Processing compliance methodology

personal data in the school environment

This methodology contains only general principles on the protection of children's privacy and data,

parents and legal representatives and their application in the field of education.

Steps to comply with GDPR

Basic principles and rights

Personal data protection policy

1. The best interest of the child - they must follow this principle

all entities that make decisions concerning children.

It also applies to parents who should know this principle

apply naturally, however, if there is a contradiction between them

interest and interests of the child, the court should decide. consequently

2. The child's right to privacy - no child may be

subject to arbitrary or unlawful interference with

privacy, family, home or correspondence, nor

by an unlawful attack on his honor or reputation. It can happen

to situations where the best interests of the child and the right to privacy are

contradictions. In such cases, it is possible that the right to

the protection of privacy (ie also personal data) must give way

the principle of the best interest of the child, e.g. if the teacher reveals

personal data to a social worker to protect the child if

he is suspected of neglect or

abuse.

3. Representation - children are needed to exercise most of the rights

legal representation. However, this does not mean that the position of the parent

has absolute priority over the position of the child. Children

gradually they can contribute to the adoption of decisions that affect them

concern, including their personal data. The initial level is

the right to be asked for an opinion.

Processing security starts with the basics

principles. When applying the principles and rules of personal protection

schools and school facilities must pay special attention to data

attention to the position of the child, because they always have to

respect his best interest.

- Personal data must be processed fairly,

transparent and legal.

- They should only be obtained for a specific and lawful purpose.

- All data must be adequate, relevant and limited

to the necessary extent, it is the so-called principle of minimization.

Do not process data that you do not need and only have

to be sure with yourself.

- They must be correct and continuously updated.

- Personal data cannot be stored longer than it allows

the purpose of their processing.

- Personal data must be protected.

- The operator is responsible for compliance with these principles.

1. Approach the new legislation

rationally and with prudence

The new legislation does not have a revolutionary nature, it follows on from the previous law.

The news that it brings is mainly the obligation to keep records on processing

activities and the obligation to designate a responsible person, information obligation,

reporting obligation to the authority in the event of a security breach

personal data, extension of the rights of the persons concerned, assessment of the impact it should have

character of exceptionality and should not apply to such a wide spectrum

operators.

Common personal data

•

•

•

•

•

•

The photo

Name, surname, address

Email, phone number

Date of birth

Identification number

A child's mark

•

•

•

•

•

•

•

Sensitive personal data,

the so-called a special category of personal

data according to Art. 9 GDPR

racial or ethnic origin,

political views,

religious or philosophical

belief or membership

in trade unions,

genetic data,

biometric data for an individual

identification of a natural person,

health data,

data related to sex life

or sexual orientation.

2. Differentiate processing based on the law a

consent

You don't have to worry about processing personal data based on the law, especially the school one

of the law and its related decrees. Legal obligation takes precedence

attitude and opinion of the person concerned. In the case of legal processing, it is not

consent to the processing of personal data is neither necessary nor appropriate.

It is necessary to distinguish processing beyond the scope of the law, that is, when the law directly

he does not remember a specific situation, an example of which is the publication of a photograph

student on the school's website. Schools and school facilities should check in which

cases they process personal data without being required to do so by law.

3. On what basis does the school process personal data?

Consent - used when you give a child or their parent real choice and control over how their

personal information. Despite the fact that GDPR consent allows use, it does not mean that the processing is in accordance

with it

with the requirements of the personal data protection legislation. The school must always choose the appropriate legal basis

for processing a

has other reasonable reasons for processing personal data.

Consent must be free, specific, informed, unambiguous and demonstrable. Consent is given by purpose. Upon appeal consent, the school is obliged to delete the student's data.

Appropriate legal basis: Photographs, publication of works of art at an exhibition together with data (name, surname, class);

Legitimate interest – a proportionality test is required, where the GDPR warns that you have to deal with interests that basic rights and freedoms of the person concerned, which require the protection of personal data, especially if the person concerned is

a child. It does not apply to processing carried out by public authorities in the performance of their tasks. Together with your consent at least

legal basis used.

