Personal Data Protection Policy

Review Frequency: Annual
Prepared by: Lawyer
Policy written in: October, 2019
Next review date: September, 2021

Sophio Bazadze
Director

GEORGIA
"EUROPEAN SCHOOL" Ltd
205172917

2, I. Skhirtladze st.
0177 Tbilisi, Georgia
Tel: (032) 239 59 64
info@europeanschool.ge
www.europeanschool.ge

Contents

Personal Data Protection Policy

Preamble

Personal Data Protection Policy (hereinafter referred to as "the Policy") defines how European School Ltd (hereinafter referred to as "the School") collects, processes and uses personal data. The policy sets the standards that must be in accordance with the acting Georgian legislation and international law.

The purpose of the policy is to protect the school community's personal data from unlawful and unauthorized use, and also to ensure reduction the risk of accidental loss and damage of personal data.

School management is responsible for presenting this policy to the school community, taking into account the views expressed by the school community, and ensure that appropriate work meetings are held for school staff.

The data protection policy covers all personal data processed by the school, and access by any person to any personal data held by the school or on a personal device. All school staff and contractors are required to comply with this policy. Failure to comply with the policy requirements will result in imposing of obligation by the school management.

1. Scope

This policy applies to the processing of personal data of school staff, students, parents of pupils and other individuals associated with the European School using automated, semi-automatic or non-automatic means

2. Definition of terms

The terms used in this policy shall have the following meanings:

a) Data subject - any natural person about whom personal data is processed at a European school;

b) Personal data - any information relating to an identified or identifiable natural person; A natural person is identifiable when it is possible to identify him/her directly or indirectly, in particular by an identification number or by a physical, physiological, psychological, economic, cultural or social characteristic of the person;

c) special categories of personal data – data related to a person's racial or ethnic background, political beliefs, religious or philosophical beliefs, professional affiliation, health status, sex life, convictions, administrative detention, the imposition of a preventive measure on a person, plea bargaining, diversion, recognition as a victim of crime or recognition as a victim, as well as biometric and genetic data that give possibility identify the natural person via above mentioned features;

d) data processing – any operation performed on data by automatic, semi-automatic or non-automatic means, such as collection, recording, photo imaging, audio recording, video recording, organisation, storage, alteration, restoration, request, use or disclosure by transmitting, disseminating or making the data otherwise available, alignment or combination, blocking , deletion, or destruction;

e) semi-automatic data processing - data processing by means of information technologies and non-automatic means;

f) consent – a voluntary consent on personal data processing for specific purposes expressed by a data subject orally, through telecommunication or other relevant means after receiving respective information, which allows to clearly establish the will of the data subject;

g) written consent of the data subject – a voluntary consent on personal data processing for specific purposes expressed by a data subject after receiving the respective information, which is signed or otherwise expressed by the data subject either in writing or in any other equivalent form;

h) data processor - a European school that defines the purposes and means of personal data processing and processes data through an authorized person;

i) authorized person - employee of European School Ltd, who processes personal data on behalf of European School;

j) third party – any natural or legal person, a public agency, except for a data subject, Office of State Inspector, data processor and authorized person;

k) State Inspector - an official stipulated by the Law of Georgia on State Inspectorate Service, which is responsible for overseeing the implementation of legislation regulating the data protection;

l) data depersonalisation – such modification of data that makes it impossible to connect the data to a data subject or the establishment of such connection requires disproportionately great efforts, expenses, and time;

m) direct marketing – offering goods, services, employment or temporary jobs by mail, telephone calls, e-mail, or other means of telecommunication.

3. Principles of personal data processing

The following principles should be followed when processing personal data:

1. First principle: The processing of personal data must be fair, legal and transparent;

The school should determine each processing process, determine the purpose of the processing, the types of processed personal data, the legal basis for the processing, and the evaluation of the data processing on the fundamental rights and freedoms of the data subjects.

