# Table of Contents

1. Introduction to Privacy .................................................................................................................. 2
   1.1. General Definition ......................................................................................................................... 2
   1.2. Privacy vs. Confidentiality ............................................................................................................. 2
   1.3 Privacy in Education ....................................................................................................................... 2
   1.4. Reasons for Recordkeeping .......................................................................................................... 3
2. Key Definitions and Legal Framework of Privacy ........................................................................... 3
   2.1. Privacy and Personal Data – EU Perspective ................................................................................. 3
   2.2. Privacy and Personal Data – Russia’s Perspective ......................................................................... 5
   2.3. Personal Data Types ....................................................................................................................... 6
   2.3.1. Personal Data and Schools ......................................................................................................... 7
   2.4. Processing Procedure and Consent ............................................................................................. 9
   2.5. Personal Data Breach .................................................................................................................... 12
   2.6. Overview of Personal Data Legislation in Different Countries .................................................. 13
   2.6.1. Belgium ...................................................................................................................................... 13
   2.6.2. Lithuania .................................................................................................................................... 13
   2.6.3. Poland ........................................................................................................................................ 14
   2.6.4. Albania ........................................................................................................................................ 15
   2.6.5. Belarus ....................................................................................................................................... 16
   2.7. Exemptions from Data Protection Legislation ............................................................................. 16
   2.8. Remedies and Sanctions ............................................................................................................... 16
3. Educational Privacy Principles ....................................................................................................... 18
   3.1. Student Files ................................................................................................................................. 18
   3.1.1. Information ............................................................................................................................... 18
   3.1.2. Non-discrimination .................................................................................................................... 18
   3.1.3. Principle of Finality .................................................................................................................... 18
   3.1.4. School Results .......................................................................................................................... 19
   3.1.5. Retention and Elimination ....................................................................................................... 19
   3.2. School Life ................................................................................................................................... 19
   3.2.1. Biometric Data .......................................................................................................................... 19
   3.2.2. Closed Circuit Television (CCTV) ............................................................................................ 19
   3.2.3. Children’s Photos ...................................................................................................................... 19
   3.2.4. School Statistics and Other Studies .......................................................................................... 20
4. Transparency and Access to Information in Education ............................................................... 20
   4.1. Transparency Definition and Dimensions .................................................................................. 20
   4.2. Legal Background of Transparency .......................................................................................... 20
   4.3. Concept of Access to Information .............................................................................................. 22
   4.4. Transparency in Education ......................................................................................................... 22
   4.4.1. Requirements for Schools in terms of Educational Transparency in Russia ....................... 23
   4.4.2. International Requirements for Website Transparency .......................................................... 23
   4.4.2.1. Student Learning Outcomes Statements .............................................................................. 24
   4.4.2.2. Assessment Plans .................................................................................................................. 24
   4.4.2.3. Assessment Resources .......................................................................................................... 24
   4.4.2.4. Current Assessment Activities ............................................................................................. 24
   4.4.2.5. Evidence of Student Learning ............................................................................................... 24
   4.4.2.6. Use of Student Learning Evidence ....................................................................................... 24
1. Introduction to Privacy

1.1. General Definition

*Cambridge English Dictionary* generally defines *privacy* as someone's right to keep their personal matters and relationships secret\(^1\). *Dictionary.com* treats *privacy* as freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one’s personal data or information, as by a government, corporation, or individual\(^2\). In an *American Heritage Dictionary of the English Language*, *privacy* is understood as the state of being free from public attention or unsanctioned intrusion\(^3\). *Merriam Webster Dictionary* describes *privacy* as freedom from unauthorized intrusion\(^4\).

From the legal point of view, *privacy* is the right that determines the nonintervention of secret surveillance and the protection of an individual's information. Thus, *privacy law* is any regulation or law that safeguards the intention to not be disturbed, and not collate any information pertaining to him/her\(^5\).

Privacy can be split into four categories (1) **Physical**: an imposition whereby another individual is restricted from experiencing an individual or a situation. (2) **Decisional**: The imposition of a restriction that is exclusive to an entity. (3) **Informational**: The prevention of searching for unknown information and (4) **Dispositional**: The prevention of attempts made to get to know the state of mind of an individual\(^6\).

1.2. Privacy vs. Confidentiality

It is important to separate the concepts of privacy and confidentiality. **Confidentiality** is an **obligation** often associated with professions such as teachers, lawyers and doctors being their duty to protect and hold in strict confidence all information concerning the person who is the subject of the professional relationship\(^7\). There are times when confidential information may be disclosed, but those occasions are limited.

By contrast, in regard to the above mentioned, **privacy is one’s right (freedom)** to keep certain matters of their personal life secret from others.

1.3 Privacy in Education

Privacy in education refers to practices and legislation that involve the privacy rights of individuals in the education system. The majority of privacy in education concerns are prevalent to the protection of student data, both inside and outside the classroom. Many scholars are engaging in an academic discussion that covers the scope of students’ privacy


\(^2\) [http://www.dictionary.com/browse/privacy?s=t](http://www.dictionary.com/browse/privacy?s=t)

\(^3\) [http://www.yourdictionary.com/privacy#americanheritage](http://www.yourdictionary.com/privacy#americanheritage)

\(^4\) [https://www.merriam-webster.com/dictionary/privacy](https://www.merriam-webster.com/dictionary/privacy)

\(^5\) [http://thelawdictionary.org/privacy/](http://thelawdictionary.org/privacy/)

\(^6\) Ibid.

rights, especially if they are minors, and the management of student data in an age of rapid information access and dissemination.

Examples of educational privacy include the protection of a student's academic record from being viewed by anyone other than the academic instructor, the student's parents or guardians, and the students themselves.

Other examples of student expectation of privacy include the right of children to withhold personal information from teachers within a traditional classroom setting. Such topic remains a contentious educational privacy concern in the classroom.

1.4. Reasons for Recordkeeping
An educational institution needs to process student personal data in order to function effectively and to provide students with the support they require while undertaking their studies. Personal data is processed for a variety of reasons, but all such data shall be collected and held in accordance with the law.

