PROTECTION OF PERSONAL DATA (GUIDELINES FOR EDUCATIONAL INSTITUTIONS AND STUDENTS)

ALJOŠA POLAJŽAR
University of Maribor, Faculty of Law, Maribor, Slovenia
aljosa.polajzar@um.si

Abstract The author discusses the protection of personal data by educational institutions in the context of the education process. The author introduces and explains the basic concepts in this area. It then goes on to discuss the fundamental principles of personal data protection that are relevant for any type of personal data processing, e.g. the data minimisation principle, according to which only data that are strictly necessary for the purpose of the processing may be processed. Compliance with these principles is essential for the lawful processing of personal data. Alongside the principles, each processing must be based on one of the lawful bases under the General Data Protection Regulation (GDPR). The obligations of the data controller (educational institutions) and the rights of data subjects (students) are also addressed. It is particularly important that the institution takes all necessary preventive and technological measures to ensure adequate processing. Particular diligence is also needed when dealing with special types of personal data. Finally, the consequences of possible breaches and the functioning of the supervisory authority, to which students can also turn in case of irregularities, are also highlighted.

Keywords:
personal data protection,
General Data Protection Regulation (GDPR),
data minimisation principle,
consent of the data subject,
obligations of the controller,
rights of the data subject

University of Maribor Press

DOI https://doi.org/10.18690/um.1.2023.3
ISBN 978-961-286-693-8

1 Introduction and fundamental concepts[1]

1.1 Introduction

In the area of e-learning, strict compliance with the rules related to the protection of personal data is essential. In online environments, individuals share a large amount of information about themselves, for example: age, email address, personal name, residential address, personal interests, etc. It is crucial that those who gain access to this information in the course of delivering education, treat this information in accordance with all the applicable rules (regarding the permissible handling, storage, processing, sharing, etc. of this data).

The European Union (EU) has adopted uniform rules on the protection of individuals with regard to the processing of personal data under a directly binding legal act: the General Data Protection Regulation (GDPR). The Regulation protects the fundamental rights and freedoms of individuals and, in particular, their right to the protection of personal data.[2] All educational institutions (and all their employees) operating in the EU must also comply with GDPR when processing personal data (e.g. of students). These rules comprehensively regulate the protection of personal data and apply uniformly regardless of the EU country (e.g. the same in Slovenia, France, Poland, Germany, etc.).[3]

It is true that, in the context of the GDPR, personal data is also protected (in each individual country) under the law(s) adopted by each individual EU country for this purpose. Similarly, educational (and other) institutions may also adopt various internal acts which may regulate in more detail the protection of personal data.

[1] This part of the manual was prepared by Aljoša Polajžar. The legal content is taken from the text of the provisions of the current General Data Protection Regulation (GDPR). Full name of the source: 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) (Text with EEA relevance), Official Journal L 119, available at URL: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679 (accessed 16.6.2021).
Except where specifically indicated by a footnote, illustrations, possible practical examples and advice/guidance for educational institutions and students are provided by the author.

[2] Article 1, paragraph 2 of the General Data Protection Regulation (GDPR).

[3] The Information Commissioner of the Republic of Slovenia also emphasises the importance of the GDPR for the protection of personal data in its guidelines – see: Information Commissioner, 2021, p. 5. For more on "regulation" as a generally binding EU legal act, see Borchardt, Klaus-Dieter, 2016, p. 92.

However, we would like to stress that all such acts (e.g. national laws, university regulations, etc.) must always be in line with the European regulation (GDPR). This means that they must not provide for a lower level of protection of the personal data of individuals (e.g. students) than under the GDPR, or deprive them of their rights guaranteed by the GDPR.[4] Knowledge of the common, uniform European regulation is therefore the basis for the protection of personal data in the context of each EU country and the educational institutions operating in it. For this reason, the present Manual is also based exclusively on the uniform European regulation under the GDPR.

1.2 Fundamental concepts

At the outset, it is necessary to define the fundamental concepts related to the protection of personal data:

- **"personal data"** means any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[5]

In other words, we are dealing with personal data when this information (data) is linked to a specific identifiable natural person. This information means "knowledge" about the person to whom it relates (e.g. a student's ID card number, place of birth, personal interests, email address, telephone number, IP address, etc.). In the context of our Manual, it is primarily students who will be the data subjects to whom personal data relates. Student's personal data must be adequately protected by the educational institutions.[6]

[4] This follows from a fundamental general principle of EU law – the principle of primacy. See Borchardt, Klaus-Dieter, 2016, pp. 128-130.
[5] Article 4, paragraph 1 of the General Data Protection Regulation (GDPR).
[6] See also Information Commissioner, 2021, p. 7.

We should also point out that certain categories of particularly sensitive personal data relating to an individual (e.g. data revealing racial or ethnic origin, political opinions, biometric data, etc.) are particularly protected.[7] The processing of such data is only possible under strict conditions (more on this in next chapters).

