

Selected Legal Issues in Online Adult Education: Compliance of Online Learning and Teaching Process with GDPR ¹

Inga Jekabsone

Magnetic Professional Ltd.
Bērzaunes street 6A
Riga LV-1039, Latvia
jekabsone47@gmail.com

Abstract: COVID-19 has had a major influence on the educational system. Since March 2020, the majority of teaching and learning has taken place online, including in the adult education sector. At the same time, the speedy transformation to the online mode has raised various legal issues, particularly regarding data protection, intellectual property rights, and compliance with the national legal framework. This article aims to analyse the compliance of online learning and teaching in adult education programmes with the General Data Protection Regulation (GDPR) and, on the basis of that, make recommendations to adult education entities that offer online teaching and learning process. To achieve the aim, the author uses the following research methods: a doctrinal research method, a scientific literature review, and a survey. As a result, the author identifies various legal issues regarding personal data protection during recording online teaching and learning, such as compliance with the GDPR requirements during online lecturing, compliance of e-platform providers with the GDPR, unauthorised access, data loss, and cyberattacks.

Keywords: *adult education, data protection, GDPR, online education, online teaching and learning*

¹ The article is supported by the post-doctoral research aid programme's project 'Development of online adult learning in response to COVID-19 for digitalization and economic growth of the regions in Latvia' (no. 1.1.1.2/VIAA/4/20/616).

1. Introduction

The educational system has been significantly impacted by COVID-19. Since March 2020, the majority of teaching in the adult education field has been conducted online. Adult education entities all around the world were forced to transition to online teaching mode, culminating in the adult education industry's unprecedented rapid digitisation (Morris & Rohs, 2021; Morris, 2021; Petrushenko *et al.*, 2021). Many scholars stress that forced digitalisation caused unprecedented investments in online adult education instead of other forms (Käpplinger & Lichte, 2020). In many cases, technological advancements lead to higher involvement of adult learners (González *et al.*, 2022), flexibility (Amarneh *et al.*, 2021), and improvement of digital skills (Pokhrel & Chhetri, 2021). At the same time, online learning crystallised various issues, such as the lack of technological resources (Beunoyer, Dupéré & Guitton, 2020), privacy (Neuwirth, Jović & Mukherji, 2021), security in the digital domain (Gamage, de Silva & Gunawardhana, 2020), rights of learners with disabilities (Jameson *et al.*, 2020), and overall anxiety and stress about using various technologies (James & Thériault, 2020). The urgent need to adapt to the distance-learning process led to technological development (Pregowska *et al.*, 2021), while the regulatory framework lagged behind (Nottingham, Stockman & Burke, 2022; Almeida & Carneiro, 2021).

At the EU level, European Commission has stated that digital technology is a key component of the collective effort to tackle the virus and support new ways of living and working reality during this exceptional time (European Commission, 2020). As regards education, the Digital Education Action Plan 2021–2027 supports the development of online learning at different levels of education across Europe (European Commission, 2021). Thereby, the overall political environment for the development of online adult education is supportive.

Within the article, the main primary source analysed is the General Data Protection Regulation (GDPR). In addition, the author reviews the case-law focusing on the most pressing issues within the area of data protection. Regarding the secondary sources, the author reviews the most recent contributions of academic scholars in the context of the various legal issues related to data protection in online adult education development.

In May–June 2021, the author surveyed educational institutions that provide adult education programmes in Latvia to analyse the impact of the pandemic on adult education in the country. While analysing these primary data, the author discovered that several legal issues hinder the development of online adult education. Some of these legal issues identified by the directors of the educational institutions covered practical issues, such as personal data protection during online lecturing and developing an e-platform. Within this article, the author intends to address the data protection issues in online teaching and learning in adult education programmes by providing recommendations to adult education institutions to comply with the existing legal framework.

Considering the aforementioned, the author has formulated the following research question: What are the main legal challenges of the online teaching and learning process in adult education programmes in the context of data protection?

This article aims to analyse the compliance of online learning and teaching in adult education programmes with GDPR and, based on that, make recommendations to adult education entities that offer online teaching and learning process.

