# GENERAL TERMS AND CONDITIONS

Y Generáció Iskolaszövetkezet (registered seat: 1137 Budapest, Radnóti Miklós utca 2., company registration no.: 01-02-054614, tax ID: 24146443-2-41), as service provider, in order to provide its services - as set down in the specific service framework agreement - on a high level to the customer using them, hereby defines the rights and obligations of the service provider and the customer in these General Terms and Conditions as follows, in order to meet the requirements of the GDPR.

## 1. Definitions

| | |
|---|---|
| GDPR | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) |
| Information Act | Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information |
| School cooperative | A cooperative defined in chapter II point 2 of the Cooperatives Act |
| School cooperative member | A person or organisation who is in a membership relationship with Service Provider, providing their personal contribution, employed by Service Provider to help fulfil the contract (**Member**) |
| Joint controllers | Controllers that jointly specify the purposes and means of processing (GDPR Regulation art.26) |
| Customer | Natural person or legal entity using the service provided by Service Provider |
| Labour Code | Act I. of 2012 on the Labour Code (**LC**.) |
| Civil Code | Act V. of 2013 on the Civil Code (**CC**.) |
| Service contract | A specific contract concluded between Service Provider and Customer, which contains the detailed conditions of the relationship between the Parties arising out of the service contract, especially the rights and obligations of the Parties, the service fee, the duration of the contract and contact details. |
| Service Provider | Y Generáció Iskolaszövetkezet |
| Cooperatives Act | Act X. of 2006 on cooperatives (**Cooperatives Act**) |
| Performance group | A sufficient number of school cooperative members hired by Service Provider who provide their personal contributions to help fulfil the service contract |
| Trade secret | As defined in Act LIV. of 2018 on the protection of trade secrets: trade secret means a fact, information, other data and an assembly of the foregoing, connected to an economic activity, which is secret in the sense that it is not, as a body or as the assembly of its components, generally known or readily accessible to persons dealing with the affected economic activity and therefore it has pecuniary value, and which is subject to steps made with the care that is generally expected under the given circumstances,<br>by the person lawfully in control of the information, to keep it secret. |

## 2. Scope of the Agreement

2.1. Service Provider and members of the school cooperative as per Chapter II. point 2 of the **Cooperatives Act** provide their personal contributions within the framework of a service provided by the school cooperative for third parties. Service Provider provides its services via the Members employed by it who make available their personal contributions and work capacity to the Customer in order to provide the service set down in the specific Service contract.

2.2. **Customer** orders the activities and tasks set down in detail in the framework service contract to be performed in a professional manner, which**Service Provider** undertakes to perform in line with the specific Service contract.

## 3. Data protection

3.1. Parties state that during and after the duration of the Service contract they shall mutually follow the effective Hungarian and EU data protection regulations, including, but not limited to, the provisions of the Information Act and the GDPR.

3.2. Parties state that for the members (data subjects) entrusted by the Service Provider to carry out the tasks related to the Contract, the Service Provider and the Customer are considered "joint controllers" based on the definition found in Article 26 of the GDPR. Article 26 of the GDPR on Joint controllers stipulates that in the case of activities involving joint processing the Joint controllers shall agree on data protection issues in a transparent manner by way of an agreement between them.

3.3. Controllers process those personal data of members relevant for employment at Customer based on GDPR Art.6 (1) b) - performance of a contract -, GDPR Art.6 (1) f) - legitimate interest of Controller -, and GDPR Art.6 (1) a) - consent given by data subjects.

3.4. Parties shall ensure that during their activities, the employees authorized to access the personal data of the data subject, if there is no legal confidentiality obligation, commit themselves to confidentiality regarding the personal data that they may come to know.

3.5. The Parties are aware that they may only process the personal data of the data subjects if the data subjects gives his/her freely given, specific, informed and unambiguous consent with an affirmative act (such as an oral or written statement, including statements made electronically) to the processing of data relating to the natural person. This consent shall cover all processing activities related to the same objective or objectives. The consent shall also contain that the data subject accepts that the Customer shall, for the purpose of exercising its employment rights and performing its employment obligations, transfer the personal data of the data subject to third parties (for example, processors), to the extent required.

