

Y DIÁK ISKOLASZÖVETKEZET
PRIVACY AND DATA PROTECTION
POLICY

Data Controller Name: Y DIÁK ISKOLASZÖVETKEZET

Headquarters: 1137 Budapest, Radnóti Miklós u. 2.

Company registration number: 01-02-054614

Tax number: 24146443241

E-mail: ugyfelszolgalat@ydiak.hu

Phone: + 36 30 608 1088 Represented by

Tamás Nagy, member of the Board of

Directors

APPROVED BY

Directorate Budapest,

2024.11.14

TABLE OF CONTENTS

I.	CHAPTER	1:	GENERAL	PROVISIONS
3			
II.	CHAPTER	3:	LAWFULNESS AND PRACTICE	OF DATA PROCESSING.....3
III.	CHAPTER 4: DATA PROCESSING IN RELATION TO SCHOOL COOPERATIVE MEMBERSHIP 5			
	III.1. REGISTER OF MEMBERS.....			5
	III.2. DATA PROCESSING IN RELATION TO APTITUDE TESTS.....			5
	III.3.	CONSENT	OF	LEGAL REPRESENTATIVE.....6
	III.4. DATA PROCESSING IN RELATION TO TRAINING COURSES, STUDY CONTRACTS.....			6
	III.5. PERSONAL DATA PROCESSED IN THE CONTEXT OF THE RISK OF THE COVID-19 OUTBREAK (CORONAVIRUS 2019) 7			
IV.	CHAPTER 4: PROCESSING OF DATA OF APPLICANTS FOR ADMISSION TO THE COMPANY7			
V.	CHAPTER	3:	CONTRACT-RELATED	DATA PROCESSING.....11
VI.	CHAPTER	3:	PROCESSING BASED ON LEGAL OBLIGATIONS13
VII.	CHAPTER	3:	THE COOPERATIVE'S DATA PROCESSING ACTIVITIES13
VIII.	CHAPTER 2: SERVICE PROVIDED BY COOPERATIVE TO.....			
	THIRD PERSON (EXTERNAL SERVICE), DATA TRANSFER, SHARED DATA MANAGEMENT.....			14
IX.	CHAPTER			2: WEBSITE.....17
X.	CHAPTER	4:	DATA MANAGEMENT IN RELATION TO ELECTRONIC SURVEILLANCE.....	20
XI.	CHAPTER	4:	DATA SECURITY MEASURES, RECORDS23
XII.	CHAPTER	4:	DATA	BREACH MANAGEMENT.....25
XIII.	CHAPTER 2: RIGHTS OF THE DATA SUBJECT, MAKING A REQUEST, ACTIONS BY THE CONTROLLER, REMEDIES.....			
	27			
	ANNEXEK.....			Error! Bookmark not defined.

CHAPTER I

General provisions

In order to systematize its internal data protection processes and to ensure the rights of data subjects and to avoid data breaches, Y Diák Iskolaszövetkezet (hereinafter: Cooperative, the "Company") has established the following Privacy Policy (hereinafter: "Policy").

The Rules entered into force on 25 May 2018 and were amended today. The Board of Directors is responsible for establishing and amending the Rules.

The Cooperative undertakes to conduct its data processing activities in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation, hereinafter "the Regulation") and with the provisions of the EU Regulation on the right to information self-determination and freedom of information (2011. CXII of 2011 (hereinafter referred to as the "Infotv.")).

The purpose of the Policy is to provide data subjects with clear and comprehensible information about the personal data processed by the Cooperative and its processors, the sources of collection, the purposes, legal basis and possible duration of the processing, the identity and contact details of the data controllers, the processing activities, the purposes, legal basis and recipients of the transfers.

The scope of the Policy covers the processing by the Cooperative of personal data of natural persons (including, for example, members, employees, sole proprietors, sole proprietorships, natural person customers, vendors, suppliers and other natural person contractual partners) who have a contractual relationship with the Cooperative or come into contact with the Cooperative in the course of a contractual offer. The scope of the Policy extends to the registration of contact details of natural person representatives of legal entities affiliated to the Cooperative.

For the purposes of these Regulations, the definitions of terms are those set out in Article 4 of the Regulation, for which separate definitions may be given in the various chapters of these Regulations.

For each Chapter, the recipients of personal data are: the persons who may collect, know, record, organise, store, process, erase, transmit, etc. personal data. A member of the body that carries out the Cooperative's auditing tasks (Supervisory Board) is entitled to know the personal data processed by the Cooperative in the course of his/her auditing activities, provided that he/she has signed the confidentiality declaration annexed to these Rules.

If the law provides for a longer period for the retention of data than the period set out in the Rules, the period set out in the law shall prevail.

The provisions of the Code must be communicated to all employees, members and subcontractors of the Cooperative involved in the Cooperative's core business. The employment contracts, membership agreements and contracts with subcontractors shall require compliance with the provisions of the Code, stating that it is an essential obligation of the employees and that any breach of the Code by subcontractors shall constitute a breach of contract, with all the legal consequences that this entails.

CHAPTER II

Lawfulness and practice of data processing

According to the wording of the Regulation, a **"data subject"** is a natural person who can be identified, directly or indirectly, on the basis of information and personal data relating to him or her. The processing of personal data is lawful only if and insofar as at least one of the following conditions is met:

- a) the data subject has given his or her consent to the processing of his or her personal data for one or more specific purposes;
- b) processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into the contract;
- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary for the protection of the vital interests of the data subject or of another natural person;

- e) 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;
- f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

The legal basis for the Cooperative's personal data processing is as follows:

- Voluntary and explicit consent of the data subject.
- The processing is based on a legal provision.
- The processing is necessary for the performance of a contract to which the data subject is a party or for the purposes of taking steps at the request of the data subject prior to entering into a contract.
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the interests of those parties are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. In such cases, the Cooperative will always carry out the necessary risk analysis and decide on the basis of the results of such risk analysis.

If the processing is based on consent, the Cooperative, as controller, must be able to demonstrate that the data subject has consented to the processing of his or her personal data. Consent shall be considered as an appropriate legal basis for processing if it is voluntary, specific, unambiguous and based on adequate information. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of the processing based on consent prior to its withdrawal. The withdrawal of consent shall be made possible in the same simple manner as the giving of consent.

Where the provision of data is based on a legal or contractual obligation, the possible consequence of not providing the data may be that the data subject is unable to use the services of the Cooperative.

The application of the legitimate interest legal basis requires that the legitimate interest of the controller to be protected is proportionate to the restriction of the right to the protection of personal data. To establish this, a prior balancing of interests test is required. In the balancing of interests test, the Cooperative, as controller:

- identifies his or her legitimate interest in the processing of the personal data subject to the balancing of interests test,
- establishes the interests and rights of the data subject in relation to the personal data on which the balancing of interests test is based,
- carry out an assessment of the legitimate interests of the data subject and the legitimate interests of the controller and, on that basis, determine whether the personal data can be processed.

In the case of processing based on consent, the data subject's consent to the processing of his or her personal data shall be requested on the data request form set out in Annex 1. Any other statement that clearly indicates the data subject's consent to the intended processing of his or her personal data shall be considered as consent. Silence or inaction shall not constitute consent.

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. The Cooperative may not make the conclusion or performance of the contract conditional on the consent to the processing of personal data that are not necessary for the performance of the contract. The withdrawal of consent shall be made possible in the same simple manner as the granting of consent.

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.

The processing based on the performance of a legal obligation is independent of the data subject's consent, as the processing is determined by law (or other legislation). In such cases, the data subject must be informed before the processing starts that the processing is based on the legal ground of performance of a legal obligation 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, whether the controller is processing his or her personal data on the basis of a legal obligation to which he or she is subject and the persons who may have access to the data. The information must be provided

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 publishing a reference to the legal provisions containing the aforementioned information, e.g. on a website.

CHAPTER III

Data processing related to school cooperative membership

III.1. Register of members

The following personal data of the cooperative member may be processed:

1. Signature,
2. name, birth name,
3. place and date of birth,
4. mother's name,
5. your address,
6. tax identification number,
7. Social security number,
8. phone number,
9. e-mail address,
10. address card number,
11. CV,
12. your bank account number,
13. name of educational establishment, course, year, student ID number,
14. the start and end date of membership,
15. the amount of the property contribution,
16. data on the assistance from the Community Fund;
17. if the member's relative is also a beneficiary of the Community fund, the details of the relative as set out in points 2 to 16,
18. data relating to personal contributions (remuneration, place and time of performance of tasks).

Recipients of personal data: the management of the Cooperative. Employees of the Cooperative who perform labour-related tasks, payroll and accounting staff and data processors, as well as the member registrar, may only have access to the data necessary for the performance of their tasks.

Duration of storage of personal data: 5 years after termination of membership.

Where personal data are stored, measures to ensure their protection: for paper and electronic documents, the data security measures of the Code apply. The personal data will be stored in the server room of the Cooperative's branch. The personal data will be recorded in the specific payroll software developed by the Cooperative and in the Register of Members. The programs are password-protected and can only be read by employees performing labour and payroll tasks and edited by members of the Board of Directors and project managers. Personal data is backed up hourly in the cloud. The hosting service is self-hosted.

The detailed rules on the processing and protection of personal data of members of the Cooperative, the use of the website and the use of services are set out in the Annex.

The purpose of the Information Notice is to inform the data subjects in detail about all relevant facts and circumstances related to the processing of their data before the processing starts and during the processing, in particular about the purpose and legal basis of the processing, the person entitled to process the data, the duration of the processing, the fact that the controller processes the personal data of the data subject pursuant to the provisions of the Regulation and the Infotv. The information shall include the rights of the data subject with regard to the processing and the possibilities for legal remedies. The data subjects shall be informed of the availability of the information before the processing starts.

III.2. Data processing in relation to aptitude tests

The scope of the NM Decree No. 33/1998 (VI.24.) on the medical examination and opinion on the medical fitness for work, occupational and personal hygiene extends to all employers who employ workers in the framework of organised work within the meaning of Section 87 (9) of Act XCIII of 1993 on Occupational Safety and Health. The Mvt. 87.§

9), work carried out in a school cooperative under a membership agreement for an external service is considered to be organised work.

A member (Member) performing duties in the context of personal assistance under a membership agreement may only be subjected to an aptitude test which is required by law or employment rule or which is necessary for the exercise of a right or the performance of an obligation specified in an employment rule.

Prior to the examination, the Member shall be informed in detail, inter alia, of the skills and abilities to be assessed, the means and methods to be used and the reasons for the examination. If the examination is required by law, members shall also be informed of the title and number of the law and the exact place of the law. The information on data management in relation to the suitability test is set out in the "Membership Statement" (Annex 3).

The scope of the personal data processed: the fact of professional, occupational and medical fitness for the job and the conditions required for this.

The legal basis for data processing: legislation (NM Decree 33/1998 (VI. 24.) on the medical examination and opinion on the suitability for work, occupational and personal hygiene, Act XCIII of 1993 on occupational safety and health) and the legitimate interest of the Cooperative.

The purpose of processing personal data: to perform and maintain the performance of tasks in the framework of personal cooperation.

Recipients or categories of recipients of personal data: the results of the investigation may be disclosed to the investigated Members or the investigator. The Cooperative and the recipient of the service may only receive information on whether or not the person examined is suitable for the job (specific job) and on the conditions for this. However, the details of the assessment and its full documentation are not made available to the Cooperative.

Duration of the processing of personal data: 5 years after termination of membership.

Location of personal data: stored on paper in the Member's personal file. It will be kept in a separate room, to which a key will be provided by the members of the Management Board.

III.3. Declaration of consent by legal representative

The validity of legal declarations, including the validity of consent given for the processing of minors' data, is regulated by the Civil Code and the Regulation. Pursuant to § 2:13 and § 2:14 (1) of the Civil Code, "a minor who has not attained the age of 14 years is incapable of acting. The declaration of a minor under the age of 14 is null and void, and his legal representative may act on his behalf." According to § 2:11 and § 2:12 (1) of the Civil Code, "A minor who has attained the age of 14 and is not incapacitated is a minor with limited capacity. The validity of the declaration of a minor with limited capacity to act shall, unless otherwise provided for in the Civil Code, require the consent of his or her legal representative."

If the Member has limited legal capacity, i.e. has not reached the age of 18, the written consent of the legal representative is required for entry into the Cooperative, for the establishment of a relationship for the provision of external services and for the conclusion of the membership agreement and the individual agreement.

The Co-operative processes the following data of the legal representative: signature, name, address, identity card number.

Recipients or categories of recipients of personal data: the management of the Cooperative. Employees of the Cooperative who perform labour-related tasks, payroll and accounting staff and data processors may only have access to the data necessary for the performance of their tasks.

Duration of the processing of personal data: 5 years after termination of membership.

Location of personal data: stored on paper in the Member's personal file. It will be kept in a separate room, to which a key will be provided by the members of the Management Board.

III.4. Data processing in relation to training courses, study contracts

Following the conclusion of the study contract for the qualification of swimming pool master, swimming pool master, the employees of the School Cooperative holding the position of project manager shall apply for the

training on behalf of the Member to the Wellness and Hotel Industry Adult Training Institute (SpaDium Educational and Service Ltd.), its registration

side. For the application, in order to fulfil the contract, the School Co-operative will directly transmit the Member's name, place and date of birth, mother's name, highest educational level, labour market status, telephone number, e-mail address, home address. For billing information, the School Co-operative, as the cost bearer, will provide its own information. After the application, SpaDium Training and Services Ltd. will send a confirmation e-mail to the Member. After that, a contract will be concluded between the Member and the adult education institution, using the personal data provided by the Member to the School Cooperative .

III.5. Personal data processed in the context of the Covid-19 outbreak (coronavirus disease 2019) risk

Purpose of the processing: in view of the threat of the COVID-19 epidemic (coronavirus disease 2019), our School Co-operative must be precautionary and therefore needs to obtain personal data to minimise the spread of the virus. The aim is therefore to avoid potential infections among each other. Recipients of this service will only work with school co-operative members who are not infected and do not pose a risk of infection.

Personal data processed: date of notification of infection, personal data necessary to establish the identity of the data subject, place and date of travel abroad, data relating to contact with people coming from the infected area. The questionnaires shall not contain information on the medical history of the person concerned, nor shall they require the submission of medical documentation.

Legal basis for processing: voluntary consent of the Member (Article 6(1)(a) GDPR).

Duration of data storage: personal data will be processed only for the minimum necessary period, the latest expected date of the officially declared end of the COVID-19 threat (i.e. not the emergency). If, during the period of the risk of epidemic, the Member declares that he/she no longer wishes to perform any tasks for any of the recipients of the services, leaves the school cooperative, or terminates his/her student status, the personal data will be deleted immediately.

The personal data may be disclosed to the members of the Board of Directors and to the employees of the recipients of the services to whom the Member has volunteered to perform the tasks.

CHAPTER IV.

Processing the data of applicants for admission to the company

It is an integral part of the right of informational self-determination of job applicants to be adequately informed about the identity of the controller before giving consent to data processing and to know against whom they can exercise their rights.

The Company does not advertise jobs anonymously.