The primary reasons an educational institution handles student personal data are as follows:

- Healthcare, i.e. observation of a student’s health condition to avoid accidents;
- Financial administration, e.g. payment of tuition fees, provision of scholarships;
- Security and crime prevention/detection – e.g. use of regulated CCTV, security incident reports;
- Library services – e.g. administration of membership, cards and fines;
- Provision of student ID cards, academic record books, admission/entrance passes, membership or subscription tickets etc;
- Provision and maintenance of computing facilities, including email accounts and internet access;
- Educational administration, e.g. registration, progress monitoring, timetabling, calculation and publication of assessments, provision of references;
- Accommodation - provision and management of institution owned property for students;
- Advisory services, e.g. careers counselling.

2. Key Definitions and Legal Framework of Privacy
2.1. Privacy and Personal Data – EU Perspective
Under the European Union law, the right to privacy and the right to protection of personal data are two distinct fundamental human rights. The Charter of Fundamental Rights of the European Union (CFR, 2009) recognizes the right to privacy in Article 7 and the right to the protection of one’s personal data in Article 8.

---

10 Partly from http://www.bristol.ac.uk/applicants/media/policy-documents/2017/undergraduate/personal-data.pdf as amended by the authors
Article 7 of the CFR provides that everyone has the right to respect for his or her private and family life, home and communications. Similarly, the Convention for the Protection of Human Rights and Fundamental Freedoms (1950) states that everyone has the right to respect for his private and family life, his home and his correspondence. Important is that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety etc.

One of the core elements constituting the concept of privacy is personal data. Article 8(1) of the CFR and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) specifies that everyone has the right to the protection of personal data concerning him or her. The former also reaffirms the principle that personal data must be processed fairly and for specific purposes, based on the consent of the individual concerned or some other legitimate purposes laid down by law. It also recognizes the right of individuals to access the data collected and the right to have it rectified, in case of inaccuracy or incompleteness. Compliance with such rules is entrusted to the control of an independent authority established by EU Member States.

The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

As it appears from Article 7 of the CFR, “the right to respect for … private … life” equally involves one's interest in having their personal data (information) protected from unauthorized or inappropriate actions of the third parties. In this regard, there is a number of documents adopted within the EU both supranationally and nationally.

In 1981, a Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108) was adopted. Convention 108 still remains the only legally binding international instrument in the data protection field.

Convention 108 applies to all data processing carried out by both the private and public sector, such as data processing by the judiciary and law enforcement authorities. It protects the individual against abuses, which may accompany the collection and processing of personal data, and seeks, at the same time, to regulate the transborder flow of personal data. As regards the collection and processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data.

---

15 Ibid.
stored for specific legitimate purposes and not for use for ends incompatible with these purposes nor kept for longer than is necessary.\textsuperscript{16}

In addition to providing guarantees on the collection and processing of personal data, it outlaws, in the absence of proper legal safeguards, the processing of ‘sensitive’ data, such as on a person’s race, politics, health, religion, sexual life or criminal record.\textsuperscript{17}

The convention also enshrines the individual’s right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the convention are possible only when overriding interests, such as state security or defense, are at stake.\textsuperscript{18}

Regulation 2016/679 and Directive 2016/680 of the European Parliament and of the Council define personal data as any information relating to an identified or identifiable natural person (data subject)\textsuperscript{19, 20}; 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.

2.2. Privacy and Personal Data – Russia’s Perspective

There is a concept in the Russian legislation, which has a synonymous meaning with that of the European privacy. The Constitution of the Russian Federation confirms in its Articles 23 and 24 the right to integrity of private life, personal and family secret, as well as the right to protect one’s honor and dignity.\textsuperscript{21} Under the Constitution, a state shall be prohibited invasion into an individual’s private life and shall warrant an individual protection from such invasion of the third parties.\textsuperscript{22}

The law interprets integrity of private life as an integrity of both physical and spiritual aspects of life, which is controlled by an individual and is free from external disturbance. It is, thus, family and household issues of an individual’s being, its acquaintances and friends, attitude towards religion, non-occupational activities, hobbies and other relations that a person wants to keep secret unless required by the law.

The right to integrity of private life (i.e. the right to privacy) has been stipulated in several Russian laws since 2006. It is worth emphasizing, in the first place that regulation of relationships in terms of privacy falls within the jurisdiction of the federal law, i.e. regional and local authorities and legislative bodies, as well as separate agencies and institutions may

\textsuperscript{17} Ibid.
\textsuperscript{18} Ibid.
\textsuperscript{20} Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
\textsuperscript{22} Ibid.
introduce their own privacy policies and regulations, but those have to correspond to the federal legislation.

Thus, there is the Federal Law No. 149-FZ On Information, Information Technologies and Data Protection, the first to introduce integrity of private life as a fundamental legal principle\(^{23}\), as well as the Federal Law No. 152-FZ On Personal Data that generally prohibits processing of personal data without prior consent of the data subject\(^{24}\). This ruling is underpinned by the Article 152.2 of the Civil Code of the Russian Federation restricting collection, storage, distribution and usage of any data about an individual’s private life, including private life, national origin, place of stay or residence, personal and family life unless otherwise provided by law\(^{25}\).

The concept of private life (privacy) is precisely formulated in one of the Decisions of the Constitutional Court of the Russian Federation, where the Court indicates that the right to integrity of private life shall include the opportunity to control information about oneself and prevent disclosure of personal or private matters. The Court also stipulates that the concept of private life shall include personal activities referring to a particular person and concerning this person only without being controlled by society or state and not contradicting the law\(^{26}\).

Russian legislators, however, choose to specify the concept of information considering it as any data (evidence, statements etc.) regardless of their representation and format. Russian law also takes into consideration the process of disclosing information, distinguishing between providing (actions aimed at obtaining information by or transferring information to a specific group of people) and disseminating (actions aimed at obtaining information by or transferring information to an indefinite range of persons, or general public) information\(^{27}\).

### 2.3. Personal Data Types

The Data Protection Directive comprises the following types of personal data:

- **a) Genetic Data** meaning any personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question\(^{28}\).

