PERSONAL DATA PROTECTION POLICY
in
Embassy International School Spółka z o.o.

INTERNAL DOCUMENT FOR THE PERSONAL DATA ADMINISTRATOR

Personal Data Administrator:

Embassy International School Spółka z o.o. with its registered office in Kraków at ul. Edmunda Biernackiego 10, entered into the National Court Register - Register of Entrepreneurs by the REGIONAL COURT FOR KRAKÓW ŚRÓDMIEŚCIE IN KRAKÓW, 11th DIVISION OF A NATIONAL COURT REGISTRY, under KRS number 0000569069 with a share capital of PLN 100,000.00 - fully paid up

also acting also as **a processor** within the meaning of the GDPR- in a document called " **Receiving Party** ".

Valid from: May 25, 2018.

This Personal Data Protection Policy is a list of technical and organizational measures taken by the Personal Data Administrator to process personal data in accordance with the law, in particular Regulation of the European Parliament and of the Council (EU) 2016/679 of 27/04/2016 on protection natural persons in relation to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC (General Regulation on Data Protection - **GDPR**). The adoption of appropriate measures was preceded by a risk analysis contained in a separate document. The content of the documentation contains a description of the measures used by the Personal Data Administrator to ensure adequate data protection standards.

§ 1
Definitions

The following concepts appearing in this Policy have been given meaning in accordance as defined below:

Personal Data Administrator, Administrator or **PDA - Embassy International School Spółka z o. o.** with its registered seat in Kraków at ul. Edmunda Biernackiego 10, entered into the National Court Register - Register of Entrepreneurs by the REGIONAL COURT FOR KRAKÓW ŚRÓDMIEŚCIE IN KRAKOW, 11th DIVISION OF A NATIONAL COURT REGISTRY, under KRS number 0000569069 with a share capital of PLN 100,000.00 - fully paid up

1. **Sensitive** data **-** personal data revealing racial or ethnic origin, political views, religious or ideological beliefs, trade union membership and genetic data, biometric data to uniquely identify a person or data on a person's health, sexuality or sexual orientation, as well as personal data on convictions and violations of law.
2. **Data Protection Officer** - an entity competent for personal data at the Administrator, designated by him in cases specified in the GDPR.
3. **Policy -** this policy for the protection of personal data.
4. **Enterprise -** a place of doing business by PDA.
5. **Authorized person** - an PDA employee or colleague who has been authorized to process personal data, as well as PDA itself.
6. **Processor** - an entity to whom PDA entrusted the processing of personal data.
7. **Receiving Party** - Administrator acting as a processor, referred to in art. 4 point 8 of the GDPR.
8. **Entrusting Party** - an entity being an administrator in relation to personal data entrusted by him for processing to the Receiving Party.
9. **Register of processing activities** - register of personal data processing activities carried out by PDA, referred to in art.30 of GDPR.
10. **Records of categories of processing activities** - a register of categories of processing activities carried out by the PDA in the role of the Receiving Party, referred to in art. 30 para.2 of GDPR, kept by the Receiving Party in a separate document.
11. **GDPR** - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC - a general regulation on data protection.

§ 2
Personal Data Administrator and general provisions

1. In order to ensure the highest standards of protection of personal data being processed, as well as fulfilment of legal obligations incumbent on the Administrator, the Administrator, in particular:
    a. carried out a risk analysis;
    b. on the basis of risk analysis, he developed and implemented the Policy;
    c. grants and revokes authorisations to process personal data to all persons who are to have access to the personal data processed by the Administrator ;
    d. entrusts the processing of personal data to other entities on its behalf based on the appropriate legal instrument, in particular the entrustment agreement - if applicable;
    e. keeps the Register of processing activities;
    f. keeps the Register of processing activities categories.
2. The policy is aimed at fulfilling the obligations arising from the GDPR by introducing rules to ensure the protection of personal data processed by PDA.
3. PDA, in order to protect personal data and respect for the rights of persons whose data is processed, applies the following rules:

a. legality - meaning, in particular, processing in accordance with the law and on the proper legal basis resulting from the GDPR;
b. expediency - meaning in particular processing only for the purposes for which the data has been properly collected;
c. adequacy - meaning in particular the processing of only such data as are necessary to meet a given purpose;
d. substantive correctness - meaning in particular the processing of data in accordance with the actual state;
e. accountability - meaning in particular processing in a way that demonstrates the compliance of the processing with the law;
f. transparency - meaning in particular transparent processing for data subjects, inter alia, by providing those persons with the information required by law related to the processing of data, in particular those resulting from Art. 13 of GDPR.