3.6. This means that the Customer may only accept the performance of such members of the Service Provider who give their consent to the processing of their personal data to the Customer as the controller for purposes related to the performance of this Contract. The Service Provider acknowledges this, and undertakes to inform its members used for performing the tasks related to this Contract of this requirement in advance.

3.7. The Parties warrant that they shall implement all the technical and organisational measures necessary to fulfil the requirements of the GDPR, including measures related to the security of processing. The Parties shall use the necessary expertise, and implement reliable solutions with sufficient resources.

3.8. Notwithstanding their general liability towards the data subject, the Parties agree that in the context of their legal relationship, they shall mutually exclude liability for all infringements that the other (infringing) Party commits against the data subject or towards an authority. This means that the infringing Party shall be liable for the full amount of the penalties (e.g. damages, fines) to be paid to the data subject or the data protection authority, irrespective of the legal basis of the penalties. In cases where, based on the principle of joint liability, the innocent Party is obliged to pay any amount to the data subject or the data protection (or other) authority, irrespective of the legal basis of this payment, the infringing Party shall pay (reimburse) the full amount paid by the other Party within 8 days to the innocent Party. Failing this, the innocent Party is entitled to send a written notification to the other Party terminating their temporary agency work contract with immediate effect.

## 4. The rights and obligations of the Customer in the processing of the personal data of the Members

4.1. The Customer shall ensure that during its activities, the employees authorized to access the personal data of the data subject, if there is no legal confidentiality obligation, commit themselves to confidentiality regarding the personal data that they may come to know.

4.2. Taking into account the characteristics, circumstances and objectives of the data processing, as well as the rights of natural persons, the Customer shall implement all the necessary technical and organisational measures to provide a level of data security commensurate with the level of risk. The Customer shall implement the necessary measures to ensure that the natural persons under its control, who have access to the personal data do so and process the data only in ways in line with the instructions of the Service Provider, except where EU or Member State law requires that they deviate from said instructions. The Customer shall ensure that the stored data can only be accessed via internal systems or direct access by the authorized employees, and only in connection with objectives related to the objective of data processing. The Customer shall ensure that the used tools/assets are regularly maintained and updated. The device containing the data shall be kept in a locked room furnished with adequate physical protection, and the Customer shall also ensure its physical security. The Customer shall employ persons with the appropriate competence and expertise to carry out the activities set out in this Contract. Furthermore, the Customer shall ensure that these persons are adequately trained regarding the relevant legal provisions, the responsibilities stemming from the Service Contract and the objectives and methods of data collection.

4.3. Customer shall only employ a processor if he meets the conditions set out in the GDPR and the Information Act. To use a processor, the Customer needs to ask the Service Provider to make out a private document representing conclusive evidence, in which it consents to the use of further processors (subcontractors). The consent of the Service Provider is not required with persons being the legal representatives of the Customer.

4.4. If the Customer uses processors (subcontractors) to perform specific services on behalf of the Service Provider, the Customer shall enter into a written contract with these data processors, and impose the data protection obligations contained in the Service Contract on the other processors. The other processors shall offer appropriate guarantees regarding the implementation of the required technical and organisational measures, and ensure that it processes data only in line with the requirements of the GDPR.

4.5. In case the other processors do not meet their data protection obligations, the Customer shall be fully liable to the Service Provider for the performance of the obligations of the other processors.

4.6. In matters regarding data protection and processing not regulated in these GTC and the Service Contract, Service Provider's Data Protection regulation shall apply. Customer states that Service Provider has made the Data Protection regulation available to him, he has become acquainted with the content thereof and by affixing his signature to the Service Contract, he accepts its provisions.

## 5. JOINT PROCESSING AGREEMENT

5.1. **Definition of terms**

Terms and expressions in this Joint Processing Agreement starting with capitals shall be defined below (regardless whether they are used in singular or plural later on in the text). Terms and expressions starting with capitals not defined in this Joint Processing Agreement are defined in the GDPR (especially in article 4 thereof (Definitions), e.g. Personal data, Supervisory Authority) or in the related Contracts.