- **b) Biometric Data**, i.e. personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data\(^{29}\).

---


\(^{29}\) Ibid., Par. 14.
c) **Data Concerning Health**, which is personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status\(^{30}\).

**2.3.1. Personal Data and Schools**

Although the privacy right of children is enshrined in several international legal instruments, there are no specific rules pertaining to the personal data of children in either the Data Protection Directive or the Privacy and Electronic Communications Directive\(^{31}\). Because the scope of both Directives extends to the data of “every natural person,” however, the built-in safeguards arguably apply to both children and adults. Consequently, the general principles on data quality contained in the Personal Data Protection Directive, such as fairness, proportionality, and relevance, apply to children. In addition, the general obligations that only adequate, relevant, and non-excessive data can be collected and processed govern the processing of the personal data of children. In general, controllers must take into account the circumstances of a child and his/her best interests. Moreover, the personal data of children must be accurate and current; inaccurate or incomplete data must either be erased or corrected. The Data Protection Directive’s Article 7 on the legality of processing and Article 9 on the processing of personal categories of data are also applicable to children. As far as the right of access, it can be exercised either by the child based on his/her maturity level, or by the child’s representative. Children’s data cannot be used for purposes other than those for which they were collected.

In the context of education and considering the above-mentioned types of personal data distinguished by the law, personal data an educational institution might process include, without limitation\(^{32}\):

- personal details (name, address, date of birth)
- phone numbers
- email addresses
- gender
- gender identity
- photographs
- financial information
- academic marks
- appraisals
- references
- disciplinary information
- criminal offence or conviction information
- health and disability information
- ethnicity data
- sexual orientation
- dietary requirements

---

\(^{30}\) Ibid., Par. 15.


\(^{32}\) From [http://www.bristol.ac.uk/applicants/media/policy-documents/2017/undergraduate/personal-data.pdf](http://www.bristol.ac.uk/applicants/media/policy-documents/2017/undergraduate/personal-data.pdf) as amended by the authors
• religious belief data
• caring responsibilities
• information regarding hobbies and interests
• any other legitimate personal data relating to academic support.

Information about criminal offences, health, disability, ethnicity, sexual life and religion constitutes sensitive personal data and is afforded an extra level of security and confidentiality (see Chapter IV.6.).

In justification of the foregoing list of data types, Regulation 2016/679 provides for the set of specifying definitions.

The above-indicated terms and definitions from both Regulation 2016/679 and Directive (EU) 2016/680 are almost fully embodied in the Russian legislation, where the concepts of personal data, operator (processor), processing, recipient and consent are present and defined in a very similar way to that of the European personal data protection law. Moreover, Russian law refers to such terms as specific (sensitive) personal data, biometric personal data and cross-border processing of data in separate legal provisions.

In accordance with Article 8.1., Para 1 of the Russian Federation Federal Law On Personal Data as of July 27, 2006, an educational institution shall take steps to ensure safety of personal data while processing. Such steps, among other things, include adoption of regulations concerning protection of students’ personal data.

In accordance to many of these regulations adopted by schools nationwide, the student’s personal data generally comprise:

• educational record with a progress report card;
• copy of birth certificate;
• information about family members;
• information about parents or legal representatives (guardians);
• copy of the national passport for the students above 14 years of age;
• leaving certificate confirming basic general education;
• home address and phone number;
• photographs;
• information about health condition and health limitations.

Among information that the school is not entitled to collect and process is data concerning students’ private life as well as their political and religious beliefs.

In terms of educational process it is fair to point out, that educational institutions hardly ever use genetic data (unless it is part of data concerning health, if such is collected and processed by an institution), whereas biometric and health-related data are widely processed, the former in the majority of cases for the sake of foreign students admission and identification, and the latter to be aware of the students health condition in order to prevent accidents like incidental infections or fatal casualties due to undetected condition.

2.4. Processing Procedure and Consent

Processing of personal data is defined as 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.\(^{35}\)

Unlawful or unfair processing results in appropriate penalty. For example, one of the educational institutions in Samara (Russia) executed activities that involved processing of students’ personal data. During the inspection it was discovered that, in accordance with the school director’s order, one of the employees was appointed as a responsible officer for the personal data processing. However, the actual person processing the data was another person. Thus, the educational institution violated the requirements set forth in Article 22 of the Federal Law On Personal Data by failing to inform the authorized body about changes made in the procedure of the personal data processing. The court then found the educational institution guilty and imposed penalty in the form of a warning.\(^{36}\)

The issue of legal, lawful or fair processing of personal data closely relates to the matter of consent given by the data subject to confirming their evident agreement with the processing procedure and its scope.

In accordance with the Data Protection Regulation, 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.\(^{37}\)

EU law sets out three elements for consent to be valid, which aim to guarantee that data subjects truly meant to agree to the use of their data:\(^{38}\):

- the data subject must have been under no pressure when consenting;
- the data subject must have been duly informed about the object and consequences of consenting; and
- the scope of consent must be reasonably concrete.

Only if all of these requirements are fulfilled will consent be valid in the sense of the data protection law.

Additional requirements under civil law for valid consent, such as legal capacity, naturally apply also in the context of data protection as such requirements are fundamental legal prerequisites. Invalid consent of persons who do not have legal capacity will result in the absence of a legal basis for processing data about such persons.


Consent can be given either explicitly or non-explicitly. The former leaves no doubt about the intentions of the data subject and can be made either orally or in writing; the latter is concluded from the circumstances. Every consent must be given in an unambiguous way. This means that there should be no reasonable doubt that the data subject wanted to communicate his or her agreement to allow processing of his or her data. Deducing consent from mere inactivity is not capable of delivering unambiguous consent, for instance. Where data to be processed are sensitive, explicit consent is mandatory and must be unambiguous.

The existence of free consent is valid only if the data subject is able to exercise a real choice and there is no risk of deception, intimidation or significant negative consequences a person does not gives consent.

The data subject must have sufficient information before taking his or her decision. Whether the information given is sufficient can be decided only on a case-by-case basis. Usually, informed consent will comprise a precise and easily understandable description of the subject matter requiring consent and, additionally, outline the consequences of consenting or not consenting.