4. Processed data is constantly monitored by PDA, which aims to control the data being processed and to eliminate potential threats to the security of the data being processed.

§ 3
Administrator's activity

1. As part of its activities, the Administrator, being a private entity:

a. Provides educational, care, recreation and sports services within the framework of running a business;
b. runs websites, including:
- https://www.embassyschool.pl

§ 4
Inspector for Personal Data Protection

1. Bearing in mind the above, the main activity of PDA is not Sensitive Data processing. As part of its activity PDA may process Sensitive Data in relation to:
- his employees, however, this will only take place in the scope in which PDA is obliged to do so by the provisions of generally applicable law and not on a large scale,
- selected students of the school, however, this will only take place in the scope in which PDA is obliged to do so by the provisions of generally applicable law and not on a large scale,

2. In addition, PDA does not perform processing operations as part of its operations, which, due to their nature, scope or objectives, require regular and systematic monitoring of data subjects on a large scale.

3. Considering the nature of the PDA activity, **it is not obliged** by the universally binding regulations in Poland, including the provisions of European Union law, **to appoint a Data Protection Officer** , which should be designated when:

a. the personal data administrator is a public body or entity;
b. the main activity of the personal data administrator consists in processing operations which, by their nature, scope or objectives, require regular and systematic monitoring of data subjects on a large scale;
c. The main activity of the personal data administrator is to process sensitive data on a large scale.

§ 5
Register of processing activities

1. As part of the PDA activity, the following data sets are kept:
   - **Customer Data** (DKL),
   - **Marketing Data** - Users in relation to which marketing activities are / will be carried out (DMARK),
   - **Contractor's data** (eg suppliers of goods / services, business partners) (DKON),
   - **Student Data** (DUCZ)
   - Human Resources (DKADR),
   - **Recruitment Data** (DREK).
2. PDA keeps the Register of processing activities in order to fulfil its duty resulting from the GDPR , as well as to exercise ongoing control over data processing in its enterprise.
3. The Register of personal data processing activities distinguishes, among others: items such as:
   - categories of persons whose data is processed,
   - categories of data processed,
   - the purpose of data processing,
   - the categories of recipients to whom the data are / will be disclosed, as well as
   - planned dates to delete categories of data being processed.
4. PDA will provide the Registry with processing activities at the request of the supervisory authority.
5. The template of the Register of processing activities constitutes the Annex 5 to the Policy, while the Register of processing activities itself is kept in a separate document.

§ 6
Technical / IT security

The administrator uses technical safeguards to ensure the security of the data processed in accordance with the rules provided for in this paragraph.

1. **Portable devices and other media** on which personal data are contained **may be carried out outside the Enterprise**.
2. These devices and Carriers can be transported:
3. Public transport (e.g. bus / train)
4. A private vehicle - in the passenger cabin
5. A private vehicle - in the trunk separated by hard walls (other than glass) from the passenger compartment.
6. The data is transported in a secure way. The carriers are not left in the vehicle in visible places in the absence of an authorized person. Whenever equipment or printouts are taken out of the Enterprise, the Authorized Person should exercise extreme caution. This means, in particular,

that no devices or printouts are left unattended, and that devices or printouts are used in a way that prevents third parties from reading the content on the screen or printout.

7. In order to reduce the risk of unauthorized access to data, the devices referred to in para. 1 are encrypted.
8. **Weekly backups of personal data are carried out and are stored for a period of about one month depending on the data increment.**
9. **Backups** are stored in two different places (external drives)
10. **Access to ICT equipment** used to process personal data (in particular personal computers, smartphones, tablets), as well as software intended for data processing is secured using a **login (identifier) and password** .
11. In order to ensure high standards of data protection, Embassy School applies a policy regarding access passwords to devices and programs on which data is processed. According to this policy, **access passwords** are changed whenever there is a suspicion of the unauthorized access to the data or an incident related to it.
12. ICT devices have **current anti-virus software** installed **.**
13. Devices with access to personal data are equipped with **firewalls system** .
14. The computers used for data processing use system functions that block access to the system after a specified period of inactivity - usually 5 minutes (**screensavers** protected by a password and **automatic logout after a specified period of inactivity (5 min)**).
15. Connections between the following websites and users are secured using **the SSL certificate:**