Appropriate legal basis: camera system (property protection);

Contract - processing must be necessary for the purpose of fulfilling the contract, e.g. application for the issuance of a license/card (here it can be

consent is also a suitable legal basis), dual education system (teaching contract);

Vital interest - it is suitable to use only in exceptional or life-threatening situations, e.g. in an accident or

child injuries;

Legal obligation – the school must find an obligation in the relevant law that requires the processing of personal data and find out

whether the processing of personal data is necessary to fulfill a legal obligation. Appropriate question before using this legal basis: Do I need this data to fulfill a legal obligation, for example the obligation to insure the child, to keep the child's personal file?

Public interest - the processing of personal data must be necessary to fulfill a task in the public interest or in connection with it with the exercise of public authority. The school must find out what role it fulfills in the public interest, while such a role (purpose) should also follow

by law or decree. However, it is not strictly defined as a legal obligation, for example, the obligation to conduct pedagogical

work

documentation. Appropriate question before using this legal basis: I need this data to ensure the running of the school,

education?

4. Information obligation

In the framework of providing information to children and their legal representatives, special emphasis should be placed on

providing layered information based on the use of simple, concise language that is

easy to understand. A shorter notice should contain the basic information that is provided at

obtaining personal data, to which a more detailed notice should be attached, for example

by linking to a school or school facility website, and stating that the information

you can also learn about the processing of personal data in person, for example from the responsible person, the director

kindergartens etc. It is also appropriate to place the information obligation in the premises of the school and school facilities,

for example, on the bulletin board at the entrance to the building or in the changing rooms.

Information must always be provided to the legal representative and, after reaching mental capacity, also

to the child (in a suitable form, for example at the beginning of the school year, or as part of some teaching

hours).

It is particularly important to be properly informed about the rights of the person concerned, such as the right of access,

which is usually carried out by the legal representative, but always in the interest of the child. A child may be entitled to

exercise

his or her own rights (e.g. special regulation in the Education Act according to § 144 paragraph 1 letter m) the child has the

right

for information regarding his person and his educational results...). Rights of affected persons

the school arranges properly and on time (without unnecessary delay within 1 month at the latest). If to some right

cannot be complied with, the person concerned is informed of the reasons.

You can find a sample information obligation at

https://dataprotection.gov.sk/uoou/sk/content/vzor-informacnej-povinnosti-pre-zamestnanca

5. Responsible person

Schools

a

school

devices

perhaps

in terms of the GDPR, to be designated as public authorities,

as in certain situations they decide on

rights and obligations of natural persons, as well as from

title of the position of their founder.

For this reason, all schools and school

facilities have an obligation to designate a responsible person

report the person and their contact information to the office.

6. Records of processing

activities

School

are u

leads

records

on processing activities and ensures

their continuous updating. It does not take place in the office

no registration. The records are for the case

proceedings on the protection of personal data or

controls, but they are also a good aid for revision

access rights to individual purposes

of processing, i.e. what employee has

to what purpose of processing access.

Sample of records of processing activities

you will find

https://dataprotection.gov.sk/uoou/sk/content/vzorzaznamov-o-spracovatelskych-cinnostiach

7. Security

Adoption of adequate security measures

a)

Technical measures - securing the object using mechanical means of prevention (lockable

doors, windows, grilles), safe storage of physical carriers of personal data (storage of paper documents in

lockable cabinets or safes), a device for destroying physical carriers of personal data (e.g.

device

on the

shredding

documents),

the rules

access

third parties

persons

to personal data, identification, authentication and authorization of persons, use of logos, firewall, protection against

threats coming from a publicly accessible computer network (hacker attack), rules for downloading files from

of a publicly accessible computer network, protection against spam, backup, etc.

b)

