or restriction of processing
9. The right to data portability
10. The right to protest
11. Automated decision-making on individual cases, including profiling
12. Restrictions
13. Informing the data subject about the personal data breach
14. The right to lodge a complaint with a supervisory authority (right to official redress)
15. Right to an effective judicial remedy against the supervisory authority
16. The right to an effective judicial remedy against the controller or processor

25.2. Your rights as a data subject in detail:

1. Transparency , communication and facilitating the exercise of data subject rights

1.1. The controller shall provide the data subject with all information and any particulars relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language, in particular in the case of any information addressed to children. The information shall be provided in writing or by other means, including, where appropriate, by electronic means. At the request of the data subject, information may be provided orally, provided that the identity of the data subject has been verified by other means.

1.2. The controller must facilitate the exercise of the data subject's rights.

1.3. The controller shall inform the data subject, without undue delay and in any event within one month of receipt of the request, of the measures taken in response to the request to exercise his or her rights. This time limit may be extended by a further two months under the conditions laid down in the Regulation, of which the data subject shall be informed.

1.4. If the controller fails to act on the data subject's request, 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 the failure to act and of the possibility for the data subject to lodge a complaint with a supervisory authority and to exercise his or her right of judicial remedy.

1.5. The data controller shall provide the information and the information and action on the rights of the data subject free of charge, but may charge a fee in the cases provided for in the Regulation.

The detailed rules can be found under Article 12 of the Regulation.

2. Right to prior information - when personal data are collected from the data subject

2.1. The data subject shall have the right to be informed of the facts and information relating to the processing before the processing starts. In this context, the data subject shall be informed:
a) the identity and contact details of the controller and its representative,
b) the contact details of the Data Protection Officer (if any),
c) the purposes for which the personal data are intended to be processed and the legal basis for the processing,
d) in the case of processing based onlegitimate interests the controller or third parties,
e) the recipients to whom the personal data are disclosed, and the categories of recipients, if any;
(e) where applicable, the fact that the controller intends to transfer the personal data to a third country or an international organisation.

2.2. To ensure fair and transparent processing, the controller must provide the data subject with the following additional information:
a) the duration of the storage of personal data or, where this is not possible, the criteria for determining that duration;
b) the right of the data subject to request the controller to access, rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of such personal data, and the right to data portability;
c) in the case of processing based on the data subject's consent, the right to withdraw consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of consent before its withdrawal;
d) the right to lodge a complaint with a supervisory authority;
e) whether the provision of the personal data is based on a legal or contractual obligation or is a precondition for the conclusion of a contract, whether the data subject is under an obligation to provide the personal data and the possible consequences of not providing the data;
f) the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and clear information about the significance of such processing and the likely consequences for the data subject.

2.3. If the controller intends to further process personal data for a purpose other than that for which they were collected, the controller must inform the data subject of that other purpose and of any relevant additional information before further processing.

The detailed rules on the right to prior information are set out in Article 13 of the Regulation.

3. Information to the data subject and the information to be provided to him or her where the personal data have not been obtained by the controller from him or her

3.1. If the controller has not obtained the personal data from the data subject, the data subject must be informed by the controller no later than one month after the personal data are obtained; if the personal data are used for the purpose of contacting the data subject, at least at the time of the first contact with the data subject; or, if the data are likely to be disclosed to another addressee, no later than the time of the first disclosure of the personal data, in accordance with the provisions of Article 2. the facts and information referred to in point (2), the categories of personal data concerned and the source of the personal data and, where applicable, whether the data originate from publicly available sources.

3.2. For further rules, see point 2 (Right to prior information) above.

The detailed rules for this information are set out in Article 14 of the Regulation.

4. Right of access of the data subject

4.1. The data subject has the right to obtain from the controller feedback as to whether or not his or her personal data are being processed and, if such processing is taking place, the right to access the personal data and related information described in points 2-3 above (Article 15 of the Regulation).