<p>The purpose of processing the personal data of the data subject:</p>	<p>In summary, the purpose of processing the personal data of the data subject is to establish an employment relationship. For this purpose, we process the data subject's natural person identification data, contact details, salary claims, data relating to his/her education, training, professional knowledge, previous work experience, language skills and other data relevant to the employment relationship.</p>
<p>Legal grounds for processing the personal data of the data subject:</p>	<p>intention to conclude an employment contract [Article 6(1)(b) GDPR]</p> <p>the employer's legitimate interest [Article 6(1)(f) GDPR]</p> <p>your consent [Article 6(1)(a) GDPR]</p>

<p>Description of the employer's legitimate interests in relation to the processing of data based on the employer's legitimate interests:</p>	<p>The GDPR allows the controller (employer) to base processing on a legitimate interest. An exception may be made where the interests, fundamental rights and freedoms of the data subject prevail.</p> <p>The employer has a legitimate interest in recruiting the best person for the advertised position. candidate to take on. This will be done by conducting an interview or interviews with the person concerned and, if necessary, by means of professional tests</p>
	<p>your expertise. These legitimate interests were weighed against the possible rights of the data subject that might be affected in a balancing test. As the interviews and tests are carried out in a way that respects the privacy of the data subject and as these tools are suitable for selecting the right candidate, we use these methods. The employer has a legitimate interest in being able to prove that the application process was lawful in the event that the job application is unsuccessful and the person concerned contests it. This legitimate interest has been weighed against the possible rights of the person concerned under a balancing test. However, it is in the interests of both the data subject and the employer to to avoid or resolve a potential dispute, we consider this processing based on legitimate interests to be necessary.</p>
<p>The recipients of the personal data (i.e. the persons to whom or to which the employer transfers personal data):</p>	<p>Your personal data will not be disclosed to third parties during the assessment of your application.</p> <p>Only the prospective supervisor and the manager will have access to your personal data when assessing your application.</p>
<p>The controller transfers personal data to a third country (or to an international organisation):</p>	<p>Your data will not be transferred to third countries or international organisations.</p>
<p>The duration of the storage of personal data and the criteria for determining that duration:</p>	<p>Your personal data will be processed for the following period:</p> <p>we will process all the personal data you provide until the end of the job application process, based on the legal basis that you wish to enter into an employment contract with us;</p> <p>after the job application is closed, if you are offered the job, we will process your data in accordance with the data processing rules applicable to the employment relationship and its legal basis. In such a case, you will receive a separate privacy notice; after the job application is closed, if you are not offered the job, we will process your data for the purpose of further contact if you explicitly consent to this. In this case, we will notify you if a vacancy occurs in our company. Your consent is requested for a period of 1 year;</p> <p>after the job application is closed, if you are not offered the job, we process your data on the basis of the employer's legitimate interest in being able to prove the lawfulness of the application process in the event of a dispute. In this case, we will delete your data whose processing is no longer necessary does not exist (e.g. contact details), but other data will be deleted at the end of the 6th month after the last day of the claim deadline.</p>

<p>Your rights in relation to data processing:</p>	<p>The data subject may request the employer to do so under the GDPR rules: access to personal data relating to you, i.e. you can request information about what data we process about you. You may also request a copy of this data, provided that the rights of others are not adversely affected; to correct personal data relating to him or her, for example if his or her telephone number changes during the assessment of a job application; erasure of personal data concerning him or her, except, inter alia, where the processing is necessary for the establishment, exercise or defence of legal claims; restrict the processing of personal data concerning him or her. Where data is subject to a restriction, such personal data will be stored only; other processing may be carried out only with the consent of the data subject or for the establishment, exercise or defence of legal claims or the protection of the rights of another natural or legal person or for important public interests of the European Union or one of its Member States; The data subject may object to the processing of personal data at any time on grounds relating to his or her particular situation. In such a case, the employer may no longer process the personal data, unless there are compelling reasons for</p>
	<p>not doing so.</p>
	<p>is justified by legitimate grounds which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims; receive the personal data you provide to the employer in a structured, commonly used, machine-readable format and also have the right to transmit these data to another controller (right to data portability). To exercise this right, the processing must be based on the data subject's consent or contractual intent and must be carried out by automated means. <i>Please note that we do not use automated processing when assessing applications for employment and therefore we cannot grant you this right in the context of this job application.</i></p>
<p>The right to data processing based on consent:</p>	<p>Where we process personal data on the basis of the data subject's consent, the data subject has the right to withdraw that consent at any time. However, the withdrawal of consent shall not affect the processing of personal data the lawfulness of the processing carried out.</p>
<p>Information on data processing based on law:</p>	<p>No such processing takes place in the context of the job application.</p>

Information on contractual processing:	The purpose of submitting your application is to conclude an employment contract with our company. In order to be considered, it is essential that you provide personal data such as your name, qualifications, previous employment experience and a description of your work experience and your level of language skills. Without these, your application will not be considered and will be unsuccessful.
Information about the fact of automated decision-making, including profiling:	No such processing takes place in the context of the job application.
Objection to data processing	The data subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data based on the legitimate interests of the employer, including profiling based on the aforementioned provisions. In such a case, the employer may no longer process such personal data, unless it can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims or interests, or for the purposes of the exercise of legal claims or rights relating to the processing of personal data. are related to the protection of.

Information on data security:	The employer has implemented and is implementing appropriate technical and organisational measures to ensure an adequate level of data security. Accordingly, the employer shall ensure that employment-related documents are kept physically locked in digitally encrypted files. The employer has taken measures to ensure that your personal data is secure by setting appropriate levels of access and authorisation. Accordingly, the person's employment documents (CV, interview notes, admission test results) will only be made available to the by the employer's employment department and the prospective supervisor of the person concerned.
The rights of redress in relation to data processing:	The data subject has the right in relation to the processing to. - directly to the Employer's managing director; - lodge a complaint with the supervisory authority (National Authority for Data Protection and Freedom of Information (NAIH) [postal address: 1530 Budapest, Pf. 5; phone: +36 (1) 391-1400; fax: +36 (1) 391-1410; e-mail: ugyfelszolgalat@naih.hu]; - go to court (the competent court will decide on the claim).

A DESCRIPTION OF THE PERSONAL DATA PROCESSED ABOUT JOB APPLICANTS

PERSONAL DATA	PURPOSE OF DATA PROCESSING	LEGAL BASIS FOR DATA PROCESSING	DATA SOURCE	DATA TRANSMISSION	DURATION OF DATA PROCESSING
---------------	----------------------------	---------------------------------	-------------	-------------------	-----------------------------

<p>the information provided in your CV:</p> <p>name, educational background, previous work experience, previous employers and positions held, language skills, professional competences, personal competences</p>	<p>the assessment of a job application advertised by the employer</p> <p>compliance with the employer's burden of proof in a dispute over an unsuccessful tender</p>	<p>intention to conclude an employment contract [Article 6(1) GDPR paragraph 1(b)] the employer is entitled to interest [Article 6 GDPR (1) paragraph (f)]</p>	<p>person concerned (applicant)</p>	<p>none</p>	<p>in the case of a successful application, the existence of employment. In this case, both the purpose of the processing and the legal basis for the processing may change, in which case we will provide you with a separate information notice on the processing; in the case of an unsuccessful application, in the case of consent to further contact after the closing of the application, we will provide you with a separate information notice on the processing. one year from the date of consent; in the case of an unsuccessful application, the last day of the 6th month following the last day of the 3-year period for making a claim, if no consent to further application has been given</p>
---	--	--	-------------------------------------	-------------	---

<p>an indication of the claim for remuneration and other benefits</p>	<p>the assessment of a job application advertised by the employer</p>	<p>intention to conclude an employment contract [Article 6(1) GDPR paragraph 1(b)]</p>	<p>person concerned (applicant)</p>	<p>none</p>	<p>in the case of a successful application, the conclusion of an employment contract will be deleted; in the case of an unsuccessful application, in the case of consent to a further inquiry after the closing date of the application one year from the date of consent; in the case of an unsuccessful application, in the absence of consent to further solicitation, the last day of the 3-year period for the enforcement of claims the last day of the 6th month following the day of</p>
--	---	--	-------------------------------------	-------------	--

<p>contact details: e-mail, postal address, telephone number</p>	<p>contacts in connection with the job application</p>	<p>intention to conclude an employment contract [Article 6(1) GDPR paragraph 1(b)] your consent [Article 6(1) GDPR paragraph 1(a)]</p>	<p>person concerned (applicant)</p>	<p>none</p>	<p>the final decision on the job application; in the case of consent to further enquiries, the final decision on the job application after the job application has been closed one year from the date of consent</p>
<p>data related to the selection: interview data, vocational assessment tests</p>	<p>an assessment of professional competence for the job</p>	<p>the employer's legitimate interest [Article 6 GDPR (1) paragraph (f)]</p>	<p>person concerned (applicant)</p>	<p>none</p>	<p>in the case of a successful application, the existence of employment. In this case, both the purpose of the processing and the legal basis for the processing may change, in which case we will provide you with a separate information notice on the processing; in the case of an unsuccessful application, in the case of consent to further contact after the closing of the application, we will provide you with a separate information notice on the processing. one year from the date of consent; in the case of an unsuccessful application, the last day of the 6th month following the last day of the 3-year period for making a claim, if no</p>

					consent to further application has been given
--	--	--	--	--	---

With regard to the above data processing, the Company draws attention to the fact that *if the applicant does not provide all the data strictly necessary for the evaluation, the possible consequence of not providing the data may be exclusion from the selection procedure.*

By transferring the personal data to the above recipients, the Company does not transfer the data subject's data to third countries outside the European Economic Area. The Company will not transfer the personal data to any recipient other than the addressee named above, unless the transfer is required by law, public authority or court order.

Access to and storage of data

The applications and CVs sent will be handled only by the authorised staff of the Company: the person exercising the employer's powers and the professional manager of the relevant area. The Company shall not disclose the job applications and curricula vitae received to third parties for statistical or other purposes, except in cases provided for by law, nor shall it disclose the data received to the public, nor shall it provide information on the assessment of the job applications and curricula vitae submitted, except at the request of and to the person concerned.

Where personal data are stored, measures to ensure their protection: for paper documents, the data security measures set out in the Code apply. Data will be stored on the recipients' own computers, which are password protected.

The Company protects access to the electronic HR database against unauthorised access, alteration, disclosure, deletion or destruction by establishing appropriate levels of authorisation.

**CHAPTER V
Data processing related to contracts**

Contractual partners' data management - personal data of landlords, customers, suppliers, clients, etc.

Legal basis for processing: compliance with and performance of obligations under tax law and pre-contractual measures (conclusion of contract, in case of amendment of contract: performance of contract, termination of contract).

The purpose of data processing is: to exercise the rights and fulfil the obligations of the tenant under the lease contract, and of the buyer in case of sale, to fulfil legal obligations and to settle any disputes with the landlord or seller.

Data subjects: data of natural persons who are lessors, purchasers, suppliers, integration participants, service users or who have other business relations or business contacts with the Cooperative, as defined by law.

Data processed: name, name at birth, place and date of birth, mother's name, address, tax identification number, tax number, business card number, identity card number, address, registered office, telephone number, e-mail address, website address, bank account number, customer number (customer number, order number).

The recipients of the personal data are: the employees of the Cooperative who keep records of rental contracts, the employees who perform accounting, tax and data processing tasks and the manager of the Cooperative.

Duration of storage of personal data: 5 years after termination of the contract.

Place of storage of personal data: paper documents are stored in the room of the directorate. For security reasons, documents are also stored in scanned form in the server room. They will be accessible to members of the Management Board and project managers.

The data subject must be informed before the processing is started that the processing is based on the abovementioned legal grounds and on the intention to enter into a contract or the performance of a contract. This information may be provided in the contract itself or in the information notice annexed to it or in the privacy notice published on the website.

The data subject must be informed of the transfer of his or her personal data to a data processor (e.g. an accountancy firm, etc.).

The text of the data processing clause relating to contracts with natural persons is set out in Annex 4 to these Rules, - the text of the data processing clause relating to rental contracts is set out in Annex 5 to these Rules.

Personal data of natural person representatives of legal entity partners

The scope of the personal data processed: the name, address, telephone number and e-mail address of the natural person.

The purpose of the processing of personal data: the conclusion and performance of contracts with the legal entity partner of the Cooperative, and the maintenance of business relations.

Legal basis for processing: legitimate interest of the Cooperative.

The recipients or categories of recipients of personal data: the Management Board of the Cooperative, its contracting (registrar) and its employees performing accounting tasks.

Duration of the storage of personal data: 5 years after the business relationship or the data subject's capacity as a representative has ended. Where legislation (e.g. tax law, etc.) provides for a longer period for recording or storing contracts, the period shall be that laid down in that legislation.

Place of storage of personal data: paper documents are stored in the room of the directorate. For security reasons, documents are also scanned and stored in the server room. They will be accessible to members of the Board and project managers.

The information sheet for data collection is set out in Annex 6 to these Rules. This information sheet must be presented to the person concerned by the employee who has contact with the customer, buyer, supplier or client. It shall be kept for the duration of the processing.

CHAPTER VI. Data processing based on legal obligations

Data processing for tax and accounting obligations

The Cooperative processes the data of natural persons who are customers, suppliers, integration participants, lessors, service users or who have a business relationship or other business contact with it, as defined by law.

The scope of the personal data processed: the natural person's natural identity data: name (previous name) place and date of birth, mother's name, address, tax number and tax identification number entrepreneur's identity card number. In the case of a lease, in addition to the above, the parcel number of the property(ies) subject to the lease.

Legal basis for data processing: based on the legal basis of tax legislation (e.g. Act CXXXVII of 2017 on Value Added Tax, Act CXVII of 1995 on Personal Income Tax, Act CL of 2017 on the Rules of Taxation, compliance with and performance of obligations, as well as pre-contractual measures (conclusion of contract), in case of contract modification: performance of contract).

Recipients of personal data: (may access and process the data): the Company's employees performing tasks related to the conclusion of contracts, the registration of contracts, accounting and tax tasks, and members of the Board of Directors.

Duration of storage of personal data: 7 years after termination of the contract.

Place of storage of personal data: paper documents are stored in the room of the directorate. For security reasons, documents are also scanned and stored in the server room. They will be accessible to members of the Board and project managers.

Payer data processing

The Company processes the personal data of the data subjects - employees, their family members, employees, other beneficiaries and persons in contractual relationships - with whom it has a relationship as a paying agent (CL Act of 2017 on the Rules of Taxation (Art. 7.§ 31.)) for the purposes of fulfilling its tax and contribution obligations (assessment of tax, tax advances, contributions, payroll accounting, social security administration), as required by law (legislation).

Data processed: the natural person's natural identity data: name (previous name), place and date of birth, mother's name, address, tax number and tax identification number, social security number (social security number), if the person concerned is a pensioner, the pensioner's identification number. If the tax laws impose a legal consequence, the Company may process data on the employees' health (§ 40 of the Social Security Act) and trade union (§ 47 (2) b) of the Social Security Act) membership for the purpose of meeting tax and contribution obligations (payroll, social security administration).

Purpose of processing: to comply with or fulfil obligations under tax legislation (e.g. Act CXXXVII of 2017 on Value Added Tax, Act CXVII of 1995 on Personal Income Tax, Act CL of 2017 on the Rules of Taxation), Act LXXX of 1997 on the right to social security benefits and private pensions and on the coverage of these services. *The period of storage of personal data* is 7 years after the termination of the legal relationship giving rise to the legal basis.

Recipients of personal data: employees of the Cooperative performing tax, payroll, social security (payroll) and accounting functions.

Place of storage of personal data: paper documents are stored in the room of the directorate. For security reasons, documents are also scanned and stored in the server room. They will be accessible to members of the Board and project managers.

CHAPTER VII.

Data processing activities of the cooperative

The Co-operative uses the services of an accountancy firm on a contract basis to fulfil the tax and accounting obligations laid down in special laws and to perform the duties of a paying agent in connection with tax and contribution obligations.

Company name: Ft Audit kft

Registered office: 2112 Veresegyház, Lisznyay Szabó Gábor utca

35. *Company registration number: 13-09-19923*
VAT number: 26744092-2-13
Representative: Balázs Tóth, managing director

For the purposes of monitoring the lawfulness of the data transfer and informing the data subject, the Cooperative shall keep **a data transfer register**, which shall contain the date of the transfer of personal data processed by it, the purpose, legal basis and recipient of the transfer, the categories of data subjects, the scope of the personal data transferred and other data specified in the legislation providing for the processing. The medical and personal data recorded on the data subject which are necessary for the purposes of treatment and their transmission shall also be recorded.

The data transfer records shall be kept in electronic form by the designated person on a password-protected laptop owned by the Employer. The register does not contain the specific personal data, except for the name of the data subject, but the scope of the personal data.

The Cooperative shall enter into a separate contract with the processors for the processing of data, unless the original contract with the processor already contains the applicable data protection provisions.

The Cooperative shall have the right to monitor the processor's performance of the activities under the contract. The Cooperative shall be responsible for the lawfulness of the instructions given to the Cooperative in connection with the tasks specified in the contract. The processor shall, however, immediately notify the Cooperative if the instructions given by the Cooperative or the implementation of such instructions are contrary to law.

The Cooperative must inform the natural persons concerned of the fact of the processing and, where required by law, obtain their consent to the transfer.

CHAPTER VIII.

Services provided by the cooperative to third parties (external services), data transfers, joint data management

The Cooperative, taking into account the nature of the external service regulated by Act X of 2006 on Cooperatives, will transmit the following data of the Member to the recipient of the service. Members will be informed individually in each case of any other cases.

The Cooperative and the recipient of the service (hereinafter referred to as the Parties) act as joint data controllers for the services provided under the contract between them, which joint data processing includes in particular the following personal data.

Personal data subject to joint processing

Purpose of data processing	Legal basis for data processing
<p>Name of person concerned, title of the personal involvement of the and, following the establishment of position held, date of entry, date of exit, data subjects, the legal relationship, performance educational qualifications, professional making his work available to the of the contract and fulfilment of a and work experience, curriculum vitae Client</p>	<p>Consent of the data subject pursuant to Article 6(1)(a) GDPR</p> <p>legal obligation Article 6(1)(b) and (c) GDPR</p> <p>according to Consent of the data subject pursuant to Article 6(1)(a) GDPR, and subsequent performance of the</p>
<p>E-mail address, telephone number of Contact contract after the establishment of the person concerned</p>	<p>the legal relationship Article 6 (1) GDPR</p>

paragraph b.)

The joint controllers shall jointly determine the purposes and means of the processing of personal data as defined in this Clause and shall jointly take decisions regarding the processing in accordance with the provisions of the Treaty. The Co-operative and the recipient of the service undertake to co-operate in the performance of the following tasks related to the exercise of the rights of the data subject as set out in the Regulation:

- The data subject may request information about the processing of his or her personal data and access to the personal data and the information provided for in Article 15 of the GDPR (Articles 12-15 GDPR);
- request the rectification of your personal data and the integration of incomplete personal data (Article 16 GDPR);
- may request the erasure of your personal data - "right to be forgotten" (Article 17 GDPR) or restriction of processing (Article 18 GDPR);
- object to the processing of your personal data (Article 21 GDPR);
- under the "right of portability", you have the right to receive your personal data and to transmit those data to another controller (Article 20 GDPR);
- has the right to lodge a complaint with the supervisory authority.

The Co-operative and the recipient of the service act as joint controllers for the services provided under the contract between them, the legal basis for which is the consent of the data subject pursuant to Article 6(1)(a) GDPR and, following the establishment of the legal relationship, the performance of the contract and the fulfilment of a legal obligation pursuant to Article 6(1)(b) and (c) GDPR.

The joint controllers shall jointly determine the purposes and means of the processing of personal data as set out in this Clause and shall jointly take decisions regarding the processing in accordance with the provisions of the Treaty.

