Ανοικτή Εκπαίδευση: το περιοδικό για την Ανοικτή και εξ Αποστάσεως Εκπαίδευση και την Εκπαιδευτική Τεχνολογία

Τόμ. 19, Αρ. 1 (2023)

Open Education - The Journal for Open and Distance Education and Educational Technology

GDPR and education: an approach for e-learning in Greek schools

Aikaterini Daoultzoglou

doi: 10.12681/jode.31195

Βιβλιογραφική αναφορά:

GDPR and education: an approach for e-learning in Greek schools

Aikaterini Daoultzoglou
Εκπαιδευτικός Πληροφορικής
Διεθνές Πανεπιστήμιο της Ελλάδος
katiadaoultzoglou@gmail.com
https://orcid.org/0000-0002-7134-3225

Abstract

The General Data Protection Regulation, from now on GDPR, was put into action in May 2018. It sets important guidelines that must be adhered to by any entity collecting personal information about individuals residing in the European Union. Amongst the entities that have to comply with the new Regulation are schools. This paper focuses on primary and secondary education· it covers a range of controversial issues and aims to provide an overview of a schools' obligations and responsibilities vis a vis GDPR. It determines major definitions in terms of school reality, enlightens basic blur points, and stipulates what schools as Data Controllers must do. Moreover, the special case of distance learning amidst the Covid-19 pandemic is thoroughly analyzed. Due to rush transition to e-learning platforms plenty GDPR issues occurred and they are presented in this paper. Finally, a couple of possible, mainly technical, solutions are proposed to the difficulties that might emerge in the effort to build a strong GDPR school environment. The importance of GDPR compliance is apparent and indicated in every chapter.

Keywords

GDPR, schools, personal data, e-learning, distance education, Sars-CoV2

1. Introduction

It was Clive Humby who first coined the parallelism of data to oil back in 2006 to denote that data are just like crude: "It's valuable, but if unrefined it cannot really be used." (Politou, Alepis, & Patsakis, 2018). With this comparison we can figure out the importance of data nowadays. The General Data Protection Regulation (GDPR), entered into force in the European Union (EU) in 2018, dictates the rules for collecting and processing data about EU residents and is a notable recent example of a pan European move towards stricter data privacy laws (Duncan & Joyner, 2021). As a regulation and not a directive, GDPR is directly an enforceable law in all Member States (Politou, Alepis, & Patsakis, 2018).

Education is a sector that is indissolubly connected with data and directly affected by those changes. This paper focuses on secondary education and touches upon the aspect of distance education by explaining how schools can be exposed due to the noncompliance with the new Regulation. It is a literature review that surveys researches, articles and legal Opinions so as to provide full knowledge of the GDPR application in schools and especially regarding to the Covid period. The paper in hand aims to be used as a short handbook for school administrators or as an informing tool for students, which clarifies key points about personal data in schools and about the actual legal steps taken for distance education in following 4 sections.

Firstly, in chapter 2 necessary definitions concerning schools that compound the core values of the General Data Protection Regulation are determined. After that, basic rules that every school must abide by are mentioned in chapter 3. It is very easy for clashing points to be created with artificial intelligence solutions. The educational trends do not escape the use of cloud computing (Amo, et al., 2020).

Sudden and unforeseen changes to society may have a significant impact on critical functions and services (Bergdahl & Nouri, 2020). In the wake of covid-19, school reality changed radically. Covid 19 prevention measures prompted a rapid transition from traditional to distance education. Synchronous and Asynchronous methods were used to seamlessly continue the educational procedure. Famous platforms that were used for this reason have valorized personal information for commercial purposes(Lupton & Williamson, 2017). Plenty conflicts with Data Protection Regulation were observed

and in chapter 4 are highlighted. Nevertheless, there are helpful measures that can be taken in order to avoid or limit those conflicts and are presented in chapter 5.

2.Key Terms/Definitions

Personal Data is anything that can make an individual identifiable (GDPR Art. 4(1)). Personal data can be a hobby, someone's job, marital status, natural characteristics, a bank account, an IP address. As far as *schools* are concerned, they collect various *personal* data that are considered to be: names of students, names of teaching staff, contact details of parents, addresses, medical files. Secondly, educational data such as reports, class listings, grades. Thirdly, professional records, like employment history of teachers/professors, taxation information, reports, evaluation documents. At general, any information on active and past students and their family members, information on visitors, co-workers, partners etc. (Vejmelka, Katulic, Jurić, & Lakatoš, 2020). *Sensitive* personal data at schools can be: biometric data of students (e.g. a video), religion beliefs (e.g., the choice of a student to desist from attending Religion courses), health data (e.g., allergies), several nutritional limitations (that can imply a health issue or religious creed) (Hellenic Center for Safer Internet, 2018). Sensitive personal data are highly relevant because they are subject to a higher level of protection.