- **"processing of personal data"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[8]

Any handling (any activity) of information (personal data) in relation to a filing system of personal data, *or where automated processing occurs regardless of the existence of the filing system,* will constitute processing of that data.[9] It is therefore particularly important to know when personal data may be processed or collected, recorded, disseminated, etc.

In practice, automated processing means that personal data are processed by automated means using a personal computer, mobile device, etc. Non-automated or *manual processing* of personal data will also be subject to the GDPR where the data forming part of a collection or intended to form part of a collection (e.g. a specially structured file). A filing system, on the other hand, is any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.[10] Even documents in physical form may be arranged in such a way that they systematically collect a large amount of personal data that can be easily found in a consultation of that filing system.[11]

[7] European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 96.
[8] Article 4, paragraph 2 of the General Data Protection Regulation (GDPR).
[9] Information Commissioner, 2021, p. 7. See also Article 2, paragraph 1 of the General Data Protection Regulation (GDPR).
[10] Article 4, paragraph 6 of the General Data Protection Regulation (GDPR).
[11] European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 100.

- **"controllers" of personal data**: in light of the legal rules, educational institutions (and their employees on their behalf) will collect or process personal data of their students. In this light, educational institutions will be considered as "controllers" of personal data. Educational institutions are "controllers" of personal data because they alone or jointly with other bodies determine the purposes and means of the processing.[12]

However, personal data processors will often also be involved in the processing of personal data. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[13] For example, a processor will be a recruitment agency that processes personal data as a processor for other companies (which are data controllers of their employees' personal data). However, where that agency processes personal data of its own employees, it would be acting as a controller.[14]

- **"personal data breach"** in accordance with the GDPR, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[15]

All those involved in the educational process must take particular care to ensure that the above-mentioned breaches of personal data protection do not occur. For example, Article 82 of the GDPR provides that any individual who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to obtain compensation from the controller or processor for the damage suffered.

[12] Article 4, paragraph 7 of the General Data Protection Regulation (GDPR). See also: Information Commissioner, 2021, p. 6.
[13] Article 4, paragraph 8 of the General Data Protection Regulation (GDPR).
[14] European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 107-108.
[15] Article 4, paragraph 12 of the General Data Protection Regulation (GDPR).

2 Basic principles (rules) and grounds for the appropriate handling of personal data

2.1 Principles relating to the processing (handling) of personal data

In particular, personal data controllers (in our case, educational institutions and the employees within them who collect and process students' personal data) must take particular care to comply with the fundamental principles and rules of the GDPR. The most important fundamental principles common to all processing of personal data, which the study process providers should take into account when planning their activities, are:

- **"purpose limitation"** - personal data are collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes.[16]

In other words, this means that any collection or processing of personal data of students (e.g. collection of data on their foreign language skills, residential addresses, etc.) must clearly specify the explicit purpose of the data collection (e.g. the data is requested for the purpose of students' applications to participate in an international university project, for which excellent English language skills are required). This also means that the data collected may not be used for purposes other than those for which it was collected (e.g. the language proficiency data would be passed on to commercial providers of foreign language courses, etc.). The data may only be used (processed) for the purposes for which it was collected.[17]

- **"data minimisation principle"** - personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[18]

[16] Article 5, paragraph 1, point (b) of the General Data Protection Regulation (GDPR).
[17] See also: European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 122-125.
[18] Article 5, paragraph 1, point (c) of the General Data Protection Regulation (GDPR).

This means that before collecting or processing personal data, it is important to ask ourselves which personal data we absolutely need to fulfil our purpose. For example, if we are collecting applications from students to participate in an international research project, the necessary personal data could be previous work experience, foreign language skills, etc. As a general rule, however, it would not be necessary to collect and process students' data on their religion, financial situation, sexual orientation, etc., as these personal data are not relevant and necessary for the fulfilment of our purpose (selection of students to participate in an international research project). The data must be collected to the extent and in the manner that minimally interferes with the student's right to informational privacy.[19]

- **"storage limitation"** - personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.[20]

This principle means that personal data controllers (educational institutions) must set appropriate time limits for the retention of students' personal data collected for a specific purpose. For example, there is no reason why personal data of students collected for the purpose of distance education (e.g. videos of students' assignment answers, etc.) should be kept for a longer period of time than is necessary for the assessment of that knowledge. The same applies to specific personal data provided by students in order to apply for participation in an international project. There is no reason why this data (of non-selected students) should be kept for several years after the selection procedure has been completed.[21]

- **"integrity and confidentiality"** - personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[22]

[19] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 125-127.
[20] Article 5, paragraph 1, point (e) of the General Data Protection Regulation (GDPR).
[21] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 129-130.
[22] Article 5, paragraph 1, point (f) of the General Data Protection Regulation (GDPR).