Organizational measures - education, determination of instructions that the person is obliged to apply during processing

personal data, definition of personal data to which a specific person should have access for the purpose of fulfilling it

duties or tasks, password management, control of access to the facility and protected premises of the operator

(e.g. through technical and personnel measures), the regime of maintenance and cleaning of the protected

premises, rules for processing personal data outside the protected area, treatment of employees

mobile phones, laptops and their protection, use of e-mails only for work purposes, control activity

of the operator focused on compliance with the security measures taken, specifying the method, form and

periodicity of its implementation, informing the affected persons about the control mechanism, if it is with the operator

introduced (extent of control and methods of its implementation).

Art. 24, 25, 32 GDPR – risk analysis. Art. 35 GDPR – impact assessment, from which the obligation to prepare an assessment

influence is regulated in Art. 35 par. 3 GDPR.

GDPR defines some security measures - anonymization, encryption (for example, if they are sent by e-mail

sensitive data to the parent), pseudonymization, which the operator can voluntarily introduce into its processes.

What do security mean?

measures?

• The school protects the personal data it processes against misuse by appropriate and available means. Above all

stores personal data in places, in the school environment or in a system to which they have limited access only

persons designated and authorized by the director.

• The school will take measures so that the school director or his representative has an overview of the processing of personal

data

person or responsible person. Such measures include, in particular, giving instructions on how to dispose safely

with personal data for teaching and non-teaching staff, orally or in writing, determination

work duties in the employment contract, as well as the determination of instructions within contracts concluded with third

parties,

for example, providing personal data disposal services.

• The school continuously evaluates the adopted personal data protection rules, as the personal data protection system

is a living mechanism. Some practices may turn out to be outdated or unproven.

• Each employee respects their nature when dealing with personal data, and adapts actions with it

connected. In particular, the employee does not disclose personal data without verifying that such a procedure is possible,

does not make it available

data to persons who do not demonstrate the right to obtain them. The employee will always try to provide basic information

of the person concerned; otherwise, he will refer the affected person to the responsible person or the school director.

• The school actively cooperates with the responsible person when processing personal data.

• The school immediately solves every security incident related to the protection of personal data, and that in cooperation with the responsible person and rather a record of him.

• Pedagogical documentation is permanently stored in lockable cabinets in the school offices. Class teacher they are loaned only for the time necessary to make entries. Student data should not be exported from school, provide copies to strangers and the like.

• Personal data kept in electronic form, for example in the case of an electronic student book, are kept only in a secure system. Individual teachers and other authorized persons have access to this system by school principals, only on the basis of a unique login name and password and only within the scope of the given authority by functional classification. Passwords must be protected and not shared with anyone. When working with electronic records the authorized person may not leave the computer without logging out. Parents and students have secure remote access exclusively to your own data, based on the assigned password, handed over individually to the class teacher.

• Personal files of employees are also kept securely in lockers, only the director has access to them school, or his representative and the personnel and payroll department.

• Pupil lists are not published or provided to other natural persons without the consent of legal representatives or to legal entities or state bodies that are not required to do so by law.

• If forms and templates are used for maintaining pedagogical documentation, it is necessary to check whether they don't ask for unnecessary data.

• If an employee discovers a violation of personal data protection, he will immediately prevent another unauthorized one handling of personal data and reports this fact to the school director or a responsible person.

• The school director or a responsible person is obliged to inform the employees about all significant facts and procedures in connection with the processing of personal data. They will ensure that they are properly instructed on rights and obligations in the processing of personal data and, as far as possible, provide education and retraining in the field of personal data protection.

• It is not recommended for teachers to use their own computer while working at home. On the one hand, for the reason that a

private computer resides

mostly used by other members of the household, but also cannot sufficiently ensure the safety of one's own devices. The use of service equipment should be safer. It is up to the school principal to determine the rules use of business mobile phones, tablets or laptops.