To achieve the aim, the author has formulated the following objectives:

- to analyse the GDPR requirements in the context of online teaching and learning process;
- to examine the main challenges of GDPR compliance in the context of online learning and teaching process within adult education programmes;
- to provide recommendations for adult education entities on GDPR compliance.

As regards the methodology, the author uses a doctrinal research method to analyse the legal framework of online adult education. Within the doctrinal research, the author reviews the scholarly material and existing law in the field of online adult education, focusing on data protection issues. In addition, the author analyses not only existing law related to data protection in online adult education but also comprises a search for practical solutions that fit into the existing legal system concerning online adult education. Furthermore, to ensure an interdisciplinary perspective of the research, the results of the scientific literature review and a survey of educational institutions offering adult education programmes in Latvia are incorporated into the research in the context of defining the main legal challenges of adult education entities offering online teaching and learning process.

2. The main challenges of GDPR compliance in the context of online adult teaching and learning process

Relying on the literature review as well as the survey of Latvian adult education institutions organised by the author from May to June 2021,² the author has identified and summarised some specific challenges that fall within the scope of the GDPR (see Fig. 1).

Figure 1. The main challenges experienced by adult education institutions in offering online learning and teaching process in the context of data protection.



In the next sub-chapters, the author will discuss the identified challenges in more detail.

2.1 Recording of online lectures

The surveyed adult education institutions acknowledged that one of the main issues is the recording of synchronous online lectures by making records available to learners. The teachers agreed that the availability of lectures helps adult learners acquire the lecture’s content. At the same time, the recording of a lecture involves other learners and, correspondingly, their personal data, such as the name, surname, image, and voice. In addition, academics also claim that the recordings may contain sensitive data about the teachers, such as race or sexual orientation (Brown, 2021, p. 2). According to Article 6 of the GDPR, processing of these data can be lawful if at least one of lawful bases is applied. Next, the author analyses all six possible lawful bases and how they may be applied in the case of the recording of online lectures.

² The survey, organised by the author in May–June 2021, involved 60 adult education entities in Latvia.

2.1.1 Consent

Article 6.1(a) stipulates the necessity of consent given by the data subject for processing of his or her personal data for one or more specific purposes (GDPR, Art. 6.1(a)). In the case of recording the online lecture, the adult education entity is expected to ask every teacher and learner for consent to the recording of online lectures. At the same time, consent should be freely given, specific, informed and unambiguous (European Data Protection Board, 2020a, p. 11). The consent is not considered to be freely given if the learner or teacher is unable to refuse or withdraw his or her consent without detriment (European Data Protection Board, 2020a, p. 13) (e.g., no possibility to participate in the online lectures). For example, the Zoom platform, before recording, shows the statement about the recording and in case of disagreement provides an option to leave the session. However, this practice could not be considered as consent that is freely given, since the learner cannot not participate in the online lecture. In this case, there is no real choice, the learner feels compelled to consent, otherwise, the students “endure negative consequences if they do not consent, then consent will not be valid” (Data Protection Working Party, 2011, p. 12). Here, among the negative consequences are considered the inability to participate in the synchronous teaching process, ask the teacher questions, participate in discussions, or do the assigned tasks. In addition, in this situation, there is an “imbalance of power in the relationship” (European Data Protection Board, 2020a, p. 16) between the controller (adult education entity) and the data subject (learner). This aspect mostly applies to the public authorities; however, as far as adult education entities are concerned, a part of them are publicly funded. At the same time, in the case of private entities, in the author’s opinion, the imbalance of power in the relationship still exists, since learners are provided a service from the entity and the entity provides the service to a numerically larger group of learners, perceiving it as a homogeneous formation. Therefore, the author concludes that the notifications on the online platform do not comply with the requirement of Article 6.1(a) of the GDPR.