- embassyschool.pl
- embassyschool.org
- embassyschool.com.pl

16. In the case of hardware lost containing company's data (e.g. email), the data from the device will be deleted
17. The Company uses **document shredders that meet the standards appropriate for the destruction of confidential information**, corresponding at least to DIN 5 level.

§ 7
Organizational security

PDA applies organizational safeguards to ensure the security of the data processed in accordance with the rules provided for in this paragraph.

1. PDA applies so-called the policy of a **clean desk and clean printer** , according to which on desks and devices (in particular printers and copiers) there should not be unused or unattended persons authorized documents and media containing personal data.
2. Third parties who are not authorised to process personal data, such as customers, office cleaners or couriers, may have access to the premises where data are stored. The processing of personal data takes place in conditions protecting this data against access of unauthorized persons and their embarrassment, especially such as:
    - **The doors to the office are closed** - access to the rooms where personal data are processed by unauthorized persons is only **under the control of PDA** ,
    - Unauthorized persons are in the PDA seat only **under the supervision of an authorized person** .
3. PDA uses the following measures to increase the security of personal data processing:
    - locked door,

- monitoring,
- restricted access zone, i.e. .:

- server room,
- staff,
- accounting

2) The Management Board

- fire extinguisher,
- safe for archival data,
- lockable cabinet for personnel data
- Lockable cabinet for the pupils concerned

§ 8
Human factor

In the case of **using the services of third parties, non-PDA -related by employment relationship, in particular in the case of cooperation under civil law contracts, PDA will meet the requirements specified in § 11** (entrusting the processing of personal data).

1. In positions with access to personal data, there is no frequent rotation. Such a solution allows to maintain proper standards in the field of data protection processed in the PDA Enterprise.
2. Persons having access to personal data **are not entitled to store such data on private devices** .This leads to an increase in the level of personal data security and excludes the risk of not using appropriate security measures in private devices, as well as the loss of a private device with access to personal data, which minimizes the risk.
3. Persons with access to personal data **have been duly trained** in terms of data protection and have been **acquainted with the principles of personal data protection** in order to maintain a high standard of security in PDA enterprise. The training takes place internally at PDA enterprise , after every update of the personal data processing documentation kept by PDA. Every collaborator who has access to personal data before being granted access undergoes training, and also has access to internal documentation of personal data processing (especially this Policy) and is obliged to read it. The method of training is chosen by the PDA on the basis of an individual assessment of each case.
4. In addition, persons who have access to personal data at PDA are **obliged to keep these data confidential** .
5. A template of the authorization to process personal data, which PDA may or may not use, constitutes Annex 2 to the Policy.
6. A model statement of a person authorized to process personal data, from which PDA may or may not take advantage, is attached as Annex 3 to the Policy.
7. The template for the registration of persons admitted to the processing of personal data by PDA , from which PDA may or may not benefit, constitutes Annex 4 to the Policy.

§ 9.
Entrusting processing of personal data

1. Personal data may be **entrusted by the Administrator to process on its behalf to an external entity - the Processor** .
2. In case of the need to entrust the processing of personal data to third parties, PDA:

a. will select only such **entities that guarantee the implementation of appropriate technical and organizational measures** , so that the processing meets the requirements of the GDPR and secures the applicable rights of the data subjects;

b. will entrust processing **under a contract or other legal instrument** that is subject to Union law or the law of a Member State.