The aim of the Co-operative is to provide access to work for as many of its members as possible. To this end, the Y Diák Iskolaszövetkezet shall, subject to voluntary consent, provide the following personal data of the Member to the group company **WorkNow Hungary Kft.**, a temporary employment agency (registered office., Tax number: 24105336-2-03, Company registration number: 03-09-131895, Registration decision number: BKM/01/013190-3/2021, represented by Tamás Nagy and Ádám Baksay-Szabó, jointly).

The legal basis for the processing of data for WorkNow Hungary Kft. ("With regard to the processing of applicants' data") is the voluntary consent of the Member (Article 6 (1) (a) GDPR). Without consent, the transfer of data is not possible.

The recipients of the personal data are: the recipient of the service and the employees of WorkNow Hungary Kft. performing human resources-related tasks.

The Cooperative therefore carries out joint processing with the data controller WorkNow Hungary Limited Liability Company for the following purposes:

A./ Processing of applicants' data

Goal: to provide the highest level of service to the candidate concerned, to support their job search and placement.

The scope and purpose of the data processed in the context of joint data management:

Name	identification
place and time of birth	identification
name of position applied for	necessary to identify the application
experience - name of previous workplace and job title	to be considered for the post, you must have work experience
period spent	
experience - position description	to be considered for the post, you must have work experience

education level	educational qualifications required to be considered for the post
foreign language knowledge, foreign language and level of knowledge	to be considered for the post, you must have foreign language skills
other information from the attached CV	to be considered for the post, you must have CV and relevant details for the job
attached cover letter	to be considered for the post, you must have cover letter

Data apply at following 3 for unnecessary for the legal basis for to 3 years consent to the processing of personal data, if the data subject will not be applied processing in the event of non-election

Common data management mode: a common set of data, access to which is regulated by the levels of access rights established by each controller: only the person who has a task in relation to the data set has access to it.

B./ Camera system operation

Purpose: protection of property, tools and equipment in the monitored area, protection of persons and identification of those involved, prevention of accidents in the area and investigation of the circumstances of the accidents, quality assurance reasons, clarification, investigation, detection and proof of (legal) disputes in the event of quality assurance complaints, investigation of complaints, etc.

The scope of the data processed and their purposes:

- Image: identification
- other personal data: identification.

Common mode of processing: a common set of data, access to which is regulated by the levels of access rights established by each controller: only the person who has the task and the rights to access the data set.

C./ Customer service operation

The aim: to document and more efficiently deal with the needs and problems of stakeholders and users, and to serve them.

The scope of the data processed and their purposes:

- name: identification
- personal data provided during the conversation: identification.

Common mode of processing: a common set of data, access to which is regulated by the levels of access rights established by each controller: only the person who has the task and the rights to access the data set.

The Parties undertake to cooperate in the performance of the following tasks related to the exercise of the rights of the data subject under the Regulation:

- a) The Member concerned may request information about the processing of his/her personal data and access to personal data and information under Article 15 of the GDPR (Articles 12-15 GDPR);
- b) request the rectification of your personal data and the integration of incomplete personal data (Article 16 GDPR);
- c) may request the erasure of your personal data - "right to be forgotten" (Article 17 GDPR) or restriction of processing (Article 18 GDPR);
- d) object to the processing of your personal data (Article 21 GDPR);
- e) has the right to receive your personal data and to transmit those data to another controller under the "right of portability" (Article 20 GDPR);
- f) has the right to lodge a complaint with the supervisory authority.

The Member concerned may exercise his or her rights under the GDPR in relation to and against both controllers. In view of the fact that personal data as defined above are held by both Parties

are available, the Parties shall cooperate fully in the exercise of the rights of the data subject, and, unless otherwise agreed, the controller to which the request is addressed shall respond to the data subject. Where processing entails a high risk to the rights and freedoms of natural persons (e.g. profiling, processing of a large number of sensitive data), the Parties shall carry out an impact assessment prior to processing.

The Parties shall carry out the processing solely for the performance of their tasks under the contract between them and shall not transfer personal data relating to the data subjects to third parties.

Duration of storage of data: the recipient of the service and the temporary employment agency WorkNow Hungary Kft. will process the personal data only for the shortest and most necessary period of time, the duration of which will be communicated to the Cooperative on a case-by-case basis, which will inform the Member thereof.

The detailed information on the exercise of rights of survivorship and the means of enforcing claims is set out in Annex 7 to the Rules.

Under the agreement with the Cooperative, the recipient of the service guarantees, in particular in terms of expertise, reliability and resources, that it will implement technical and organisational measures to ensure compliance with the requirements of the Regulation, including the security of data processing. In the course of its activities, the recipient of the service shall ensure that persons authorised to have access to the personal data concerned are bound by an obligation of confidentiality with regard to the personal data they have access to, unless they are otherwise subject to an appropriate legal obligation of confidentiality. The recipient of the service must guarantee that it has adequate hardware and software facilities and undertakes to implement technical and organisational measures to ensure the lawfulness of the processing and the protection of the rights of the data subjects. The Cooperative shall be entitled to verify the existence and implementation of the contractual data security commitments by the recipient of the service.

The Cooperative is obliged to inform the natural persons concerned about the processing and, if required by law, to obtain their consent.

The recipient of the service must guarantee that it implements appropriate technical and organisational measures to ensure a level of data security appropriate to the level of risk, taking into account the nature, context and purposes of the processing and the rights of natural persons. It shall take measures to ensure that natural persons acting under its authority who have access to personal data may process those data only in accordance with the instructions of the Cooperative, unless they are required to do otherwise by Union or Member State law. It shall ensure that access to the data stored is restricted, either through an internal system or by direct access, to authorised persons and only in relation to the purposes for which the data are processed. Ensure the necessary regular maintenance and development of the tools used. It shall place the data storage device in a secure enclosure with appropriate physical protection and shall ensure that it is physically protected. It shall employ persons with the appropriate knowledge and experience to perform the tasks specified in the contract. He shall also ensure that the persons he employs are trained in the provisions of data protection law to be complied with, the obligations laid down in this contract and the purpose and method of data collection.

The Cooperative and the recipient of the service shall, in the course of the contractual cooperation, process personal data only and exclusively to the extent necessary for the performance of the contract, concerning the employees, contributors or assistants of the other party. Such data shall be treated confidentially and shall be made accessible only to those of their employees, collaborators or assistants to whom it is justified and necessary. They shall not otherwise transfer, disclose or make available such data to third parties. They shall take all necessary steps, including obtaining appropriate consents, which may be necessary for the lawful processing of personal data.

CHAPTER IX.

Website, customer service, community page

The Company's website <https://www.ydiak.hu> can be visited by any person without providing any personal data to the Data Controller, however, the Company (Data Controller) records and stores certain data that do not constitute personal data (hereinafter: Other Data) in relation to the User. Other Data means the data on the User's computer which, during the visit to the Website

are generated, in particular data related to the User's use of the Website and browsing habits (e.g. time of visit, pages viewed, browser program used).

Website visit data

I. References and links: the website of the Data Controller may also contain links to other websites that are not operated by the Data Controller, but are merely for the information of visitors. The Controller has no control

over the content and security of websites operated by partner companies and is therefore not responsible for them. Please review the privacy policy and data protection statement of the sites you visit before providing any form of information on those sites.

II. Cookies: the Data Controller, having regard to the provisions of Article 155, paragraph 4 of Act C of 2003, according to which "Data may be stored on the electronic communications terminal equipment of a subscriber or user or access to data stored therein may be granted only on the basis of the clear and full consent of the user or subscriber concerned, including the purpose of the processing", provides the following information on the analytical tools it uses, i.e. cookies. The Data Controller uses the following cookies, the purpose of which is set out below:

a. Cookies that are strictly necessary

Such cookies are essential for the proper functioning of the website. Without the acceptance of these cookies, the Data Controller cannot guarantee that the website will function as expected, nor that the user will have access to all the information the user is looking for. These cookies do not collect personal data from the data subject or data that can be used for marketing purposes. Examples of cookies that are strictly necessary are Performance cookies, which collect information on whether the website is working properly, whether there are any errors in its operation. By indicating possible errors, they help the Data Controller to improve the website and indicate which parts of the website are the most popular.

b. Functional cookies i. These cookies ensure a consistent presentation of the website tailored to the needs of the data subject and remember the settings chosen by the data subject (e.g. colour, font size, layout).

c. Targeting cookies i. Targeting cookies ensure that the ads displayed on the website are tailored to the interests of the data subject. The website mainly contains advertisements related to the services and products provided by the Data Controller and are intended to facilitate the data subject's access to more favourable offers.

d. Third-party cookies i. A cookie provided by a third party, such as a social networking site, may appear on the website to allow you to share or like specific content, and send information to the third party that can later be used by the third party to display ads to you on other websites.

The cookie also helps to improve the ergonomics of the website, to create a user-friendly website, to enhance the online experience of visitors.

III. Analytics, Facebook pixel: The data controller embeds JavaScript code in the website (or any subpage thereof) using a tool called Facebook pixel (formerly known as conversion tracking pixel), which sends a message to Facebook when a user visits the page or performs an action on the page. This both helps the Data Controller to understand the return on its advertising spend and makes it easier to serve ads to users who are more likely to convert outside of Facebook. Facebook pixel does not collect, store or transmit any personal data. For more information about how Facebook pixels are used and how they work, please visit www.facebook.com.

IV. Facebook remarketing: the Data Controller places a set of code on the website (or any subpage thereof), the purpose of which is to make the Data Controller's advertisement or advertisement available to the user visiting the website while using Facebook. The Facebook remarketing code set does not collect, store or transmit any personal data. For more information on the use and operation of the code set, please visit www.facebook.com.

Google Adwords remarketing: the Data Controller places a set of code on the website (or any subpage thereof), the purpose of which is to make the Data Controller's advertisement or advertisement available to the user visiting the website while they are browsing the Google Display Network websites and/or searching for the Data Controller or a term related to the Data Controller's services in Google. The code set

does not collect, store or transmit personal data. For more information on the use and operation of the code set, please visit <http://support.google.com>.

Therefore, the Data Controller does not use analytics systems to collect personal data.

The Data Controller reminds users that most Internet browsers automatically accept cookies, but visitors have the option to delete or automatically reject them.

As each browser is different, the user can set his preferences for cookies individually, using the browser toolbar.

The Data Controller draws users' attention to the fact that they may not be able to use certain features of the website if they choose not to accept cookies.

Data processing related to the operation of customer services

The Data Controller operates a customer service for the purpose of handling consumer complaints, informing consumers, improving quality, documenting and more efficiently handling the needs and problems of the customers and users. Legal basis for processing: consent of the data subject.

Data subjects: all natural persons, including natural persons acting on behalf of an organisation, who wish to contact or maintain contact with the Data Controller through the customer service.

Scope and purpose of the data processed:

Name

the information provided during the interview personal data

identificati on

The purpose of data management: to document and more efficiently deal with the needs and even problems of data subjects and users, and to serve data subjects.

Duration of processing: at the request of the data subject, until erasure, or failing that, until 6 months, or, if the data subject has entered into an agreement with the Controller, until the expiry of the limitation period for the rights and obligations arising from the legal relationship in relation to which the Controller processes the personal data.

Request for quotation

The Data Controller allows data subjects to request an offer from the Data Controller by providing the following details. The request for an offer is based on voluntary consent.

Data subjects: all natural persons who request an offer from the Data Controller in connection with a given service, providing their personal data.

Scope and purpose of the data processed:

name* identification phone number
contact e-mail address* contact

content of question/request*

Reply

Indication of selected service

necessary for the offer

service (special) details/question

The purpose of the processing is to provide the data subject with a suitable offer and to maintain contact.

The activity and process involved in the processing is as follows: the data subject sends his or her data to the Data Controller through a channel or means made available to him or her by the Data Controller. The Controller receives the data by e-mail. The Data Controller shall prepare an offer in response to the data subject's request for an offer or, if necessary to obtain information for the offer, contact the data subject at the contact details provided by the data subject and, in the light of the information, prepare the offer and deliver it to the data subject by the same means as the request for an offer was received, unless the data subject provides otherwise. Data subject, for the purposes of the processing

voluntarily consent to being contacted by the Data Controller, if he/she provides his/her contact details in the course of the request for an offer, in order to clarify the offer or to confirm the order.

Duration of processing: until the expiry of the offer.

Social media presence and marketing

The data controller is accessible on the Facebook community portal and other social networking sites. The use of social networking sites, including in particular the Facebook page, and the contact, communication and other operations permitted by the social networking site, through the Facebook page, with the Data Controller is based on voluntary consent.

Data subjects: natural persons who voluntarily follow, share or like the social networking pages of the Data Controller, in particular the page on facebook.com or the content on it.

Scope and purpose of the data processed:

public name of the public concerned	identification	his public photo
identification		
public email address		contact
your message sent via the relevant social networking site		contact, basis for response
the result of an assessment or other action by the data subject		for quality improvement or other operations

The Data Controller communicates with data subjects via the Community Site only when the data subject contacts the Data Controller via the Community Site, and thus the purpose of the scope of the data processed becomes relevant when the data subject contacts the Data Controller via the Community Site.

The purpose of the presence on social portals, in particular Facebook, and the related data processing is to share, publish and market the content of the website on the social networking site. The data subject voluntarily consents to the following and liking of the Controller's content under the terms and conditions of the social networking site. By way of example, the data subject can subscribe to the news feed published on the Facebook wall by clicking on the "like" link on the Facebook wall, and thereby consent to the publication of news and offers of the Controller on his/her own wall, and unsubscribe by clicking on the "dislike" link on the same wall, and delete unwanted news feeds on the wall by using the settings on the wall. You can rate the Data Controller textually and numerically, if the social networking site allows you to do so. The Data Controller may also publish on its social networking sites, in particular on Facebook, images/video clips of various events, services of the Data Controller, etc. The Data Controller may link the Facebook page to other social networking sites in accordance with the rules of the social networking site facebook.com, so that the publication on the Facebook page shall be understood to include publication on such linked social networking sites. If it is not a public image or a public performance (Civil Code 2:48), the Data Controller will always ask for the written consent of the data subject before publishing the images.

The data subject can obtain information about the data processing of a given social networking site on the social networking site concerned, and accordingly, information about the data processing of the Facebook page can be obtained [at www.facebook.com](http://www.facebook.com).

Duration of processing: until erasure at the request of the data subject.

CHAPTER X.

Processing of data related to electronic surveillance

Purpose of data processing: the Cooperative uses a camera surveillance system at its headquarters for the protection of persons and property, human life and physical integrity. The Cooperative has carried out a balancing of interests test before starting the processing.

In carrying out the balancing of interests test, the legitimate interest of the Cooperative as a legal basis will be legitimate if it is established that the interest of the Cooperative outweighs the data subject's right to the protection

of his or her personal data or the protection of his or her privacy. The balancing of interests test consisted of the following steps for each camera:

1. whether the use of a camera is strictly necessary in the place in question or whether there are alternatives to avoid data processing,

- b) the identification of the legitimate interest justifying the processing, the purpose of the processing and the related period of processing,
- c) the balancing of interests test should examine the following circumstances for all cameras:
 - protecting machinery and other tangible property on the property,
 - the interests of the data subject, i.e. the fundamental right to the protection of personal data (primarily the right to an image)
 - guaranteeing the rights of the data subject and ensuring enforcement; - the data security measures taken and planned before the processing starts; - the time-limited nature of the processing.

Location of cameras: cameras must not be operated for the primary, explicit purpose of monitoring workers and their activities. The use of an electronic surveillance system with the purpose, even if not declarative, of influencing the behaviour of workers at work may be considered unlawful. It is prohibited to place a camera in a room where observation could be offensive to human dignity, in particular in changing rooms, showers, toilets or, for example, in a doctor's room or waiting room. In addition, in principle, electronic surveillance systems should not be used in rooms designated for the purpose of employees' breaks, such as the staff canteen. If no one is legally allowed to be present in the workplace (in particular outside working hours or on public holidays), the entire workplace (e.g. changing rooms, toilets, break rooms) can be monitored.

The Cooperative may only use electronic surveillance systems to monitor parts of buildings, premises and areas owned or used by it, or events occurring there, but not to monitor public areas. The field of view of the camera may be directed towards an area consistent with its purpose.

If the camera surveillance is directed at an area where both employees and customers (visitors, guests) may be present, the Cooperative must of course also ensure that the information notice pursuant to Section 28 (2) d) of the Act on the Protection of the Right to Information is placed.

The Cooperative shall post a prominent sign at the entrance to the site, at the entrance doors, informing the public in advance of the use of the electronic monitoring system. The information shall be provided for each camera, indicating precisely the purpose for which the camera is installed in the area and the area or equipment to which the camera is directed. Accordingly, the Company shall keep a list of the cameras installed, indicating the exact location where the camera is installed, the direction of the angle of view, the purpose of the surveillance and the legal basis for the surveillance. The list of cameras actually in operation and the information provided is attached as Annex 8 to these Regulations. The information shall include the legal basis for data processing, the identification of the legal entity operating the electronic surveillance system, the place and duration of storage of the recording, the persons entitled to access the data, the persons and bodies to whom the recording may be disclosed and in what circumstances, the rights of the data subjects in relation to the electronic surveillance system and the means by which they may exercise their rights, and the means of redress available to them in the event of a breach of their right to information.

Duration of data processing: the duration of storage of the recordings (personal data) recorded by the electronic surveillance system is 8 working days from the date of their creation. In determining this duration, the Cooperative has taken into account the principles governing data processing, such as the principles of data minimisation and limited storage. After the storage period, the recording is automatically deleted.