In addition, scholars agree that consent should also be active and should not rely on silence or inactivity, because the act of consenting is not voluntary and/or under the control of the individual (van Ooijen & Vrabec, 2018, p. 97). The teacher’s question at the beginning of an online lecture about objections to recording of the lecture is thus not compliant with the GDPR. Another potential situation is when a learner is asked consent before entering into a contractual relationship with the adult education entity. In this case,

the learner is not forced to give his or her consent. There is a choice to agree with this precondition before starting to attend the programme. In case the applicant disagrees with being recorded, the adult education entity may propose other options, such as participating in face-to-face or distance-learning programmes where the recording of synchronous lectures is not made. In addition, the applicant is free to choose another adult education entity where recording is not intended. However, offering to give consent after entering into a contractual relationship with an adult education entity, in the author's opinion, could create an imbalance of power in the relationship. In addition, it endures negative consequences, in case the learner refuses to give consent as he or she is forced to miss the online synchronous lectures. Of course, the learner can terminate the contractual relationship. However, there is a requirement for adult education entities to ensure that consent is well-informed.

Regarding the consent issue concerning recording lectures, some scholars (for example, Prof. Matt Fisher from the University of Oxford) argue that, most importantly, there is no "surreptitious recording" and there is "a consent of some kind," such as posted notices (Brown, 2021, p. 6). Regardless, this approach does not address the issue of the real choice of learners. In addition, Prof. Fisher continues that in the case of pre-recording lectures without learners being present, by recording and uploading their lectures, they consent to the processing of their own personal data contained in the recording (Brown, 2021, p. 6). However, in this case, the author reviews a scenario in which learners are also present during the lecture.

2.1.2 Contractual obligation

Article 6.1(b) states that processing is required for the fulfilment of a contract to which the data subject is a party, or to take actions at the data subject's request prior to entering into a contract (GDPR, Art. 6.1(b)). In the case of recording online lectures, adult education entities can indicate in the agreements with teachers and learners that online lectures will be recorded. Thereby, by signing the agreement, teachers and learners agree that their personal data will be processed. This lawful basis, in the author's opinion, is an optimal solution for making sure that teachers and learners have agreed to their data processing during online lectures. At the same time, to avoid any potential conflicts in the future, adult education entities are advised to inform teachers and learners about this requirement prior to the signing of the agreement.

2.1.3 Legal obligation

Article 6.1(c) of the GDPR states that the processing of data is required to comply with a legal obligation imposed on the controller (GDPR, Art. 6.1(c)). To illustrate this with an example, the only legal norm that could potentially apply in Latvia is Section 30(3⁵) of the Education Law of the Republic of Latvia, which stipulates that the founder of an educational institution is expected to “create and develop the education quality system of the educational institution” (Education Law of the Republic of Latvia, 1998). Although it can be argued that recording synchronous online lectures is a part of the quality system, there are counterarguments that there may be other measures to ensure the quality of the teaching and learning process. At the same time, this legal norm applies only to educational institutions. However, as discussed in sub-chapter 2.3, licenced natural and legal persons can also implement adult education programmes (informal learning programmes). Thereby, for natural and legal persons implementing adult education programmes, Article 6.1(c) could not be considered a lawful basis for recording online lectures. In the author’s opinion, the use of the lawful basis stipulated in Article 6.1(c) of the GDPR or recording synchronous online lecture is also rather controversial for registered educational institutions as Section 30(35) of the Education Law of the Republic of Latvia can be interpreted differently.

2.1.4 Vital interests

Article 6.1(d) of the GDPR states that processing is required to protect the vital interests of a data subject or another natural person (GDPR, Art. 6.1(d)). According to Recital 46 of the GDPR, vital interests are “essential for the life of the data subject or that of another natural person” (GDPR, Recital 46). In the case of the recording of synchronous online lectures, the author cannot justify how this action could protect the vital interest of the teacher, the learners, or any other natural person. In addition, Recital 46 of the GDPR also explains that the protection of vital interests may be implemented if “processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread.” Theoretically, adult education entities might claim that they have decided to provide online or hybrid lectures and record them for the purpose of controlling the spread of the epidemics. In this case, for example, the adult education entity can monitor that those learners who are vaccinated participate in the face-to-face learning process, while non-vaccinated or infected learners participate in the online learning process. However, in the author’s opinion, there are more effective measures for how

to monitor epidemics and their spread, thereby the lawful basis stipulated in Article 6.1(d) of the GDPR may not be valid in the case of recording online lectures.