3. The contract or legal instrument referred to in paragraph 2 points b., should contain at least the following elements:

a. definition of:
- **subject and duration of processing** ,
- **the nature and purpose of the processing,**
- **the type of personal data entrusted,**
- **the category of data subjects,**
- **duties and rights of PDA** ;

b. indication that the **Processor:**
- **processes personal data only upon a documented PDA order** - which also applies to the transfer of personal data to a third country or an international organization - unless such obligation is imposed by Union law or the law of the Member State to which the processor belongs; in this case, prior to the start of processing, the processor informs the PDA of this legal obligation, unless such law prohibits such information on the grounds of important public interest;
- ensures that **persons authorized to process personal data commit themselves to confidentiality** or are subject to an appropriate statutory obligation of secrecy;
- **takes all measures required by Art. 32 of GDPR;**
- **observes the conditions for using the services of another processor, referred to in Art. 28 para. 2 and 4 of GDPR**
- **taking into account the nature of the processing, as far as possible, PDA helps through technical and organizational measures to meet the obligation of the data subject** to fulfil his or her rights set out in Chapter III of the GDPR;
- **having regard to the nature of the processing and the information available to him, it helps the PDA to fulfil the obligations set out in Article 32-36 of GDPR/0} ;**
- **after terminating the provision of processing services, depending on the PDA decision, deletes or returns to it any personal data and deletes all existing copies thereof** , unless Union or Member State law requires the storage of personal data;
- **makes available to PDA all information necessary to demonstrate compliance with the obligations** set out in Article 28 of the GDPR and **enables** and **facilitates the PDA or auditor authorized by PDA to carry out audits** , including inspections and contributes to them.

1. The model contract for entrusting the processing of personal data , which PDA may, but does not have to use, constitutes Annex No. 1 to the Policy .

2. The register of recipients of personal data, which may be managed by the Administrator, is included in Annex 7 to the Policy.

§ 10
The request of the data subject

1. Where the data subject reports **to PDA as a personal data administrator a request** for:
   a. access to the content of its personal data,
   b. correcting its personal data,
   c. deletion of its personal data,
   d. requests to limit the processing of its data,
   e. raising objections to the processing of its data,
   f. request to transfer its personal data, this request will be subject to **verification by an Authorized Person** .

2. The verification is to lead, above all, to the assurance that:
   a. the request comes from the data subject;
   b. there are reasons justifying the fulfilment of the request and the fulfilment of the request will not violate the generally applicable law.

3. In order to meet the requirement referred to in paragraph 2 point a., an authorized Person may, for example, check if the request has been sent from the email address assigned to the user's account in the Software.

4. In the event that the verification referred to in paragraph 2 point a., will not result in obtaining reliable information that the request comes from the data subject or that an authorized Person has justified doubts about the identity of the natural person submitting the request, the authorized person will ask the data subject, to provide evidence to prove its identity, taking into account the nature of the person's request and the consequences that may result from this request.

5. In the event that the person submitting the request does not provide evidence to prove his/her identity, or the evidence does not authenticate that person's identity, the Authorized Person refuses to make the request, informing the person making the request, indicating the grounds for refusal.

6. In the event that the result of the above verification is positive, the Authorized Person begins the further verification stage referred to in paragraph 2 point b.
7. The authorized Person performs his/her duties under this paragraph in a manner allowing to demonstrate their fulfilment, e.g. by means of e-mails sent to the data subject.

8. **Providing information on actions taken in connection with the request of the** data subject:
- it is carried out without unnecessary delay , however not later than within 1 month of receiving the request ;
- it concerns both the fulfilment of the request and the refusal to comply with it;
- is free of charge.

9. If the data subject has forwarded his request electronically, if possible, the information is also transmitted electronically, unless the data subject requests a different form.

10. In the event that the Authorized Person has not acted in connection with the request of the data subject, he/she shall immediately, but not later than one month after receiving the request, inform the data subject about:

- reasons for inaction;
- the possibility of lodging a complaint to the supervisory body;
- the possibility of using legal protection measures before a court.

11. Where a request of a complex nature is made by a data subject or in the case of submitting requests in a number causing difficulty in their recognition within one month of receipt, the authorized Person is entitled to extend the deadline for providing information to the data subject by a maximum of 2 months. In this case, within one month of receipt of the request, the Authorized Person will inform the data subject of the extension of the deadline and its reasons.

12. If the data subject reports evidently unjustified or excessive demands, in particular due to his or her continuing nature, the authorized person may:

- retrieve a reasonable fee from the data subject, including the administrative costs of providing information, carrying out communications or taking the action sought;
- refuse to take action in connection with the demand.

13. The authorized person takes the above decisions, taking into account the fact that he/she has an obligation to demonstrate that the request is clearly unreasonable or excessive.