The legal basis for the processing of personal data may be derived from:

- *The data subject has expressed his or her consent to the processing of personal data for one or more specific purposes on the basis of expression of free will;*
- *The processing of personal data is necessary to conclude (and / or perform) a contract with a data subject and / or to discuss his / her statement, e.g. Monitoring staff performance, to provide annual assessments, conclude contract with staff or school students;*
- *Data processing is necessary for the school to fulfil its legal obligation;*
- *The processing of personal data (other than a contract) is necessary to protect the vital interests of data subject (life or health), for example to carry out the emergency medical care;*
- *The processing of personal data is necessary for the performance of societal and / or public interest or function and it is carried out according to the law; (For example, the order of the Minister of Education, Science, Culture and Sport of Georgia stipulates informing the Center for Educational Quality Enhancement and enrolment of the student in the education management information system);*

- *The processing of personal data is necessary for the legitimate interests of the school, as there is no interest in the data subject, which takes precedence over the legitimate interests of the school.*
- *Special category data processing is permitted only with the written consent of the data subject or in the following cases:*
  a) processing of the data relating to conviction and state of health is necessary, given the nature of labour obligations and relations, including for making a decision on the employment;
  b) data processing is necessary to protect the vital interests of a data subject or a third party and the data subject is physically or legally incapable of giving his/her consent to the processing of data;
  c) the data is processed by a European school for the protection of the health of the natural person and, if this is necessary for the management or operation of the health care system;
  d) a data subject has made public his/her data without the explicit prohibition of their use;
  E) The data is processed for the purpose of realizing the right of education of persons with special educational needs.

Guideline

The authorized person shall explain to the data subject in a precise and comprehensible manner the legal basis for the processing of personal data, its purpose and shall provide him/her with complete information on data processing. Consent means a free will on his/her data processing for specific purposes expressed by a data subject orally, through telecommunication or other relevant means after receiving respective information,

The authorized person processing the personal data must prove that the data subject agrees to the processing of his/her personal data. Also, the data subject must be informed that he / she has the right to refuse consent and is entitled to revoke previously issued data processing consent at any time.

This policy is accompanied by the consent forms of students (Appendix 1) and European School Staff (Appendix 2) for the processing of personal data.

Minors enjoy the exclusive right to protection of personal data, as they may not be aware of the risks, consequences, safeguards and rights associated with the processing of personal data. Personal data of minors should only be processed with the consent of the parent or other legal representative.

The processing of personal data must be transparent to the data subject. Any information and communications related to the processing of personal data shall be easily accessible and understandable to the data subject and also conveyed in clear and simple language. The data subject should be provided

with information about the purpose of personal data processing and also, information about data processing rules, risks, safeguards and rights. In case if the data subject gives personal data to the authorized official of the school, the date of receipt of the data should be indicated. If the school has obtained personal data independently of the data subject, then the data should be stored for a reasonable period of time.

The European School Admissions and Enrolment Office shall only require the information (documents) containing the student's personal data as specified by the legislation of Georgia, so that student may be registered in the Education Management Information System (emis.ge). It is inadmissible to request the information not specified by the order of the Minister of Education, Science, Culture and Sport of Georgia.

The Human Resource Management Service may require the information (documents) containing the personal data of European school staff which are required to conclude a labour contract between a European school and an employee. The list of documents is defined by the Labour Code of Georgia and order of the Minister of IDPs from the Occupied Territories, Labour, Health and Social Affairs of Georgia.

2. Second principle: Restriction on the processing of personal data ("Goal Restriction")

Data may be processed only for specific, clearly defined, and legitimate purposes; The processing of personal data must be relevant to the purposes of their processing and limited by the need to achieve those goals. Personal data should only be processed only when the purpose of the processing cab not be reasonably achievable in other ways.

Guideline

Further processing of data for the purposes that are incompatible with the original purpose shall be inadmissible; In order to determine whether the purpose of further processing is relevant to the original purpose of collecting personal data, the processor must consider the following, after satisfying all initial processing requirements:

- *The relationship between the personal data originally obtained and the purpose of further processing of the data should be defined, especially if it relates to particular categories of data;*

- *The context of the initial obtaining of personal data should be assessed and a reasonable judgement should be made as to whether the data subject would give consent to the further processing of the data;*

- *The consequences of further processing of personal data for the data subject must be assessed;*

- *Availability of appropriate safeguards between initial and subsequent processing operations.*

3. Third principle: Data processing must be adequate, relevant and only by volume achievable for the purpose of processing ("Data Minimization")

Data may be processed only to the extent necessary for achieving respective legitimate purpose. Data shall be adequate and proportionate to the purpose for which they are processed;

Guideline

The volume of personal data processing implies only the processing of data required to achieve a legitimate purpose. It is inadmissible to process the data irrelevant to the purpose.