2.1.5 Public interest

Article 6.1(e) of the GDPR states that processing is required to carry out a task in the public interest or in the exercise of official power vested in the controller (GDPR, Art. 6.1(e)). In this context, a task in the public interest is the one which is laid down by law. For example, in the case of adult education, a specific task in the public interest could be issuing a state-recognised educational document to a learner who has acquired education by graduating from a formal adult education programme (justified in Section 11(2) of the Education Law of the Republic of Latvia). In terms of recording online lectures, the legislator has not delegated any official tasks to adult education entities that could justify the fact of recording. Thereby, the lawful basis stipulated in Article 6.1(e) of the GDPR may not be valid in the case of recording online lectures.

2.1.6 Legitimate interests

Article 6.1(f) of the GDPR defines that processing is required for the controller's or a third party's legitimate interests unless such interests are outweighed by the data subject's interests or basic rights and freedoms that need personal data protection, particularly if the data subject is a minor (GDPR, Art. 6.1(f)). Recital 47 clarifies that legitimate interests could exist in the relationship where "the data subject is a client or in the service of the controller" (GDPR, Recital 47). In the case of adult education, the adult education entity as data controller provides a service (adult education programme) to the client (learner). To improve the service provided, adult education entities can decide to record their online lectures, so that learners are able to repeatedly watch the recording thereby improving their understanding. The recordings are also useful for those learners who did not attend the lecture; they can acquire the knowledge independently. In addition, adult education entities can justify the recording of online lectures to ensure a higher quality of the service provided by controlling the quality of teachers.

At the same time, scholars (e.g., Truong *et al.*, 2021; Daoultzoglou, 2023) agree that legitimate interest (as well as consent) as a legal basis can be appropriate during online or blended teaching processes since online or blended educational systems only process data for an explicit purpose which

is in ways that clients would reasonably expect whilst having minimal privacy impact.

However, in any case, the presence of a legitimate interest would require careful consideration, including whether a learner might reasonably expect the processing of personal data for quality purposes during the lectures. Learners can argue that their interests and fundamental rights override the interests of the adult education entity. In this context, Mateeva (2022) suggests that the code of conduct should outline and explain the legal foundation for data processing in education, analysing the sense of balance and highlighting the benefits over the fundamental rights and sovereignty of the people whose data is being collected.

In the author's opinion, in the case of recording online lectures, the legitimate interest of adult education entities to improve the quality of the teaching and learning process overrides the interests and fundamental rights of the learners.

2.2 Compliance of online platform providers with GDPR

The next challenge identified is the compliance of online platform providers with GDPR. Since the platforms are expected to process personal and, perhaps, special category data on the behalf of educational institution, online platform providers are deemed as “third-party processors” under Article 4(10) of the GDPR. Educational institutions indicated that in the process of online teaching and learning, they use the assistance of a technology or software platforms such as Microsoft Teams, Zoom, and Google Meet. Most of these platforms demand, at the very least, the names and email addresses of the learners, teachers, and administrative staff members who use the service. This information is required by the platform to manage identity, accounts, and log-ins. As regards the compliance of the educational e-platforms with the GDPR, scholars and practitioners recommend teachers and learners avoid using personal email addresses wherever feasible (da Conceicao Freitas & da Silva, 2021, p. 5). In addition, these platforms may also make use of photos, music, and/or free-text messaging. Platforms may also gather data via the use of cookies or other online identifiers. Potentially, there are several security risks related to educational platforms. For example, several security vulnerabilities have been discovered as a result of the widespread usage of EdTech for ERT, such as hackers intruding on sessions, a behaviour known as “zoombombing” (Angiolini *et al.*, 2020, p. 4). Therefore, care should be taken to monitor who has access to join the online lectures.