In the light of this principle, it is essential that educational institutions choose technological solutions for the processing (storage, collection, etc.) of personal data that ensure adequate information security. Only in this way will the data collected from students (e.g. their email addresses, transaction account numbers, student ID numbers etc.) be protected against misuse by unauthorised third parties.[23]

- **"lawfulness, fairness and transparency"** - personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.[24]

This principle will be furtherly described below in the Manual, as **"lawfulness" refers** to the choice of the appropriate legal basis for the processing (e.g. the processing is based on the student's informed consent; it is necessary for compliance with a legal or contractual obligation of the educational institution, etc.).[25]

- **"transparency"** refers to the requirement to provide all necessary information to individuals (students) regarding the collection, processing of their personal data (e.g. who is collecting the data, who will process it, for what purposes, for how long, etc.) – see Chapter 3 of Part I of the Manual.[26]

2.2 Grounds for processing (student consent and other grounds)

Any processing of personal data must, inter alia, respect all of the aforementioned fundamental principles and be based on one of the specified legal bases under Article 6 of the GDPR. The following legal bases will be particularly relevant in the context of distance education:

- **The processing is necessary for compliance with a legal obligation to which the controller is subject**[27]

[23] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 131-134.
[24] Article 5, paragraph 1, point (a) of the General Data Protection Regulation (GDPR).
[25] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 117-118.
[26] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 118-122.
[27] Article 6, paragraph 1, points (c) and (e) of the General Data Protection Regulation (GDPR).

In certain cases, educational institutions are obliged to collect and process certain personal data of their students for the purpose of carrying out the study process. For example, for the purpose of carrying out education, it is necessary to keep a list of students registered for a particular exam (their personal names, registration ID number, sequential entry to the exam, etc.).[28]

– **The processing is necessary for the performance of a contract to which the data subject is a party**[29]

Educational institutions may also be linked to their students on a contractual basis (the student enters education on the basis of a contract). Again, educational institutions may process the personal data of students that are strictly necessary for the performance of this contract (e.g. the student's enrolment data, etc.).[30]

– **Consent of the data subject**[31]

One of the most important legal bases for processing personal data is consent. Under the GDPR, "data subject consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[32]

It is important to note that the data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal. The data subject shall be informed thereof before the consent is given. Consent shall be as easy to withdraw as to give.[33]

[28] See also Information Commissioner, 2020.
[29] Article 6, paragraph 1, point (b) of the General Data Protection Regulation (GDPR).
[30] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 151.
[31] Article 6, paragraph 1, point (a) of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 142-151.
[32] Article 4, paragraph 11 of the General Data Protection Regulation (GDPR).
[33] Article 7, paragraphs 2 and 3 of the General Data Protection Regulation (GDPR).

For example, students applying to participate in an international research project, etc., will normally be required to provide consent at the end of the form for the processing of the personal data provided for that specific purpose. In the present case, educational institutions will have to carefully follow all the above rules on consent and ensure that the student's consent is free, explicit and informed. The student should also be made aware of the possibility to withdraw consent afterwards.

2.3 Processing of special categories of personal data

We would also like to highlight Article 9 of the GDPR, which, in the light of the basic principles already outlined, lays down specific conditions for the processing of special types of (particularly sensitive) personal data[34], which may also be encountered in the course of the provision of education. The Article provides that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[35]

However, this rule does not apply if one of the specified exceptions under Article 9 of the GDPR applies. In the context of education, the relevant exception is under point (a), which provides that the prohibition does not apply where the data subject has given his or her explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the data subject may not derogate from that prohibition. Furthermore, the relevant ground under point (c) may be that the processing is necessary to protect the vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent. Also relevant is the exception under point (f) that processing is necessary for the establishment, exercise or defence of legal claims or whenever the courts are acting in their judicial capacity. The latter could be relevant in the case of a specific legal dispute between a student and an educational institution. Furthermore, in times of health crises the ground under point (i) may be relevant: processing is necessary for reasons of public interest in the

[34] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 96, 159-165.
[35] Article 9, paragraph 1 of the General Data Protection Regulation (GDPR).

field of public health, such as protection against serious cross-border health risks on the basis of Union law or the law of a Member State which provides for appropriate and specific measures to safeguard the rights and freedoms of the data subject. Finally, it is worth mentioning the ground under point (j), which may be relevant in the context of the performance of research: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR on the basis of Union or Member State law which is proportionate to the aim pursued, respects the essence of the right to data protection and ensures appropriate and specific measures to safeguard the data subject's fundamental rights and interests.[36]

2.4 Conclusion

The conditions that the processing is necessary for the performance of a contract (e.g. an education contract) or necessary for compliance with a legal obligation of the controller (e.g. the provision of education under a specific programme) may be particularly relevant at the time of distance education in the light of the epidemiological measures related to COVID-19. In such cases, the collection and processing of personal data through online classrooms may be necessary for conducting the educational process in certain cases (e.g. where it is not possible to conduct the examination in person, it may be necessary to have a video link between the professor and the student, etc.). [37]

However, we would like to stress that the basic principles of the processing of personal data (the principle of data minimisation, the principle of transparency, purpose limitation and storage limitation) should be respected or complied with in all cases by the providers of the educational process.