• Obligations and recommendations in the processing of personal data can be incorporated, for example, into school regulations,

work order, internal directive for the protection of personal data.

• Non-discrimination – some data, for example data related to race or disability, may discriminate against a child. These the information is obtained in order to ensure that the school or school facility is informed about students with cultural, language or economic difficulties and it is necessary to pay extra attention to them. In processing such information would the criteria should have been the principle of the best interest of the child and the principle of purpose limitation. There should be no mention of the student's religion

take no unnecessary conclusion in case the data is needed only for administrative purposes (e.g. taking classes religion, preference for certain foods). Information about the assets and income of the child's family can also be a source discrimination, but they are processed in the interest of the child, for example, if a parent requests an allowance or a reduction of the fee obligation.

All information that could lead to discrimination must be protected by appropriate security measures, for example processing them in separate files, by qualified and designated persons, under the condition of confidentiality and next.

• Access to data – the data listed in the student's personal file must be subject to strict confidentiality. Access the data must be provided to legal guardians (a child if mature enough) and must be strictly regulated and limited to school authorities, school inspectors, health workers, social workers and law enforcement authorities.

In some cases, providing data in an anonymized form will also suffice. In the opinion of the office of schools and school facilities

data from the pupil's documentation are authorized to be provided only to persons who prove their claim on the basis of authorization

established by a special law. It is always necessary to consider all risks when providing cooperation, to prevent unauthorized ones

to inspect and read the student's documentation, to prevent unauthorized copying, data transfer, modification or deletion records and to introduce measures that will allow to determine and verify to whom the data has been made available. The main entities with which you school

exchange data are other state authorities, other schools and school facilities and social protection authorities. The most important aspects

providing data is to make sure whether the school is authorized to do so (based on the law, public interest, consent), or where they have

to be data given guarantees their security, to make sure that the persons concerned are informed about the recipients. If data is sent

by e-mail, make sure that these are your work e-mails, or use encryption, in case you make a mistake in the addressee there will be no potential risk to the rights of the persons concerned. Do not provide by phone, e-mail or in person without verification,

that you are communicating sensitive data with an authorized person.

• Not every teacher or non-pedagogical employee has access to all data processed by the school, but only to data that he absolutely needs for his work. For example, a class teacher has access to the data of students and their parents only within him

of the assigned class, only the educational advisor has access to data on the student's health, examination reports and reports,

senior teaching staff, class teacher. The school principal, deputy principal, control authorities will probably have access to the entire database. A parent only has the right to access data about their child.

9. Brokerage agreements - required

fulfillment of requirements according to Art. 28 GDPR. As long as it

will not be possible due to the other's disapproval

of the contracting party, it will be more appropriate to terminate

cooperation

with

like this

subjects,

on the grounds that it does not meet GDPR requirements.

School, or school facility is responsible for

processing of personal data, even if it is

intermediary involved in the processing.

10. Notification obligation in case

personal data protection violations - school

must without undue delay, no later than 72

hours after this fact

she learned

to announce

violation

protection

personal data of the office, with the exception of the case,

when a violation is not likely

will lead to a risk to the rights and freedoms of individuals

persons. However, every incident is worth having

documented, even if it is not reported to the authority.

In case of high risk, the school must

also notify the affected persons. Form for

notification is published on the website of the office.

11. Data retention and archiving period

period - in accordance with the received registration

in order and according to the deadlines set

by a special law. Personal data

they keep only for the time that is necessary

to achieve the purpose of processing, incl

archiving.

12. Performed by a school or school facility

cross-border processing or transfers

personal data to third countries? Free movement

personal data between the Slovak Republic and

is guaranteed by EU member states; basic

assuming the processing of personal data at

any processing operation with personal

data, both within the EU and outside it, is

fulfillment of the principle of legality, so it must be

based on a legal legal basis according to

Art. 6 par. 1 GDPR.

13.

Voluntary

option

certifications,

accreditation, introduction of the code of conduct.