The recordings are not backed up separately. Digital recordings are not accessible from an external network.

The legal basis for CCTV surveillance is the legitimate interest of the Cooperative, both for data subjects who enter the monitored area voluntarily and of their own free will and for employees (Article 6(f) of the Regulation). The interest of the protection of the Cooperative as described above takes precedence over the rights, interests and personal freedom of the data subjects (employees, business partners, visitors). Furthermore, it has been established that this is the most effective means for the Cooperative to ensure the protection of its assets. Although the personal rights of the data subjects (including specifically their right to their image) are infringed, the Cooperative will put in place appropriate safeguards to counterbalance this. The balancing of interests test is set out in Annex 9 to these rules.

Scope of the data processed: the surveillance system records the image of the person entering the area monitored by the cameras and, together with this, the action (moving image) that is visible on the recording. The camera surveillance system does not record sound. The cameras operate continuously.

Data security measures: the monitor for viewing and reviewing the images is positioned in such a way that it cannot be viewed by anyone outside the authorised circle while the images are being broadcast. To this end, the monitor is placed in a locked room that can be opened with a key.

Persons authorised to view the recordings: members of the Board of Directors.

The Co-operative does not use an external data processor, it operates the camera system and manages the recordings internally.

It is considered as use of the recordings:

- to investigate security incidents involving personal data,
- to prepare a complaint in the event of suspicion of a criminal offence or irregularity,
- to respond to written requests from public authorities,
- in disciplinary proceedings to establish the facts or investigate an accident at work
- the data subject, and whose rights or legitimate interests are affected by the taking of the photograph, in order to ensure the exercise of his or her rights.

The recorded images may be handed over to the investigating or administrative authority or police in the case of a suspected crime or offence, or other judicial or administrative proceedings. The transmission of the footage may only take place with the permission of the Directorate. The footage may be used to investigate an accident at work or for disciplinary proceedings in order to establish the facts of the case.

Access to the stored recordings must be carried out in a secure manner and in such a way that the identity of the controller can be identified. The review of stored image records and backups of image records shall be documented. The Cooperative shall keep a record of the viewing of the recordings, the reason for viewing, the time of viewing and the person who viewed the recording in an Excel spreadsheet.

After the detection of an offence, the recording of the offence and the initiation of the necessary official proceedings must be immediately taken and the authority must be informed that the offence was recorded.

The exercise of rights of interest is facilitated by the application form in Annex 10, which must be sent by post or hand-delivered to the Management Board.

Right of access

The data subject is entitled to request information on the processing of his or her personal data, the purpose, legal basis, duration of the processing, the criteria for determining the retention period, the circumstances and effects of a personal data breach, the measures taken, the legal basis and purpose of the transfer, the recipients of the transfer, the rights of the data subject, the exercise of rights and the means of enforcement. *Right to restriction (blocking) of processing*

The data subject may, on the basis of the procedural rules detailed in the previous point, request the blocking of the record - i.e. that the Cooperative does not delete the record - on the grounds of legitimate interest within 30 days, i.e. within the automatic deletion period. If the request is lawful and the part of the record concerned can be consulted at a later date. The Data Controller shall identify the part of the record concerned by clearly indicating the limited nature of the processing and shall ensure that it is stored separately from other data. The blocking shall last as long as the storage of the data is necessary for the reason indicated by the data subject and the data cannot be deleted.

The Data Controller shall also indicate in the minutes the fact of the blocking or the refusal to block the data, the reason for the blocking, the time of the blocking and the name of the person who provided the information. The identity of the data subject shall be verified, but the release of the records shall not be subject to any further condition (such as the verification of a right or legitimate interest). Once the identity of the data subject has been verified, the Controller shall block or disclose the recordings as requested.

The Data Controller is obliged to release the recordings if requested by a court or public authority. However, the controller shall not release copies of records which contain personal data of data subjects other than the applicant. The Data Controller may not request the purpose for which the recording is used.

Right of access

The data subject may request access to the images of him or her within 3 days of the date on which the image was taken. Pending a decision on the request, the recordings cannot be deleted and must be processed without delay. Access shall be granted at a pre-arranged time within 30 days of receipt of the request. The data subject may request a copy of the record provided that the rights of another data subject are not adversely affected.

Right to object

The data subject shall have the right to object to the processing by letter or e-mail addressed to the representative of the Cooperative, if the legal basis for the processing is the legitimate interest of the Controller. The data subject may also make the request by filling in the appropriate form in Annex 5. The administrator shall decide on the request within 25 days of its receipt at the latest. The Data Controller shall give reasons for refusing the request and shall block the data until the decision is taken. An objection to the processing and the decision to that effect shall not prevent the automatic deletion of the image.

Right to erasure

The data subject may request that the Controller erase the recording containing his or her personal data if the processing is unlawful. The Management Board shall decide on the request within 25 days at the latest.

In the event of a breach of the right to the protection of personal data and the exercise of the right in this regard, the data subject may seek legal remedy in accordance with the provisions of Article 23 of the Data Protection Act. The data subject is also entitled to lodge a complaint with the National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C. 1530 Budapest, Pf. 5., ugyfelszolgalat@naih.hu) in accordance with the provisions of Section 22 of the Infotv.

CHAPTER XI.

Data security measures, records

The Cooperative shall take the technical and organisational measures and establish the procedural rules necessary to enforce the Regulation and the Infotv.

The Cooperative will take appropriate measures to protect the data against accidental or unlawful destruction, loss, alteration, damage, unauthorized disclosure or access.

The Cooperative treats personal data as confidential. It imposes a confidentiality obligation on employees with regard to the processing of personal data. The Cooperative limits access to personal data by setting privilege levels.

The Board of Directors has unrestricted access to the full range of personal data of persons employed by the Cooperative. This right includes the right to modify, rectify, erase and archive personal data. Additional employees may access personal data only within the scope of their duties as defined in their job description. The data controller shall be responsible for the processing, modification, deletion, transmission, disclosure and accurate and traceable documentation of the data within the scope of his or her activities. The Cooperative protects its IT systems with firewalls and virus protection. Security

requirements for personal data **processed on paper** at the Cooperative:

- any personal data, regardless of the medium on which it is presented, is only disclosed to the may only be known to authorised persons, may not be accessed by unauthorised persons and may not be disclosed to unauthorised persons,
- documents must be kept in a lockable, dry room with fire and property protection equipment,
- a member of the Cooperative's staff carrying out data processing may leave the office or the room where the data processing is taking place only by locking the documents or by closing the room, - the documents must be locked up after the work has been completed, - these safety rules also apply to working at home.

Security requirements for the protection of personal data **stored on a computer or in a network or cloud** at the Cooperative:

- computers used to process personal data must be subject to the same security requirements regardless of whether the computer is owned by the Company or the employee,
- personal data stored on the computer, network or in the cloud can only be accessed with a valid, personal and identifiable authorisation, and passwords are changed by the Cooperative on a continuous basis, at least monthly,
- where the purpose for which the personal data are processed has been fulfilled, the time limit for processing has expired or the lawfulness of the processing has ceased for any reason, the file containing the data be irretrievably deleted in such a way that the data on it can no longer be retrieved,
- firewall security and other virus protection on computers must be provided,
- personal data must be backed up continuously on computers and regularly on network systems,

- the Cooperative shall continuously ensure the IT protection of the personal data it processes by using appropriate modern IT tools and methods.

The Cooperative 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 limited to those persons who need it for the performance of their duties, under controlled conditions and for a specific purpose.

When personal data are processed automatically, the controller and the processor take additional measures to ensure that:

- prevent unauthorised data entry;
- preventing the use of automated data processing systems by unauthorised persons using data transmission equipment;
- the verifiability and ascertainability of the bodies to which personal data have been or may be transmitted using data transmission equipment;
- the verifiability and ascertainability of which personal data have been entered into automated data processing systems, when and by whom;
- the recoverability of the installed systems in the event of a failure, and
- that errors in automated processing are reported.

The Cooperative will ensure that incoming and outgoing electronic communications are monitored to protect personal data.

Only the competent administrators shall have access to documents in the course of work or processing, and documents containing personal data of personnel, payroll and labour and individuals who have a contractual relationship with the Cooperative shall be kept securely locked and it shall be ensured that only authorised persons have access to the keys to these rooms (lockers).

The **Board of Directors of the Cooperative** is **responsible** for data protection:

- is responsible for ensuring the personal, material and technical conditions necessary for the protection of personal data processed by the Cooperative,
- is responsible for ensuring that the Cooperative complies with and enforces data protection legislation and this Policy,
- is responsible for remedying any data protection deficiencies identified at the Cooperative, - publish the Cooperative's privacy policy and be responsible for keeping it up to date.

The Cooperative's **employees** are responsible for data protection:

In the course of their daily work, the employees of the Cooperative must pay particular attention to the provisions of the Company's data protection policy and, on the basis of this policy, to ensure the security and integrity of the personal data they process and to prevent the occurrence of data protection incidents.

Data protection responsibilities of the **IT professional**:

- performs administrative tasks,
- performs the installation of software and hardware prior to commissioning;
- back up and log data stored on servers;
- ensure access to and modification of the data stored on the servers by the authorised persons and ensure that the stored data are not destroyed;
- in the event of a virus infection, perform virus removal from the infected IT device;
- maintains computers and the network as required, ensures that the servers are in working order, and carries out the servicing of IT equipment, where this can be done without the assistance of a specialist service technician;
- restart IT systems, restore applications and data on the network in the event of a failure;
- on the basis of a written request from the head of the department, assists in setting the individual code, password and access rights of the data controllers for the servers for which he or she has administrative rights;
- assist data controllers in the use of computer applications and database management, if required.

The Cooperative has **not appointed a Data Protection Officer**, taking into account that none of the cases listed in Article 37(1) of the Regulation applies, namely:

- the Company is not a public authority or other body with a public-service mission,
- does not include processing operations which, by their nature, scope and/or purposes, require systematic and systematic large-scale monitoring of data subjects,
- its main activity does not include the processing of large numbers of special categories of personal data within the meaning of Article 9 of the Regulation and of data relating to decisions on criminal liability and offences referred to in Article 10.

The Cooperative keeps records of the personal data it processes, the data it transfers to its data processors and third parties, and any data breaches that occur.

CHAPTER XII. Handling data protection incidents

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). Examples of incidents include: loss of a laptop on which personal data is stored, unsecure storage of personal data; unsecure transmission of data, unauthorised copying or transmission of customer and customer partner lists, attacks against servers, hacking of websites.

The Cooperative's Board of Directors is responsible for the prevention and handling of data protection incidents and compliance with the relevant legal requirements. Access and attempted access to IT systems shall be logged and analysed on an ongoing basis. If the Cooperative's supervisory employees detect a data breach in the course of their duties, they should immediately notify the Cooperative's management.

Employees of the Cooperative must immediately report to the Board of Directors if they become aware of a data protection incident or an event that may indicate a data protection incident.

The data protection incident can be reported to the Cooperative's central e-mail address, telephone number, where employees, contractors, data subjects can report the underlying events.

In the event of a data breach notification, the Cooperative's Management Board - with the involvement of the data security officer - will immediately investigate the notification, identify the incident, decide whether it is a real incident or a false alarm. It must 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 number of data unauthorisedly accessed during the incident,
- d. the persons involved in the incident,
- 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.

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. The Supervisory Authority should be notified under the conditions set out in data protection legislation.

The Cooperative shall inform the data subjects of the occurrence of a personal data breach if it poses a high risk to the data rights or freedom of the natural persons concerned. The information shall be clear, unambiguous and comprehensible.

The Cooperative may choose not to inform the data subjects if:

- has taken appropriate technical and organisational measures to make it impossible for unauthorised persons to gain access to the data concerned by the data breach,
- took measures after the data breach occurred to ensure that there is no high risk to the rights and freedoms of data subjects,
- information could only be provided through disproportionate efforts, in which case a measure must be taken to ensure that the persons concerned are effectively informed.

Records of data breaches are kept in electronic form by the designated person. The register contains the scope of personal data, not the specific personal data, except for the name of the Employee, Member.

Records of data breaches must be kept (Annexes 13 and 14), which include:

- 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.

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

Impact Assessment, Interest

Weighing Impact Assessment

If a new data processing process - with regard to its nature, scope, circumstances, purposes is likely to result in a high risk to the rights and freedoms of natural persons, the Company will carry out an impact assessment on how the processing will affect the protection of personal data before starting the processing. Similar data processing operations presenting similar risks may be carried out in the context of a single impact assessment. The impact assessment will, as a general rule, be carried out by the DPO. If not, the Company is obliged to seek the professional advice of the DPO.

After the impact assessment has been carried out, it shall ensure that the impact assessment is revised as necessary, but at least in the event of a change in the risk posed by the processing operations, and that the risk assessment is carried out again. The risk review shall be carried out at least every 3 years.

In addition, the Data Controller is obliged to carry out a risk analysis in relation to the processing of personal data, which includes the following steps:

- identify the risks associated with the processing of personal data,
- setting up a risk list,
- identifying the likely main causes and likely negative impacts of each risk, and - develop preventive and corrective risk management processes based on these.

It is necessary to identify the sources of risk, defining the elements of risk prevention and corrective target management, the system of resource management and distinguishing between objective and subjective risk elements. The analysis should lead to the development of a complete risk assessment system, in which a complete risk potential and risk prioritisation (not identical to the system of measures) should be established. The process and results of the analysis should be documented. The risk potential should be defined in terms of probability -

- small
- Medium
- and high-occurrence risks, or in terms of - small
- Medium
- and high-profile risks.

This definition will form the basis for the subsequent risk management process, both preventive and corrective. The DPO is responsible for carrying out the risk analysis.

Where the impact assessment carried out concludes that the data management process is likely to present a high risk, the Institute shall consult the Authority before starting the data management process.

Balance of interests

According to the provisions of the Data Protection Act, processing without consent is possible if there is a legitimate interest to do so, provided that the Data Controller complies with its obligation to provide information. Article 6(1)(a) to (f) of the GDPR shall apply when examining the legal basis for processing.

Where the legal basis is Article 6(1)(f) of the GDPR, the processing will be lawful if and insofar as the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.

In order to assess the lawfulness of processing, the Company will apply a balancing of interests test, in which the necessity of the purpose of the processing and the proportionality of the restriction of the rights and freedoms of the data subjects will be assessed and duly justified.

CHAPTER XIII.

The rights of the data subject, the submission of the data subject's request, the controller's actions and remedies

Rights of data subjects

According to the wording of the Regulation, a "**data subject**" is a natural person who can be identified, directly or indirectly, on the basis of information and personal data relating to him or her.

Before executing the request for enforcement, the Company is obliged to identify the person making the request (the use of a login and password associated with the user profile may be sufficient for identification purposes in the default case). If the Company has reasonable doubts about the identity of the natural person submitting the request, it may request additional information necessary to confirm his/her identity.

Request for information

The Data Subject has the right to be informed about the processing of his or her personal data and to exercise his or her rights. If you have such a request, please contact the Company in writing (by email). The Company will provide the requested information in writing as set out in this Privacy Notice. The Company may refuse to comply with the request if it can prove that it is unable to identify the data subject.

The right to request information does not extend to data processed under the law.

Right of access

The Data Subject has the right to receive feedback from the Company, upon request, on whether his or her personal data is being processed. If such processing is ongoing, he or she is entitled to have access to the personal data processed and to the following information:

- a) the purposes of the processing,
- b) the categories of personal data concerned,
- c) the recipients or categories of recipients to whom or with whom the personal data have been or will be disclosed, including in particular recipients in third countries or international organisations,
- d) where applicable, the envisaged period of storage of the personal data or, if this is not possible, the criteria for determining that period,
- e) the Data Subject's right to request the controller to rectify, erase or restrict the processing of personal data concerning him or her and to object to the processing of such personal data,
- f) the right to lodge a complaint with a supervisory authority,
- g) if the data were not collected from the data subject, any available information on their source,
- h) the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and clear information on the significance of such processing and its likely consequences for the data subject.

The Data Subject shall have the right to access the data collected concerning him or her and to exercise this right simply and at reasonable intervals in order to ascertain and verify the lawfulness of the processing.

The practice of granting access rights at the Company

Upon the Data Subject's request, the Company will provide a copy of the personal data that are the subject of the processing. If the Data Subject has submitted the request by electronic means or if the processing of personal data is carried out by electronic means, the information shall be provided in a commonly used electronic format, unless the Data Subject explicitly requests otherwise.

The Company shall respond to the Data Subject's request without undue delay and within 30 days at the latest, and shall give reasons if it does not comply with any request.

The request for a copy of personal data is normally free of charge. The Company may charge a reasonable fee, based on administrative costs, for copies requested in more than one copy or where a simpler, faster, more cost-effective method of requesting the data than that requested by the Data Subject would be available.

Right to rectification

The Data Subject is entitled to have inaccurate personal data relating to him or her corrected by the Company without undue delay upon his or her request.

Taking into account the purpose of the processing, the Data Subject also has the right to request the completion of incomplete personal data. Supplementation may take place by means of a supplementary declaration made by the Data Subject.

Right to erasure ("right to be forgotten")

The Data Subject is entitled to have the Company delete personal data relating to the Data Subject without undue delay upon his or her request, and the Company is obliged to delete personal data relating to the Data Subject without undue delay if one of the following grounds applies:

- 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 on the basis of the relevant provision of the Regulation and there is no overriding legitimate ground for the processing, or the Data Subject objects to the processing because it is for direct marketing purposes (including profiling);
- d) the personal data have been unlawfully processed;
- e) personal data must be erased in order to comply with a legal obligation under Union or Member State law applicable to the Company;
- f) personal data are collected in connection with the provision of information society services directly to children.