For instance, a photograph is characterized as personal data as well, because individuals may be directly or indirectly identified. So, a photograph from a school event is 'suitable' to store or upload when we ensure that people depicted in this picture are not identifiable. Blurring the faces of depicted students could be a solution, but patently, it is not efficient to blur a child's face but save it in a file named with the child's forename (Hellenic Center for Safer Internet, 2018).

'Processing' means any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, erasure or destruction; (GDPR Article 4(2)). GDPR affects every entity which processes personal data as part of their activities. Schools which are "rich" in data fall within the scope of this Regulation. This Regulation has brought about many changes in the way of electronic storage, process and transmission of data (Hellenic Center for Safer Internet, 2018).

The key distinction to be noted is between the "Data Controller" and the "Data Processor". 'Controller' means the *natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union (Article 4(7))* while 'processor' means *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR Article 4(8)).*

The Data Controller is the organization which determines the reasons for which data will be processed and the manner in which this will be done. The data processor is a third party which processes data on behalf of a data controller, for example when providing outsourced services (Unknown, Data Protection Toolkit - Personal Data Breaches: are you prepared?, 2018).

Schools hold significant amounts of personal data about a variety of data subjects. The Data Subject is the individual person about whom personal data is held. The key focus is likely to be on data about pupils, but it is important to remember that schools will also hold personal data about parents, employees and non-employed staff, and contacts at the local authority such as social workers, cleaners who represent Data Subjects as well.

In terms of the Greek school community, the Ministry of Education is the organization who determines the purpose for which, and the manner in which data are processed in educational procedure. Schools do appertain to the Ministry so they are entities under the direct supervision of the Data Controller (the Ministry) that are authorized to process personal data. So, from now on schools might be referred to as Data Controllers but are actually the authorized body that acts under the direct monitoring of the Data Controller. The Data Processor is a person or organization who processes data *on behalf of* and *on the orders* of a controller, such as a catering supplier the school uses.

Personal data in schools are collected, stored and processed on a daily basis, which entails for the Data Processor, knowledge of different regulations (Vejmelka, Katulic, Jurić, & Lakatoš, 2020). As Data Controllers, schools should define their own policies,

for instance policies about trips and activities, catering and free school meal management, safeguarding, medical information and administration.

3.Preparedness and Obligations

Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing (Recital 39 (12)). Figure 1 illustrates some of schools' obligations in terms of GDPR compliance. As a result, both teaching and administrative staff should be extremely careful and apply in their every-day school life some essential rules that contain physical and technical security practices. For example, storage only at school equipment,antivirus protected computers, secure printing, clear screens at regular intervals, automated locking to unused devices, encrypted external mediums, strong passwords, data protection auditing are some of the measures that can be taken to ensure organization's data safety and security. It is a tremendous fact thatin 2020 23.6 million accounts had set a "123456" password (not only at schools, in organizations general) (Hunt, 2020).They all must therefore sign an inside Privacy school Policy where they commit to follow the rules and take full responsibility of their actions in and out of school's facilities, so as school can provide safe and secure access to technologies and ensure the smooth running of the school (Department for Education, n.d.).

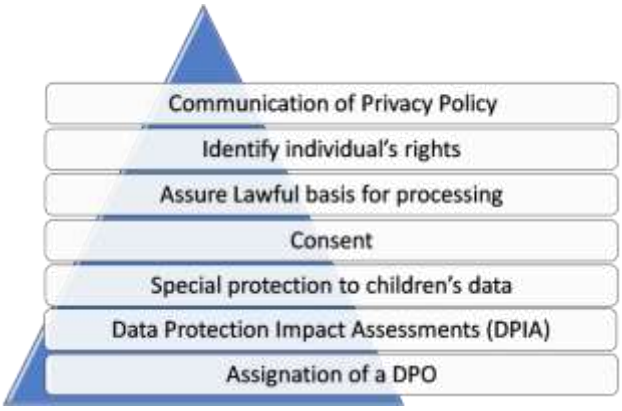

Figure 1: School's obligations

Secondly, articles 15 – 22 describe the eight rights that GDPR provide toindividualsand those are:

- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction of Processing
- Right to be notified
- Right to Data Portability
- Right to Object
- Right to Reject Automated Individual Decision-Making and Profiling

Briefly, data subjects have the right to be informed about the collection and use of their personal data, to access their personal data which have been collected concerning them, to object to school's data processing, including profiling, when it is on relevant grounds. What is more, they can request to copy or transfer personal data easily from one IT environment to another in a safe and secure way. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her or the rectification of inaccurate or incomplete personal data without undue delay. Once a user lawfully requests to remove their data, the erasure should be performed in the backups as well (Politou, Alepis, & Patsakis, 2018).Third parties must also be informed as well.