- **"Contract**" may mean any of the following, or the combination of these
    - A stand-alone contract;
    - A framework contract, general terms or main service agreement; or
    - An implementation contract, special conditions, furthermore, it may mean a sub-agreement entered into on the basis of a framework contract, general terms or main service agreement;
- **"Data protection regulations**" means the GDPR or any legal regulations of the EU or one of its member states related to the protection of personal data that are obligatory for the Parties to follow;
- **"EEA**" means the European Economic Area, which comprises the member states of the EU as well as Iceland, Liechtenstein and Norway;

- **"GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- **"Personal Data Involved in Co-operation"** means the Personal Data processed in connection with the Services;
- **"Processing**" means any operation or set of operations which is performed on Personal Data Involved in Co-operation or on sets of personal data created from these, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; furthermore, any other activity considered to be Processing based on Data protection Regulations (especially, but not limited to, the act on informational self-determination and freedom of information);
- **"Services**" means all services performed by Parties for each other, in line with the individual Service Contracts concluded between them;
- **"Service Provider**" means the Service Provider or any person acting with his authorization who has access to the Personal Data Involved in Co-operation in connection with the Services;
- **"Data Subject"** means any identified or identifiable natural persons with related Personal Data as per the definition of the GDPR.
- **"Responsibility Matrix"** means a table forming part of this Joint Processing Agreement showing how the tasks related to this agreement are to be divided between the Parties, with an indication of which Party is responsible for which tasks.

**5.2. General provisions**

Parties have defined the Services together. As part of this, they have defined the purposes and means of Processing related to the Services. As per Article 26 of the GDPR, the Parties count as Joint Controllers in every case involving processing. Parties shall at all times keep the Data Protection Regulations as well as any further applicable laws on Customer Confidentiality.

The subject and purpose of processing on the part of the Parties:

On the part of Y GENERÁCIÓ: Establishing and maintaining membership status.

Y GENERÁCIÓ as Service Provider is a school cooperative as per Chapter II. point 2 of Act X. of 2006 ("Cooperatives Act"), whose members (henceforth: Members) provide their personal contributions within the framework of a service provided by the school cooperative for third parties. The service in question is making available the personal contributions, work capacity of the Members for Customer. Y GENERÁCIÓ provides its services via the Members employed by it.

On behalf of the Customer: Processing the personal data, carried out for employment purposes, of members sent by Y GENERÁCIÓ with the aim of working.

Categories of data subjects:

Those members of Y GENERÁCIÓ who are working at Customer

**Duration of processing:**

- Y GENERÁCIÓ: 5 years following the termination of membership status,
- Customer: 5 years following the end of working; should a member not be employed by Customer, then 1 year from the time member's data were transmitted.

**Scope of the processed personal data:** member's name, mother's name, place and date of birth, contact information, school qualifications, professional and work experience.

Parties do not process special personal data and personal data regarding criminal records.

Parties state that in order to facilitate the provision of services, they may share further data with each other based on a member's voluntary consent.

Parties state that the sharing of personal data shall only be performed with the utmost security measures in place, ensuring the proper protection of the data shared.

**Location of processing activity**: Parties' registered seat.

**Legal basis of personal data processing:** Controllers process those personal data of members relevant for employment at Customer based on GDPR Art.6 (1) b) - performance of a contract -, GDPR Art.6 (1) f) - legitimate interest of Controller -, and GDPR Art.6 (1) a) - consent given by the data subjects.

**Jurisdiction and applicable law:** Processors have their registered seats in Hungary, they perform the processing in Hungary, thus - applying opinion 0836-02/10/HU WP 179 8/2010 on applicable law by the Working Party 29 - Hungarian law shall govern the entire processing and all related procedures.

### 5.3. The effective date of the Joint Processing Agreement

This Joint Processing Agreement shall enter into effect when duly signed by the last Party (henceforth: "the effective date of the Joint Processing Agreement").
This Joint Processing Agreement shall remain in effect without time limitation, irrespectively of the termination of the Contracts and the ceasing of the Services.

### 5.4. Responsibility Matrix

Both Parties undertake to use the Personal Data Involved in Co-operation only for the purpose of the Services. In line with the Data Protection Regulations, Parties shall define their respective scopes of responsibilities regarding compliance with Data Protection Regulations in a transparent manner. For this end, Parties undertake to comply with the contents of the Responsibility Matrix. This Responsibility Matrix reflects Parties' tasks regarding Processing activities. The contents of the Responsibility Matrix shall be further defined by the Parties in the Framework Service Contract.