The Company is not obliged to delete the data if the processing is necessary for the following reasons:

- a) to exercise fundamental rights (the right to freedom of expression and information);
- b) where processing is mandatory (to comply with an obligation under EU or Member State law that requires the controller to process personal data);
- d) for reasons of public interest (e.g. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, where the right to erasure would be likely to render such processing impossible or seriously jeopardise it); or
- e) to bring, enforce or defend legal claims.

The right to erasure shall not entail, in particular, the erasure of personal data relating to the Data Subject which the Data Subject has provided for the performance of a contract, if and for as long as the personal data in question are necessary for the performance of that contract.

Furthermore, the right to erasure does not apply in cases where the duration of the processing is determined by law, e.g. in the case of an invoice, as the invoice must be kept for 8 years under the law.

If the Company has disclosed the personal data and is required to delete it, it will take reasonable steps, including technical measures, taking into account the available technology and the cost of implementation, to inform the data controllers that have processed the data that the Data Subject has requested them to delete the links to or copies or duplicates of the personal data in question. The exception rules also apply in this case.

Right to restriction of processing

The Data Subject is entitled to have the Company restrict processing 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 that allows the Company to verify the accuracy of the personal data);
- b) the processing is unlawful and the Data Subject opposes the erasure of the data and requests instead the restriction of their use;
- c) the Company 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 accordance with the relevant provision of the Regulation; in this case, the restriction shall apply for the period until it is established whether the legitimate grounds of the Company as controller prevail over the legitimate grounds of the data subject.

If the processing is restricted, such personal data, except for storage, may only be processed 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 for important public interests of the Union or of a Member State.

The Company will inform the Data Subject (at whose request the processing was restricted) in advance of the lifting of the restriction.

Right to data portability

The Data Subject has the right to receive personal data concerning him or her provided by the Data Subject to the Company in a structured, commonly used, machine-readable format and the right to transmit such data to another controller without hindrance from the Company, if:

- a) the processing is based on consent or a contractual legal basis; and
- b) the processing is carried out by automated means.

In exercising the right to data portability, the Data Subject has the right to request, where technically feasible, the direct transfer of personal data between controllers.

Please note that the right to data portability can only be exercised if the above cumulative conditions are met (i.e. if the processing is based on consent or a contract AND the processing is automated). The right to data portability does not extend, for example, to data processed under a legal provision.

According to the guidelines of the Article 29 Data Protection Working Party (WP29), since the right to data portability only applies to data processing by automated means, it does not apply to paper-based data processing.

Right to object

The Data Subject has the right to object at any time, on grounds relating to his or her particular situation, to the processing of his or her personal data based on the Company's legitimate interest. In such a case, the Company may no longer process the personal data unless it can demonstrate 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.

Where personal data are processed for direct marketing purposes, the Data Subject has 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 these purposes.

Measures taken at the request of the person concerned

The Cooperative, as data controller, shall inform the data subject without delay, and at the latest within one month of receipt of the request, of the measures taken in response to the request to exercise his or her rights. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The Cooperative shall inform the data subject of the extension in writing (including by e-mail if the request was sent by e-mail) within one month of receipt of the request, stating the reasons for the delay.

If the Cooperative fails to take action on the data subject's request, it shall inform the data subject without delay, but no later than thirty days after receipt of the request, of the reasons for the failure to take action and of the right to lodge a complaint with the supervisory authority (NAIH) and to seek judicial remedy. The Cooperative shall provide the information requested under the right to information and the information and action related to the exercise of certain rights, in principle free of charge. However, if the request of the person concerned

is clearly unfounded or excessive, in particular because of its repetitive nature, the Cooperative, having regard to the administrative costs involved in providing the information or information requested or in taking the action requested:

- a) charge a reasonable fee, or
- b) may refuse to act on the request.

The burden of proving that the request is manifestly unfounded or excessive lies with the Company.

The Cooperative, as the Data Controller, shall provide the information and the information on the rights of the data subject (Articles 15-22 and 34 of the Regulation) and the action to be taken in accordance with Articles 13 and 14 of the Regulation free of charge. If the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive nature, the Cooperative may refuse to act on the request.

The burden of proving that the request is manifestly unfounded or excessive shall be on the Cooperative.

Remedies

Without prejudice to any other administrative or judicial remedy, 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 he or she considers that the processing of personal data relating to him or her infringes the Regulation. Without prejudice to other administrative or non-judicial remedies, the 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.

Without prejudice to the administrative or non-judicial remedies available, including the right to lodge a complaint with a supervisory authority, the data subject shall have an effective judicial remedy if 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 not in accordance with the Regulation. 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 of habitual residence of the data subject.

The data subject may lodge a complaint regarding the Cooperative's data management practices with the National Authority for Data Protection and Freedom of Information (in short: NAIH, tax address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c., postal address: 1530 Budapest, Pf.: 5., telephone: +36 (1) 391-1400, fax: +36 (1) 391-1410, email: ugyfelszolgalat@naih.hu, website: <https://www.naih.hu>), or with a court. The competent court has jurisdiction to hear the case. The action may also be brought before the Tribunal of the place where the person concerned is domiciled or resident, at the person's choice.

ANNEXES

**Annex No. 1
Factsheet**

on the processing of contact details of natural person representatives of legal person contracting partners

DATA MANAGER:	Y Diák Iskolaszövetkezet
HEADQUARTERS:	1137 Budapest, Radnóti Miklós utca 2.
COMPANY REGISTRATION NUMBER:	01-02-054614
TAX NUMBER:	24146443241
NAME OF REPRESENTATIVE:	Tamás Nagy Member of the Board
CONTACT AVAILABILITIES:	e-mail address: ugyfelszolgalat@ydiak.hu telephone number: + 36 30 608 1088
the name of the person concerned	
schedule:	
the name of the legal entity represented:	
is based in:	
the work telephone number of the person concerned:	
the e-mail address of the data subject:	

INFORMATION:

- the purpose of the processing:** Contract performance, business relations
- the legal basis for the processing:** The legitimate interest of the Company
- the recipients of the personal data:** Employees of the Company performing contractingrelated tasks;
- the duration of the storage of personal data:** 5 years from the date of the business relationship or the date on which the person concerned became a representative.

The Company's Privacy Policy is available on the above mentioned website, the detailed Privacy and Data Protection Policy is available at the Company's branch at Radnóti Miklós u. 2, 1137 Budapest, Reception. Upon written request, both will be sent to the above mentioned e-mail address.

I have taken note of the above information and information.

Budapest, 2018.....

Name: _____

Signature: _____

Annex No 2

DATA PROTECTION DOCUMENT

The Y Diák Iskolaszövetkezet, as the Data Controller of the website available under the domain name www.ydiak.hu (hereinafter referred to as the Website), hereby publishes information on the processing of data within the framework of the services related to the Website.

By accessing the Website and using the services of the Data Controller, users visiting the Website and using the services of the School Co-operative (hereinafter referred to as "Data Subjects") accept all the terms and conditions set out in this Privacy Policy (hereinafter referred to as "Policy"), therefore, please read this Policy carefully before using the Website or using the services.

For the purposes of this Policy, a Data Subject is: any specified natural person identified or identifiable, directly or indirectly, on the basis of personal data, whose data is processed by the School Cooperative.

1. Data of the Data Controller

DATA MANAGER:	Y Diák Iskolaszövetkezet
HEADQUARTERS:	1137 Budapest, Radnóti Miklós utca 2.
COMPANY REGISTRATION NUMBER:	01-02-054614
ADJUSTMENT:	24146443241
NAME OF REPRESENTATIVE:	Tamás Nagy Member of the Board
CONTACT AVAILABILITIES:	e-mail address: ugyfelszolgalat@ydiak.hu telephone number: + 36 30 608 1088

The School Co-operative Data Controller (hereinafter referred to as the "School Co-operative" or the "Controller") undertakes to conduct its data processing activities in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (General Data Protection Regulation, hereinafter referred to as the "General Data Protection Regulation" or "GDPR") by adopting appropriate internal rules and technical and organisational measures: Regulation) - and of the European Parliament and Council Regulation (EC) No 45/2001 of 21 December 2011 on the right to information selfdetermination and freedom of information (1). CXII of 2011 (hereinafter referred to as the "Infotv.").

2. Scope of personal data processed

Registration, pre-contractual

The services provided by the School Co-operative are available through the on-line registration form "Register for your employment" and at the customer service (1137 Budapest, Radnóti Miklós u. 2.) in person (hereinafter referred to as "the **Form**") for all Data Subjects who, as full-time students of the School Cooperative, wish to provide their personal services to third parties within the framework of the services provided by the School Cooperative, and for all Data Subjects who wish to establish an employment relationship with the School Cooperative.

When filling in the form, the following data of the Data *Subject* will be recorded: *name* (surname, first name, name at birth), *place and date of birth* (year/month/day), *e-mail address*, *telephone number*, *permanent address* (country, city, postcode, street, house number), *nationality*, *educational data* (semester status, school level, section, name of institution, degree course), *language skills*, *previous employment data*, *region of interest*, *jobs of interest*. The School Co-operative does not verify the personal data provided to it, and the Data Subject is solely responsible for the accuracy of the data provided.

The School Co-operative shall keep the Data Subject's recorded data in a secure manner and shall process it solely for the purpose of providing the service, in the manner and for the period set out in this Policy.

The School Co-operative does not handle Members' photographs, and therefore does not accept CVs or photo IDs with a photograph. If the Member fails to do so, the School Co-operative will consider that the Member expressly consents to the processing of his/her photograph (portrait) until such time as the School Co-operative deletes the

photographic section. The School Co-operative shall carry out the deletion without delay, but within 2 working days at the latest.

Conclusion of contracts by electronic means

- a) *the technical steps for concluding the contract are as follows:*
 1. complete registration on <https://ydiak.hu/> and upload your student status certificate,
 2. electronic signature and completion of required fields on documents sent by email from <https://app.docuSign.com/> (membership agreement, membership application, membership declaration)
 3. accept the completed documents by clicking on the finish button.
- b) *the contract to be concluded is a written contract, the contract will be recorded by our School Cooperative, the contract will be made available at a later date*
- c) *the means for identifying and correcting errors in the electronic recording of data prior to the conclusion of the contract are as follows:* the data required for the conclusion of the contract are provided electronically by the Member and are recorded in the contract by the School Co-operative. The terms and conditions of the performance of the service (identity of the service recipient, specific tasks, remuneration, deadline for payment of the remuneration, starting date, place and duration of performance) are recorded partly on the basis of the School Co-operative's advertisement and partly on the basis of the information provided by the Member by telephone or e-mail. The Member is obliged to verify the data provided before signing.
- d) *language of the contract:* Hungarian.

Procedure to be followed when consent of the legal representative is given:

1. The Member will send the email address of his/her legal representative from the email address provided during registration to ugyfelszolgalat@ydiak.hu.
2. Electronic signature and completion of mandatory fields by the legal representative on the "Declaration of consent of legal representative" document sent by e-mail from <https://app.docusign.com/>.
3. Accept the completed documents by clicking on the "Finish" button.

The Member uploads a photo/scan of his/her student ID during the online registration. In doing so, he/she is required to keep his/her face out of the way, i.e. no photo is allowed. In the event that he/she fails to do so, the School Association will consider that he/she expressly consents to the processing of this personal data, as set out above, until such time as the School Association deletes the photographic part. The School Co-operative will carry out the deletion without delay and at the latest within 2 working days.

Newsletter subscription:

On the Website, the Data Subject also has the possibility to subscribe to the newsletter of the Data Controller through a dedicated interface. To subscribe to the newsletter, the following personal data must be provided:

- full name;
- e-mail address.

Following the conclusion of a membership agreement

The School Cooperative processes the Data Subject's data that are relevant for the establishment, performance and termination of the membership agreement with the Data Controller in accordance with the applicable legal requirements. The data to be recorded in the membership agreement are: name, name at birth, address, place of birth, date, mother's (maiden) name, tax identification number, student ID number, student card number, bank account number, telephone number, e-mail address.

Data provided in the entry form: name, maiden name, sex, address, place of birth, date of birth, mother's (maiden) name, tax identification number, tax number, student ID number, bank account number, telephone number, nationality, e-mail address, name of educational institution, grade.

Data processed in the case of an individual agreement: name, place of birth, date, data related to the performance of the membership agreement (time, place of performance, remuneration).

Declaration of consent by legal representative

If the member is under 18 years of age, the written consent of his/her legal representative is required to join the school cooperative, to establish a relationship for the provision of external services and to conclude the membership agreement and the individual agreement. The Data Controller processes the following data of the legal representative.

After the conclusion of the contract, the following personal data will be processed:

- the field of activity in which he/she performs or has previously performed under his/her membership; the name and place of business of the service recipient where he/she performs or has previously performed under his/her membership; the unit and amount of remuneration per unit of work; the title and amount of other benefits, the working hours;
- Details of training completed: title of qualification;
- Data needed for accounting: periods of employment (number of hours), time sheets for the performance of duties.
- Accounting data: data on the fees and other benefits, reimbursements of expenses and related deductions and tax payments made by the Data Controller to the Member during the legal relationship
- Other data related to the performance of the legal relationship: data related to work equipment, work clothing, access cards, usernames, passwords received under the obligation to pay; information related to cash or inventory shortages, damage, injury, accident at work, member or cooperative claims.
- Other data: electronic content, including documents, information, e-mails and other electronic communications, produced or transmitted using the information technology systems of the Data Controller, the recipient of the service and the processors.

Request for quotation

On the Website, the Data Subject has the possibility to request an offer from the Data Controller via a dedicated interface. To request an offer, the following personal data must be provided:

- full name;
- phone number;

- e-mail address;
- the position of contracting authority.

The additional questions required for the request for a quote (company name, what job you are looking for, number of staff required, expected start date and duration of service, how did you hear about us, details of the request for a quote), as it concerns a legal entity, do not involve personal data.

3. Legal basis for processing

The legal basis for the processing of the personal data of Applicants is the voluntary consent of the Applicant to the processing of his/her personal data given by accepting this Information Notice, Article 6(1)(a) of the Regulation.

The legal basis for Members' processing of data relating to the legal relationship is that

- a) processing is necessary for the performance of an agreement (contract) for personal data processing between the Members and the Controller, Article 6(1)(b) of the Regulation,
- b) the data controller has a legitimate interest in the processing for the performance of a contract with the recipient of the service, Article 6(1)(f) of the Regulation,
- c) the processing is necessary for compliance with legal obligations, Article 6(1)(c) of the Regulation,
- d) processing is necessary for health purposes, in order to assess the ability of members to perform their duties, Article 9(2)(h) GDPR.

4. Purpose of data processing

The purpose of the data processing is to ensure the provision of the services offered by the School Cooperative (membership, personal assistance in the context of student work, sending newsletters, employment, service and contracting). The School Co-operative shall process and store the Data Subject's personal data solely for these purposes, shall not use them for any other purpose, and may disclose them to third parties only with the Data Subject's prior written consent or on the basis of an official obligation.

In accordance with Act XLVIII of 2008 on the Basic Conditions and Certain Restrictions of Economic Advertising Activities, the School Cooperative may send newsletters to the e-mail address of the Data Subject provided during registration only with the Data Subject's express consent. The consent of the Data Subject may be withdrawn at any time, without restriction and without giving reasons, free of charge. The School Cooperative may also send advertising mail to a natural person as the recipient of the advertising by direct marketing without the prior and express consent of the recipient, in which case the School Co-operative shall ensure that the recipient of the advertising may at any time prohibit the sending of the advertising free of charge and without restriction. In the event of a prohibition, no further direct marketing of advertising may be sent to the person concerned.

The School Co-operative uses the data for the following purposes in connection with the services it provides:

In the case of a membership relationship, the purpose of the processing is the performance, maintenance and termination of the membership relationship between the School Co-operative and the Data Subject, in particular the performance of administrative tasks related to the performance of the duties (including personnel tasks, calculation and transfer of income and social security accounts) and HR controlling (including the efficient business organisation of human resources).

The Data Controller shall, on the basis of the Data Subject's explicit and voluntary consent, transfer the Data Subject's personal data to a third party (the recipient of the service) for the purpose of processing for the performance of the tasks related to the membership agreement, as defined in the individual agreement on the performance of tasks, to the extent necessary for the performance of the tasks within the framework of the cooperative membership.

The purpose of the processing is therefore:

- the rights and obligations of the Parties under an agreement based on the membership relationship between the Member and the Data Controller and on a contract between the Data Controller and the recipient of the service for personal assistance in the performance of an external service can be fulfilled,

- On the one hand, the Data Controller must comply with its obligations relating to the performance of its duties, employment protection, taxation, reporting and record-keeping, and other legal obligations in relation to the legal relationship.

In the event of a request for an offer, the Data Subject will contact the natural person at the telephone number or e-mail address provided and, in accordance with the parameters provided by the Data Subject, will make an offer with a view to concluding a contract with the legal entity represented.

5. Access to personal data, processing and transfer of data

The School Co-operative may not use personal data for purposes other than those stated. For the purposes set out in point 4, only persons employed by the School Co-operative at the time may have access to the Data Subject's personal data and they may not disclose it to third parties, except as provided in this notice. The School Cooperative is only entitled to use a data processor for the purposes of the purpose set out in point 4.