Thirdly, there must be a valid lawful basis to process personal data (GDPR Recital 40). No single basis is 'better' or more important than the others; Schools are classified as public authorities, so the public task basis is likely to apply to much of their processing. If the processing is separate from their tasks as a public authority, then the school may instead wish to consider whether consent or legitimate interests are appropriate particular circumstances (Office, n.d.). Lawful basis and reasons for processing must be determined before the beginning of the processing, and it should be documented in school's privacy notice. A school needs to consider its basis carefully.

Where processing is based on consent (either of parents or of children), school must demonstrate that the data subject has consented to processing of their personal data (GDPR Article 7(1)). Recital 43 of GDPR aims to ensure that consent is freely given.

Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. So, any additional processing operation, demands additional consent, under the GDPR. It should be stressed that school admins should act proactively and manage to get the consent early (Duncan & Joyner, 2021).

Minors merit specific protection regarding their personal data, as they are identified as vulnerable natural persons and may be less aware of the risks, consequences and safeguards (Recital 38). Processing of data relating to children is noted to carry certain risks and further restrictions may be imposed (Smith, Gibbons, & Kuncewicz, 2021). Data controllers (i.e., schools) hence have to tailor their notices accordingly assuming the level of comprehension of the age groups.

Privacy by design encounters the privacy taken into account throughout the entire software or system engineering and roll out process, from design to production and operation (Europe, 2018). It stands for privacy being incorporated within the lifecycle of an IT system or process development as early as its initial specifications setting and design. (Cranor & Spiekermann , 2009). With the rise of GDPR, data implementation by design and by default is now a data controller's obligation (GDPR Article 25). So, schools as Data Controllers shall implement appropriate technical and organizational measures, such as pseudonymization, or data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to protect the rights of data subjects, under the GDPR requirements.

Privacy has both a personal value and a cultural/society value. Children do not have an understanding of privacy, like adults have. They give descriptions of privacy like "to be alone", "to hide secrets or special things", "to not talk to strangers" (Zhang-Kennedy, 2017). This means that school platforms designers to convey a message to children about consent and data protection. So not only a good, GDPR compliant privacy policy is needed to be designed, but also those designs should be child-friendly from a designer that understands the context in which those children are familiar with (Dempsey, Sim, & Cassidy, 2018).

Last but not least, every organization or company which processes personal data in the Union, under the provision of article 37, is required to appoint a DPO.Ministry of Education as a Data Controller, via its 'representatives', that are schools, must

designate a named DPO in order to comply with new legislation. His/her contact details should be available to data subjects and their role is monitory, advisory and informative, and acts as an intermediary between organization (school) and the supervisory authority (Data Protection Authority).

To sum up, data must be lawfully, fairly and transparently collected. It must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. It needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. It must be accurate, and where necessary, kept up to date(Smith, Gibbons, & Kuncewicz, 2021).

Adherence to the GDPR is important from an ethical standpoint, but also from a legal standpoint (Duncan & Joyner, 2021). Fines for non-compliance with GDPR reach up to €10 million - €20 million total worldwide annual turnover of the preceding financial year. Furthermore, extra cost can burden schools' budget in case of a cyber attack. Attacks happen across and from all nations and regions (Phillips, 2021)· in the UK, for instance, one in five schools, i.e., almost 25% have been a victim of cyber-crime in the education sector (Ashton, 2018).

4.E-learning and GDPR issues

I. *Synchronous and Asynchronous Education*

With the spread of global pandemic Sars-CoV-2 in March of 2020 there was a huge 'pile' of GDPR issues, and many ambiguous questions arose. All Greek educational institutions ceased accepting students onsite and turned to online teaching platforms in order to continue the educational process. However, this happened extremely fast · both public and private schools had to adapt their teaching methods using alternative tools in a fast-track procedure, without the proper analysis and design of needs and requirements. As a result, there are identified points of impact with GDPR elements. Some of those issues headed to the road of justice, where the Greek DPA took some decisions and imposed a couple of reprimands on the Ministry of Education for severe infractions of GDPR ordinances, as mentioned later.

First, we have to define what Distance Education means. Britannica's entry includes the following: "Distance learning, also called distance education, e-learning, and online learning, a form of education in which the main elements include physical separation of teachers and students during instruction and the use of various technologies to facilitate student-teacher and student-student communication". With no doubt, advances in technology have changed people's lives and affect the educational sector as well. The use of computers and internet is not just something that is recommended but it is becoming even more necessary. In this sense, electronic learning (e-learning) is now the key term that refers to the process of modernization of education (Stanojević, Cenić, & Cenić, 2018). There are two types of distance learning methods: synchronous and asynchronous and therefore several teaching platforms have been implemented to cover those needs.