4. Fourth principle: Data Validity and Accuracy ("Accuracy")

Data must be valid and accurate and, where necessary, updated. Data which is collected without legal grounds and irrelevant to processing purposes, shall be blocked, deleted, or destroyed;

Guideline

Authorized persons should ensure that the data is up-to-date and complete, as incomplete and outdated information can lead to inaccurate data processing. In some cases, it may be necessary to inform the data subject that the incompletely processed data has been corrected.

5. Fifth principle: Term of storage of data

Data may be stored only for the period and volume which is necessary for achieving data processing purposes. After achieving the data processing purposes, the data shall be interlocked, deleted or destroyed, or stored in a form to exclude a person's identification, unless otherwise determined by the Law.

Guideline

The authorized person shall inform the data subject about the term of data storage prescribed by the legislation of Georgia. If the legislation does not stipulate the term of data storage, then the term of storage should be strictly minimal. To prevent unauthorized storage of personal data for an extended period of time, the authorized person should set a deadline after which the data will be deleted or periodically reviewed.

6. Sixth principle: Data security and confidentiality

Data processing should be done in manner which protects data security from unauthorized and illegal use.

Guideline

Data security refers to the ability of the network or information system to withstand accidental events, unlawful and harmful acts that endanger the access, authenticity, integrity or confidentiality of archived or transmitted data.

- Authorized person shall be obliged to take such organisational and technical measures, which ensure the protection of data against accidental or unlawful destruction, change, disclosure, access, or any other form of unlawful use, and accidental or unlawful loss.

- Measures taken for data protection shall be adequate to the risks related to the processing of data.

- Authorised person and any employee of European School, who participates in the processing of data, shall be obliged not to exceed the scope of powers granted to him/her. In addition, they shall be obliged to protect data secrecy, even after the termination of the term of his/her office.

- Measures for data protection shall be defined by the legislation of Georgia.

7. Seventh principle: Accountability

The school and persons authorized for data processing are responsible for ensuring that the school's personal data protection policy complies with applicable Georgian legislation.

Guideline

- *The responsibilities and functions of the persons authorized to process personal data shall be determined by the order of the school principal;*

- *The school principal approves the plan for implementation of personal data protection policy for each school year. School teachers, members of Supervisory Board and contractors should receive appropriate training to understand and implement the requirements of personal data protection law;*

- *The order of school principal shall designate a person authorized by the European School to provide resources and support for meeting the requirements of personal data protection;*

- *The order of school principal shall designate persons who will supervise the supervision of personal data protection legislation;*

- The school principal approves the training plan; Documentation of personal data processing and personal data protection impact assessment.

4. Special category personal data

The processing of special categories of personal data is associated with a high risk of limiting the data subject's fundamental rights and freedoms. Special category data shall be processed with the consent of the data subject when:

a) processing of the data relating to conviction and state of health is necessary, given the labour obligations and relations, including for making a decision on the employment;
b) data processing is necessary to protect the vital interests of a data subject or a third party and the data subject is physically or legally incapable of giving his/her consent to the processing of data;
c) the data are processed in order to protect public health, the health of a natural person by health care institutions (employees), and if this is necessary for the management or operation of the health care system;
d) a data subject has made public his/her data without the explicit prohibition of their use;
e) the data is processed in cases provided for by the Law of Georgia on International Protection;
f) the data is processed to operate a unified migration data analytic system;
g) the data is processed for the purpose of realizing the right of education of persons with special educational needs.
h) Data is processed for the purpose of discussing the issue referred to in Article 11, paragraph 2 of the Law of Georgia on violence against women and/or elimination of domestic violence, protection and support of victims of violence.

3. If data processing is carried out under the second paragraph of this article, it shall be prohibited to make the data public and disclose the data to a third party without the consent of the data subject.