In order to achieve the purpose of the processing, in particular to make a job offer, to participate in a selection procedure, to establish a legal relationship, the data subject may provide his/her CV to the contracted customer (service recipient) offering the actual job opportunity, on the basis of his/her explicit and voluntary consent pursuant to point 4. The School Co-operative's contracted customers shall be entitled to see the CVs only to the extent and for the duration necessary for the selection and shall be obliged to delete the personal data of which they have knowledge after the vacancy has been filled.

The data subject may prohibit the disclosure of his/her CV by giving written notice to Y Diák Iskolaszövetkezet, and has the right to request information about when and to whom his/her CV was disclosed. For the purposes of monitoring the lawfulness of the transfer and informing the data subject, the School Co-operative shall keep a register of transfers, which shall include the date of the transfer of personal data processed by it, the legal basis and recipient of the transfer, the scope of the personal data transferred and other data specified in the legislation providing for the processing

In the case of any data transfer to a recipient of a service that carries out its processing activities in a third country, the Data Controller will only transfer the personal data of the Data Subject with the prior appropriate information and explicit consent of the Data Subject.

After the conclusion of the study contract for the qualification of swimming pool master, swimming pool master, the employees of the School Cooperative holding the position of project manager shall apply for the training on behalf of the Member to the Wellness and Hotel Industry Adult Training Institute (SpaDium Educational and Service Ltd.) on its registration page. For the application, in order to fulfil the contract, the School Association directly transmits the Member's name, date and place of birth, mother's name, highest educational qualification, labour market status, telephone number, e-mail address and home address. For billing information, the School Co-operative, as the cost bearer, will provide its own information. After the application, SpaDium Training and Services Ltd. will send a confirmation e-mail to the Member. A contract will then be concluded between the Member and the adult education institution, using the personal data provided by the Member to the School Cooperative.

6. Duration of processing

The School Co-operative will process personal data for the duration of the purpose of the processing, such as registration on the Website and sending the Newsletter, until the Data Subject requests the deletion of his/her data or withdraws his/her consent to the processing of his/her personal data or to the receipt of the Newsletter. In the case of a request for tenders, if no contractual relationship is established with the legal entity represented by the Data Subject, in that case it will delete the personal data provided without delay. If a contractual relationship has been established, the data will be deleted 5 years after its termination, unless the relationship between the Data Subject and the legal entity is terminated earlier. In this case, the personal data will be kept for 5 years from that date.

during registration, prior to the conclusion of the contract personal data collected	personal data processed after the conclusion of the contract the date of cancellation
---	--

<p>- if the applicant does not establish a legal relationship with the Data Controller within one year of the start of the processing, the Data Controller shall delete the applicant's personal data within 25 days of the request after the end of the school term/semester concerned or at the applicant's request. delete,</p>	<p>- personal data which are used to support an accounting document or which contain such data which form an integral part of documents containing such data, after a period of 8 years from the last day of the year in which the data were generated;</p>
<p>- if the Candidate enters into a legal relationship with the Data Controller, the provisions of the other column shall apply to the deletion of the Candidate's personal data.</p>	<p>- personal data which are relevant for the performance of the task in connection with legislation and other data forming an integral part of documents containing such data, after 8 years from the last day of the year in which the data were generated;</p> <p>- the Member, or the data controller, or the service recipient of the service for claims personal data necessary for the processing of personal data and other personal data which form an integral part of documents containing such data, after 8 years from the last day of the year in which the data were generated;</p> <p>- any other personal data after 1 year from the last day of the year in which the legal relationship ended.</p>

7. Who has access to personal data, processing of data

Access to the Data Subject's personal data may be exercised by the Management Board of the School Cooperative, by the coordinator and project manager, and by the recipients of the services to which the Data Subject has expressly and voluntarily consented to the transfer of his/her personal data.

The Data Controller reserves the right to involve a data processor in the future, which it will inform the Data Subject about by amending this Notice.

The register of members is governed by the Civil Code. 3:355 of the Civil Code. Anyone, i.e. not only the members, but also third parties may inspect the register of members if they prove their interest. For example, if a new member who intends to join the cooperative wishes to take over the position of a former member, he or she may be interested in checking what information is kept in the register of members of the cooperative.

8. Different rules on the processing of personal data of Data Subjects who wish to establish an employment relationship with the School Co-operative

It is an integral part of the right of informational self-determination of job applicants to be adequately informed of the identity of the controller before giving consent to data processing and to know against whom they can exercise their rights. The School Co-operative does not advertise jobs anonymously.

The purpose of the processing of personal data is: filling the vacant / vacant position, evaluating the application, the application, concluding an employment contract with the selected person. In order to ensure the applicant's right of informational self-determination, he/she will also be informed if the Company has not chosen him/her for the job in question. This will be done within 5 working days of the rejection decision.

If the Company has selected one of the applicants for the advertised job, the purpose of the processing ceases to exist and the personal data of the applicants not selected shall be deleted, with the following exception. At the

same time, the obligation to erase shall also apply if the data subject changes his or her mind or withdraws his or her application during the application process.

The personal data that may be processed include: the name, date and place of birth, mother's name, address, qualifications, copies of relevant certificates, telephone number, e-mail address, CV, application. If the School Co-operative identifies specific personal data in the application, it will delete them immediately.

The School Co-operative does not ask for a CV with a photo. If the applicant nevertheless submits a CV with a photograph, the School Co-operative will consider that he/she has given his/her express consent to its processing. The School Co-operative will draw the applicant's attention to this fact in the job advertisement.

Legal basis for processing: consent of the data subject.

Recipients of personal data: employees entitled to exercise employer's rights at the Company, employees performing labour and personnel-related tasks and the professional manager of the relevant area.

Duration of storage of personal data: 5 working days after the end of the selection process. Personal data of unselected candidates will be deleted on the 6th day. The personal data of candidates who withdraw their applications will also be deleted.

The School Co-operative may retain applications beyond this period only on the basis of the express, unambiguous and voluntary consent of the data subject, provided that their retention is necessary for the purposes of the processing in accordance with the law. Such consent shall be requested from the applicants after the closure of the recruitment procedure and at the latest until the evaluation of the application. In the case of explicit consent, the application file will be deleted from the School's database on the last day of the 12th month following its evaluation. During the 12 months, the data processed will only be used for the recruitment and selection process or to determine whether the candidate concerned would be suitable for another vacant post. If the data subject withdraws his/her consent within this period, his/her personal data will be deleted from the date of withdrawal.

If an application is received without a job advertisement, the School Co-operative will contact the applicant to ask if he/she agrees to keep his/her application for the above 12 months. Failure to do so will result in the deletion of both the paper application and the application sent by e-mail.

The applications and CVs sent to us will be handled only by the School Co-operative's authorised staff: the employer and the Head of Profession in the relevant area. The School Co-operative shall not disclose the job applications and curricula vitae received to third parties for statistical or other purposes, except in cases provided for by law, nor shall it disclose the data received to the public, nor shall it provide information on the assessment of the job applications and curricula vitae submitted, except at the request of and to the person concerned.

Location of personal data and measures to ensure their protection: paper documents are kept in a separate room with a key for the members of the Management Board. Documents received electronically will be stored on a password-protected computer for the personal use of Tamás Nagy, member of the Management Board.

The School Corporation protects access to the electronic HR database against unauthorized access, alteration, disclosure, deletion or destruction by establishing appropriate levels of privilege.

9. Principles of data management and security by the School Co-operative

The School Co-operative's computer systems and other data storage space are located in the server room of the School Co-operative's headquarters at Radnóti Miklós u. 2, 1137 Budapest. When selecting, acquiring and operating its IT equipment, the School Cooperative shall take into account and ensure that the personal data handled is accessible only to authorised persons, its origin is verifiable and authentic. The School Co-operative shall ensure that technical, IT, organisational and internal measures are taken to maintain the security of data processing and an appropriate level of protection against risks related to data processing. The information technology system and network are protected against computer fraud, espionage, sabotage, vandalism, fire and flooding, computer viruses, computer intrusions and attacks leading to denial of service. The School District informs Data Subjects that electronic messages transmitted over the Internet, regardless of protocol (e-mail, web, ftp, etc.), are vulnerable to network threats that could lead to fraudulent activity, contract disputes, or disclosure or modification of information. It takes all reasonable precautions to protect against such threats. It will monitor systems to ensure that any security discrepancies are recorded and evidenced.

The School Corporation will use its best efforts to ensure that the data is not accidentally damaged or destroyed. It shall impose the above commitment on its employees involved in data processing activities.

The Data Controller shall ensure the security of the data in the most up-to-date manner possible. The Data Controller undertakes to ensure that in the event of a data breach occurring despite the measures set out above, the Data Controller will immediately

suspend the service and publishes a statement until the error is rectified, and keeps records of data breaches and actions taken.

10. Rights of the Data Subject in relation to the data processed

- Withdrawal of consent: where the legal basis for processing is consent (e.g. providing the bank account number of a legal representative, notification of an insurance claim), the data subject who has given consent has the right to withdraw consent at any time without giving reasons. Following the withdrawal of consent, the personal data of the person concerned will no longer be processed by the School Cooperative and will be deleted. Withdrawal of consent shall not affect the lawfulness of the processing which preceded it.
- Right of access: at any time, you can contact us to ask whether we process your personal data and, if so, to request further information about: *the purposes of the processing, the legal basis for the processing, the personal data we process, the categories of personal data we process, the recipients or categories of recipients (including data processors we use) to whom or which we have disclosed or will disclose the personal data (in case of transfers to third countries, the safeguards to ensure adequate protection of the data), the legal basis for the transfer, the duration of the storage of the data, the right of the data subject to obtain from the controller the rectification, erasure or restriction of the processing of personal data relating to him or her and to object to the processing of such personal data, the right to lodge a complaint with the NAIH, the source of the data, the circumstances of the possible personal data breach, its effects and the measures taken to remedy it*
- Right to rectification or integration: if you become aware that any of your personal data is incorrect, inaccurate or incomplete, please provide us with the correct or additional data as soon as possible so that we can make the rectification or integration.
- Right to erasure ("right to be forgotten"): you can request the erasure of your personal data. In particular, we may refuse to erase your data if we need or may need it to comply with a legal obligation or to pursue a claim. We may also erase the data if the data are no longer necessary for the original purpose of processing; the processing is unlawful; or we are required to erase the data by European Union or national law.
- Right to restriction of processing: you may request restriction of processing during the processing if (i) you contest the accuracy of the personal data, in which case the restriction will be for a period of time that allows us to verify the accuracy of the personal data; (ii) the processing is unlawful but you oppose the erasure of the data and instead request restriction of their use; (iii) we no longer need the personal data for processing purposes but you require them for the establishment, exercise or defence of legal claims. In the event of restriction, we will only store the data and will not carry out any further processing unless you consent to such further processing or unless such further processing is necessary for the protection of your rights, the rights of a third party or is in the public interest. In case of restriction of processing, we will inform you in advance of its lifting.
- Right to data portability: if we process your personal data electronically (on the basis of consent or a legal contract), you can request that we provide you or another person you designate with the personal data we have provided to us in a commonly known and easily usable electronic format.

Applications must be submitted electronically [via](mailto:ugyfelszolgalat@ydiak.hu) ugyfelszolgalat@ydiak.hu, by post or hand-delivered to the Project Manager. We will respond to your request within a maximum of 25 days.

How to claim:

- *Contacting the data controller*

If you consider that we are not acting lawfully in processing your personal data, please first communicate your comments or requests to us as the data controller so that we can process and handle your comments as quickly and efficiently as possible.

- *Contacting the data protection authority, making a complaint*

In the event of unlawful data processing, you also have the right to turn to the National Authority for Data Protection and Freedom of Information (NAIH) and initiate its proceedings. Contact details of the NAIH:

Website: <http://www.naih.hu/>

address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

postal address: 1530 Budapest, Pf.: 5. e-mail

address: ugyfelszolgalat@naih.hu

- *Right to apply to the courts*

You are also entitled to pursue your claim in court. The courts have jurisdiction to hear the case. You can bring your claim before the court where we are based or before the court in your place of residence or domicile.

The personal data provided in the exercise of your rights as a data subject will be processed for five years on the basis of the legitimate interest of the Data Controller in order to fulfil the request and to ensure the provability of the fulfilment.

11. Handling and reporting data breaches

Prevention and handling of data protection incidents and compliance with the relevant legal requirements are the responsibility of the School Co-operative's Board of Directors. Access and attempted access to IT systems should be logged and analysed on an ongoing basis. If employees of the Cooperative with supervisory authority become aware of a data breach in the course of their duties, they must immediately notify the Cooperative's Board of Directors.

The data breach can be reported to the School Co-operative's central e-mail address, where employees, contractors, data subjects can report the underlying events.

In the event of a data security incident, the School Co-operative's Board of Directors - with the involvement of the data security officer - will immediately investigate the report, identify the incident and decide whether it is a genuine incident or a false alarm. It must be investigated and determined:

- g. the time and place of the incident,
- h. a description of the incident, its circumstances, its effects,
- i. the scope and number of data unauthorisedly accessed during the incident,
- j. the persons involved in the incident,
- k. a description of the measures taken to deal with the incident,
- l. a description of the measures taken to prevent, remedy or reduce the damage.

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. The Supervisory Authority should be notified under the conditions set out in data protection legislation.

The Cooperative shall inform the data subjects of the occurrence of a personal data breach if it poses a high risk to the data rights or freedom of the natural persons concerned. In this case, the information shall also be clear, unambiguous and comprehensible.

The School Cooperative may choose not to inform the data subjects if:

- has taken appropriate technical and organisational measures to make it impossible for unauthorised persons to gain access to the data concerned by the data breach,
- took measures after the data breach occurred to ensure that there is no high risk to the rights and freedoms of data subjects,
- information could only be provided through disproportionate efforts, in which case a measure must be taken to ensure that the persons concerned are effectively informed.

Records of data breaches are kept in electronic form by the designated person. The register contains the scope of personal data, not the specific personal data, except for the name of the Employee, Member.

Records of data protection incidents must be kept, including:

- g. the scope of the personal data concerned,
- h. the scope and number of data subjects affected by the data breach,
- i. the date of the data breach,
- j. the circumstances and effects of the data breach,
- k. the measures taken to remedy the data breach,
- l. other data specified in the legislation providing for the processing.

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

12. Child protection

By providing data and information in relation to the use of the School Co-operative's Services, the Data Subject declares that his or her capacity to act in relation to the provision of the data and information concerned is not limited. If the Data Subject is legally "incapacitated" or "of limited capacity" in relation to the provision of the data and information, including as set out in point 2, and is not entitled to make an independent declaration in this regard under the applicable law, the Data Subject shall obtain the consent of a third person (e.g. legal representative, guardian) named in the law in relation to the provision of the information.

The validity of legal declarations, including the validity of consent given for the processing of minors' data, is regulated by the Civil Code and the Regulation. Pursuant to § 2:13 and § 2:14 (1) of the Civil Code, "a minor who has not attained the age of fourteen years is incapable of acting. The declaration of a minor under the age of 14 is null and void, and his legal representative may act on his behalf." According to § 2:11 and § 2:12 (1) of the Civil Code, "A minor who has attained the age of 14 and is not incapacitated is a minor with limited capacity. Unless otherwise provided for in the Civil Code, the declaration of a minor with limited capacity to act requires the consent of his or her legal representative." In the context of processing of personal data based on consent, the Regulation states that "the processing of personal data in relation to information society services offered directly to children is lawful when the child is at least 16 years of age. In the case of children under the age of 16, the processing of personal data of children is lawful only if and to the extent that consent has been given or authorised by the person having parental authority over the child."

Where the School Co-operative becomes aware that its Services are intended to be used by a person who is clearly "incapacitated", in particular a child under the age of 16 acting without parental or guardian authorisation, it will use all reasonable endeavours to delete any information held by the child and will ensure that such information is not passed on to or used by anyone else.

We ask Data Subjects to tell the School Association immediately if they become aware that a child has provided us with personal data or information about him or herself without the permission of his or her parent or guardian. Parents and guardians are encouraged to teach their children (especially when using the Internet) to handle their personal information safely and responsibly.

Annex No. 3
DOCUMENT
for the Member to attend an aptitude test

A Member may only be subject 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 defined in an employment rule. Prior to the examination, employees shall be informed in detail, inter alia, of the skills and abilities to be assessed and the means and methods of the examination.

If the legislation requires the test to be carried out, workers should be informed of the title of the legislation and the exact place where it is located. The Cooperative fulfils this obligation in this Information Notice.

The scope of the personal data processed: the fact of professional, occupational and medical fitness for the job and the conditions required for this.

The legal basis for data processing: legislation (NM Decree 33/1998 (VI. 24.) on the medical examination and opinion on the suitability for work, occupational and personal hygiene, Act XCIII of 1993 on occupational safety and health) and the legitimate interest of the Cooperative.

Purpose of the processing of personal data: to perform or maintain a task in the context of personal assistance, to fill a job.

Recipients or categories of recipients of personal data: the results of the investigation may be disclosed to the investigated Members or the investigator. The Cooperative may only receive information that the investigated whether or not the person is suitable for the job (the job in question) and what conditions must be met. However, the details of the assessment and its full documentation are not made available to the Cooperative.

Duration of the processing of personal data: 5 years after termination of membership.

Location of personal data: stored on paper in the Member's personal file. It will be kept in a separate room, to which a key will be provided by the members of the Management Board.

The legislation requiring the medical examination is NM Decree No 33/1998 (VI. 24.) on the medical examination and opinion on the medical fitness for work, occupational and personal hygiene.