### 5.5. Authorized persons

Neither Party may communicate or reveal Personal Data Involved in Co-operation to any third parties without the prior written permission of the other Party. Parties may only communicate Personal Data Involved in Co-operation to their employees / managers to the extent needed for them to be able to perform the Services (i.e. as much information as these people must really know to perform their tasks), to comply with Data Protection Regulations or with the prior written consent of the other Party.

All Parties shall undertake any necessary measures to ensure the trustworthiness of their employees with access to the Personal Data Involved in Co-operation; they shall, moreover, ensure that their employees keep their obligations arising from this Agreement.

All Parties shall ensure and prove that those employees with access to the Personal Data Involved in Co-operation have signed a confidentiality agreement (this may happen by way of the employees' work contract containing a non-disclosure clause), or that they are bound by suitable confidentiality obligations stipulated by law.

### 5.6. Security

All Parties shall implement suitable technological and organisational measures as per article 32 of the GDPR in order to ensure the security, confidentiality, integrity and availability of the Personal Data Involved in Co-operation. When implementing the above, each Party shall protect the Personal Data Involved in Co-operation against personal data breaches ("Personal Data Breach"), considering the current state of science and technology, the costs of implementation as well as the type, scope, circumstances and purposes of Processing, and also the risk to natural persons' rights and liberties, which may vary in terms of probability and severity.

### 5.7. Personal Data Breach

All Parties shall inform the other Party of any Personal Data Breach without undue delay, within no more than 24 hours of discovering it. When informing the other Party, they shall supply all reasonable details, such as the type of the Personal Data Breach, including the number and categories of Data Subjects and of the Personal Data Involved in Co-operation.
Under no circumstances may Parties disclose the Personal Data Breach to a third party without the prior written consent of the other Party. An exception is when the disclosing of the Personal Data Breach to third parties is stipulated by law or a Supervisory Authority.

In the case of a Personal Data Breach, Parties shall work together in good faith to set up a plan of action in order to mitigate the impact of the breach as well as to end it without any undue delay. Parties shall make arrangements concerning the conditions of executing their plan of action.

**5.8. Data transfers**

Neither Party may transmit the Personal Data Involved in Co-operation outside the area of the EEA without the prior written consent of the other Party.

**5.9. Hiring subcontractors**

In cases where Parties jointly or separately hire Subcontractors to perform specific Processing activities, the Parties shall ensure that they place sufficiently binding data protection obligations on their Subcontractor(s) by way of the contract entered into with them, especially that (i) the Subcontractors shall provide sufficient guarantees for performing technological and organisational measures in a manner that is in line with the provisions of Data Protection Regulations, and (ii) that it should enable the Party considered a Controller to receive an executed audit report regarding the Subcontractors in question.

**5.10. Co-operation and the rights of the Data Subjects**

In order to ensure that Processing is carried out in a suitable manner, both Parties undertake to reply with due care in writing to any reasonable queries by the other Party. They shall have five (5) working days available to do so. As per the Data Protection Regulations, Data subjects may exercise certain rights, especially, but not limited to, those in chapter 3 of the GDPR („**The rights of data subjects**"). The tasks and the responsibility regarding the proper procedures related to the exercising of Data subjects' rights shall basically be borne by the Party identified in the Responsibility Matrix. Parties undertake to aid the other Party in every case and to the extent possible with suitable technological and organisational measures in performing the requests related to the exercising of Data subjects' rights - taking the characteristics of Processing into account.

Upon the request of the other Party, each Party shall co-operate with the relevant Supervisory Authorities in performing their tasks. Should a court and/or any Supervisory Authority commence proceedings against a Party, the other Party shall co-operate in good faith and render assistance to the Party involved without undue delay or charging any fees, to the extent such aid is necessary during the proceeding in question.