To be valid, consent must also be specific. This goes in hand with the quality of information given about the object of consent. In this context, the reasonable expectations of an average data subject will be relevant. The data subject must be asked again for consent if processing operations are to be added or changed in a way which could not reasonably have been foreseen when the initial consent was given.

The Data Protection Directive does not mention a general right to withdraw consent at any time. It is widely presumed, however, that such a right exists and that it must be possible for the data subject to exercise it at his or her discretion. There should be no requirement to give reasons for withdrawal and no risk of negative consequences over and above the termination of any benefits, which may have derived from the previously agreed data use.

In terms of consent, the Russian law notes that personal data processing shall proceed given the consent of the data subject to process their personal data. Operators (processors) and other parties that gained access to personal data shall neither disclose it to the third parties, nor disseminate it without prior consent of the data subject, unless otherwise provide for by law.

According to the current Russian law, publicly accessible sources of information are created for the purposes of information support. Such information sources might include data subjects’ names, dates and places of birth, as well as their addresses, phone numbers, information about their occupation, or other personal data obtained only upon valid consent of the data subjects. The above-mentioned data shall be excluded from the publicly accessible information sources at any time upon request of the data subject, or under the decision of the court or other appropriate state authorities.

Similarly to the European provisions, Russian legislation decrees that the data subject’s consent to process their personal data shall be free, unrestricted and pursue the subject's own interest. Consent shall also be specific, informed and conscious. A data subject or its representative may give consent to process its personal data in any form that allows confirmation of such consent.

Importantly, in order to receive any personal data from the students or their parents, Russian schools have to provide the so-called approval sheets to be filled in by the data subjects.
stating their consent to the fact of processing of personal data by the educational institution (Article 9 of the Federal Law *On Personal Data*).

As opposed to the European Data Protection Directive, Russian law explicitly ensures the possibility for the data subject to withdraw its consent for personal data processing at any time\(^{39}\).

As far as specific (sensitive) personal data is concerned, Russian legislation, subsequent to the European, includes health-related information into this category stating that it is prohibited to collect and process such data unless:

- there exists a prior written consent of the data subject;
- this data is made publicly accessible by the data subject;
- such processing is conducted to protect data subject’s or other persons’ life, health or other crucial interests in case it is impossible to acquire the data subject’s consent;
- such processing is conducted for medical purposes, or to determine a medical diagnosis or to provide medical care, in case such processing is conducted by a professional medical worker obliged to keep medical secrecy in accordance with the legislation\(^{40}\).

Interestingly, Article 41 of the Federal Law *On Education in the Russian Federation* ensures student's healthcare including maintaining special conditions to prevent diseases and foster healthy lifestyle, conducting medical examinations, anti-epidemic and preventive activities etc\(^{41}\).

However, educational institution cannot retrieve information about student’s health condition without consent of the students or their legal representatives.

Thus, this issue is regulated by the Federal Law *On Fundamentals of Healthcare of the Russian Citizens*, which provides for keeping confidential the information (data) constituting medical secrecy of a person without right to disclose it unless:

- such data is necessary to conduct medical examination of a person, who is unable to express his/her will due to his/her medical condition;
- there exists a threat of spreading an infectious disease;
- upon request of appropriate authorities;
- medical care is provided for a minor\(^{42}\);
- in a number of other cases.

According to the current legislation, an educational institution shall produce its own local regulations concerning processing of pupils’/students’ personal data. Such document shall include:

- general provisions;

\(^{39}\) Ibid., Art. 9.


• definition and scope of personal data of pupils/students and their parents (legal representatives);
• procedures of access to and processing of personal data;
• ways of personal data protection;
• rights and obligations of parents (legal representatives);
• responsibility for disclosure of personal data.

In one of the cases related to the consent issue, Oktyabrskaya Secondary School situated in the City of Petukhovo, Kurgan Region (Russia) had a website that gave its visitors an opportunity to provide feedback of the school activities. Visitors could send a message, while at the same time the website collected personal information of this visitor (name and e-mail address). Such personal data processing took place without any consent to it. Besides, the website did not contain any document that would determine the school’s policy in terms of personal data processing. The court ruled for holding the legal entity responsible for an administrative offence, which inflicted a penalty in the form of warning.

Summarizing the definitions and concepts outlined above, it is worth mentioning that all of them are applicable in the field of education, since they describe general ideas of privacy and data protection and can be modified to suffice the needs of an educational process/institution for the sake of defending students’ and teacher’s rights.

2.5. Personal Data Breach
The concept generally means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

To demonstrate the practical mechanism of data breach and its remedy in real-life circumstances, it is recommended to examine the cases given below.

While applying for school enrollment, a mother of future first-grader explicitly indicated in a special document that she was unalterably opposed to the transition of her daughter’s personal data, including photographs and phone numbers to the third parties. In fall, a classroom was redecorated, and the help of parents was needed to perform the works. Some of the parents received text messages on behalf of the parents’ committee asking for assistance. A first-grader’s mother complained to the Prosecutor’s Office of the Kazan Privolzhskiy District that her phone number was given to the third parties without her consent. In reply of the district prosecutor as of January 16, 2017 it is stated that upon official examination, principal of Gymnasium No. 40 was passed on recommendation to bring the liable persons to disciplinary action. An administrative trial was initiated against a teacher in regard to violating the procedure of collection, storage, usage and dissemination of personal data. A teacher is facing a fine of 500 to 1000 rubles.

---

In another case that was considered in Karelia, in the course of examination conducted by the Prosecutor’s Office it turned out that an official website of the Loukhskaya Secondary School contains a program of professional upbringing, which not only includes general information, but also discloses children’s and parents’ names, addresses, phone numbers and places of work. Moreover, the website, enumerated pupils from incomplete or underprivileged families, and indicated some of the pupils’ bad habits and chronic diseases. These data were made publically available without consent of the persons in question in contradiction to the Federal Law On Personal Data. Taking into consideration the violation of privacy rights of pupils and their parents, as well as a right for personal and family secret, Prosecutor’s Office initiated an administrative trial against the legal entity and the principal based upon Article 13.11 of the Administrative Code of the Russian Federation. Having examined the case, the Magistrate’s Court imposed a penalty of 5000 rubles upon a legal entity, while at the same time imposing a disciplinary punishment and a fine upon the principal. Illegally posted information was deleted from the school website46.