Therefore, as a general guideline for personal data controllers (educational institutions and their employees), it may serve to ask: Is there an adequate basis for collecting or processing students' personal data? Does the collection or processing respect the principles of data minimisation (only the data necessary for the purpose of processing are processed) and transparency (students are provided with all

[36] Article 9, paragraph 2 of the General Data Protection Regulation (GDPR).
[37] See, for example, its opinion on "Distance education and the protection of personal data" (Information Commissioner, 2020).

necessary information concerning the processing of their data)? Will the processing of personal data in any case be carried out in an appropriate technical and organisational manner to ensure its security (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)? In particular, when choosing technological solutions, it is important to bear in mind whether our legitimate purpose/objective (because of which we are collecting and processing personal data) could be achieved in a way that would be less intrusive into the students' right to privacy. [38]

3 Rights of individuals (students) and obligations of controllers (educational institutions)[39]

Data subjects (e.g. students enrolled in education) also have certain important rights relating to their personal data.

3.1 Rights exercised directly with the educational institution (data controller of students' personal data)

Right of access and information: the data subject has the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed and, where this is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

[38] On the importance of respecting the fundamental rules/principles of personal data protection, see also: Information Commissioner, 2021, pp. 8-9.

[39] This chapter is based on the provisions of the GDPR. As an example of the information provided by the University of Maribor regarding the protection of personal data, see for basic information: https://www.um.si/univerza/varstvo-osebnih-podatkov/Strani/default.aspx (accessed 1.6.2021) and for information regarding the rights of the individual: https://www.um.si/univerza/varstvo-osebnih-podatkov/Strani/Pravice-posameznika.aspx (accessed 16.6.2021). For more information on individuals' rights, see also the Information Commissioner's Guidelines (2021), pp. 10-17.

- where possible, the envisaged period of retention of the personal data or, if this is not possible, the criteria to be used to determine that period;
- the existence of a right to obtain from the controller the rectification or erasure of personal data or the restriction of the processing of personal data concerning the data subject, or the existence of a right to object to such processing;
- the right to lodge a complaint with the supervisory authority;
- where the personal data are not collected from the data subject, any available information concerning their source;
- the existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[40]

In practice, this means that it is important that the collection or processing of personal data is transparent (individuals must be informed in advance and have the right to request relevant information).

Right to rectification: the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.[41]

Right to erasure ("right to be forgotten")[42] : the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

[40] Article 15, paragraph 1 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 216-219.
[41] Article 16 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 219-221.
[42] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 221-227.

- the data subject withdraws the consent on the basis of which the processing is carried out and where there is no other legal basis for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data must be erased in order to comply with a legal obligation under EU or Member State law to which the controller is subject.[43]

However, an individual (e.g. a student) does not have the right to have his/her personal data forgotten or deleted if processing is necessary:

- to exercise the right to freedom of expression and information;
- for compliance with a legal obligation to process under EU law or the law of a Member State to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the field of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- to assert, exercise or defend legal claims.[44]

Right to restriction of processing:[45] The data subject has the right to obtain from the controller the restriction of processing where one of the following applies:

- the data subject contests the accuracy of the data for a period which allows the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject objects to the erasure of the personal data and requests instead the restriction of their use;
- the controller no longer needs the personal data for the purposes of the processing, but the data subject needs them for the establishment, exercise or defence of legal claims;

[43] Article 17, paragraph 1 of the General Data Protection Regulation (GDPR).
[44] Article 17, paragraph 3 of the General Data Protection Regulation (GDPR).
[45] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 227-228.

- the data subject has raised an objection to the processing, pending verification whether the legitimate grounds of the controller override those of the data subject.[46]

Where the processing of personal data has been restricted in accordance with these rules, such personal data (with the exception of their storage) shall be processed only with the consent of the data subject, or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person, or for important reasons in public interest of the EU or of a Member State.[47]

Right to object:[48] The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her based on point (e)[49] or (f)[50] of Article 6(1) of the GDPR, including profiling based on these provisions. The controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.[51] The data subject shall be explicitly informed of the right to object at the latest at the time of the first communication with him or her and shall be presented with this right clearly and separately from any other information.[52]

In practice, the student thus has the possibility to request the erasure, rectification or restriction of the processing of personal data that he or she has provided to the educational institution (provided that the conditions set out above are fulfilled). The student may have an interest in carrying out these actions in different situations. For example, if he or she so wishes, he or she may request the erasure of the personal data provided for the purpose of applying to participate in a research project for which he or she has not been selected. Similarly, if his/her personal data are

[46] Article 18, paragraph 1 of the General Data Protection Regulation (GDPR).
[47] Article 18, paragraph 2 of the General Data Protection Regulation (GDPR).
[48] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 229-233.
[49] The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
[50] The processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.
[51] Article 21, paragraph 1 of the General Data Protection Regulation (GDPR).
[52] Article 21, paragraph 4 of the General Data Protection Regulation (GDPR).

incorrectly indicated in the publications on the website of the educational institution (e.g. an error in the personal name of a student who participated in a particular project), he/she may request that this information to be corrected.