An interesting aspect regarding the relationship between educational institutions and educational platform providers is analysed within the context of joint controllership, where the processing would not be possible without the participation of both parties, in the sense that the processing by each party is “inextricably linked” (European Data Protection Board, 2020b, p. 3). In the case of *Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV* [2019], the Court of Justice of the European Union stated that the operator of a website who embeds a social plugin on that website that transmits the user’s personal data to Facebook must be deemed a controller for the activities consisting of the collection and transfer of the user’s data (*Fashion ID v. Verbraucherzentrale* [2019]). Similarly, if the educational platform uses data collected during educational activities for other purposes, the adult education entity may be classified as a joint controller for the transmission of that information, because without the processing of data for educational purposes, in which the adult education entity is a controller, the platform may not have access to data and may not use it for other purposes. As a result, each party’s processing might be described as “inextricably connected” (Globocnik, 2019, p. 1037). In the situation of joint controllership, the distribution of obligations between the controller and the processor, as well as towards the data subjects, must be legally established. This (contractual) agreement “would give clarity and may be utilised to demonstrate openness and responsibility” (European Data Protection Board, 2020b, p. 43). This means that, when attracting a platform provider, an adult education entity should make a specific assessment, taking into consideration all relevant factual circumstances, to determine whether the two entities (the adult education entity and the platform provider) are deciding both and jointly the methods and/or purposes of the processing.

2.3 Unauthorised access

The literature review also identified the issue of unauthorised access. It is argued that unauthorised access is one of the most obvious risks if there is no authentication mechanism associated with each learner and teacher (Almeida & Carneiro, 2021, p. 28). Another danger that may develop is the theft of access credentials, which may be the responsibility of the user or the adult education entity. In the agreement between the adult education entity and learner, it should be indicated what security measures (the principle of integrity and confidentiality, Article 5.1(f) of the GDPR) are ensured from both sides, for example, periodically changing the passwords, and sharing of access credentials should not be allowed.

2.4 Data loss

Academic scholars have identified also data loss as a potential threat. This issue also relates to compliance with the principle of integrity and confidentiality (GDPR, Art. 5.1(f)). Regarding this issue, scholars advise that the protection obligations must ensure that data is stored in protected equipment and not in unprotected files (Bandara, Ioras & Maher, 2014, p. 730). The author thus concludes that adult education entities are expected to ensure various measures to protect their equipment and files.

2.5 Cyberattacks

Furthermore, adult education entities may face cyberattacks. An increased number of people working remotely as well as an overall tendency to spend more time in cyberspace has resulted in a rapid upturn in the number of successful cyberattacks. For example, according to the FBI, in May 2020, the number of successful cyberattacks in the United States increased by 600% compared to February 2020 (FBI, 2020). It should be stressed that the human factor is identified as the weakest link to corporate and personal information security due to behavioural, social, and cultural vulnerabilities (Borkovich & Skovira, 2020, p. 243). For example, Ross Kelly argues that 90 per cent of successful hack attacks or incidents are ascribed to human error or behaviour (Kelly, 2022). As regards adult education, attackers could gain unauthorised access, leak data, or use stolen learners' data to phish individual users. To avoid cyberattacks, scholars recommend that educational institutions minimise private information contained within e-learning platforms, opt for a software-as-a-service solution over a local client, block third-party providers from getting direct access, and audit vendors and their security documentation (Barth, 2022). All involved parties—adult education entities, teachers, and learners—are expected to pay attention to potential threats of cyberattacks. In the author's opinion, employees of adult education entities, as well as teachers working from home, should receive regular support from adult education entities to tackle the various challenges concerning cybersecurity. Good practice includes an organisation of training where employees are informed about potential risks and actions that should be taken; development of easy-to-read guides on organisation cybersecurity policy, including staff responsibilities (NCSC, 2022). In addition, teachers and other employees of adult education entities are responsible for implementing various precautionary measures, including recusing distractions, since they are not putting only employers' devices and data at risk, but also personal security and assets.

3. Recommendations for adult education entities on GDPR compliance

In this chapter, the author provides recommendations for the challenges discussed above.

In order to address the issues of recording online lectures, adult education entities should decide on the application of appropriate lawful basis as discussed previously:

- In the event of consent (in accordance with Article 6.1(a) of the GDPR), the author advises developing a statement, clearly indicating the fact of recording online lecturing, what personal data will be processed, and for what purpose. For example, for the purpose of ensuring the quality of the teaching process as well as the availability of teaching materials, the adult education entity will use the following personal data of learners and teachers: the learners' and the teachers' names and surnames, images, and voice. It is advised that a potential learner or teacher signs the statement physically or electronically (electronic signature of the opt-in option) before entering into a contractual relationship with an adult education entity. In this way, potential learners or teachers may refuse to provide consent without any negative circumstances as they have the option to do business with another adult education entity that does not provide recording.
- In the case of contract (according to Article 6.1(b) of the GDPR), the author recommends including a clause in the contract with teachers and learners about recording online lectures. Similarly, the clause should contain what personal data will be processed, and for what purpose.
- If legitimate interests are involved (Article 6.1(f) of the GDPR), adult education entities are recommended to involve the description of legitimate interests (quality assurance of online teaching and learning) as well as what personal data will be processed, and for what purpose, during the recording of online lectures in their privacy policy. Also, in this case, the agreement with the privacy policy should be provided by all parties.

In addition, adult education entities are expected to assure that the recordings are available on the internal platform for a certain period according to the set purpose, thereby ensuring compliance with Article 5.1(e) of the GDPR. Also, in accordance with Article 5.1(f) of the GDPR, restricted access should be ensured as well.

To tackle the challenge of compliance of online platform providers with the GDPR, adult education entities should check the online platform provider's level of compliance with the GDPR as well as sign the contract if requirements of Article 28.3 of the GDPR are indicated.

Regarding the issues of data loss, unauthorised access and cyberattacks, adult education entities are expected to develop a security system, thereby ensuring compliance with Article 5.1(f) of the GDPR. Good practice to address the above problems includes a requirement to periodically change all passwords, use strong passwords, encrypt electronic data, install firewalls and antivirus software, keep devices locked when not in use, disable "auto-complete" settings, store data in protected files, etc.

4. Conclusion

The analysis of the main challenges of adult education entities in the context of data protection has shown that the main issues concern the recording of online lectures, compliance of e-learning platforms with the GDPR, unauthorised access to resources of adult education entities, potential data loss, and various cyberattacks.

In accordance with the results of the conducted survey of educational institutions that offer online adult education, the compliance of recording online lectures with the requirements of the GDPR is topical.

The author has concluded that adult education entities have three options on how they can ensure the lawfulness of recording online lectures in accordance with the GDPR, namely, based on consent, contractual relationships and legitimate interests. In all the cases, there are various matters to be considered, for example, freely given, specific, informed, and unambiguous consent must be given before entering the contractual relationship; a clause in the contract between the adult education entity and learner (or teacher) must contain information on the purpose of the recording online lectures; privacy policy must include information of legitimate interests (assurance of the quality of online teaching and learning). However, there are still practical issues, such as the right to withdraw the consent at any time, including after the recording is made, or doing the recording on an e-platform based on the silence of participants.

Inga Jekabsone, PhD, MBA, LL.M is a postdoctoral researcher working at the innovative adult education institution Magnetic Professional Ltd., focusing on research into adult education. She defended her PhD at the University of Latvia in 2017 in the field of public administration. In addition, the researcher obtained LL.M in technology law at the Riga Graduate School of Law in 2022. Dr Jekabsone is the author of numerous scientific publications in various scientific fields: technology law, public administration, adult education, and e-commerce.

References

- Almeida, F. & Carneiro, P.** (2021), 'Challenges of Privacy in E-learning in the Context of COVID-19,' in S. Jackowicz & I. Sahin (eds.) *Online Education during the COVID-19 Pandemic: Issues, Benefits, Challenges, and Strategies*, ISTES Organisation. Retrieved from <https://www.istes.org/challenges-of-privacy-in-e-learning-in-the-context-of-covid-19-109-s.html> [accessed 10 Dec 2022]
- Amarneh, B. M.; Alshurideh, M. T.; Al Kurdi, B. H. & Obeidat, Z.** (2021), 'The Impact of COVID-19 on e-Learning: Advantages and Challenges,' in *Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021)*, Cham: Springer, pp. 75–89.
https://doi.org/10.1007/978-3-030-76346-6_8
- Angiolini, C.; Ducato, R.; Giannopoulou, A. & Schneider, G.** (2020), 'Remote Teaching during the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education,' *Opinio Juris in Comparatione*, vol. 1, no. 1, pp. 45–72.
- Bandara, I.; Ioras, F. & Maher, K.** (2014), 'Cyber Security Concerns in E-Learning Education,' in *Proceedings of ICERI2014 Conference, 17th–19th November 2014, Seville, Spain*, pp. 728–735.
- Barth, B.** (2022), 'Rush to Adopt Online Learning under COVID-19 Exposes Schools to Cyberattacks,' *SC Media*. Retrieved from <https://www.scmagazine.com/home/security-news/newsarchive/coronavirus/race-to-adopt-online-learning-under-covid-19-exposes-schools-to-cyberattacks/> [accessed 10 Dec 2022]
- Beaunoyer, E.; Dupéré, S. & Guitton, M. J.** (2020), 'COVID-19 and Digital Inequalities: Reciprocal Impacts and Mitigation Strategies,' *Computers in Human Behaviour*, vol. 111, art. 106424.
<https://doi.org/10.1016/j.chb.2020.106424>
- Borkovich, D. B. & Skovira, R. J.** (2020), 'Working from Home: Cybersecurity in the Age of Covid-19,' *Issues in Information Systems*, vol. 21, no. 4, pp. 234–246.