4.2. Where personal data are transferred to a third country or an international organisation, the data subject is entitled to be informed of the appropriate safeguards for the transfer in accordance with Article 46 of the Regulation.

4.3. The controller must provide the data subject with a copy of the personal data which are the subject of the processing. For additional copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.

Detailed rules on the right of access of the data subject are laid down in Article 15 of the Regulation.

5. The right to rectification

5.1. The data subject shall have the right to obtain from the Data Controller, upon his or her request and without undue delay, the rectification of inaccurate personal data relating to him or her.

5.2. Taking into account the purpose of the processing, the data subject has the right to request the completion of incomplete personal data, including by means of a supplementary declaration.

These rules are set out in Article 16 of the Regulation.

6. Right to erasure ("right to be forgotten")

6.1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to him or her without undue delay at his or her request, and the controller shall be obliged to erase personal data relating to him or her without undue delay if.
a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
b) the data subject withdraws the consent on which the processing is based and there is no other legal basis 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 must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;
f) personal data are collected in connection with the provision of information society services directly to children.

6.2. The right to erasure cannot be exercised if the processing is necessary
a) to exercise the right to freedom of expression and information;
b) to comply with an obligation under Union or Member State law to which the controller is subject or to carry out a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) on grounds of public interest in the field of public health;
d) for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes, where the right of erasure would be likely to render such processing impossible or seriously jeopardise it; or
e) to bring, enforce or defend legal claims.

Detailed rules on the right to erasure are set out in Article 17 of the Regulation.

7. Right to restriction of processing

7.1. Where processing is restricted, such personal data, except for storage, may be processed only with the consent of the data subject or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or of an important public interest of the Union or of a Member State.

7.2. The data subject shall have the right to obtain restriction of processing by the controller at his or her request if one of the following conditions is met:
a) the data subject contests the accuracy of the personal data, in which case the restriction applies for the period of time necessary to allow the Controller to verify the accuracy of the personal data;

b) the data processing is unlawful and the data subject opposes the erasure of the data and requests instead the restriction of their use;
c) the controller no longer needs the personal data for the purposes of processing, but the data subject requires them for the establishment, exercise or defence of legal claims; or
d) the data subject has objected to the processing; in this case, the restriction applies for the period until it is established whether the legitimate grounds of the controller override those of the data subject.

7.3. The data subject shall be informed in advance of the lifting of the restriction on processing.

The relevant rules are set out in Article 18 of the Regulation.

8. Obligation to notify the rectification or erasure of personal data or restriction of processing

The controller shall inform each recipient to whom or with which the personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves a disproportionate effort. The controller shall inform the data subject, at his or her request, of these recipients.

These rules are set out in Article 19 of the Regulation.

9. The right to data portability

9.1. Under the conditions set out in the Regulation, the data subject has the right to receive personal data relating to him or her which he or she has provided to a controller in a structured, commonly used, machine-readable format and the right to transmit those data to another controller without hindrance from the controller to whom the personal data have been provided, if.
a) the processing is based on consent or on a contract; and
b) the processing is carried out by automated means.

9.2. The data subject may also request the direct transfer of personal data between controllers.

9.3. The exercise of the right to data portability shall be without prejudice to Article 17 of the Regulation (Right to erasure ("right to be forgotten"). The right to data portability shall not apply where the processing is 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 set out in Article 20 of the Regulation.

10. The right to protest

10.1. The data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her which are in the public interest or are necessary for the performance of a public task (Article 6(1)
e)) or on the basis of legitimate interest (Article 6 (f)), including profiling based on those provisions. In such a case, the controller may 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.

10.2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such purposes, including profiling, where it is related to direct marketing. If the data subject objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for those purposes.

10.3. These rights must be explicitly brought to the attention of the data subject at the latest at the time of the first contact with the data subject and the information must be clearly displayed separately from any other information.