14. The responsible person in the PDA enterprise for the implementation of the rights of data subjects, including verification and response to demands are: Ewelina Sołtys and Paulina Jędrzejewska

§ 11
Reporting violations
by PDA acting as an administrator of personal data

1. In the event of a breach of personal data protection, PDA without undue delay - if possible, no later than within 72 hours after finding the violation - **reports it to the appropriate supervisory authority, unless it is unlikely that this violation would risk the violation of the rights or freedoms of individuals** .
2. The application meets the requirements set out in the GDPR.
3. For a notification submitted to the supervisory authority after 72 hours, the PDA shall attach an explanation of the reasons for the delay.
4. **The administrator documents any violation of personal data protection** , including the circumstances of personal data breach, its consequences and the remedial actions taken.
5. **If the breach of the protection of personal data may cause a high risk of violation of the rights or freedoms of individuals, PDA without undue delay informs the data subject about such violation** , under the conditions indicated in the GDPR, unless :

a. PDA has implemented appropriate technical and organizational security measures and these measures have been applied to the personal data of the breach, in particular measures such as encryption, making it impossible to read to unauthorized persons to access these personal data;

b. PDA The ADO has subsequently taken measures to ensure that the rights or freedoms of the data subject referred to in this paragraph are not likely to be infringed;
c. the notification would require a disproportionately large effort.In this case, a public message is issued or a similar measure is put in place by which the data subjects are informed in an equally effective manner.
6. The template for the register of personal data breaches, which the PDA may or may not take advantage, is attached as Annex 6 to the Policy .

§ 12
The activity of the Administrator as the Receiving Party

1. The Receiving Party and any person acting under the Receiving Party authorization and having access to personal data shall process it **only at the request of the Entrusting Party** , unless required by Union law or the law of a Member State.
2. The Receiving Party shall keep a **Register of the processing activities category** in order to fulfill its obligation resulting from the GDPR, as well as to control the data processing in his company on a current basis.
3. The **Register of categories of processing activities** distinguishes, among others: categories of processing carried out on behalf of each of the Entrusting Parties.
4. The Receiving Party shall provide the Register of categories of processing activities at the request of the supervisory or Entrusting Authority.
5. The template for the Register of processing activities categories is attached as Annex 8 to the Policy, while the Register of the processing activities categories is kept in a separate document.
6. The Receiving Party shall immediately inform the Entrusting Party, if in his opinion, the order issued to him in connection with the last paragraph of § 11 section 3 letter b by the Entrusting Party is in violation of the GDPR or other provisions of the Union or the Member State on data protection.
7. The Receiving Party applies to the requirements set out in § 11 section 3.
8. The Receiving Party does not use the services of another processor without **prior detailed or general written consent of the Entrusting Party**.
9. In the case of general written consent, the Receiving Party informs the Entrusting Party of any intended changes regarding the addition or replacement of other processors, thus giving the Entrusting Party the opportunity to object to such changes.
10. Where the services of another processing entity is used, the Receiving Party will impose on it - under a contract or other legal act that is subject to Union law or the law of a Member State - the same data protection obligations as in the contract or other legal act between the Entrusting Party and the Receiving Party - in particular the obligation to provide sufficient guarantees for the implementation of appropriate technical and organizational measures to ensure that the processing complies with the requirements of the GDPR.
11. In the event that the data subject asks **the applicant to** submit **a request** regarding:
    a. access to the content of its personal data,
    b. correcting its personal data,
    c. deletion of its personal data,
    d. requests to limit the processing of its data,
    e. raising objections to the processing of its data,
    f. requests to transfer its personal data,

The Receiving Party, if possible and taking into account the nature of the processing, **will help the Entrusting Party to fulfil his duty to respond to these demands** through appropriate technical and organizational measures.

12. In the event of a breach of the protection of personal data, the Receiving Party **shall report such violation to the Entrusting Party** without undue delay.

13. The Receiving Party, taking into account the nature of the processing and the information available to him, **assists the Entrusting Party in complying with the obligation to report breaches of personal data protection to the supervisory body** .

14. The Receiving Party provides the Entrusting Party with all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and enables the Entrusting Party or the auditor authorized by the Entrusting Party to carry out audits, including inspections, and contributes to them.