3.2 Rights that students can exercise with the external national supervisory authority

Right to lodge a complaint with a supervisory authority: every data subject has the right to lodge a complaint with a supervisory authority, in particular in the EU country where he or she is habitually resident, where he or she has his or her place of work or where the alleged infringement has occurred – if he or she considers that processing of personal data concerning him or her infringes GDPR provisions.[53] The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.[54]

Supervisory authorities: each EU country shall provide one or more independent public authorities competent to monitor the application of this Regulation in order to protect the fundamental rights and freedoms of individuals with regard to processing and to facilitate the free flow of personal data within the EU.[55]

For individuals (students), the supervisory authority can be important in practice, as each supervisory authority has the following tasks in its territory:

- promote public awareness and understanding of the risks, rules, safeguards and rights related to processing;
- promote awareness among controllers and processors of their obligations under GDPR;
- provide information to any data subject, upon request, on the exercise of his or her rights under the GDPR and, to that end, cooperate, where appropriate, with supervisory authorities in other Member States;

---

[53] Article 77, paragraph 1 of the General Data Protection Regulation (GDPR).

[54] Article 77, paragraph 2 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 237-238.

[55] Article 51, paragraph 1 of the General Data Protection Regulation (GDPR).

- deal with complaints lodged by the data subject;
- cooperate with other supervisory authorities, including by exchanging information, and provide mutual assistance to ensure consistency in the application and enforcement of GDPR.[56]

The performance of these tasks by each supervisory authority is free of charge for the data subject.[57]

It follows from the above that students may also directly contact an independent external state authority for the protection of personal data (in Slovenia, the Information Commissioner) in the event of alleged irregularities in the handling of their personal data. Nevertheless, it would be appropriate (in line with the spirit of the relationship between the students and the educational institution) that in case of alleged irregularities, the student should first contact the educational institution, which will check whether everything is in line with the rules and rectify any irregularities. If the individual (e.g. the student) is not satisfied with the solution, he/she can, of course, also contact the aforementioned national authority. We would also like to point out that the authority will help the individual (student) free of charge (the question, complaint, letter, etc. can also be sent to the authority by e-mail, telephone, etc.). There are no costs involved, as is the case, for example, with court proceedings.

It is also worth noting that in the case of cross-border studies (for example, if students are studying remotely (or coming) from a country other than the country where the educational institution is based), they have the right to contact the supervisory authority in their home country or in the country where the educational institution is based. As mentioned above, the supervisory authorities of the different countries have the duty to cooperate with each other, which will help to resolve the issue at hand.

[56] Articles 57 and 58 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 194-199.
[57] Article 57, paragraph 3 of the General Data Protection Regulation (GDPR).

3.3 Obligations of controllers (educational institutions) and processors of personal data

The GDPR further **specifies a number of obligations for controllers of** personal data (in our case, educational institutions). Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.[58] Where proportionate to the processing activities, the measures taken pursuant to those obligations shall include the implementation by the controller of appropriate data protection policies.[59]

Furthermore, the **concept of personal data protection by design and by default is also important**.[60] The GDPR provides that, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.[61] It further provides that the controller shall implement appropriate technical and organisational measures to ensure that, by default, only the personal data necessary for each specific purpose of processing are processed. This obligation applies to the amount of personal data collected, the scope of their processing, their retention period and their accessibility. In particular, such measures shall ensure that personal data are not automatically accessible to an

[58] Article 24, paragraph 1 of the General Data Protection Regulation (GDPR).

[59] Article 24, paragraph 2 of the General Data Protection Regulation (GDPR).

[60] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 183-185.

[61] Article 25, paragraph 1 of the General Data Protection Regulation (GDPR).

indeterminate number of individuals without the intervention of the individual concerned.[62]

The GDPR also imposes an obligation to keep records of **processing activities**.[63] Each controller and the controller's representative, where one exists, shall keep a record of the processing activities of personal data under its responsibility. This record shall contain the following information:

(a) the name and contact details of the controller and, where they exist, of the joint controller, the controller's representative and the data protection officer;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and types of personal data;
(d) the categories of users to whom personal data have been or will be disclosed, including users in third countries or international organisations;
(e) where applicable, information on transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;
(f) where possible, the time limits foreseen for the deletion of different types of data;
(g) where possible, a general description of the technical and organisational safety measures.[64]

Article 32 of the GDPR also places an important emphasis on the **security of processing**.[65] The provision provides that, taking into account the latest technological developments and the costs of implementation, as well as the nature, scope, circumstances and purposes of the processing, and the risks to the rights and freedoms of natural persons, which vary in likelihood and severity, the controller and the processor shall ensure an appropriate level of security in relation to the risk, by implementing appropriate technical and organisational measures, including, but not limited to, the following measures, as appropriate:

(a) pseudonymisation and encryption of personal data;

[62] Article 25, paragraph 2 of the General Data Protection Regulation (GDPR).
[63] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 178-179.
[64] Article 30, paragraph 1 of the General Data Protection Regulation (GDPR).
[65] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 165-169.