5. Rights of a Data Subject

The data subject has the following rights in relation to processing of his/her data:

1. The data subject has the right to receive information on data processing which includes:

- *Data on person authorized by the school on data processing;*
- *Purpose and legal basis for data processing;*
- *Definition of legitimate interest in data processing from school;*
- *Information about the transfer of data to third parties;*
- *Revoking consent given for data processing;*
- *Apply to the State Inspector of Georgia for data processing;*
- *Further information on further use of processed data;*
- *Has the right to request from the school the clarification on the volume of data processing;*
- *Request to update or correct inaccurate or incomplete data;*
- *Right to delete, destroy data. This right is not absolute and may be exercised only in certain cases;*
- *Request from the school to transfer the transmitted data to other persons;*
- *The data subject has the right to appeal. He /she has the right to appeal to the State Inspector or the court. A data subject shall have the right to request from the reviewing authority to block data before taking a decision.*
- *The data subject has the right to request termination of data processing. This right is not absolute and only applies in certain cases.*

6. Photography and digital images and their publication

Photography and the use of digital devices to record school activities are an integral part of school community life. While participating in school life, all subjects related to the school may have photo (analog / digital) and film (analog / digital) recording devices. The use of personal data in these formats aims to build and communicate with the school community.

Examples of where photography or film can be used:

- *Recording pictures during employee activities;*
- *Presentation of images in study materials or published in digital or analogue form with internal digital sign marking or on message / presentation boards;*
- *To check the school staff;*
- *Recording of school events such as training events, recruitment events, open days and symposia via the school website or direct digital stream;*

- *Keep up-to-date records of school achievements and public events in the form of digital media (photography / film) which is stored on the school's website and other social media (Facebook, Instagram, Twitter, etc.).*

The image will appear at all events where digital images are recorded for the purpose of building a school community. The data subject must assume that all events in the community involve the recording of digital images.

All school staff should be familiar with the school's child protection policy as a guide when it is advisable to take digital images of children.

Digital images of children depicting, for example, children's academic performance, sports achievement, and art achievements and events are defined in accordance with the school's child protection policy. Where the data subject is named, they have the right to appeal.

7. Social media

Social media (Facebook, Instagram, WhatsApp. LinkedIn, Dropbox and etc) can be used by school staff in connection with school activities. Personal social media accounts may not be used for school activities.

The school's public relations manager is responsible for the school's social media communication. In exceptional cases, if it is necessary to use personal accounts, the school employee must obtain the prior consent of the public relations manager. If approved, the school's personal data protection policy should be followed.

8. Use of personal mobile phones, tablets, laptops, computers or other mobile devices

It is forbidden to copy and store personal data collected by the school on personal devices such as personal cell phones, tablets, laptops, computers or others.

9. Video surveillance in the European school building

Video surveillance is conducted in the European school building (as well as on the outer perimeter of the building, entrances, corridors, classrooms and work rooms), the yard and playgrounds for sole purposes of protecting juveniles from harmful impact, juvenile safety and also for exam / testing purposes.

The location of the video surveillance must include a relevant warning sign. In this case, a data subject shall be considered to be informed about the processing of his/her data.
Workplace surveillance system may be installed only in exceptional cases, if it is necessary for human security and property protection, as well as for exam / test purposes and if these purposes may not be reached by other means.
Video surveillance shall be inadmissible in changing rooms and public places of hygiene.
School Technical Support Center shall be obliged to create a filing system, designated for the storage of video recordings. In addition to the recordings (images/voice), the system shall contain information about the date, place, and time of data processing.
The term of storage of data obtained under this Rule shall be determined by the legislation of Georgia.

10. Sharing of personal data

Without the legal basis, it is inadmissible to share personal data of school community members with third parties outside the school. State agencies may be legally empowered to request from school the personal data of employees. In every such case, the authorized person must check the legality of the claim.

11. Data processing for direct marketing purposes

Data, obtained from publicly available sources, may be processed for direct marketing purposes.

Regardless of the purpose of data collection, the following data may be processed for direct marketing purposes: a name (names), address, telephone number, e-mail address, fax number.
Any data may be processed for direct marketing purposes on the basis of written consent given by a data subject as prescribed by legislation of Georgia.
A data subject shall have the right to request at any time a data processor to discontinue use of his/her data for direct marketing purposes.
A data processor shall be obliged to stop the processing of data for direct marketing purposes and/or shall ensure that an authorised person stops data processing for direct marketing purposes within not later than 10 working days of receipt of the request from a data subject.
While processing the data for direct marketing purposes, a data processor shall be obliged to notify a data subject of the right under the article 5 of this policy and shall ensure that the data subject has the possibility to request termination of data processing for direct marketing purposes in the same manner as the direct marketing is carried out, and/or to determine available and adequate means to request termination of data processing for direct marketing purposes.