15. The Receiving Party shall take appropriate measures to ensure that personal data not provided by the Entrusting Party conducting the audit are not disclosed during the audit.

16. In order to ensure the security of the processed data, the audit may be carried out only after the Entrusting Party and all persons used by the Entrusting Party have entered into an agreement, submitted by the Receiving Party, obliging them to duly protect any information obtained in connection with the audit.

17. The Receiving Party cooperates with the competent authorities for the protection of personal data, in the scope of the performed tasks.

§ 13
Final Provisions

1. An integral part of the Policy is the GDPR - in its current wording. The administrator ensures that the security measures of the processed data are applied at a high level.
2. The attachments below constitute an integral part of the Policy.

List of attachments:

Annex No. 1 - Model contract for entrusting the processing of personal data
Annex No. 2 - Template of authorization to personal data processing
Annex No. 3 - Template of the statement of the person authorized to data processing
Annex No. 4 - template of registration of persons admitted to the personal data processing
Annex No. 5 - template of the Processing Activities Register
Annex No. 6 - Register of personal data violations
Annex 7 - Register of recipients
Annex No. 8 - Model Register of processing activities categories

Annex No. 1 – Template of contract for entrusting the processing of personal data

ENTRUSTMENT AGREEMENT FOR THE PROCESSING OF PERSONAL DATA ("Agreement")

concluded between:

Embassy International School Spółka Z O.O. with its registered office in Kraków at ul. Edmunda Biernackiego 10, entered into the National Court Register - Register of Entrepreneurs by the REGIONAL COURT FOR KRAKÓW ŚRÓDMIEŚCIE IN KRAKOW, 11th DIVISION OF A NATIONAL COURT REGISTRY, under KRS number 0000569069 with a share capital of PLN 100,000.00 - fully paid up

hereinafter referred to as the " **Administrator** ",

and

< *data of the processor>*

hereinafter referred to as the " **Processing Party** ",

which reads as follows:

§ 1

GENERAL PROVISIONS

1. This Agreement is concluded in connection with the contract conclusion by the Parties < *precise specification of the contract being the basis for cooperation>* (" **Main Agreement** ").
2. On the basis of the Agreement, i.e. on the terms and in the scope indicated therein, the Administrator entrusts the Processing Party with processing personal data < *indication of the category of persons whose data relate to, e.g. PDA Customers>* (" **Data** "), and the Processing Party undertakes to process Data within the limits set out in the Agreement and generally applicable laws.
3. The Processing Party processes the Data only on the documented Administrator's instructions.

§ 2

REPRESENTATIONS OF THE PARTIES

1. The Administrator represents that he has the status of personal data administrator within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95 / 46 / EC (General Data Protection Regulation - " **the GDPR** "), in respect of Data.
2. The Administrator represents it he has an appropriate basis for processing Data, and entrusting Processing Data to it does not violate the rights of third parties.
3. The Processing Party ensures that persons authorized by it to process the Data will be obliged to keep them secret or will be subject to an appropriate statutory obligation to keep them secret.

4. The Processing Party ensures that it takes all the measures required by the applicable law, in particular art. 32 of GDPR, according to which the Processor implements the appropriate technical and organizational measures taking into account the state of technical knowledge, implementation cost and nature, scope, context and purposes of processing and the risk of violating the rights or freedoms of individuals with different probability of occurrence and threat severity to ensure the security level corresponding to this risk.

§ 3

THE SCOPE OF PROCESSING

1. Processing of Data by the Processing Party will take place only for the purpose of implementing the Main Agreement.
2. Pursuant to the Agreement, the Processing Party will process the so-called ordinary data, i.e. not subject to additional regulations such as

a. [...]
b. [...].

3. The Administrator undertakes not to provide data:

a. revealing racial or ethnic origin,
b. revealing political views, religious or ideological beliefs,
c. revealing affiliation to trade unions,
d. genetic,
e. biometric
f. *concerning the health, sexuality or sexual orientation of the person concerned.*

§ 4

METHOD OF AGREEMENT PERFORMANCE

1. When processing Data, the Processing Party undertakes to implement all measures required by the applicable law (including by the GDPR), including appropriate technical and organizational measures to ensure the security of personal data processing corresponding to the risk of violating the rights and freedoms of individuals with different probability of occurrence and hazard .By implementing appropriate measures, the Processing Party will take into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk referred to in the previous sentence.