(b) the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.[66]

Furthermore, the GDPR provides that the determination of the appropriate level of security shall take into account, in particular, the risks posed by the processing, in particular due to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[67]

The controller and the processor shall also ensure that any natural person acting under the authority of the controller or the processor who has access to personal data may not process it without the controller's instructions, unless required to do so by EU or Member State law.[68]

Data controllers also have a specific obligation to **notify the supervisory** authority of a personal data breach. In the event of a personal data breach, the controller shall notify the competent supervisory authority without undue delay and preferably not later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to jeopardise the rights and freedoms of natural persons. Where notification to the supervisory authority is not given within 72 hours, it shall be accompanied by a statement of the reasons for the delay.[69]

In accordance with the GDPR, the notification must contain at least:

(a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the types and approximate number of personal data records concerned;

[66] Article 32, paragraph 1 of the General Data Protection Regulation (GDPR).
[67] Article 32, paragraph 2 of the General Data Protection Regulation (GDPR).
[68] Article 32, paragraph 4 of the General Data Protection Regulation (GDPR).
[69] Article 33, paragraph 1 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 171-173.

(b) a communication of the name and contact details of the data protection officer or other contact point from whom more information can be obtained;
(c) a description of the likely consequences of the personal data breach;
(d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, as well as measures to mitigate any adverse effects of the breach, if appropriate.[70]

The controller has an obligation to document any personal data breach, including the facts relating to the personal data breach, its effects and the corrective measures taken.[71]

Data protection impact assessment and prior consultation are two important obligations of the data controller (educational institution). A data **protection impact assessment (DPIA)** shall be carried out where it is possible that the type of processing, in particular through the use of new technologies, taking into account the nature, scope, context and purposes of the processing, may result in a high risk to the rights and freedoms of natural persons. In such cases, the controller shall therefore carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before processing. A single assessment may address a set of similar processing operations presenting similar high risks.[72] The GDPR provides that when carrying out a data protection impact assessment, the controller shall seek the opinion of the Data Protection Officer, where appointed.[73]

For our case, it is relevant that a data protection impact assessment is required in particular in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

[70] Article 33, paragraph 3 of the General Data Protection Regulation (GDPR).
[71] Article 33, paragraph 5 of the General Data Protection Regulation (GDPR).
[72] Article 35, paragraph 1 of the General Data Protection Regulation (GDPR).
[73] Article 35, paragraph 2 of the General Data Protection Regulation (GDPR).

(b) large-scale processing of special categories of data within the meaning of Article 9 of the GDPR.[74]

The GDPR further specifies that the data protection impact assessment shall provide at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing and, where applicable, the legitimate interests pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to their purpose;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(d) measures to address risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.[75]

Depending on each individual case and the technology deployed, the data protection impact assessment may be crucial for the lawful functioning of educational institutions. Especially in light of the large amounts of student's personal data that the educational institutions are processing.

Furthermore, the GDPR foresees an **obligation of prior consultation**.[76] The controller shall consult the supervisory authority before processing where it is apparent – from the data protection impact assessment referred to in Article 35 of the GDPR – that the processing would result in a high risk if the controller did not take measures to mitigate the risk.[77] Where the supervisory authority considers that the envisaged processing would infringe the GDPR, in particular where the controller has not adequately identified or mitigated the risks, the supervisory authority shall, within a period of up to eight weeks after receipt of the request for consultation, advise the controller in writing. This period may be extended by a further six weeks, taking into account the complexity of the envisaged processing.

[74] Article 35, paragraph 3 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 179-181.
[75] Article 35, paragraph 7 of the General Data Protection Regulation (GDPR).
[76] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 179-181.
[77] Article 36, paragraph 1 of the General Data Protection Regulation (GDPR).

The supervisory authority shall inform the controller and, where necessary, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay. That period may be suspended until the supervisory authority has obtained the information it requested for the purposes of the consultation.[78]

The Data Protection Officer also plays an important role in ensuring the protection of personal data within the organisation.[79] The controller and the processor shall appoint a data protection officer whenever processing is carried out by a public authority or body. The data protection officer may be a member of the controller's or processor's staff or may perform the tasks on the basis of a service contract. The controller or processor must publish the contact details of the data protection officer and communicate them to the supervisory authority.[80]

The Data Protection Officer also has a specific position. The controller and the processor shall ensure that the data protection officer is involved in an appropriate and timely manner in all matters relating to the protection of personal data.[81] The controller and the processor shall also assist the data protection officer in the performance of these tasks by providing the means necessary for the performance of the tasks and access to personal data and processing operations, and by maintaining the expertise of the data protection officer.[82] The controller and the processor shall ensure that the data protection officer does not receive any instructions in the performance of his tasks. The data protection officer shall not be dismissed or penalised for the performance of his or her tasks. The DPO shall report directly to the highest management level of the controller or processor.[83]

Data subjects may contact the Data Protection Officer in relation to any matter concerning the processing of their personal data and the exercise of their rights under the GDPR.[84] The Data Protection Officer shall be bound by the obligation