The asynchronous teaching method allows users to study at whatever time, at any place, at their own pace. Students can participate in multiple activities, such as filling online quizzes, solve exercises, submit assignments, watch slideshows and videos, and in some cases live chat with the professor. The student can receive immediate feedback about their performance. Besides that, some platforms like Cognii, Nuance, Carnegie with the help of AI mechanisms monitor students' progress, extract conclusions, alert professors and subsequently create profiles. When school directors use an online system must always bear in mind that by collecting personal data on proprietary platforms the latter have a commercial motive to exploit these data (Lupton & Williamson, 2017).

Building a profile presupposes the collection of data and keeping records of students' every interaction with the system, even the day and time they last logged. This philosophy is opposite to Article 22 of GDPR, about profiling and automated decision-making systems. Children are not aware of possible ramifications of this datafication, and little do they know about how companies exploit and use their personal data. They are converted to 'calculable', 'datafied' persons whose data are used as input in algorithms to export valuable statistics and build distributed systems (Lupton & Williamson, 2017).

Synchronous teaching methods include teleconference meetings where participants have real time access with their tutor, and the traditional lesson is replaced with a

video call. Instructors have to prepare their material properly and try to adjust the learning procedure through a virtual classroom where they manage to simulate the actual class and cover the needs of students. Means of communication are camera, microphone and user's screen. Some platforms store teleconference sessions that the student or tutor can rewatch again. Popular platforms that incorporate teleconference technologies and suggested for educational purposes are Cisco's WebEx, Google's Google Meet, Zoom, Microsoft Teams.

Common features shared by all platforms are flexibility, ease of use and user friendliness. A Learning Management System (LMS) is a web-based software package that might combine both synchronous and asynchronous interaction. It is widely used to improve students' learning experience. It is designed to plan, implement and evaluate learning, give performance feedback and manage students' activities(Kasim & Khalid, 2016).

Transparency reflects the idea of visibility meaning that there is nothing to hide by the means of any intermediate obstacle between personal information and data subject (parent or child). In any case "transparency increases trust in applications" (Murmann & Fischer-Hubner, 2017).

II. *Related Work*

Table 1 illustrates the characteristics of each learning method (synchronous and asynchronous) and their clashing points with GDPR elements, as those were recorded by Mougiakou at al. (Mougiakou, Papadimitriou, & Virvou, Synchronous and Asynchronous Learning Methods under the light of General Data Protection Regulation, 2020). Synchronous learning methods use means such as camera, microphone, sharing screen and exchanging files. Asynchronous learning methods might utilize an ITS (Intelligent Tutoring System) where it stores user's answers, preferences, maintains historical records, allows users' communication with a chat box, and keeps tracking of users' options. It provides personalized experience to the student due to a smart inference mechanism.

Table 1: Characteristics of the two categories of learning methods and their impact with GDPR elements [21]

	GDPR Transparency				
Means/ GDPR elements	Consent	To be informed	To be forgotten	Of access	To object
Microphone	X	X	X		
Camera	X	X	X		
Sharingscreen	X	X	X		
Exchangingfiles	X	X	X	X	X
Text, slides, images, videos		X	X	X	X
Assignments (exercises, quizzes, games)	X	X	X	X	X

So, before the sharing of personal data such as a student's name, face, voice, the platform must inform and request user's consent for the availability of data they share when using those means. Additionally, the right to be informed, to be forgotten, the right of access and to object must be exercised as well in a proper and friendly to minors way in order to reassure transparency with GDPR requirements.

III. *The Greek Case Study*

Educational process inconstantly developing and improving, and teaching aids also are modernizing (Stanojević, Cenić, & Cenić, 2018). What actually happened in Greece the last two years during the pandemic with the closure of schools was a hybrid mixture of synchronous and asynchronous methods to replace physical teaching.LMSs were the learning tools that were mostly used. In that way, the educational procedure was smoothly continued, without the fear of spreading the virus.

Nevertheless, user data collection and processing, within the case of minors or adolescents is a zone of special concern. Many issues ensued and even more questions remained unanswered till recently, such as:

- Who is the data controller of children's personal data?
- Who is the data processor of children's personal data?
- What is the retention period of those data after the sessions' end?
- Is there a legal base for data collection, storage, and processing?

- Are minors aware of their rights? (Of Access, to be Forgotten, to be Informed)
- Are those rights fully covered by those applications or are they trespassed?
- Do students provide their consent where needed?
- Do those systems take advantage of AI elements?
- And eventually, are those platforms GDPR compliant?