For the purposes of the Regulation:

- a) *occupational aptitude test:* an assessment of the demands of a particular job and workplace, and of the ability of the person being tested to cope with them;
- b) *aptitude test:* a medical examination to assess a person's fitness before they start work or during their training and retraining;
- c) *personal hygiene fitness assessment:* to establish that the infectious disease of a person working in an epidemiologically priority work area does not endanger the health of others or, in certain cases, that the carrying of a pathogen does not endanger the health of others;
- d) *worker:* a person who carries out an activity in an epidemiologically priority work area in the context of nonorganised work;

Article 3 of the Regulation regulates which skills and abilities are to be assessed during the aptitude test:

3. § (1) Opinion on suitability:

- a) in the case of fitness for the job, for the job designated by the employer,
- b) in the case of occupational aptitude, for the occupation or vocational training concerned; in the case of jobseeker, for vocational training, retraining, occupational groups or occupations which the person concerned can be assigned to,
- c) in the case of personal hygiene competence, for activities in a work area of major epidemiological importance happens.

(2) Medical examinations of professional and occupational aptitude may be preliminary, periodic or exceptional. In the cases specified in § 8, a final examination shall be added to the examination and opinion on fitness for employment. At the request of the teacher, the parent or the pupil, the following shall be carried out on

a pupil applying for admission to a vocational training establishment - a school medical examination for career guidance.

(3) The personal hygiene assessment may be preliminary, periodic or unscheduled.

(4) The purpose of the examination of occupational and professional aptitude is to assess whether the worker, student or trainee is a jobseeker:

a) strain caused by the work and the working environment aa) it does not endanger his or her health, physical or mental integrity, ab) it does not adversely affect his or her state of health,

(ac) not cause damage to the physical, mental or psychological development of his or her offspring;

b) whether his or her possible chronic illness or disability does not pose an accident hazard in the performance of the job or in learning and practising the profession;

c) if working in jobs or professions of major epidemiological importance, whether his/her personal hygiene and health status does not endanger the health of others and whether he/she is employable in the job in question;

d) in what job or occupation and under what conditions he or she can be employed without risk of disability if he or she is temporarily or permanently disabled;

e) remain in your current job or continue your studies in your chosen profession;

f) suffers from a disease that requires regular occupational health surveillance in the course of his or her work;

g) if you are working abroad, whether you are medically fit to carry out the designated professional duties in that country.

(5) The purpose of the personal hygiene fitness assessment is to assess whether the health of the person performing the work - if the activity is carried out - in the work areas of major epidemiological importance does not endanger the health of others, and whether he or she can continue to work in the given work area.

(6) The assessment of occupational, professional and personal hygiene fitness for work and the assessment of employability does not include the determination of the degree of change in working capacity, the degree of disability, or the mental capacity and state of mind.

I, the undersigned Member, certify by my signature that I have read this Prospectus, understand its provisions and take note of them.

Budapest,

Name: _____

Signature: _____

Annex No. 4
the (amended) contract concluded oncontract
Annex ... to the

Factsheet a.....the processing of personal data relating to the conclusion of the contract

The Company, in compliance with its obligations under Regulation (EU) No 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 Regulation (EC) No 95/46/EC (General Data Protection Regulation), and Act CXII of 2011 on the right to information and freedom of information, as data controller, informs the.....(*seller, buyer, tenant, landlord, service recipient, etc.*) to process your data as described below:

a) natural person contracting party

- b) natural person identification data (name, previous name, place and date of birth, mother's name of the natural person who signed the contract), c) your address;
- d) entrepreneur's card number,
- e) the number of the farmer's identity card,
- f) tax identification number, tax number.

The legal basis for processing is based on: compliance with and performance of obligations under the Civil Code, tax legislation and pre-contractual measures (conclusion of contract, in case of contract amendment: performance of contract).

Recipients of personal data: (data may be accessed and processed): employees and data processors performing tasks related to the conclusion and registration of contracts, accounting and tax tasks of the Company.

Duration of storage of personal data:

- 5 years after the termination of the contract.

The Company informs you that the detailed rules on data management and your rights regarding the processing of your personal data are set out in the Privacy and Data Management Policy available at the Customer Service Office at 2 Radnóti Miklós u., 1137 Budapest,

I have read and taken note of the information contained in this leaflet.

Budapest,

.....
Name, signature

Annex No. 5

a.....the (amended) rental contract concluded on

Annex ... to the

Factsheet the processing of personal data relating to the conclusion of the rental contract

The Lessee, in compliance with its obligations under Regulation (EU) No 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 Regulation (EC) No 95/46/EC (General Data Protection Regulation) and Act CXII of 2011 on the right to information self-determination and freedom of information, informs the Lessor that it processes the data described below

a) natural person contracting party

aa) natural person identification data (name, previous name, place and date of birth, mother's name of the natural person who signed the contract), ab) personal identification number in the case of natural persons subject to the Act on the Registration of Personal Data and Address of Citizens, ac)

your address;

b) for the entity contractor

ba) the name, surname and address of the chief executive officer or the company director, and the name, surname and function of the legal representative, bb) the surname, forename and address of the natural person authorised to act on its behalf, d) The parcel number of the rented area.

Legal basis for processing: compliance with and performance of obligations under tax law and pre-contractual measures (conclusion of contract, in case of amendment of contract: performance of contract, termination of contract).

The purpose of data processing: to exercise the rights and fulfil the obligations of the owner under the lease contract, to comply with legal obligations and to settle any disputes with the tenant.

The data subjects are: the data of natural persons who are landlords, users of the service or have a relationship or business relationship with the Company, as defined by law.

Data processed: name, name at birth, place and date of birth, mother's name, address, tax identification number, tax number, business card number, identity card number, address, registered office, telephone number, e-mail address, website address, bank account number, customer number (customer number, order number).

The recipients of the personal data are: the Company's employees who register rental contracts, its employees who perform accounting and tax tasks, and its data processors and the Company's manager.

Duration of storage of personal data: 5 years after termination of the contract.

Place of storage of personal data: paper documents are stored in the room of the Management Board. For security reasons, documents are also stored in scanned form in the server room. They will be accessible to members of the Board and project managers.

The data subject must be informed before the processing is started that the processing is based on the abovementioned grounds and on the intention to enter into a contract or the performance of a contract. The information may be provided in the form of.

in the contract or in the information notice annexed to it or in the privacy notice published on the website.

The Tenant informs the Landlord that the detailed rules on data management and the rights related to the management of personal data are set out in the Privacy and Data Management Policy posted in the Customer Service Office at 2 Radnóti Miklós u., 1137 Budapest,

I have read and taken note of the information contained in this leaflet.

Budapest,

..... Landlord

Annex No. 6.A

Data request form

Processing of personal data based on consent

the name of the person concerned: birth name:	
place and date of birth:	
mother's name:	
your address:	
phone number:	
your e-mail address:	
other personal data: (if the processing requires additional data, e.g. tax number, social security number, etc.)	

INFORMATION:

the name of the controller: is based in:	Y Diák Iskolaszövetkezet 1137 Budapest, Radnóti Miklós utca 2.
name of representative:	Tamás Nagy Member of the Board
Website:	www.ydiak.hu
the purpose of the processing:	Applying for a job, applying for a job
the legal basis for the processing:	the data subject's consent.
the recipients of the personal data: (who can view)	directorate, professional head of area
the duration of the storage of personal data:	5th working day after the end of the selection process.

INFORMATION ABOUT THE RIGHTS OF THE DATA SUBJECT:

The above-mentioned partner hereby expressly consents to the processing of personal data (contact name, e-mail address, telephone number, etc.) of the partner's contacts by Y Diák Iskolaszövetkezet as the data controller. The purpose of the processing is to maintain contact and exchange information related to the service activity during the performance of the contract between the parties. Personal data may be processed for this purpose only. The controller shall make every reasonable effort to safeguard the personal data processed and to prevent unauthorised access and use during the processing.

As a data subject, you have the right to request the controller to access, rectify, erase or restrict the processing of personal data concerning you and to object to the processing of such personal data, as well as the right to data portability.

You have the right to withdraw your consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of your consent prior to its withdrawal.

You have the right to lodge a complaint with the supervisory authority (National Authority for Data Protection and Freedom of Information (NAIH) 1025 Budapest, Szilágyi Erzsébet fasor 22/c.). The provision of data is not a prerequisite for the conclusion of a contract and you are not obliged to provide personal data. Possible consequences of not providing the data: the applicant for the vacancy will not be contacted.

Detailed information on the processing of personal data can be found in the Privacy and Data Protection Policy available on the Company's website.

I have taken note of the above information and information.

I give my consent voluntarily and without any external influence to the processing of my personal data for the purposes indicated above.

Budapest,

Annex No. 6. B.

Consent to the transfer of personal data, joint processing

the name of the person concerned:	
place and date of birth:	
your address:	
your e-mail address:	

INFORMATION:

the name of the controller: is based in:	Y Diák Iskolaszövetkezet 1137 Budapest, Radnóti Miklós utca 2.
name of representative:	Tamás Nagy Member of the Board
Website:	www.ydiak.hu
the purpose of the processing:	enabling wider access to work, providing the highest level of service to the candidate concerned, helping them to find a job and find a job support.
the legal basis for the processing:	consent of the data subject

Y Diák Iskolaszövetkezet will, subject to voluntary consent, transfer the personal data of the Member listed below to the group company **WorkNow Hungary Kft.**, a temporary employment agency (registered office: 6321 Újsolt, Rákóczi utca 9., Tax number: 24105336-2-03, Company registration number: 03-09-131895, Registration decision number: BKM/01/013190-3/2021, represented by Tamás Nagy and Ádám Baksay-Szabó, jointly and severally).

The Cooperative and WorkNow Hungary Kft. act as joint data controllers in the provision of services under a contract between them, the legal basis for which is the GDPR consent pursuant to Article 6(1)(a). In the absence of consent, the transfer of data shall not be possible. The joint controllers shall jointly determine the purposes and means of the processing of personal data as defined in this point and shall jointly take decisions regarding the processing in accordance with the provisions of the Treaty.

The recipients of the personal data: employees of WorkNow Hungary Kft. performing human resources-related tasks of the temporary employment agency.

The scope and purpose of the data processed in the course of joint processing:

Name	identification
place and time of birth	identification
name of position applied for	necessary to identify the application
special data, such as health data	specific data will only be processed if it is necessary for the assessment of the vacancy
experience - name of previous workplace and job title	to be considered for the post, you must have work experience
period spent	
experience - position description	to be considered for the post, you must have work experience
education level	to be considered for the post, you must have education level
foreign language knowledge, foreign language and level of knowledge	to be considered for the post, you must have foreign language skills
other information from the attached CV	to be considered for the post, you must have CV and relevant details for the job
attached cover letter	to be considered for the post, you must have cover letter
Data apply at following 3 for up to 3 years consent to the processing of personal data, if the data subject	necessary for the legal basis for processing in the event of non-election

is not admitted

Common data management mode: a common set of data, access to which is regulated by the levels of access rights established by each controller: only the person who has a task in relation to the data set has access to it.

INFORMATION ON THE RIGHTS OF THE DATA SUBJECT:

The aforementioned Member hereby expressly consents to Y Diák Iskolaszövetkezet, as the data controller, transferring the personal data specified above to WorkNow Hungary Kft. and to jointly and severally process it with it. The purpose of the processing is to ensure access to employment for the widest possible range of people. Personal data will be processed for this purpose only. The data controller shall make every effort to safeguard the personal data processed and to prevent unauthorised access and use during the processing.

As a data subject, you have the right to request the controller to access, rectify, erase or restrict the processing of personal data concerning you and to object to the processing of such personal data, as well as the right to data portability.

You have the right to withdraw your consent at any time, without prejudice to the lawfulness of the processing carried out on the basis of your consent prior to its withdrawal.

You have the right to lodge a complaint with the supervisory authority (National Authority for Data Protection and Freedom of Information (NAIH) 1025 Budapest, Szilágyi Erzsébet fasor 22/c.). The provision of data is not a prerequisite for the conclusion of a contract and you are not obliged to provide personal data. Possible consequences of not providing the data: the applicant for the vacancy will not be contacted.

Detailed information on the processing of personal data can be found in the Privacy and Data Protection Policy available on the Company's website.

I have taken note of the above information and information.

I give my consent voluntarily and without any external influence to the processing of my personal data for the purposes indicated above.

Budapest,

Annex No. 7
PRIVACY POLICY

Dear School Co-operative Member!

*****. (registered office: *****.; company registration number: *****; tax number: *****; acting on behalf of: *****) in connection with the performance of a task **by the service recipient**, we inform you of the following:

The data controller is:

DATA MANAGER:	Y Diák Iskolaszövetkezet
HEADQUARTERS:	1137 Budapest, Radnóti Miklós utca 2.
COMPANY REGISTRATION NUMBER:	01-02-054614
TAX NUMBER:	24146443241
NAME OF REPRESENTATIVE:	Tamás Nagy Member of the Board
CONTACT AVAILABILITIES:	e-mail address: ugyfelszolgalat@ydiak.hu telephone number: + 36 30 608 1088

Subject to the nature of the external service regulated by Act X of 2006 on Cooperatives, the Cooperative shall transmit the following data of the Member to the recipient of the service. Members will be informed individually in each case of any other cases.

The Cooperative and the recipient of the service (hereinafter referred to as the Parties) act as joint data controllers for the services provided under the contract between them, which joint data processing covers in particular the following personal data.

Data subject to joint processing personal data	Purpose of data processing	Legal basis for processing
Name of person concerned, title of position held, date of entry, date of exit, educational qualifications, professional and work experience, curriculum vitae	The personal involvement of data subjects, their work Making available to the Customer	Article 6 GDPR concerned (1)(a), and then the legal relationship once established performance of contract and legal obligation Article 6 GDPR (1) (b) and (c)
E-mail address, telephone number of the person concerned	Contact	Article 6 GDPR concerned (1)(a), and then the legal relationship performance of a contract after its conclusion Article 6(1)(b) GDPR according to

Members will be informed individually in each case of any other cases.

The joint controllers shall jointly determine the purposes and means of the processing of personal data as set out in this Clause and shall jointly take decisions regarding the processing in accordance with the provisions of the Treaty.

The Co-operative and the recipient of the service undertake to co-operate in the performance of the following tasks related to the exercise of the rights of the person concerned as set out in the Regulation:

- a) The data subject may request information about the processing of his or her personal data and access to personal data and information under Article 15 of the GDPR (Articles 12-15 GDPR);
- b) request the rectification of your personal data and the integration of incomplete personal data (Article 16 GDPR);
- c) may request the erasure of your personal data - "right to be forgotten" (Article 17 GDPR) or restriction of processing (Article 18 GDPR);
- d) object to the processing of your personal data (Article 21 GDPR);
- e) under the "right of portability", you have the right to receive your personal data and to transmit those data to another controller (Article 20 GDPR);
- f) has the right to lodge a complaint with the supervisory authority.

Applications must be submitted electronically [via](mailto:ugyfelszolgalat@ydiak.hu) ugyfelszolgalat@ydiak.hu, by post or hand-delivered to the Project Manager. We will respond to your request within a maximum of 25 days.

The data subject may exercise his or her rights under the GDPR in relation to and against both controllers. Given that the personal data as defined above are held by both Parties, the Parties should cooperate fully in the exercise of the rights of the data subject, and unless otherwise agreed, the controller to which the request is addressed should respond to the data subject.

Where the processing involves a high risk to the rights and freedoms of natural persons (e.g. profiling, processing of a large number of sensitive data), the Parties shall carry out an impact assessment prior to the processing.

The Parties shall carry out the processing solely for the performance of their tasks under the contract between them and shall not transfer personal data relating to the data subjects to third parties.

Duration of storage of data: the recipient of the service will process the personal data only for the shortest and most necessary period of time, the duration of which will be communicated to the Cooperative on a case-by-case basis, which will inform the Member thereof.

The detailed information on the exercise of rights of survivorship and the means of enforcing claims is set out in Annex 7 to the Rules.

Under the agreement with the Cooperative, the recipient of the service guarantees, in particular in terms of expertise, reliability and resources, that it will implement technical and organisational measures to ensure compliance with the requirements of the Regulation, including the security of data processing. In the course of its activities, the recipient of the service shall ensure that persons authorised to have access to the personal data concerned are bound by an obligation of confidentiality with regard to the personal data they have access to, unless they are otherwise subject to an appropriate legal obligation of confidentiality. The recipient of the service must guarantee that it has adequate hardware and software facilities and undertakes to implement technical and organisational measures to ensure the lawfulness of the processing and the protection of the rights of the data subjects.

The Cooperative is entitled to verify the existence and implementation of the contractual data security commitments with the recipient of the service.

The Cooperative is obliged to inform the natural persons concerned about the processing and, if required by law, to obtain their consent.

The recipient of the service must ensure that it implements appropriate technical and organisational measures to guarantee a level of data security appropriate to the level of risk, taking into account the nature, context and purposes of the processing and the rights of natural persons. It shall take measures to ensure that natural persons acting under its authority who have access to personal data are only allowed to process those data in accordance with the instructions of the Cooperative, unless they are required to do otherwise by Union or Member State law. It shall ensure that access to the data stored is restricted, either through an internal system or by direct access, to authorised persons and only in relation to the purposes for which the data are processed. Ensure the necessary regular maintenance and development of the tools used. It shall place the data storage device in a secure enclosure with appropriate physical protection and shall ensure that it is physically protected. It shall employ persons with appropriate knowledge and experience to carry out the tasks specified in the contract. It shall also ensure that training of the persons it uses with regard to the provisions of the data protection legislation to be complied with, the obligations contained in this contract and the purposes and methods of data collection.