2.6. Overview of Personal Data Legislation in Different Countries

2.6.1. Belgium47

The Data Protection Directive has been implemented into Belgian law by the Law on the protection of privacy in relation to the processing of personal data48.

A minor under the age of discernment can consent to their personal data being processed through their legal representative (Article 1 §8, DPL), who can withdraw the minor's consent at any time on the minor's behalf.

There is no fixed age at which minors are deemed to have reached the age of discernment, but in a recommendation of 16 September 2002 (Recommendation 38/2002), the Privacy Commission held that minors usually obtain the required insight between the age of 12 and 14.

There is also a regional (Flemish) law called the Decree on Publicity (transparency) of Governance. The instances responsible for appropriate implementation of the law are: Commission for the protection of the personal life (privacy commission) and the Flemish monitoring committee.

For instance, one of the cases related to privacy issues dealt with a Flemish pupil awarded a B-certificate (allowing him to proceed in school, yet with some limitations). However, neither the pupil, nor his parents had received the report of such assessment. Therefore, they were not informed about their possibilities to appeal the school decision. The court decided that the facts of the case manifest violation of the Decree on Publicity of Governance (Article 35) as well as Violation of the Codex on Secondary Education (Article 115/6, §4, 2°).

2.6.2. Lithuania

The main legislative framework for personal data protection is established in the Law on the Legal Protection of Personal Data, which implements the Directive 1995/46/EC. The law lays down the basic personal data protection principles, processing standards and rights of data

---

46 http://prokuratura.karelia.ru/struktura/gorodskie-i-rayonnye-prokuratury/prokuratura-loukhskogo-rayona/loukhi_news/page_2784/?forBlind=on
47 See https://uk.practicallaw.thomsonreuters.com/2-502-2977?__lrTS=20170413125855005&transitionType=Default&contextData=(sc.Default)
subjects. Unfortunately, the law does not specifically regulate the processing of personal data of minors. According to the Law the State Data Protection Inspectorate is responsible for its supervision and monitoring of the implementation.

2.6.3. Poland

As a member of the EU Poland implemented Directive 95/46/EC on data protection by the Personal Data Protection Act of 29 August 1997. This law regulates the processing of personal data defining it in accordance with the EU Regulation and Directive.

Until the age of 18, a child does not have full legal capacity, and the following rules apply:

- Up to 13 years of age, a child has no legal capacity and, therefore, any legal action can be taken in his name only by the parents as legal representatives (except for contracts generally concluded in everyday matters).
- When a child is between 13 to 18 years of age, he can perform legal actions if the consent of the parent(s) is provided.

Parents are the statutory representatives of a child that remains under parental authority. If the child remains under the parental authority of both parents, each of them can act alone as the legal representative of the child.

However, parents must decide important matters concerning the child jointly. There is no definition of "important matters concerning the child". This concept has been interpreted by courts to include matters relating to the child's:

- Residence (including where he will live during holidays).
- School.
- Future career.
- Medical treatment.

In one of the cases, there was a conflict between the complainant and the school over the complainant’s allegation that his son had been “physically and mentally bullied” at school, which led to the situation where the complainant had moved his children to other institutions. M. P. (complainant) submitted to the principal letters describing the situation and urging him to inform of actions taken by the school in question. As a result, the school took steps that, in the opinion of the principal, were to clarify the situation and prevent similar incidents in the future. The complainant argued that at the meeting of the Association’s Board and at the Parents’ Council meeting his letters, the teachers’ notes and summaries of the psychologist's consultations were read. According to the complainant, both bodies discussed the case of his family described in the above letters without his authorization to make the correspondence public. On those grounds, the complaint lodged a complaint with the Inspector General for Personal Data Protection in which he requested the removal of his family’s personal data and reinstated compliance with the law. The Inspector dismissed the complaint of M.P, so the latter appealed the Inspector’s decision to the court of first instance. The court revoked the appealed decision and the preceding decision. The court noted that the Inspector had collected the evidence in a negligent manner and used incomplete documents presented by the

50 See https://uk.practicallaw.thomsonreuters.com/6-520-7945?__lrTS=20170413130810421&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1
school in the present case. According to the Court of First Instance, given the incomplete nature of the documents, at the present stage it was not possible to determine whether they contained the so-called sensitive data. The Inspector appealed to the court of higher instance, but the latter fully shared the opinion of the court of first instance, ordering the Inspector to reconsider the case.

2.6.4. Albania
In Albania there exists the Law no. 9887, dated 10.03.2008 “On personal data protection” as amended. It provides the same definition of personal data as the European legislation including a concept of “sensitive personal data” meaning any information related to the natural person in referring to his racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, criminal record, as well as with data concerning his health and sexual life51.

The protection of privacy is equally guaranteed in the Albanian Constitution and some other related laws. Although none of them mentions children specifically, since these laws are applicable to every person and are considered as basic human rights.

According to some sources, there are laws that can protect children’s privacy, but the laws are not implemented, and both parents and teachers violate children’s privacy on a regular basis. Since the violations come within the family or at school, for a child to complain to the relevant authorities would be rather impossible, because of lack of legal aid. The same can be said about children’s privacy at police stations, pre-trial detention centers and prisons52.

The Commissioner for the Right to Information and Protection of Personal Data carried out an administrative investigation in July 2016 with the purpose of controlling implementation by the Elbasan Regional Educational Directorate of the Law No. 9887 and relevant bylaws.