Considering the aforementioned adversities in between GDPR orders and modern learning methods' tools, the negative responses to those questions and the lack of transparency are foreshadowed. In the case of Greek public schools, first answers were given in September of 2020 through opinion 04/2020 by the Hellenic DPA (Data Protection Authority, 2020). So, Data Controller is the Greek Ministry of Education while Data Processor is Cisco Hellas S.A., a company that the Ministry entered into a contract with. The latter company is referred to as a third party. The Ministry of Education published the company's Privacy Data Sheet and confirms that only anonymized metadata are kept by Cisco Hellas only 3 months after the end of contract for research and statistical reasons, but users' data are totally erased at expiration date of the contract. Also, any AI feature is deactivated, such as "Face Recognition" and "People Insights". The provisions of public education and public interest objectives were determined as legal base for personal data processing (GDPR Article 6 (1)). Data subjects, i.e., students are informed about the procedure of Distance Learning (GDPR Article 12-14) and all relevant information are included inn. 57233 ministerial decree (Government Gazette, 2020). Only live streaming of a teaching lesson is allowed, while video recording or storing is prohibited and disabled. Finally, according to Article 63 of n.l.4686/2020, in cases of partial or total suspension of operation of an educational institute due to emergency or unforeseen reasons, synchronous distance learning can be applied.

To sum up, regarding all the above facts, the Data Protection Authority judged Synchronous Distance Learning as legal, taking into account that:

- Educational procedure is a public commodity and must necessarily be continued with best-fit adjustments
- Synchronous Distance Learning is a useful educational tool with high utility especially in pandemic periods

- Personal data processing can be conducted in a compatible with GDPR way.
- A three-month period of time is given to Ministry of Education in order to make the proper changes and achieve compliance

On the other hand, there are many logical but not 'lawful' leaps about the previous statements. Several research took place by analyzing thoroughly Ministry's claims and therefore Decision 50/2021 of DPA (Data Protection Authority, 2021)contains the five (5) reprimands that were imposed to the Ministry of Education for violations of GDPR, specifically infringement of articles 6, 13, 5 (1), 12, 37 (7), 25(1), 35 (9) and 46(!). Afterwards, DPA gave a two-month period notice to confront with Articles 6, 13, 5(1), 12, 37(7), 25(1) and four months to reckon with Article 46 as described in the Decision (Data Protection Authority, 2021).Ministry submitted the memorandum at less than two months from the end of first deadline according to DPA's communiqué (DPA, 2022), but there is not an announcement for the second one. Table 2 demonstrates all the violations referring to each Article separately. Analytically:

Table 2: Opinion 50/2021 summary

Article	Category/Provision	Violation
Article 6	Lawfulness of processing	Processing is necessary for specific purposes where actually kids' personal data are kept for seven years for analytics and performance measurement of the platform
Article 13	Information to be provided where personal data are collected from the data subject	Data controller did not provide the data subject with privacy policy, its identity, and purpose of personal data processing as they were obliged to. The one that was provided was too general, unstructured, unsuitable for kids (difficult to understand) and vague.
Article 5(1)	Principles relating to processing of personal data	The "lawfulness, fairness and transparency" constitutes data protection's fundamental principle and this is not to be reassured. Sophisticated research is missing by Cisco.
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject	Data Processing information must be characterized by a "concise, easily accessible form", being "intelligible", "easy to understand", using "clear and plain language". It has been noted that kids were not aware of risks and they were provided with less and not straightforward information than they should.

Article 37(7)	Designation of the data protection officer	The Ministry of Education lacks in updating special applications or the Ministry's website with DPO's contact information, as Art. 37 (7) defines
Article 25(1)	Data protection by design and by default	End-to-end encryption is missing, and data minimization is not applied because the provided function would be 'less effective'
Article 35 (9)	Data protection impact assessment	"Controller shall seek the views of data subjects on the intended processing". This movement can prove high level of transparency and therefore high level of trust to the data controller, but Ministry of Education did not only omit this obligation but also it characterizes this as a stalling of time
Article 46	Transfers subject to appropriate safeguards	''A controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards''. According to Cisco's Privacy Data Sheets user's data are kept only in Europe. But the Ministry says that Cisco uses different mechanisms that have to be followed in order to freely provide the WebEx platform. And those contractual clauses are integrated in the "Master Data Protection Agreement". Based on this agreement data must be transferred to the established in the USA Cisco. So, it is outside the European territory and falls under American Law, where there is not a sufficient level of personal data protection.