2. Considering the nature of the processing, the Processing Party will, as far as possible, help the Administrator, through appropriate technical and organizational measures, meet the obligation to respond to requests of the data subject in the exercise of its rights, as set out in Chapter III of the GDPR - if, in the particular case, they are attributable to the Administrator.

3. Taking into account the nature of the processing and the information available to him, the Processing Party will help the Administrator to meet the obligations set out in Art.32-36 of GDPR, if they attributable to the Administrator.

4. **The Processing Party** may use the services of another processing entity (hereinafter referred to as " **another processor** ") only with the prior detailed or general written consent of the Administrator. In the case of general written consent, the Processing Party will inform the Administrator about any intended changes regarding the addition or replacement of other Subsequent Processors, thus giving the Administrator the opportunity to object to such changes.

5. In the agreement with the next processor, the Processing Party will oblige it to comply with the same data protection obligations that were imposed on the Processing Party in the Agreement. These obligations will include, in particular, providing sufficient guarantees to implement the appropriate technical and organizational measures to ensure that the processing complies with the requirements of the GDPR.

6. If the subsequent processor fails to fulfil its data protection obligations, the full responsibility for the Administrator for fulfilling the obligations of this Subsequent Processor rests with the Processing Party.

7. The Processing Party shall make available to the Administrator all information necessary to demonstrate fulfilment of the obligations specified in art.28 of GDPR and enables the Administrator or the auditor authorized by the Administrator to carry out audits, including inspections, and contribute to them - when such duties are incumbent on the Administrator.

8. In connection with the obligation set out in para.7, the Processing Party shall immediately inform the Administrator if, in his opinion, the instruction given to it constitutes a breach of the GDPR or other provisions of European Union law or Polish provisions of universally binding law regarding data protection.

§ 5

TERM OF AGREEMENT

1. The agreement is terminated upon the termination of the Main Agreement.

2. Data processing takes place during the term of the Agreement.

3. Upon termination of the Agreement, the Processing Party shall delete or return to the Administrator (depending on the Administrator's decision) any personal data and delete all existing copies thereof, unless European Union law or Polish law of general law require the storage of personal data.

4. In matters not regulated in the Agreement, universally binding provisions of Polish or European law as well as the provisions of the Main Agreement shall apply.

Annex No. 2 - Template of authorization for the processing personal data

AUTHORIZATION
for the processing of personal data administered by:
Embassy International School Sp. z o.o.
KRS number 0000569069

Hereby, as the Personal Data Administrator of the Embassy International School with its registered office in Kraków (address: ul. Edmunda Biernackiego 10; 30-043 Kraków), in accordance with art. 5 para.1 letter f in relation to Art.29 of *Regulation* (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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*):

from 25/05/2018 I grant you **.....** authorization to process personal data administered by **Embassy International School Sp. z o.o.** , for the purposes of ...., in particular to:

- data processed on paper media:
- IT system and its devices:
- personal data processed as part of the participation in the following data processing activities:

I grant you the following authorised person ID :

.....

The authorized person is obliged to process personal data to the extent and in the manner required to perform his duties towards the Administrator of Personal Data.

I oblige you to comply with the provisions on the protection of personal data and the Personal Data Processing Document introduced and implemented by the Administrator.

This authorization may be revoked at any time. This authorization expires upon termination or expiration of the employment contract, mandate contract, contract for specific work or other civil law contract linking you with Embassy International School Sp. z o. o.

....

(date and signature of PDA)

I declare that I am familiar with this document .

....
Date and Employee's signature:

Annex No. 3 - Template of the statement of the person authorized to process the data

DECLARATION BY A PERSON AUTHORIZED TO PERSONAL DATA PROCESSING

I, the undersigned **.....** I declare that I am familiar with the regulations regarding the protection of personal data, as well as internal rules of processing personal data implemented by the Administrator of Personal Data - **Embassy International School Sp. z o. o.** seated in Krakow at ul.Edmunda Biernackiego, KRS No. 0000569069, in particular with:

a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46 / EC - the General Data Protection Regulation ("GDPR");

b) internal documentation of personal data processing used by PDA.