- Brown, A.** (2021), 'Who Owns Online Lecture Recordings?' *HEPI Policy Note*, vol. 32. Retrieved from <https://www.hepi.ac.uk/wp-content/uploads/2021/11/Who-owns-online-lecture-recordings.pdf> [accessed 10 Dec 2022]
- da Conceicao Freitas, M. & da Silva, M. M.** (2021), 'GDPR and Distance Teaching and Learning,' in *16th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6. <https://doi.org/10.23919/CISTI52073.2021.9476409>
- Daoulzoglou, A.** (2023), 'GDPR and Education: An Approach for e-Learning in Greek Schools,' in *INTED2023 Proceedings*, pp. 154–163. <https://doi.org/10.21125/inted.2023.0069>
- Data Protection Working Party (2011), Opinion 15/2011 on the Definition of Consent (WP187), 01197/11/EN, 13.7.2011. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf [accessed on 10 Dec 2022]
- Education Law of the Republic of Latvia, *Latvijas Vēstnesis*, 343/344, 17.11.1998. Retrieved from <https://likumi.lv/ta/id/50759-izglitiba-likums> [accessed 10 Dec 2022]
- European Commission (2020), *Digital Technologies—Actions in Response to Coronavirus Pandemic. Shaping Europe's Digital Future, European Commission*. Retrieved from <https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic> [accessed 10 Dec 2022]
- European Commission (2021), *Digital Education Action Plan (2021–2027). European Education Area*. Retrieved from <https://education.ec.europa.eu/focus-topics/digital/education-action-plan> [accessed 10 Dec 2022]
- European Data Protection Board (2020a), *Guidelines 05/2020 on Consent under Regulation 2016/679*. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [accessed 10 Dec 2022]
- European Data Protection Board (2020b), *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*. Retrieved from https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en [accessed 10 Dec 2022]
- Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV* [2019], CJEU Case C-40/17, ECLI:EU:C:2019:629.
- FBI (2022), *Internet Crime Report 2020*, Federal Bureau of Investigation, Internet Crime Complaint Centre. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [accessed 10 Dec 2022]
- Gamage, K. A. A.; de Silva, E. K. & Gunawardhana, N.** (2020), 'Online Delivery and Assessment during COVID-19: Safeguarding Academic Integrity,' *Education Sciences*, vol. 10, no. 11, art. 301. <https://doi.org/10.3390/educsci10110301>