Consequently, it is easily implied that schools, despite the plenty Covid confirmed cases, did not turn to distance learning throughout the 2021-2022 academic year because the above-mentioned reprimands were not totally solved. They were maybe foreseeable somehow to an extent, since further research was made and a lot of infringements of GDPR were more than obvious. Those platforms must be built under a culture of transparency in data processing activities that are supported by a privacy by default and privacy by design approach(Osano, 2021).

5.Proposed solutions

We live in a computer era that requires us more and more frequently to make radical changes in the implementation of the teaching process and get modernized to overcome the weaknesses of still dominant traditional teaching (Stanojević, Cenić, & Cenić, 2018). But it requires a special effort to make information attractive and understandable to children of different ages, for example by visualization or producing short video clips (Lievens & Verdoodt, 2018). How can new, essential-to-education technologies be combined with GDPR orders? Mougiakou at al. suggest a couple of ways (Mougiakou, Papadimitriou, & Virvou, Intelligent Tutoring Systems and Transparency: The Case of Children and Adolescent, 2018) that synthesize graphic solutions to Regulation's requirements. Pop-up notice or adjacent clickable check boxes could inform/ask students over the right to allow or deny consent.

With a popular to the students illustrated icon, for instance a small door with the sign 'enter', students can enter in an environment where they can see their data that are maintained by the platform, check the recipients of those data, the rights that they can exercise, to read terms and conditions of digital services provided. In this way Right to be Informed is illustrated and minors can be informed about several notifications such as Privacy Policy, data Breaches, Data Controller's contact information, Data Collection retention period, possible rule changes, educational purposes of data processing.

The student must be provided with a delete option through an understandable icon resembling a recycle bin. With this, they can delete all/some of their personal data that are stored and the Right to be Forgotten can be smartly depicted. For exercising the Right to object, a flagship sign like a traffic stop can represent the data processing refusal option.

Future school preparedness plans (national planning) must include digital tools that function well for distance education and are GDPR compliant (Bergdahl & Nouri, 2020).

Finally, Amo et al. propose a framework that can be implemented inside the physical classroom composed of seven principles to foster privacy, that is called LEDA (Local Educational Data Analytics)(Amo, et al., 2020). It advocates the philosophy "better act local with no data transfer outside the classroom" than "remote connection with data

transfer to cloud computing". The "local first" principle does not exclude any technology; it just opens up a new field of research that keeps remote solutions at bay. The so-called zero distance technology is about protocols such as Wi-Fi, Bluetooth, NFC, QR codes or barcodes combined with a camera. The adoption of this principle can ensure non-leakage, non-misuse, non-prohibited or inappropriate storage and non-processing without permission.

6.Conclusions

At present, most of the population in the European Union has been activated into thinking about data regulation and protection due to the GDPR over the last four years (Nevaranta, Lempinen, & Kaila, 2020).

The global pandemic crisis of Covid has more or less has affected every part of our everyday life; education included. As a result, our habits have changed, education standards have altered, the children's rights have been affected.

Schools therefore have to adjust their everyday life to the new reality as well. That means that several changes need to be applied by schools, which as authorized entities by the Data Controller, have to meet many obligations.

The term 'dataveillance' refers to collecting information using forms of data (Raily, 2013). Unlike other sectors, education is yet to fully realize the benefits of digital and advanced AI techniques, and there are great opportunities to improve learning outcomes and to enable better teaching (Gray, 2020). Distance learning platforms, planted on the cloud, take advantage of those techniques by providing personalized feedback and by building separate profiles for students. Schools turned to this method and to distance learning during covid-19 pandemic as the only way to continue the educational procedure. But there are many clashing points with GDPR that have to be confronted. Nine articles have violated in regard to transparency, lack of privacy policy and DPO's contact information, territorial scope of data and discrepancy according data retention period.

Survey conducted at Croatian schools indicates that approximately 56% of teachers/principals are fully or partially familiar with GDPR and the rest not familiar at all (Vejmelka, Katulic, Jurić, & Lakatoš, 2020). Future work should examine the current

situation in Greece; specifically, by enumerating how many schools are actually GDPR compliant, by comparing to what extent teaching staff is informed about several provisions and restrictions of the new law, and perhaps by measuring how easily schools have achieved the transition to the new Regulation. Both qualitative and quantitative results would be helpful to map the standing state and to identify the 'gaps' in Greek schools. Afterwards, efforts need to be made in order to bridge those gaps, if they exist, by providing the proper technical, legal and administrative support.