I undertake to comply with the above-mentioned regulations and internal rules applied in the Company, including among others:

1. maintaining company secrets, in particular the confidentiality of personal data to which I have or will have access in connection with the performance of official duties or employee duties;
2. not using personal data for non-retaliatory purposes;
3. confidentiality of data protection methods;
4. use of IT equipment and software only in connection with the performance of employee duties;
5. use only legal software from PDA;
6. due care for equipment and software in accordance with the personal data protection documentation;
7. use of mobile devices in accordance with the personal data protection documentation.

I understand that the conduct contrary to the above obligations may be considered by the PDA who is an Employer as a serious breach of employee duties.

.....
signature of an authorized person

Annex No. 4 - the model of registration of persons admitted to the processing of personal data

RECORDS OF PERSONS ADMITTED BY PDA TO THE PROCESSING OF PERSONAL DATA

No.	Name and surname of the authorized person	ID of Authorized person	Date of granting rights	The date of expiry of rights	Position / Character of cooperation	Category of shared data	Scope of Authorities	Software
1.								
2.								
3.								
4.								

Abbreviations for determining permissions:
P - the right to view data
W - the right to enter data
M - the right to modify data
U - the right to delete data
K - the right to make backup copies

.....

.

Annex No. 5 - the template of the Processing Activities Register

PROCESSING ACTIVITIES REGISTER
made by

Embassy International School Sp. z o.o. with its seat in Kraków at ul. E. Biernackiego 10, KRS No. 0000569069

e-mail: .....
tel. no. .....
("PDA")

Data Protection Officer: * .....,
e-mail: .....

Categories of people whose data is processed	**Categories of data processed**	**The purpose of data processing**	**Categories of recipients to whom the data are / will be disclosed ****	**Transmission of data outside the European Economic Area ****	**Planned dates of deletion of the category of data being processed**
E.g. Customer data	E.g. Name, surname, e-mail address	E.g. Implementation of contracts	E.g. Accounting office	E.g. Yes, to [...] / No	E.g., the end of the period in which PDA will be subject to legal obligations related to accounting
E.g. Contractors' Data	E.g., name, surname, address of the registered office				

A general description of technical and organizational security measures:
.....
.....
.....

.....
.....
.....
.....
.....
A detailed description can be found in the Data Protection Policies applied by PDA.

* If its designation is mandatory.
** When transferring data outside the European Economic Area, please indicate to which country. In the case of a transfer referred to in art. 49 par. 1 of GDPR second paragraph, please indicate the documentation of appropriate safeguards (this applies only to special situations when there is no decision stating an appropriate degree of protection such as Privacy shield for the US or the appropriate safeguards specified in art. 46 of GDPR)

Annex No. 6 - Register of personal data violations

Date of the event occurrence	Circumstances of personal data breach	Effects of the infringement	Remedial actions taken

Annex 7 - Register of recipients of personal data for PDA as data controller *
***** Does not apply to data entrusted to processing!**

Name of the recipient / recipient category	Collections of disclosed data

Annex No. 8 - Register Template of processing activities categories

Register of processing activities categories
made by

Embassy International School Sp. z o.o. with its seat in Kraków at
ul. E. Biernackiego 10
KRS number 0000569069
as

Processing entity
on behalf of
seperate personal data administrators ("PDA")

The list of PDAs who have entrusted the Processing Entity with the processing of personal data included in the Annex to this Register.

Categories of people whose data is processed	**Categories of performed processing operations**	**Transfer of data to a third country (outside the EEA)**
E.g., customers / employees of the PDA store	*E.g., storage, copying, deleting*	

A general description of technical and organizational security measures:
The processing entity has implemented appropriate security measures for the personal data processed and the scope of such processing, such as:

- making backups
- anti-virus software
- system firewalls
- policy of a clean desk and a clean printer
- fire extinguisher

A detailed description shall be provided in the Data Protection Policy of the Processing Entity.

WARNING! If the Registry is made available to the Entrusting Party, do not give it the whole content of the attachment - only its details!

Annex PDA List

Name / surname of the personal data Administrator	**Contact details**	**Data Protection Officer *** (name surname / name + contact

		details)
		NO/[…]

*** Inspector's data will be provided only if the PDA has appointed an Inspector.**