12. Personal Data Breach Notification

In accordance with this Policy and the Law on Personal Data Protection, in the event of a data breach, the school shall take measures to manage the breach of personal data protection. Where there is a high risk for a data subject's rights and freedoms, infringement information may be reported to local authorities and the State Inspector of Personal Data Protection.

All school employees, contractors and those who process, use, manage personal data, are obliged to report the date or time of the data breach, and details of the incident to the data protection supervisor and the school principal.

13. Obligations of European School

If the data are disclosed, a data processor and an authorised person shall be obliged to ensure the registration of the following information: which data have been disclosed, to whom, when and on what legal grounds. This information shall be stored together with the data on a data subject, during the storage period.

14. Final provisions

Changes and additions to this Policy may be made by order of the Director of the European School.

Data Protection Statement & Parental Consent Form

(Consent to Processing or Publication of Personally Identifiable Data, Photos and Video and Sound Recordings of Students)

Please read the Parent Information attached prior to completing this form.

1) Publication of personal data

In suitable cases we plan to make accessible to broader public information on events in the sphere of our school. This concerns also personal data. We therefore intend to publish text and photo material generated in particular within the framework of the pedagogic work or school events. What comes into consideration apart from class pictures is, by way of example, personal information on school outings, class trips, school exchanges, (sports) competitions, educational projects or the Open Day.

I/we hereby consent to publication of the above personal data including photo material of the person designated above in the following media: *Please tick box!*

☐ information board in school building
☐ annual report/school yearbook
☐ press (print version)
☐ World Wide Web (Internet) under school's homepage www.europeanschool.ge, Facebook, Instagram

Please refer to information below!

☐ photos
☐ other personal data (surname, first name, form)

Granting of rights of photos will not be remunerated and shall also cover the right to editing provided such editing does not entail disfiguring. Class pictures will be included in the annual report only with alphabetical lists of names; for the rest, photos will remain without name identification.

2) Photographs of Students:

The school maintains a database of photographs of school events held over years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Photographs may be published on our school website or in brochures, yearbooks, newsletters, local and national newspapers and similar school related productions. In the case of website photographs, student names will not appear on the website as a caption to the picture. If you or your child wish to have his/her photograph removed from the

school website, brochure, yearbooks, newsletters etc. at any time, you should write to the school principal.

If you are happy to have your child's photograph taken as part of school activities and included in all such records, ***Please tick box*** ☒

If you would prefer not to have your child's photograph taken and included in such records, ***Please tick box*** ☐

3) Making of Video Recordings

I/we hereby consent to the making of video recordings during classes:
Please tick box!

☐ video recording in sports lessons
☐ video recording in school events
☐ sound recording in school events

The recordings will be used only during classes but not for performance ratings of student behavior and not passed on to third parties.

This consent may be withdrawn anytime for the future. Such withdrawal may refer also only to a part of the media or the type of data or photos. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. In the case of printed material, consent shall not be withdrawable once the printing order has been made. In the event of withdrawal, the pertinent data will in future no longer be used for the purposes mentioned above and erased from the pertinent Internet offers without delay. If consent is not withdrawn, it shall be valid for the duration of school attendance with the data being erased upon the end of school attendance. Video recordings will be erased upon completion of the work assignment but no later than the end of the school year or the end of the course level or when the above purpose has been reached.
Consent is given on a voluntary basis. No disadvantages shall accrue from refusal to giving your consent or withdrawing it.

Vis-a-vis the school you have the right of access to your personal data; you moreover have the right to rectification, erasure or restriction, and the right to object to processing and a right to data portability. You moreover have the right to lodge a complaint with the data protection supervisory authority, the State Inspector of Georgia.

<u>Publication in the Internet / Data Protection Note:</u>
In the event of publication in the Internet, the personally identifiable data (including photos) may be retrieved and stored anytime and for an unlimited period of time worldwide. Such data may hence

also be retrieved via so-called search engines. In such an event, it cannot be excluded that other persons or companies may link the data with other personal data available in the Internet, thereby producing a personality profile, altering data or using them for other purposes.

Data Protection Policy:
A copy of the full Data Protection Policy is available upon request from the school office. You and your child should read it carefully. Please sign this document to state that you consent to your data/your child's data being collected, processed and used in accordance the school's Data Protection Policy during the course of their time as a student in the school.