References

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *new media & society, 19*(5), pp. 780-794. doi:10.1177/1461444816686328

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020, May 25). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *applied sciences*. doi:10.3390/app10103660

Amo, D., Torres, R., Canaleta, X., Herrero-Martín, J., Rodríguez Merino, C., & Fonseca, D. (2020, October 20). Seven principles to foster privacy and security in educational tools: Local Educational Data Analytics. *TEEM.* Salamanca,Spain: Association for Computing Machinery. doi:10.1145/3434780.3436637

Ashton, C. (2018). *www.itgovernance.co.uk*. Retrieved October 11, 2021, from Cyber attacks hit a fifth of schools and colleges: https://www.itgovernance.co.uk/blog/cyber-attacks-hit-a-fifth-of-schools-and-colleges

Bergdahl, N., & Nouri, J. (2020, September 2). Covid-19 and Crisis-Prompted Distance Education in Sweden. *Technology, Knowledge and Learning*, pp. 443-459.

Chai, W. (2021, January). Retrieved from https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Cranor, S., & Spiekermann , L. (2009). Engineering Privacy IEEE transactions on Software Engineering. *1*(35), pp.67-82.

Data Protection Authority. (2019, September 10). Decision n.21/2019. Athens.

Data Protection Authority. (2020, September 7). Opinion 4/2020. Athens.

Data Protection Authority. (2021, November 16). Decision 50/2021. Athens.

Dempsey, J., Sim, G., & Cassidy, B. (2018). Designing for GDPR - Investigating Children's Understanding of Privacy: A Survey Approach. *British HCI.* Belfast,UK: BCS Learning and Development Ltd.

Department for Education, U. G. (n.d.). *Data Protection: a toolkit for schools. Open Beta: Version 1.0*. Retrieved from https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

DPA. (2022, January 16). Retrieved July 1, 2022, from https://www.dpa.gr/el/enimerwtiko/deltia/enimerosi-shetika-me-tin-efarmogi-tis-apofasis-tis-arhis-gia-ti-diadikasia

DPA. (2022, January 16). *Data Protection Authority*. Retrieved July 14, 2022, from https://www.dpa.gr/el/enimerwtiko/deltia/enimerosi-shetika-me-tin-efarmogi-tis-apofasis-tis-arhis-gia-ti-diadikasia

Duncan, A., & Joyner, D. (2021, June 22-25). With or Without EU: Navigating GDPR Constraints in Human Subjects Research in an Education Environment. *L@S'21, Virtual Event*. doi:10.1145/3430895.3460984

Duncan, B. (2018). Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing? *CLOUD COMPUTING 2018 : The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization.*

Europe, E. A. (2018). *Handbook on European data protection law*. Retrieved from https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

European, C. (n.d.). *Who does the data protection law apply to?* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

Evers, W.-M. ,. (2021, April 29). *Massive school data breach shows we need better privacy policies*. Retrieved from https://thehill.com/opinion/technology/550959-massive-school-data-breach-shows-we-need-better-privacy-policies

Government Gazette. (2020, May 15). Opinion 57233/Y1. Retrieved from https://www.minedu.gov.gr/publications/docs2020/20200515_%CE%A6%CE%95%CE%9A1859_%CF%84%CE%92_15-05-2020_%CE%A3%CF%8D%CE%B3%CF%87%CF%81%CE%BF%CE%BD%CE%B7-%CE%B5%CE%BE-%CE%B1%CF%80%CE%BF%CF%83%CF%84%CE%AC%CF%83%CE%B5%CF%89%CF%82-%CE%B5%CE%BA%CF%80%CE%B1%CE%

Gray, S. (2020, July 21). Artificial intelligence in schools: Towards a democratic future. *London Review of Education, 18*(2), pp. 163-177. doi:10.14324/LRE.18.2.02

Hellenic Center for Safer Internet. (2018, May 19). *saferinternet4kids.gr*. Retrieved from GDPR in Schools: https://saferinternet4kids.gr/wp-content/uploads/2018/11/gdpr-in-schools.pdf

Hunt, T. (2020, August). *"Pwned Passwords", Have I Been Pwned*. Retrieved from https://haveibeenpwned.com/Passwords

Kasim, N., & Khalid, F. (2016). Choosing the right learning management system (LMS) for the higher education institution context: A systematic review. *International Journal of Emerging Technologies in Learning*, pp. 55-61. doi:10.3991/ijet.v11i06.5644

Kaspersky, G. (2013). *Global Corporate IT Security Risks.* Retrieved 2021, from Kaspersky Lab.

Katulić, A. (2019, January 23). The obligations of libraries under the general data protection regulation: challenges, approaches, and possible solutions. *Vjesnik bibliotekara Hrvatske 61*.