The administrative investigation found that the Regional Educational Directorate had no regulation regarding the protection of personal data and it did not sign any confidentiality agreement with the teachers. The teachers’ data, such as ID number, were published on the portal of the Regional directorate53. The personal files created by school psychologists for students with special needs, mental health problems and problematic behavior were to be preserved up to 3 years after students’ graduation, but there was no established procedure to put it into effect. The results of the tests conducted with teachers to evaluate their performance were published on the Regional Education Directorate portal. Having analyzed the facts, the commissioner decided that the abovementioned facts constituted an administrative violation of Articles 27 and 28 of the Personal Data Protection Law. The publication of the unique ID on the regional directorate website violated the privacy of teachers who were identified through a code that was attached to the ID. The Commissioner concluded that the identified violations of the personal data security of students and teachers were serious and constituted and administrative offence. The Regional Education directorate

53 www.darelbasan.arsimi.gov.al
was fined 100,000 Albanian Leks (approximately 800 Euro) for the violation of the obligations stipulated in the Articles 27 and 28 of the law “On personal data protection.”

2.6.5. Belarus

The basic legislation governing the collection, storage and use of personal data in Belarus is the Law on Information, Informatisation and Information Protection of 2008 (455-Z). Personal data is defined as the ‘basic’ (e.g., name, date of birth and gender) and ‘additional’ (e.g., tax registration, military service obligation and educational data) individual personal data that must be submitted to the Population Register under Belarusan law, as well as other data enabling the identification of an individual.

2.7. Exemptions from Data Protection Legislation

The Data Protection Directive permits EU Member States to adopt legislation to restrict the rights of data subjects for the following reasons, including:

- national security, public security, and defense;
- prevention, investigation, detection, and prosecution of criminal offenses or violations related to codes of ethics of regulated professions;
- important economic or financial interests of the EU or a Member State; and
- the protection of data subjects or the rights and freedoms of others.

In addition, the Privacy and Electronic Communications Directive allows the adoption of legislative measures by the EU Members to retain personal data for a limited period and for the purposes stated above.

2.8. Remedies and Sanctions

EU Members are required to provide means of redress to data subjects whose personal data have been infringed. Thus, the Personal Data Protection Directive provides data subjects with the following rights:

- Administrative remedies before the national supervisory authority;
- Judicial remedies for any breach of rights guaranteed by national law;
- Compensation by the controller for the damage suffered for any processing in violation of the rules; a controller may avoid liability in whole or in part, however, by proving that he/she is not responsible for the violation.

When implementing EU law, Member States are also obliged to make provisions in their national legislation for sanctions to be imposed in case of infringement.

In Albania, for instance, there is no specific duty to report data breaches, but the legislator sanctions the unauthorized disclosure of confidential information. The Law provides for a fine

---

55 See http://www.lexology.com/library/detail.aspx?g=f8279c06-f1f4-45cd-9fe0-52e5fde904a9
56 See https://www.loc.gov/law/help/internet-privacy-law/eu.php#_ftn32
57 Directive 95/46/EC, supra note 7, Art. 28, Para. 4.
58 Ibid., Art. 22.
59 Ibid., Art. 22-23.
60 Ibid., Art. 24.
61 The International Comparative Legal Guide to: Data Protection 2016. A practical cross-border insight into data protection law, 3rd edition. Published by Global Legal Group, p. 13. Available at:
ranging from ALL 10,000 up to ALL 150,000. Moreover, in some specific cases, the confidential information breach may constitute a criminal offence punishable by a fine or imprisonment of up to two years.

Importantly, during the recent years, the Albanian Commissioner has been very proactive in issuing various recommendations, orders and administrative sanctions to data controllers and processors focusing attention on raising awareness with respect to the rights and obligations deriving from the provisions of the applicable legislation.

In Belgium\(^62\), the processing of personal data in breach of the DPL may constitute a criminal offence (Articles 37 to 39, DPL) and attract a fine of EUR 550 up to EUR 110,000. The court can also order confiscation of the media containing the personal data to which the offence relates; erasure of the data; or prohibition of the control of any processing of personal data, directly or through an agent, for a period of up to two years.

According to the Polish law\(^63\), in the case of any breach of the provisions on personal data protection, the General Inspector can order compliance with the law by means of an administrative decision. Failure to comply with this decision may result in a maximum fine of about EUR 50,000. Furthermore, non-compliance with the PDPA may be a criminal offence. The following violations of the PDPA may give rise to criminal liability and inflict the following penalties for the liable persons: partial restriction of freedom; prison sentence of up to three years; or an additional fine.

In Lithuania\(^64\), Any violation of data protection rules involves administrative liability. This applies to any illegal processing of personal data, as well as any violation of the norms, which apply to the processing of personal data and the protection of privacy, as defined in the law on electronic communications. The unlawful processing of data (e.g., the unlawful use of someone’s e-mail address or other personal data, irrespective of the purpose of that use) will lead to fines of between 500 and 1,000 litas (EUR 145-290), with fines between LTL 1,000 and 2,000 for repeat offenders.

In Russia\(^65\), non-compliance with data protection laws can be punishable with civil (moral damages), administrative (fines) and criminal sanctions (imprisonment).

Finally, it is important to note that Russian data protection laws have been enforced quite heavily in recent years, and data subjects have sent many complaints to Roskomnadzor. There has also been a growing number of appeals by data operators against the orders and decisions of Roskomnadzor imposing different sanctions on data operators and blocking their Internet resources. As a result, the national case law and court practice relating to sanctions for non-compliance with Russian data protection laws continues to develop constantly. In the near future, the Russian Government may strengthen the sanctions for data breaches, at least from the administrative liability perspective, by amending the applicable law.

\(^62\) See https://uk.practicallaw.thomsonreuters.com/2-502-2977?__lrTS=20170413125855005&transitionType=Default&contextData=(sc.Default)

\(^63\) See https://uk.practicallaw.thomsonreuters.com/6-520-7945?__lrTS=20170413130810421&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

\(^64\) http://www.ebaltics.com/00705594

\(^65\) See https://content.next.westlaw.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&__lrTS=20170516055929769&firstPage=true&bhcp=1
3. Educational Privacy Principles

The Article 29 Data Protection Working Party has issued a number of opinions on the protection of personal data of children, including an opinion addressed to school authorities. This opinion is concerned with the protection of information about children. It is aimed primarily at those who handle children’s personal data. In the context of schools, this will include teachers and school authorities in particular. The purpose of the document is to analyze the general principles relevant to the protection of children’s data, and to explain their relevance in a specific critical area, namely, that of school data.