10.4. The data subject may also exercise the right to object by automated means based on technical specifications.

10.5. Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subject shall have the right to object, on grounds relating to his or her particular situation, 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 relevant rules are set out in the Article of the Regulation.

11. Automated decision-making on individual cases, including profiling

11.1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

11.2. This entitlement does not apply in the case of a decision to:
a) necessary for the conclusion or performance of a contract between the data subject and the controller;
b) is permitted by Union or Member State law applicable to the controller which also lays down appropriate measures to protect the rights and freedoms and legitimate interests of the data subject; or
c) is based on the explicit consent of the data subject.

11.3. In the cases referred to in points (a) and (c), the controller shall take appropriate measures to safeguard the rights, freedoms and legitimate interests of the data subject, including at least the right to obtain human intervention by the controller, to express his or her point of view and to object to the decision.

Further rules are set out in Article 22 of the Regulation.

12. Restrictions

EU or Member State law applicable to a controller or processor may limit the scope of rights and obligations (Articles 12-22, 34, 5 of the Regulation) by legislative measures if the limitation respects the essential content of fundamental rights and freedoms.

The conditions for this restriction are set out in Article 23 of the Regulation.

13. Informing the data subject about the personal data breach

13.1. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must inform the data subject of the personal data breach without undue delay. This information shall clearly and plainly describe the nature of the personal data breach and shall include at least the following:

(a) the name and contact details of the Data Protection Officer or other contact person who can provide further information;
c) explain the likely consequences of the data breach;
d) describe the measures taken or envisaged by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

13.2. The data subject need not be informed if any of the following conditions are met:
a) the controller has implemented appropriate technical and organisational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the data unintelligible to persons not authorised to access the personal data;
b) the controller has taken additional measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
c) information would require a disproportionate effort. In such cases, the data subjects should be informed by means of publicly disclosed information or by a similar measure which ensures that the data subjects are informed in an equally effective manner.

Further rules are set out in Article 34 of the Regulation.

14. The right to lodge a complaint with a supervisory authority (right to official redress)

The data subject has the right to lodge a complaint with a supervisory authority - in particular the supervisory authority of his or her habitual residence, place of work or place of the alleged infringement

Member State - if the data subject considers that the processing of personal data concerning him or her infringes the Regulation. The supervisory authority with which the complaint has been lodged must inform the customer of the procedural developments concerning the complaint and the outcome of the complaint, including the customer's right to judicial remedy.

These rules are set out in Article 77 of the Regulation.

15. Right to an effective judicial remedy against the supervisory authority

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

15.2. Without prejudice to any other administrative or non-judicial remedy, any data subject shall have the right to an effective judicial remedy if the competent supervisory authority does not deal with the complaint or does not inform the data subject within three months of the procedural developments concerning the complaint lodged or of the outcome of the complaint.

15.3. Proceedings against the supervisory authority shall be brought before the courts of the Member State in which the supervisory authority is established.

15.4. If proceedings are brought against a decision of a supervisory authority on which the Board has previously issued an opinion or taken a decision under the consistency mechanism, the supervisory authority must send the opinion or decision to the court.

These rules are set out in Article 78 of the Regulation.

16. The right to an effective judicial remedy against the controller or processor

16.1. Without prejudice to the administrative or non-judicial remedies available, including the right to lodge a complaint with a supervisory authority, every data subject shall have an effective judicial remedy if he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data not in accordance with this Regulation.

16.2. Proceedings against the controller or processor shall be brought before the courts of the Member State in which the controller or processor is established. Such proceedings may also be brought before the courts of the Member State in which the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in its exercise of official authority.

These rules are set out in Article 79 of the Regulation.

XI. CHAPTER 2
CERTAIN PROCESSING ACTIVITIES - APPENDICES

24. Certain processing activities

The internal rules for each processing operation are set out in the following Appendices to this Policy - which the Data Controller must apply when it actually carries out the activity described in the Appendix.