- Globocnik, J.** (2019), 'On Joint Controllershship for Social Plugins and Other Third-Party Content—A Case Note on the CJEU Decision in Fashion ID, IIC,' *International Review of Intellectual Property and Competition Law*, vol. 50, no. 8, pp. 1033–1044. <https://doi.org/10.1007/s40319-019-00871-4>
- González, J. L. A.; Castillo, B. S. A.; Pauca, M. J. V. & Chávez, M. del R. C.** (2022), 'Educational Technology Applied to Adult Education,' *International Journal of Health Sciences*, vol. 6, no. S1, pp. 142–148. <https://doi.org/10.53730/ijhs.v6nS1.4758>
- James, N. & Thériault, V.** (2020), 'Adult Education in Times of the COVID-19 Pandemic: Inequalities, Changes, and Resilience,' *Studies in the Education of Adults*, vol. 52, no. 2, pp. 129–133. <https://doi.org/10.1080/02660830.2020.1811474>
- Jameson, J. M.; Stegenga, S. M.; Ryan, J. & Green, A.** (2020), 'Free Appropriate Public Education in the Time of COVID-19,' *Rural Special Education Quarterly*, vol. 39, no. 4, pp. 181–192. <https://doi.org/10.1177/8756870520959659>
- Käpplinger, B. & Lichte, N.** (2020), "'The Lockdown of Physical Co-operation Touches the Heart of Adult Education": A Delphi Study on Immediate and Expected Effects of COVID-19,' *International Review of Education*, vol. 66, pp. 777–795. <https://doi.org/10.1007/s11159-020-09871-w>
- Kelly, R.** (2022), 'Almost 90% of Cyber Attacks Are Caused by Human Error or Behavior,' *Chief Executive*. Retrieved from <https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/> [accessed 10 Dec 2022]
- Mateeva, Z.** (2022), 'Code of Conduct Regarding the Protection of Personal Data in Higher Education—Criteria and Procedures for Approval,' in *Proceedings of INTCESS 2022: 9th International Conference on Education & Education of Social Sciences, 17–18 January 2022*. <https://doi.org/10.51508/intcess.202274>
- Morris, T. H.** (2021), 'Meeting Educational Challenges of Pre- and Post- COVID-19 Conditions through Self-Directed Learning: Considering the Contextual Quality of Educational Experience Necessary,' *On the Horizon*, vol. 29, no. 2, pp. 52–61. <https://doi.org/10.1108/OTH-01-2021-0031>
- Morris, T. H. & Rohs, M.** (2021), 'Digitization Bolstering Self-Directed Learning for Information Literate Adults—A Systematic Review,' *Computers and Education Open*, vol. 2, art. 100048. <https://doi.org/10.1016/j.caeo.2021.100048>
- Neuwirth, L. S.; Jović, S. & Mukherji, B. R.** (2021), 'Reimagining Higher Education during and Post-COVID-19: Challenges and Opportunities,' *Journal of Adult and Continuing Education*, vol. 27, no. 2, pp. 141–156. <https://doi.org/10.1177/1477971420947738>
- Nottingham, E.; Stockman, C. & Burke, M.** (2022), 'Education in a Datafied World: Balancing Children's Rights and School's Responsibilities in the Age of Covid 19,' *Computer Law & Security Review*, vol. 45, art. 05664. <https://doi.org/10.1016/j.clsr.2022.105664>

- Petrushenko, Y.; Onopriienko, K.; Onopriienko, I. & Onopriienko, V.** (2021), 'Digital Learning for Adults in the Context of Education Market Development,' in *11th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany, pp. 465–468.
<https://doi.org/10.1109/ACIT52158.2021.9548555>
- Pokhrel, S. & Chhetri, R.** (2021), 'A Literature Review on Impact of COVID-19 Pandemic on Teaching and Learning,' *Higher Education for the Future*, vol. 8, no. 1, pp. 133–141. <https://doi.org/10.1177/2347631120983481>
- Pregowska, A.; Masztalerz, K.; Garlińska, M. & Osial, M. A.** (2021), 'Worldwide Journey through Distance Education—From the Post Office to Virtual, Augmented and Mixed Realities, and Education during the COVID-19 Pandemic,' *Education Sciences*, vol. 11, no. 3, art. 118.
<https://doi.org/10.3390/educsci11030118>
- Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC, *OJ L* 119/1, 4.5.2016.
- Truong, N.; Sun, K.; Wang, S.; Guitton, F. & Guo, Y.** (2021), 'Privacy Preservation in Federated Learning: An Insightful Survey from the GDPR Perspective,' *Computers & Security*, vol. 110, art. 102402.
<https://doi.org/10.1016/j.cose.2021.102402>
- Van Ooijen, I. & Vrabec, H. U.** (2018), 'Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective,' *Journal of Consumer Policy*, vol. 42, no. 1, pp. 91–107.
<https://doi.org/10.1007/s10603-018-9399-7>