The document distinguishes between the fundamental principles (in the general sense as well as in the sense of the Directive 95/46/EC) and education-related principles by demonstrating how fundamental principles can be specified with regard to the school context. For the purposes of the Module, it is worth having a closer look at the school-related principles.

3.1. Student Files

3.1.1. Information

There are countries where legislation permits school authorities to require forms, containing personal data, to be completed for the purpose of creating student files. On forms such as these the data subjects should be informed that their personal data will be collected, processed, and for what purpose, who are the controllers, and how the rights of access and correction can be exercised. Personal data must only be included in student files where necessary for the legitimate purposes pursued by the schools and should not be used in a way incompatible with these purposes (Article 6, b of the Directive) The data required must not be excessive.

3.1.2. Non-discrimination

Some of the data contained in the above-mentioned forms can possibly cause discrimination, for example, data relating to race, immigrant status, or suffering from certain disabilities. This information is usually collected to make sure that the school is aware of, and devotes the necessary attention to, pupils with cultural (for example, linguistic) or economic difficulties.

All data that might lead to discrimination must be protected by proper security measures, such as processing in separate files, by qualified and designated people, subject to professional secrecy, and other appropriate measures. The consent to the processing of all data that can cause discrimination must be clear and unambiguous.

3.1.3. Principle of Finality

There are cases where school authorities provide the names and addresses of their pupils to third parties, very often for marketing objectives. This constitutes a breach of the finality principle, as data intended for school aims are being used for incompatible purposes. In accordance with Art. 6. 1) b) of Directive 95/46/EC, children’s data cannot be used for purposes incompatible with the one that justified their collection. If data of parents and/or pupils are requested by a third party for marketing purposes, their transmission should always

---


67 Ibid., p. 12

68 Ibid.
be subject to the prior information and consent of the legal representatives (and of the children, depending of their maturity)\(^69\).

### 3.1.4. School Results
There are countries with long established traditions of publishing results. The purpose of this system is to allow comparison of results and facilitate possible complaints or recourse. Schools shall, in those countries, strictly follow the rules set by national law and publish only the minimum of personal data necessary for that purpose.

A special problem concerns the publication of school results on the internet, which is a convenient way of communicating them to the interested persons. The risks inherent in this mode of communication demand that access to the data should only be possible with special safeguards. This might be achieved by using a secure website, or personal passwords assigned to the legal representatives or, when they are already mature, to the children.\(^70\).

### 3.1.5. Retention and Elimination
The general principle whereby no data should be kept for longer than is necessary for the purpose for which it has been collected is applicable to this context as well. Therefore, careful consideration should be given as to which data from school files should be kept, either for educational or professional reasons, and which should be erased, for example, those concerning disciplinary procedures and sanctions\(^71\).

### 3.2. School Life
Data protection questions emerge in some areas of daily school life. There are means of control of the school population, especially pupils, which can be particularly intrusive.

#### 3.2.1. Biometric Data
Over the years, there has been an increase in access control in schools. This access control may involve collecting, at entry, biometric data such as fingerprints, iris, or hand contours. The proportionality principle should be applied to the use of these biometric means as well. It is strongly recommended that legal representatives have available to them a simple means of objecting to the use of their children’s biometric data. If their right to object is exercised, their children should be given a card or other means to access the school premises concerned\(^72\).

#### 3.2.2. Closed Circuit Television (CCTV)
There is an increasing tendency to use CCTV in schools for security reasons. There is no recommended solution valid for all aspects of school life and for all parts of schools. The capacity of CCTV to affect personal freedoms means that its installation in schools requires special care. This means that it should only be installed when necessary, and if other less intrusive means of achieving the same purpose are not available. The choice of location of CCTV cameras should always be relevant, adequate and non-excessive in relation to the purpose of the processing.

#### 3.2.3. Children’s Photos
Schools are often tempted to publish (in the press or on the internet) photos of their pupils. Special attention should be drawn to the publishing by schools of photos of their pupils on the

\(^{69}\) Ibid., p.13  
\(^{70}\) Ibid., p.14  
\(^{71}\) Ibid., p. 15  
\(^{72}\) Ibid.
internet. An evaluation should always be made of the kind of photo, the relevance of posting it, and its intended purpose. Children and their legal representatives should be made aware of the publication. In the case of collective photos, namely of schools events, and always in accordance with national legislation, schools might not require prior consent from the parents where the photographs do not permit easy identification of pupils. Nevertheless, in such cases schools must inform children, parents and legal representatives that the photograph is going to be taken and how it will be used. This will give pupils the opportunity to refuse to be included in the photograph73.

3.2.4. School Statistics and Other Studies
In most cases, personal data are not needed to obtain statistics (nevertheless, it can happen in exceptional cases; for instance: when statistics are made on professional integration). According to Art. 6 e) of the Directive, statistical results should not lead to any identification of data subjects, be it direct or indirect.

4. Transparency and Access to Information in Education

4.1. Transparency Definition and Dimensions
Cambridge English Dictionary generally defines transparency as the quality of being done in an open way without secrets74. According to the Merriam Webster Dictionary, if something is transparent it is characterized by visibility or accessibility of information especially concerning business practices75. Transparency International (2006) defines transparency as the clarity of the regulations and procedures within the organization on one hand, and between the organization and the citizens using their services on the other hand. This includes open procedures, goals and targets in the work of the institution. It also includes ensuring the right of citizens to obtain the necessary information76.

Transparency is contrary to secrecy. Secrecy means to hide actions intentionally and deliberately, whereas transparency is considered an instrument which provides information on the facts that concern the public, the ability of citizens to participate in political decisions, and the responsibility of the government in the legal process.

The dimensions of transparency are: clarity, openness, accuracy, ease of access to information and participation in decisions made at the various administrative levels.

All these dimensions shall be consistent with the supreme public interest. Thus, transparency does not require the disclosure of secrets that could affect the security of the state or individuals77.