-	Appendix from e-mail account for the use of by checking data processing related to the use of your e-mail address
-	Appendix computer, laptop, tablet by checking about about data management
-	Appendix a workplace internet usage by checking on the control of Internet use about data management
-	Appendix on the control of the use of company mobile phones about data management
-	Appendix a GPS navigation system using the on data processing in connection with the use of the
-	Appendix on data management in relation to entry and exit from the workplace
-	Appendix on data management in relation to CCTV surveillance at the workplace
-	Appendix on making a telephone voice recording for customer services about data management
-	Appendix on the processing of visitors' data on the website. Information about cookies (cookie)
-	Appendix on data processing related to registration on the website
-	Appendix on data processing related to the newsletter service
-	Appendix on data management in the online shop
-	Appendix on data management in connection with the organisation of the prize draw
-	Appendix on data processing for direct marketing purposes
-	Appendix on anti-money laundering/anti-terrorist financing obligations and processing for the purposes of restrictive measures
-	Appendix a other data controller on behalf of other service providers carried out by on the rules for the processing of personal data by another data controller

XII. CHAPTER 3
FINAL PROVISIONS

25 Establishment and amendment of the Rules

The Managing Director of the Company is authorised to establish and amend the Rules.

26. Measures to make the Code known

The provisions of this Code shall be communicated to all employees of the Company

and shall be required in employment contracts to be observed and enforced by all employees.

(employed) essential job duties. A model employment contract clause is set out in **Annex 7 to** these Regulations.

27. ANNEXEK

1. Annex 1Application form for the processing of personal data based on consent
2. Annex 1 Information on the rights of the natural person concerned with regard to the processing of his or her personal data
3. Annex 2Information on the processing of personal data and the rights of employees
4. Annex 1Information on aptitude tests for workers
5. Annex 1Contractual clauses on data management
6. Annex 1Protection records (Excel)
    4. Records of processing activities
    5. Data processor register
    6. Records of data protection incidents
7. Annex 1.1Contractual clause on the knowledge, application and confidentiality of the data management policy

28. APPENDICES:

-	Appendix from e-mail account for the use of by checking data processing related to the use of your e-mail address
-	Appendix computer, laptop, tablet by checking about about data management
-	Appendix a workplace internet usage by checking on data management in connection with the monitoring of
-	Appendix on data management related to the control of the use of company mobile phones
-	Appendix a GPS navigation system using the data processing in connection with the use of the
-	Appendix on data management in relation to entry and exit from the workplace
-	Appendix on data management in relation to CCTV surveillance at the workplace
-	Appendix on data processing in connection with the making of a telephone voice recording for customer services
-	Appendix on the processing of visitors' data on the website. Information about cookies (cookie)
-	Appendix on data processing in connection with registration on the website
-	Appendix on data processing related to the newsletter service
-	Appendix on data management in the online shop
-	Appendix on data management in connection with the organisation of the prize draw
-	Appendix on data processing for direct marketing purposes
-	Appendix on data processing for the purpose of complying with anti-money laundering/anti-terrorist financing obligations and restrictive measures
-	Appendix a other data controller on behalf of other service providers carried out by on the rules for the processing of personal data by a third party

Celt, _____2018_____snow _____day

Managing Director

A guide:

In the Rules, in all Annexes and Appendices, the parts marked in blue should be reviewed, you will see what is not needed in your own company and what is not - the latter should be deleted.

You may also find gaps in your sample - you can then fill them.

Since the Regulation has no implementing practice, it is also possible that we interpret things differently. (There is plenty of uncertainty here, e.g. even the amendment to the Infortv. does not mean anything - and if it appears, we may have to start all over again.)

If you do not agree with the sample solutions in the Code, use your own.

You should go through each of the annexes, appendices and records of the data management policy - and the changes you make to the policy should be reflected in them!

Publisher: Adonet.hu Zrt. - Budapest 2018
www.onadozo.hu