The Cooperative and the recipient of the service shall, in the course of the contractual cooperation, process personal data only and exclusively to the extent necessary for the performance of the contract, concerning the employees, contractors or assistants of the other party. Such data shall be treated confidentially and shall be made accessible only to those of their employees, collaborators or assistants to whom it is justified and necessary. They shall not otherwise transfer, disclose or make available such data to third parties. They shall take all necessary steps, including obtaining appropriate consents, which may be necessary for the lawful processing of personal data.

How to claim:

- *Contacting the data controller*

If you believe that we are not acting lawfully in processing your personal data, please first communicate your comments or requests to us as the data controller so that we can process and handle your comments as quickly and efficiently as possible.

- *Contacting the data protection authority, making a complaint*

In case of unlawful data processing, you also have the right to contact the National Authority for Data Protection and Freedom of Information (NAIH) and initiate its proceedings. Contact details of the NAIH:

Website: <http://www.naih.hu/> address: 1125
Budapest, Szilágyi Erzsébet fasor 22/c postal
address: 1530 Budapest, Pf.: 5. e-mail address:
ugyfelszolgalat@naih.hu

- *Right to apply to the courts*

You are also entitled to pursue your claim in court. The courts have jurisdiction to hear your case. You can bring your claim before the court where we are based or before the court in your place of residence or domicile.

The personal data provided in the exercise of your rights as a data subject will be processed for five years on the basis of the legitimate interest of the Data Controller in order to fulfil the request and to ensure the provability of the fulfilment.

Y Diák Iskolaszövetkezet
Tamás Nagy
Member of the
Board

Annex No.8
Information on the use of electronic surveillance

DATA MANAGER:	Y Diák Iskolaszövetkezet
HEADQUARTERS:	1137 Budapest, Radnóti Miklós utca 2.
COMPANY REGISTRATION NUMBER:	01-02-054614
TAX NUMBER:	24146443241
NAME OF REPRESENTATIVE:	Tamás Nagy Member of the Board
CONTACT AVAILABILITIES:	e-mail address: ugyfelszolgalat@ydiak.hu telephone number: + 36 30 608 1088

Please note that our Company operates an electronic surveillance and recording system (camera system) in the client area in the associated units (corridor, entrance door, server room). When you enter the monitored area (room) indicated by this sign, the electronic surveillance system will record your image and your actions.

1./ **The legal basis for CCTV surveillance is the** legitimate interest of our Company, both for data subjects who enter the monitored area voluntarily and of their own free will and for employees (Article 6(f) of the Regulation).

2./ **The purpose of the recording is** to protect human life and limb, to prevent and detect infringements in order to protect persons and property, to prove infringements, to document the circumstances of any accidents occurring in the customer premises and to protect the private areas of the public for the persons concerned, necessary for the performance of the tasks of the service provider. Our Company uses electronic surveillance because, based on the preliminary studies carried out, it is the most effective means of achieving the above objectives. Having taken into account all the circumstances of the data management, our Company has concluded that the operation of the system is lawful, taking into account the short storage time of the recordings, the careful data security measures, the safeguards to ensure the exercise of the rights of the data subject, in the interest of the security of the property and the safety of you and the persons on the property.

3./ **The place of storage of the recordings (personal data) recorded by the electronic surveillance system is** the registered office of our Company, the storage period of the recordings is 8 working days from the date of their creation. In determining this duration, our Company has taken into account the principles of data management, such as data economy and limited storage. After the storage period, the recording is automatically deleted.

The recordings are not backed up separately. Digital recordings are not accessible from an external network.

4./ **Scope of the data processed:** the surveillance system **records** the image of the person entering the area monitored by the cameras and, together with this, the action (**moving image**) that is visible on the recording. The camera surveillance system **does not record sound**. The cameras operate continuously.

5./ **Categories of recipients of personal data recorded by camera:** recipients of personal data recorded by camera: members of the Board of Directors. The Cooperative does not use an external data processor to operate the camera system and manages the recordings internally. We keep records of the views and the person who carries them out, the reason for and the time of access to the data, and the content of any data transfers, in accordance with our internal rules.

Cases of use of the recording:

- to investigate security incidents involving personal data,
- to prepare a complaint in the event of suspicion of a criminal offence or irregularity,
- to respond to written requests from public authorities,
- in disciplinary proceedings to establish the facts or investigate an accident at work
- the data subject, and whose rights or legitimate interests are affected by the taking of the photograph, in order to ensure the exercise of his or her rights.

6./ **Exercise of your rights:** If your rights or legitimate interests are affected by the recording, you may request our Company within three days of the recording to.

- provide information about what is shown about you in the recording (right of access),
- block the recording of your data (right to restriction of processing),
- object to the processing by post or e-mail to the administrator if you consider that your personal rights prevail over the interests of our Company,
- we will delete the recording we made of you,
- have access to the recordings made about you (right of access).

The application form can be requested electronically via info@fhgasztro.hu and delivered by post or in person to the HR Director. Our Company will respond to your request within a maximum of 25 days. The right to rectification is conceptually excluded in the present case, given that the records cannot be modified. The right to rectification may apply to the personal data provided in the exercise of the right as a data subject. The Data Controller will also respond to your request in this regard within 25 days. The records will only be transmitted to third parties by our company on the basis of a legal obligation (e.g. a request from a public authority).

7./ Enforcement options:

If, in your opinion, our data processing does not comply with the legal requirements or has violated your rights, you may bring a civil action before the court (Art.23 of the Information Act).

you can also contact the National Authority for Data Protection and Freedom of Information (1125 Budapest, Szilágyi Erzsébet fasor 22/C. Phone: +3613911400 Fax: +3613911410, email: ugyfelszolgalat@naih.hu) (Infotv. § 22)

The personal data provided in the exercise of your rights as a data subject will be processed for five years on the basis of the legitimate interest of the Data Controller in order to fulfil the request and to ensure the provability of the fulfilment.

INFORMATION ON THE INSTALLATION OF CAMERAS

	CAMERA LOCATION, ANGLE OF VIEW	ENDORSED AREA, EQUIPMENT	METHOD OF OBSERVATION	PURPOSE OF MONITORING
1.	entrance	main entrance and immediate surroundings	recorded	asset protection, monitoring of movements in the branch, detection and prevention of illegal activities, the safety of individuals
2.	customer reception area	client room for a reception area	recorded	asset protection, monitoring of movements in the branch, detection and prevention of illegal activities, the safety of individuals
3.	server room	Room	recorded	asset protection, surveillance of movements in a branch, offences detection, prevention

The location and angle of view of each camera (the area they monitor) is shown in the plan attached to the information sheet.

Y Diák Iskolaszövetkezet represents:
Tamás Nagy Member of the Board

Annex No.9

Data Protection Interest Assessment Test

In examining the legal basis for data processing, the provisions of Article 6 (1) (a) to (f) of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: the Regulation) and the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: the Infotv.) shall apply. If the legal basis is Article 6(1)(f) of the Regulation: the processing will be lawful if and insofar as the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data. In order to assess the lawfulness of the processing, an interest test should be carried out, in which the necessity of the purposes of the processing and the proportionality of the restriction of the rights and freedoms of the data subjects should be assessed and duly justified. In the balancing of interests test, the Company shall:

- identifies his or her legitimate interest in the processing of the personal data subject to the balancing of interests test, and
- before starting the envisaged processing, considers whether the processing of personal data is strictly necessary for the purposes for which it is intended: whether alternative means are available which allow the envisaged purposes to be achieved without processing personal data; and
- establishes the interests of the Data Subjects in relation to the personal data subject to the balancing of interests test, the fundamental rights concerned as a counterweight to the interests of the Data Subject, and
- weigh the interests of the Data Controller against the interests and fundamental rights of the Data Subjects and, on this basis, determine whether the personal data can be processed.

The interests and fundamental rights of the data subject:

Under the provisions of the Fundamental Law, everyone has the right to the protection of their personal data. The explicit purpose of the Infotv. is to set out basic rules for data processing in order to ensure that the privacy of natural persons is respected by data controllers. The Infotv. also lays down the principle that personal data may only be processed for specific purposes, for the exercise of a right and for the performance of an obligation. At all stages of processing, the purpose of the processing must be fulfilled and the collection and processing of data must be fair and lawful. Only personal data that is necessary for the purpose of the processing and is adequate for the purpose shall be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose. The unauthorised processing of personal data or the processing of personal data for purposes other than those for which they are intended, or the failure to take measures to ensure data security, is also punishable under the Criminal Code.

The Data Subject, as a natural person, has a legitimate interest in the protection of:

- exercise their right to information self-determination,
- be able to decide how others process their own personal data,
- the privacy of data controllers is respected,
- the legal provisions promoting the exercise of the right to information self-determination and ensuring the protection of personal data and, through this, privacy are enforced

The safeguards, guarantees:

In addition to the mandatory information provided at the time of data collection, the Data Subject may at any time request information on the material circumstances of the processing, which the Company shall provide in writing as soon as possible, but not later than 25 days from the receipt of the request. The Data Protection and Security Policy is available on the Company's website and contains a detailed description of the purposes, legal basis, duration and other characteristics of the processing in accordance with the law. The Data Subject may request information on the processing of his/her personal data and may request the rectification or, except for processing required by law, the erasure of his/her personal data by the means indicated when the data were collected or by contacting the Data Controller at the contact details indicated:

Subject of the interest test In relation to the electronic surveillance system operated at the Company's headquarters, weighing the interests of the Company and the data subjects (persons voluntarily entering the monitored area and employees)

Purpose of the envisaged processing	<ul style="list-style-type: none"> • the protection of the property on which the Company's premises are located, • ensuring the safety of persons and property on the property, • the protection of property on the property, • preventing offences and crimes, • assist the competent authority in the event of an offence or crime.
Legal basis for the envisaged processing (GDPR-matching)	<p>Pursuant to Article 6(1)(f) of the GDPR, processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.</p> <p>The camera system does not fall under the scope of Act CXXXIII of 2005 on the Rules of Personal and Property Protection and Private Investigation.</p>
By processing the data scope of personal data concerned	<ul style="list-style-type: none"> • image and behaviour of employees • the image and behaviour of contractual (business) partners • the image and behaviour of visitors and guests
Source of personal data	provided by the data subjects (by entering or staying on the property)
Duration of processing	<ul style="list-style-type: none"> • 8 working days
Recipients • the members of the Board of Directors of the data	
The system used by the Company guarantees given before installation	<ul style="list-style-type: none"> • prior regulation of rights, entitlements and obligations (who, when and how can view the recordings, how long they are kept, how data subjects can exercise their rights, etc.) respect the principle of gradualism, i.e. always apply the solution with the least damage to interests and rights • requiring the controller to follow a procedure following internal camera rules • a camera installation plan which takes into account the basic requirements for camera placement (no cameras in canteens, changing rooms, toilets, no hidden cameras, etc.) and takes maximum account of privacy. • conducting an interest assessment test

FINDINGS

Views of stakeholders consulted during the balancing test No objections to the camera system were received by the test provider during the test. The camera is also considered necessary by the employees to prevent possible theft.

The legitimate interest of the Company	Protect the Company's premises, buildings, property, and the safety and security of its employees, business partners and visitors, and its property. Reason: the need to install a camera system arose because <ul style="list-style-type: none">• a history of petty theft• has a deterrent effect
Necessity of the processing	The Company is of the opinion that the camera system is the most effective tool to prevent offences and crimes and, in the event of such an incident, to detect the incident and find the perpetrator and initiate the prosecution. The use of an electronic surveillance system designed to influence the behaviour of employees in the workplace may also be considered unlawful. It also follows from the principle that it is not possible to install a camera which monitors only a worker and his activities. Exceptions to this rule are workplaces where the life and physical safety of the worker may be at risk, so that cameras may be used exceptionally in assembly halls, smelters, industrial plants or other installations where there is a risk of danger. It follows from the practice of the Constitutional Court that a camera may only be operated for the purpose of protecting the life and limb of workers if the danger is real and immediate, i.e. the potential danger cannot be a constitutionally acceptable purpose for data processing. However, the employer must prove this in the balancing of interests test. The same requirement applies where the employer operates its camera system for the purpose of protecting property.
Violation of the rights and freedoms of data subjects	In the course of taking and storing the recordings, and in the course of viewing and otherwise using them, the right of the data subjects to have their images taken may be infringed
Balance of Fundamental Law	<ul style="list-style-type: none">• the protection of the Company's property is a fundamental right under the interests• the rights and freedoms of the data subjects are not violated due to the limited storage time of the recordings made and the strict regulation of access rights• the system you want to install will also benefit stakeholders by helping to protect the personal safety and property of employees, business partners and visitors• the Company undertakes to include in its data protection policy, or in its specific policy for the camera system only, safeguards which guarantee the protection of the rights of the data subjects• the Company undertakes to prepare and make available to the data subjects, as carefully as possible, the information to employees and visitors on the CCTV system in order to protect the rights and freedoms of the data subjects

THE RESULT OF THE BALANCING OF INTERESTS TEST

Basis for The Data Controller assesses that the legal basis for the processing of the camera system is **processin** compatible with the legitimate interest referred to in Article 6(1)(f) of the GDPR and that the **g** use of the camera system does not harm the interests or fundamental rights and freedoms of the data subjects in such a way that the legitimate interests of the Company are overridden. The processing is necessary (otherwise the purposes of the protection of property cannot be fully ensured) and proportionate (the purpose is proportionate to the harm to the personal rights of the data subjects - the right to be photographed) according to the Controller's view. The legitimate interest of the Controller is therefore superior to the personal rights of the data subjects and the Controller guarantees the safeguarding of the data subjects' rights.

Before deciding to implement the electronic surveillance system, the Company considered **all alternative solutions that would achieve the same objective, e.g.** protecting the property with a fence, employing a security service, having a concierge, adequate lighting, installing security locks, burglar-proof windows, etc. However, these were not found to be as suitable for preventing burglary and theft or other crimes against property.

The Company has decided to process personal data relating to the camera system because it complies with Article 6(1)(f) GDPR as regards its legal basis.

Annex No. 10
Request to exercise the rights of the data subject

I, the
undersigned, name of
the person concerned:
place and date of
birth: your address:
contact details:

I wish to exercise my rights in relation to the electronic monitoring system operated by the Data Controller¹ :

- request information;
- request blocking (restriction of processing);
- request insight;
- request cancellation;
- protest

Exact location and time of recording:

Please submit the result of the assessment of the application by the following means (email, post, on-site visit):

.....

With regard to my personal data, please inform me of the following:

.....
.....

I request the blocking of my personal data provided above:

.....
.....
.....

Please visit above provided on personal my personal data to access to my personal data

to:

.....

..... I request the deletion of
my personal data provided above:

¹ Underline where appropriate.

.....
.....

I object to the processing of my personal data and the reasons for this:

.....
.....

I acknowledge that the personal data I have just provided will be processed by the Data Controller for a period of 5 years on the basis of its legitimate interest in order to fulfil the request or to provide evidence of fulfilment.

Celt,

signature

Annex No. 11
Protocol for viewing camera images

1. Data of the recording subject to data insight:

1.1 Recording location (where the camera is operating):

1.2 Scope/time duration of the recording viewed (expressed in date-hour-minute format) and the start or end time of the real-time recording:

2. Names of persons involved in accessing the data (basis of their access rights):

3. Place and time of data access:

4. Rationale and purpose of data access:

5. On the basis of the insight, a proposal for further processing (underline as appropriate):

- use the recording for the purpose of further (civil/criminal) proceedings

- transferring the relevant record to the competent authority at the request of the competent authority - destruction of the record in accordance with the law, termination of data processing

- other:

6. Other relevant events detected during and in relation to the circumstances of the data access Cf.:

.....

.....
Name of data controller

Annex No. 12

Register of persons with right of access

Name of the right of access	Working title	Eligibility date of surrender	Eligibility date of termination

Annex No. 13
Data breach notification list

I. Individuals affected by the data breach: (in the event of data loss, with a path to access data from the redundant backup location)

Name and contact details of the person concerned:

1.
2.
3.
4.

II. Details of the organisation or scope of organisational data/information affected by the data breach:
(in case of data loss, with a path to access the data from the redundant backup location)

Name, address, tax identification number and contact details of the organisations concerned:

1.
2.
3.
4.

The notification regime: the first priority is to notify the individuals concerned.

Celtic:

.....
signature Data Protection Officer

Annex No. 14

DATA PROTECTION INCIDENT-NYPOTENT

The Company is subject to the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information No.

§ (1a) of the GDPR, shall keep records of data protection incidents for the purpose of monitoring the measures taken in relation to the data protection incident and informing the data subject.

The Company shall keep a record of all data protection incidents, and shall keep a record of the incident record sheets filed.

...../20.../AVINC

DATA BREACH RECORD SHEET

The date of the data breach:

The department involved in the data breach:

Relevant circumstances in which the data breach was detected:

Scope of personal data affected by the data breach: the scope

and number of data subjects affected by the data breach

Description of the circumstances of the data breach: the impact of the data breach:

Description of the measures taken to respond to the data breach:

Place, date

.....

data protection officer

Annex No. 15
DATA DESTRUCTION PROTOCOL

...../20...

To be completed by the employee responsible for data destruction!

Name of the employee responsible for
data destruction: mother's name:
place and date of birth:
trunk number:

The destruction was authorised:

The members of the three-member committee present at the destruction
are: 1.

2.

3.

Place and time of data destruction (date-hour-minute):

Subject of destruction:

The method of data destruction

shredding machine burning

crushing

grinding

grinding

g

other:

.....
signature of the employee responsible for data
destruction