Student:		
[place and date]		
	and	
[parent's or legal guardian's signature]		[above age 14: Student's signature]

Personal Data Statement and Employee Consent Form

(Consent to Processing or Publication of Personally Identifiable Data of Employees)

1) Personal Data Processing/Storage

1.1 The school intends to process/storage following personal data of present and prospective employees, over the course of recruitment or employment:

1. Biographical Information;
2. Identification Information;
3. Education Details;
4. Contact Information;
5. Criminal Record Certificate and Health information (e.g. medical certificates submitted to us);
6. Photograph;
7. Bank Account information;
8. Work Position Information;
9. Payroll information, including salary.
10. Performance information, including management metrics, appraisals, feedback.
11. Building Access/leave Data.

1.2 The above mentioned personal data may be shared to third parties for school to implement legal duties. Employee Data may be transferred to third parties for the following employment purposes: manage employee benefits, including administering remuneration, insurance, payroll, pensions and other employee benefits and tax, including disclosure to accountants, hosting mobile service providers, governmental bodies in cases provided for by law. To facilitate employee's professional development, the school may give personal data to group of training provider companies.

1.3 HR may use personal data to contact employee and manage relationship with them, oversee compliance with policies and applicable law, assess performance, for promotions and appraisals and for training purposes .To manage recruitment of employees, including legal eligibility for work, hires, promotion and succession planning.

1.4 Personal data of present employees is processed/stored for the duration of the employment contract.

1.5 Personal Data of past employees is processed/stored no longer than necessary for the purpose for which it was obtained. In any case, no longer than 70 years.

1.6 Personal Data of potential employees is processed/stored no longer than necessary for the purpose for which it was obtained. In any case, no longer than 1 year.

1.7 Maintaining the security and integrity of employee personal data is a high priority and we endeavor to maintain appropriate administrative, technical, personnel and physical measures to safeguard personal data against loss, theft, and unauthorized uses or modifications. Therefore, hardcopy of personal data is stored/held in store room and is safeguarded from unauthorized uses. To safeguard data, school controls access to buildings, rooms, cabinets for 24 hours where data, computers, media or hardcopy materials are held.

1.8 Personal data is stored in authorized person's computer system, which is locked with a password. Servers are protected by power surge protection systems through line-interactive uninterruptible power supply (UPS) systems. Users have restricted access to data files. The school ICT controls access to files, folders or entire hard drives encryption. To safeguard data, school controls access to buildings, rooms, cabinets for 24 hours where data, computers, media or hardcopy materials are held.

2) Personal Data Publication

The school maintains a database of employee photographs. It has become customary to take photos of employees and publish them on school website in order to promote workplace culture, to convey employer branding image and give information to potential employees for organizational structure.

In case you consent to publication of above mentioned personal data, please tick a corresponding box:

☐ If you are happy to have your photograph published on the school website www.europeanschool.ge, or other social networks

Please tick box!

☐ Photograph

☐ Biographic Information

I hereby consent to the above policy of processing/storage of my personal Data.

Employee:
[place and date]
[Employee's signature]

Appendix 3

Procedure for recording and reporting personal data breach (incident)

Preamble

This document is drawn up based on Personal Data Policy of the European School. The purpose of this document is to define the procedures for recording violations related to the personal data at the European school and response of the person responsible for supervision of personal data at school.

1. Definition of terms

The terms used in this Rule shall have the same meaning as in the European School Personal Data Protection Policy and the European School Personal Data Risk Assessment Document.

2. Obligations of school staff

School staff are obliged to record incidents of breach or alleged breach of personal data of data subject and report to the person conducting supervision of personal data.

In case if, there is a high risk for a data subject's rights and freedoms, information about personal data breach should be reported to local authorities and the State Inspector of Personal Data Protection. The personal data supervisor is responsible for sending the notification.

The incident notification should include details of the incident, the date and time when it was committed (Appendix - Incident reporting form).

The supervisor is authorized to advise the school staff if necessary.

Incident reporting form

Name and surname of the school employee who reported the incident	
Time and date of the incident	
Details of the incident	
Does the incident present a high risk of violating the data subject's rights and freedoms?	
Yes	
No	
Please justify	
Need for consultation	
Yes	
No	
Name, surname and position of the consultant	
What was the consultation about?	
Decision made	
Is it necessary to inform State Inspector or local authorities?	
Yes	
No	
Employee signature	
Date of decision making	