In a more general sense, Parties undertake to co-operate in good faith and to make any other information available to each other as are required for them to meet their obligations described in this clause. If necessary, the Party named in the Responsibility Matrix shall perform a data protection impact assessment and conduct a preliminary consultation with the relevant Supervisory Authority. Parties state that Y GENERÁCIÓ shall collect and process the personal data it receives regarding the Principal Contract, which it shall process and transfer to Customer for the purpose of performing what is set down in the Principal Contract.

Parties acknowledge that the personal data set forth in this agreement shall only be processed for the purpose of performing the Principal Contract.

Parties shall ensure that all persons authorised to process personal data undertake confidentiality commitments or are under statutory confidentiality obligations regarding Worker data. The confidentiality obligation in this point shall bind Parties both for the duration of the Agreement, and following its termination without time limitation. The confidentiality obligation in this point extends to all such employees and agents of Parties who are entitled to learn Worker data based on this Agreement. Parties shall bear full liability for the actions of the persons listed above. Parties, by concluding the appropriate contracts, and also otherwise, guarantee that the data subjects listed here keep their confidentiality obligations.

**5.11. Auditing**

Both Parties (in the case of an audit this Party is henceforth referred to as "**the Requesting Party**" reserves the right to conduct an audit at any time at their own expense concerning the other Party's („**the Audited Party**") performance of Processing regarding compliance with the obligations stipulated in this article. The audit shall be performed by a group of the Requesting Party's internal auditors or persons appointed by the Requesting Party, who shall keep their confidentiality obligations, and on the condition that the auditors may not be the Audited Party's direct competitors, unless they were appointed by some judicial or regulatory authority.

In order to enforce their above right to auditing, the Requesting Party shall notify the Audited Party in a registered letter with return receipt at least twenty-five (25) days in advance. The Requesting Party shall also inform the Audited Party about the chosen panel of auditors if the selected panel of auditors is a third party. The Audited Party shall co-operate in good faith with the auditors appointed in line with this paragraph. The audit shall be conducted, if possible, in a manner so as not to disturb Processing and the Audited Party's activities. Should the audit report highlight faults in Audited Party's Processing activities, the Parties shall have a meeting in which they set up a plan of action to be followed. Should any Supervisory Authority wish to access the audit report on Audited Party, the latter consents to the Supervisory Authority in question and its appointed person(s) accessing the report made by Requesting Party.

**5.12. Termination of Services**

Parties shall jointly determine what is to be done with the Personal Data Involved in Co-operation once the Services are no longer being provided.

**5.13. Insurance, damages**

The Parties agree that – as long as it is available on the Hungarian insurance market – all Parties shall take out and maintain an insurance policy with a sound insurance company for all such risks regarding which their liability may arise in connection with this Joint Processing Agreement. It is especially crucial for the insurance to cover any consequences of Personal Data Breaches and the damages due as per this point, including official fines, except where prohibited by law.

Parties acknowledge that if they violate the provisions of the Agreement or commit an infringement regarding Worker data, or the other Party suffers any damage as a result of any act on their part that is against the GDPR and/or Hungarian legislation, they shall indemnify the other Party, especially but not exclusively for any costs incurred during an official or court proceeding, as well as any fines or legal claims by third parties.

**5.14. Other provisions**

This Joint Processing Agreement may only be modified in writing, if duly signed by both Parties. Should there be any discrepancy between this Joint Processing Agreement and any Contracts, then this Joint Processing Agreement shall govern, unless this Joint Processing Agreement stipulates otherwise. This Joint Processing Agreement falls under the jurisdiction of Hungarian law. In the case of any disputes arising from this Joint Processing Agreement, Parties shall attempt to reach an amicable agreement. Should that fail to produce results, Parties shall settle their disputes at the relevant court, in line with the Code of Civil Procedure in effect at the time.

**6. Final and miscellaneous provisions**

6.2. The Parties shall aid the activities of each other to make contractual performance possible, and shall immediately inform the other Party in writing in case they become aware of such material circumstances that may concern the Contract.

6.3. Regarding the formality of the Contract, the Parties agree that the Contract may only be amended, terminated or cancelled in writing, with expressly stated contractual amendments.

6.4. In matters not regulated in this Service Contract, the provisions of the Civil Code and the legislation in force related to the subject and contents of the Service Contract shall be considered authoritative.