[78] Article 36, paragraph 2 of the General Data Protection Regulation (GDPR).
[79] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 175-178.
[80] Article 37, paragraphs 1, 6 and 7 of the General Data Protection Regulation (GDPR).
[81] Article 38, paragraph 1 of the General Data Protection Regulation (GDPR).
[82] Article 38, paragraph 2 of the General Data Protection Regulation (GDPR).
[83] Article 38, paragraph 3 of the General Data Protection Regulation (GDPR).
[84] Article 38, paragraph 4 of the General Data Protection Regulation (GDPR).

of secrecy or confidentiality in the performance of his or her duties under Union or Member State law.[85]

Furthermore, the Data Protection Officer has at least the following tasks:

(a) informing and advising the controller or processor and the employees carrying out the processing of their obligations under the GDPR and other provisions of Union or Member State law on data protection;
(b) monitoring compliance with the GDPR, other provisions of Union or Member State law on data protection and the controller's or processor's policies on the protection of personal data, including the assignment of tasks, awareness-raising and training of staff involved in processing operations and related audits;
(c) advising, where requested, on the data protection impact assessment and monitoring its implementation;
(d) cooperation with the supervisory authority;
(e) acting as a contact point for the supervisory authority on issues relating to processing, including prior consultation, and, where appropriate, consultation on any other matter.[86]

It can be concluded that all these obligations of the controller (the educational institution) contribute to a systemically higher protection of students' personal data within the organisation. Both the prior data protection impact assessment procedures when implementing new systems and the appointment of a Data Protection Officer play an important role. The latter is an important point of contact both for the supervisory authorities monitoring the compliance of the educational institution's practices with the GDPR and for the individuals (students) whose data are processed.

3.4 Consequences of personal data breaches

Compliance with the provisions of the GDPR is important not only because of the importance of protecting individuals' rights, but also because of the potential consequences that breaches may bring.

[85] Article 38, paragraph 5 of the General Data Protection Regulation (GDPR).
[86] Article 39, paragraph 1 of the General Data Protection Regulation (GDPR).

As already mentioned, the GDPR provides that any individual who has suffered material or non-material damage as a result of an infringement of GDPR provisions has the right to obtain compensation from the controller or processor for the damage suffered.[87] Any controller involved in processing shall be liable for the damage caused by processing in breach of the GDPR. The processor shall be liable for the damage caused by the processing only where it has failed to comply with the obligations under GDPR specifically addressed to processors or where it has exceeded or acted contrary to the lawful instructions of the controller.[88] The controller or processor shall be exempted from liability if they prove that they are in no way responsible for the event giving rise to the damage.[89]

Another important form of liability is the liability to commit an offence or to pay a penalty (administrative fine) for breaches of the rules on the protection of personal data.[90] As a general rule, the fines imposed should be proportionate, effective and dissuasive for the offenders.[91]

In deciding whether to impose an administrative fine and the amount of the administrative fine in each case, due account shall be taken of the following:

(a) the nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected by the breach and the level of damage suffered by them;
(b) whether the infringement is intentional or due to negligence;
(c) any measures taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor, taking into account the technical and organisational measures adopted by the controller or processor in accordance with the GDPR;
(e) any relevant previous infringements by the controller or processor;

[87] Article 80, paragraph 1 of the General Data Protection Regulation (GDPR).
[88] Article 80, paragraph 2 of the General Data Protection Regulation (GDPR).
[89] Article 80, paragraph 3 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 246-247.
[90] See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 247-248.
[91] Article 83, paragraph 1 of the General Data Protection Regulation (GDPR).

(f) the degree of cooperation with the supervisory authority in remedying the breach and mitigating any adverse effects of the breach;
(g) the types of personal data concerned by the breach,
(h) how the supervisory authority became aware of the infringement, in particular if and to what extent the controller or processor notified the infringement to the supervisory authority;
(i) where warning measures of the supervisory authority under other provisions of the GDPR have been previously ordered against the controller or processor concerned in relation to the same subject matter, compliance with those measures;
(j) commitment to approved codes of conduct or approved validation mechanisms; and
(k) any other aggravating or mitigating factors relating to the circumstances of the case, such as financial benefits gained or losses avoided resulting directly or indirectly from the infringement.[92]

In addition, GDPR rules provide that if a controller or processor intentionally or negligently infringes several provisions of the GDPR in the same or a related processing operation, the total amount of the administrative fine shall not exceed the amount set for the most serious infringement.[93]

We would also like to highlight the level of administrative fines that can be imposed on the controller or processor of personal data. Infringements of the following provisions may be subject to administrative fines of up to EUR 10,000,000 or, in the case of a company, up to 2% of the total worldwide annual turnover in the preceding financial year, whichever is higher: obligations of the controller and the processor (e.g. to provide for the protection of personal data by default, to keep records of processing activities, to consult and report to the supervisory authority, to provide for a prior impact device for the protection of personal data, etc.) – Articles 35 to 39 of the GDPR.[94]

[92] Article 83, paragraph 2 of the General Data Protection Regulation (GDPR).
[93] Article 83, paragraph 3 of the General Data Protection Regulation (GDPR).
[94] Article 83, paragraph 4 of the General Data Protection Regulation (GDPR).