Lievens, E., & Milkaite, I. (n.d.). A children's rights perspective on privacy and data protection in the digital age. Ghent University, Faculty of Law & Technology. Retrieved from https://www.ugent.be/re/mpor/law-technology/en/research/childrensrights.htm

Lievens, E., & Verdoodt, V. (2018). Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. *Computer Law and Security Review, 34*, pp. 269-278. doi:10.1016/j.clsr.2017.09.007

Marković , M., Debeljak, S., & Kadoić , N. (2019, February 27). Preparing Students for the Era of the General Data Protection Regulation (GDPR). *TEM Journal, 8*(1), pp. 150-156. doi:10.18421/TEM81-21

Mougiakou, E., & Virvou, M. (2017). Based on GDPR privacy in UML: Case of e-learning program. *8th International Conference on Information, Intelligence, Systems & Applications (IISA).* Larnaca,Cyprus: IEEE. doi:10.1109/IISA.2017.8316456

Mougiakou, E., Papadimitriou, S., & Virvou, M. (2018). Intelligent Tutoring Systems and Transparency: The Case of Children and Adolescent. *9th International Conference on Information, Intelligence, Systems and Applications (IISA)*, pp. 1-8. doi:10.1109/IISA.2018.8633652

Mougiakou, E., Papadimitriou, S., & Virvou, M. (2020). Synchronous and Asynchronous Learning Methods under the light of General Data Protection Regulation. *11th International Conference on Information, Intelligence, Systems and Applications*, pp. 1-7. doi:10.1109/IISA50023.2020.9284341

Murmann, P., & Fischer-Hubner, S. (2017). *Tools for achieving usable ex post transparency: a survey,*. Retrieved from IEEE Access

Nevaranta, M., Lempinen, K., & Kaila, E. (2020, October 21). Students' perceptions about data safety and Ethics in learning analytics. *2020 Conference on Technology Ethics, Tethics 2020, 2737*, pp. 23-37.

Office, I. C. (n.d.). *Lawful basis for processing*. (ico.org.uk) Retrieved December 12, 2021, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Osano, N. (2021, May 21). *The Eight User Rights Under the GDPR*. Retrieved from privacypolicies.com: https://www.privacypolicies.com/blog/gdpr-eight-user-rights/

Phillips, B. (2021, September). UK further education sector journey to compliance with the general data protection regulation and the data protection act 2018. *Computer Law & Security Review, 42*. doi:https://doi.org/10.1016/j.clsr.2021.105586

Politou, E., Alepis, E., & Patsakis, C. (2018, February 16). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, pp. 1-20.

Raily, R. (2013). 'Raw Data' is an Oxymoron, Dataveillance and countervailance. *Gitelman L (ed.)*, pp. 121-45.

Smith, T., Gibbons, N., & Kuncewicz, S. (2021). *blmlaw.com*. Retrieved from GDPR:12 STEPS: https://www.blmlaw.com/expertise/gdpr-are-you-prepared-/gdpr-12-steps

Stamoulou, P. (2018). *The DPO's role and responsibilities under the GDPR framework.* Thessaloniki.

Stanojević, D., Cenić, D., & Cenić, S. (2018, July 6). Application of computers in modernization of teaching science. *(IJCRSEE) International Journal of Cognitive Research in Science, Engineering and Education, 6*(2), pp. 89-104. doi:10.5937/ijcrsee1802089S

Unknown. (2018, June 15). *Data Protection Toolkit - Personal Data Breaches: are you prepared?* Retrieved from https://www.nicva.org/data-protection-toolkit/templates/personal-data-breaches-are-you-prepared

Unknown. (2018, March 19). *perkinscoie.com.* Retrieved from Article 28 Checklist - Privacy & Security: https://www.perkinscoie.com/en/gdpr/gdpr-article-28-checklist.html

Unknown. (2021, January). *itgovernance.co.uk*. Retrieved from Cyber Security 101 – A guide for schools: https://www.itgovernance.co.uk/reports/cyber-security-a-guide-for-schools

Vanezi, E., Kapitsaki, G., Kouzapas, D., Philippou, A., & Papadopoulos, G. (2020). DiálogoP - A Language and a Graphical Tool for Formally Defining GDPR Purposes. *14th International Conference on Research Challenges in Information Sciences, RCIS 2020.385*, pp. 569-575. Limassol: LNBIP. doi:10.1007/978-3-030-50316-1_40

Vejmelka, L., Katulic, T., Jurić, M., & Lakatoš, M. (2020). Application of the General Data Protection Regulation in Schools: A Qualitative Study with Teachers, Professional Associates and Principals. *43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, pp. 1463-1469. doi:10.23919/MIPRO48935.2020.9245209

Zhang-Kennedy, L. (2017, May). Multimedia approaches for improving children's privacy and security knowledge and persuading behavior change. 84. Ottawa.