4.2. Legal Background of Transparency
The concept of transparency in the European legislation is closely related to that of privacy and personal data processing. Preliminary provision 39 of the Regulation 2016/67978 decrees

73 Ibid.
75 https://www.merriam-webster.com/dictionary/transparent
77 Ibid.
that any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.

Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.

The Regulation further enacts that the principle of transparency requires any information addressed to the public or to the data subject to be concise, and, additionally, where appropriate, visualisation to be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising79.

Importantly, the Regulation takes into consideration the interests of children emphasizing that they merit specific protection. Thus, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand80.

Moreover, the principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. The data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing81.

Finally, in order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be

---

79 Ibid., preliminary provision 58.
80 Ibid.
81 Ibid., preliminary provision 60.
encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services82.

Although any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law, this does not in prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned83.

4.3. Concept of Access to Information

Pursuant to the above mentioned provisions, freedom of information is an inherent dimension of transparency. Freedom of information can be defied as access by individuals to information held by public authorities84.

4.4. Transparency in Education

National Institute for Learning Outcomes Assessment (US) treats transparency as making meaningful, understandable information about student learning and institutional performance readily available to internal and external audiences. Information is meaningful and understandable when it is contextualized and tied to institutional goals for student learning. Meaningful information may include disaggregated results, by major field, student level, gender, race and ethnicity, and by providing longitudinal analyses and perspectives and/or comparisons with national norms or peer institutions85.

The present-day use of the term in Russian education practices tends to be distributed among three models:

- **operational transparency**, i. e. equal accessibility of education for everyone, independent from inherent characteristics (age, current knowledge level), which is provided, inter alia, by means of distance learning and non-system educational services; possibility of learning at a pace which is comfortable for the student;
- **institutional transparency**, i. e. trying to consider interests of all education process participants; providing to education consumers the possibility of taking active participation in building and developing the education system, in assessing and managing the quality of educational services (including through governance boards: governing councils, community councils, etc.); consideration of external sociocultural conditions and demands of contemporary society by the education system;

82 Ibid., preliminary provision 100.
85 http://www.learningoutcomeassessment.org/TransparencyFrameworkIntro.htm
information transparency, i.e. providing a two-way exchange of information among different players of the education process or any other parties concerned to ensure that stakeholders’ demand for information about activities of the education system is satisfied and that educational institutions and/or governing bodies can get the necessary feedback.\textsuperscript{86}

4.4.1. Requirements for Schools in terms of Educational Transparency in Russia

Subsequent to the Russian Federal Law on Education, there is a Regulation of the Government of the Russian Federation as of July 10, 2013 No. 582\textsuperscript{87} enacted that specifies the scope and content of information that an educational institution shall post on an open source web-site in order to correspond to the Federal Laws On the Personal Data and On Education in the Russian Federation.

According to the Regulation, an educational institution shall post on its official website, among other information provided for by the law:

a) information concerning: date of incorporation of an educational institution, its address, opening hours, phone numbers and e-mails; structure and governing bodies of an educational institution; names and positions of the administrative persons; level of education provided by an educational institution; modes of study available; set duration of training provided; description of an educational program; academic calendar/schedule; number of pupils/students studying on a budgetary basis as well as for a tuition fee; languages of instruction; federal state educational standards; head of an educational institution and its deputies, including their names, positions, phone numbers and e-mails; teacher staff indicating their degrees, qualifications and work experience, as well as their names, positions, disciplines taught, academic ranks and titles, advanced professional training and retraining; scholarships and social support; employment of graduates;

b) copies of articles of association and license for exercising educational activities;

c) other information in correspondence to the current legislation.

An educational institution shall update the available information within 10 working days since its alteration.

Importantly, the software used for web-site support shall ensure, among other things, a possibility to back-up data and data protection from its deletion, modification and blocking as well as other illegal or inappropriate actions;

4.4.2. International Requirements for Website Transparency

The National Institute for Learning Outcomes Assessment (NILOA) has developed a Transparency Framework\textsuperscript{88} to support institutions in sharing evidence of student learning on and off campus. The Framework is based on a review of institutional websites and identifies six key components of student learning assessment. Institutions may use the Framework to


\textsuperscript{87} Regulation of the Government of the Russian Federation as of July 10, 2013 No. 582 On the approval of requirements for posting and updating of information concerning educational institution on the official website of an educational institution in the data telecommunications network Internet.

examine their institutional websites to gauge the extent to which evidence of student accomplishment is readily accessible and potentially useful and meaningful to the intended audience. Each section of the Framework suggests a component of student learning assessment that may be of interest to specific audiences and outlines opportunities to advance public understanding.

The Framework also incorporates basic premises about website communication. For instance, information placed on websites should be meaningful and understandable to multiple audiences. To effectively communicate with various audiences, the website should enable users to provide feedback or offer comments on the posted material.

A fully transparent website might well contain information about the six components indicated below.

4.4.2.1. Student Learning Outcomes Statements
Student learning outcomes statements clearly state the expected knowledge, skills, attitudes, competencies, and habits of mind that students are expected to acquire at an institution of higher education.

4.4.2.2. Assessment Plans
Campus plans for gathering evidence of student learning might include institution-wide or program specific approaches that convey how student learning will be assessed, the data collection tools and approaches that will be used, and the timeline for implementation.

4.4.2.3. Assessment Resources
Assessment resources encompass information or training provided to faculty and staff to help them understand, develop, implement, communicate, and use evidence of student learning.

4.4.2.4. Current Assessment Activities
Current assessment activities include information on a full range of projects and activities recently completed or currently underway to gauge student learning, make improvements or respond to accountability interests.

4.4.2.5. Evidence of Student Learning
Evidence of student learning includes results of assessment activities. This may include evidence of indirect (e.g. surveys) and direct (e.g. portfolio) student learning as well as institutional performance indicators (e.g. licensure pass rate).

4.4.2.6. Use of Student Learning Evidence
This component represents the extent to which evidence of student learning is used to identify areas where changes in policies and practices may lead to improvement, inform institutional decision-making, problem identification, planning, goal setting, faculty development, course revision, program review, and accountability or accreditation self-study.