However, even higher fines – up to EUR 20,000,000 or, in the case of a company, up to 4% of the total worldwide annual turnover in the previous financial year, whichever is higher – can be imposed for breaches of the fundamental rules of processing, which we have also presented in this article: the basic principles of processing, including consent, breach of the rights of the data subject, etc. These are in particular the fundamental rules that we have presented in our article.[95]

4 Conclusion

Respect for the protection of personal data is one of the most important issues in the provision of (online) education. In the course of their work, educational institutions manage a large amount of students' personal data. To this end, the GDPR comprehensively regulates the rules for the appropriate handling of personal data. These EU-wide uniform rules must be respected by all educational institutions operating in the EU.

As a starting point, it is important to start from the basic concepts (personal data, processing of personal data) that condition the application of the GDPR rules. Of particular importance are the initial fundamental principles relating to the processing of personal data (purpose limitation, data minimisation, storage limitation, integrity and confidentiality, etc.). Thus, personal data may only be processed for a specific legitimate purpose; to the extent necessary for the fulfilment of these purposes etc. The processing must also be based on one of the lawful legal bases under Article 6 GDPR. In this respect it is particularly important that the student's consent complies with all the standards under the GDPR. In the context of the provision of education, the ground that the processing is necessary for compliance with a legal obligation to which the controller is subject may also be relevant. Particular diligence must also be taken into account when dealing with special types of (sensitive) personal data for which there are specific rules for processing.

Therefore, as a general guideline for personal data controllers (educational institutions and their employees), it may serve to ask: Is there an adequate basis for collecting or processing students' personal data? Does the collection or processing respect the principles of data minimisation (only the data necessary for the purpose

[95] Article 83, paragraph 5 of the General Data Protection Regulation (GDPR).

of processing are processed) and transparency (students are provided with all the necessary information concerning the processing of their data)? Will the processing of personal data in any case be carried out in an appropriate technical and organisational manner to ensure its security (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)? In particular, when choosing technological solutions, it is important to bear in mind whether our legitimate purpose/objective (because of which we are collecting and processing personal data) could be achieved in a way that would be less intrusive into the students' right to privacy.

Furthermore, the GDPR regulates a number of obligations of the controller (educational institutions) and the rights of data subjects (students, employees). The data subject can exercise directly with the educational institution the right of access to information concerning the processing of personal data, the right to rectification of personal data, the right to erasure (right to be forgotten), the right to restriction of processing and the right to object. In the event of a breach, the individual may also have recourse to an independent external supervisory authority, to which he or she may lodge a complaint.

In this context, controllers (educational institutions) also have important obligations to ensure systemic security and lawful processing of personal data. Thus, when implementing various technological solutions in the educational process, they must take into account the concept of protection of personal data by design and by default, the consistent keeping of records of processing activities where necessary and the security of processing. In certain cases, it is mandatory or advisable to carry out a data protection impact assessment analysing the level of risk to the protection of personal data. A specially designated data protection officer also plays an important role for the protection of personal data within the organisation (educational institution).

In the event of irregularities, it should be stressed that students can contact the educational institution or the competent national supervisory authority. Employees or the educational institution must take particular care in handling personal data, as any breaches may result in liability for damages, and employment or criminal offences.

Students and employees can always find out more about personal data protection on the websites of the educational institution or national data protection authority. Another possibility is to contact the data protection officer within the organisation or the supervisory authority directly.

Notes

The author originally prepared the Manual in the Slovenian language. Versions in other languages represent a translation of the author's version written in Slovenian.

References

Borchardt, Klaus-Dieter, Fundamentals of European Union Law, 2016, URL: http://publications.europa.eu/resource/cellar/5d4f8cde-de25-11e7-a506-01aa75ed71a1.0008.03/DOC_1 (accessed 26.6.2021).

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law: 2018 edition, Publications Office of the European Union, Luxembourg 2018, URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (accessed 26.6.2021), pp. 122-125.

Information Commissioner, 2021 (Guide to personal data protection for individuals), URL: https://www.ip-rs.si/fileadmin/user_upload/Pdf/vodniki/Vodnik_po_varstvu_osebnih_podatkov_za_posameznike.pdf (accessed 26.6.2021).

Information Commissioner, 2020, Opinion: 'Distance education and personal data protection', Date: 06.04.2020, Number: 07120-1/2020/274, URL: https://www.ip-rs.si/mnenja-gdpr/6048a487a0e79 (accessed 26.6.2021).

University of Maribor, Personal Data Protection, URL: https://www.um.si/univerza/varstvo-osebnih-podatkov/Strani/default.aspx (accessed 26.6.2021).

University of Maribor, Individual Rights, URL: https://www.um.si/univerza/varstvo-osebnih-podatkov/Strani/Pravice-posameznika.aspx (accessed 26.6.2021).

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) (Text with EEA relevance), Official Journal L 119, available at URL: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679 (accessed 26.6.2021).