EJLT European Journal of Law and Technology

Every Student Can Learn, Just not on the Same Day: An Analysis of Data Protection and Cybersecurity Challenges for E-Learning Platforms in the COVID19 Crisis

Sandra Schmitz-Berndt[*]

Abstract:

When the American cartoonist George Evans stated that every student can learn, just not on the same day and in the same way, he probably did not imagine the despair of pupils trying to access an e-learning platform during a national lockdown period. With the COVID19 crisis, online learning became an everyday commodity almost overnight. However, not all schools were prepared to swiftly switch from in class to distance teaching. Concerns were raised with regard to data protection and cybersecurity, which in some cases led to the implementation of "home-made" solutions.

Taking the example of the federalist state of Germany where education is within the sole competence of the Länder, this paper will explore the functioning and technical implementation of several e-learning platforms and address the data protection challenges. In terms of cybersecurity, this paper also analyses the applicability of the NIS Directive to the various platforms and outlines the consequences for platform providers. In light of the acceleration of the revision of the NIS Directive due to the COVID-19 crisis, we take the example of learning platforms to outline the flaws of the 2016 Directive before we critically evaluate selected aspects of the NIS 2.0 proposal of December 2020.

Keywords: Online learning, data protection, NIS Directive

[*] Postdoctoral Researcher in Law, University of Luxembourg

1 Introduction

Within the on-going COVID19 pandemic, educational institutions have been and still are affected by lockdowns. In late April 2020, education institutions in approximately 180 countries had been temporarily closed.[1] In late January 2021, schools in almost 60 countries remained closed or had closed again.[2] The closure in April 2020 affected 85% of the world's student population.[3] With the unprecedented increase in distance teaching, school closures led to a transformation of education. The rapid transition to distance teaching, however, did not run smoothly. A 2020 public consultation by the European Commission revealed that almost 60% of respondents had not used distance and online learning before the crisis.[4] With preparedness of teachers to use digital technologies in the EU varying widely, even strong national economies struggle with digitalization in schools. Germany with the largest national economy in Europe and the world's fourth largest by nominal GDP was far from well prepared for a rapid shift to distance teaching. Remarkably, Germany notoriously lags behind in digitalisation.[5] This is not a mere issue of infrastructure, which indeed is spotty in places with particular shortage in rural areas and economically challenged regions, but also an issue of computer literacy with teachers[6] and parents[7]. In addition, legal uncertainty towards the use of technology in distance education persists.

Section II of this paper outlines the setting for e-learning in Germany addressing structural problems for distance teaching as well as a general reservation towards the use of online

---

[1] World Bank Group, The COVID-19 pandemic: shocks to education and policy responses (2020), 11 <https://openknowledge.worldbank.org/bitstream/handle/10986/33696/148198.pdf?sequence=4&isAllowed=y> last accessed 31 August 2021.

[2] See World Bank Education COVID-19 school closures map updated on 15 March 2021 <https://www.worldbank.org/en/data/interactive/2020/03/24/world-bank-education-and-covid-19> last accessed 31. August 2021.

[3] United Nations University, Institute for Environment and Human Security, Five facts on e-learning that can be applied to COVID-19 (25 September 2020) <https://ehs.unu.edu/news/news/five-facts-on-e-learning-that-can-be-applied-to-covid-19.html> last accessed 31. August 2021.

[4] European Union, Digital Education Action Plan 2021-2027 (2021) <https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en> last accessed 31. August 2021.

[5] Peter Hille, COVID: Schools are in lockdown and e-learning is a struggle (Deutsche Welle, 06 January 2021) <https://www.dw.com/en/covid-germany-schools-lockdown-digitalization/a-56147857> last accessed 31 August 2021; Ben Knight and Sabine Kinkartz, COVID: German schools 'under-equipped and unprotected' <https://www.dw.com/en/covid-german-schools-under-equipped-and-unprotected/a-56098662> last accessed 31. August 2021.

[6] DPA, Digitalisierung: SPD-Chefin will unfähigen Lehrern helfen (heise online, 12 December 2020) <https://www.heise.de/news/Digitalisierung-SPD-Chefin-will-unfaehigen-Lehrern-helfen-4987859.html>last accessed 31. August 2021.

[7] Only 46% of German parents self report above basic IT skills level and 19% reporting low or no skills, see R Vuorikari, A Velicu et al, How families handled emergency remote schooling during the Covid-19 lockdown in spring 2020, EUR 30425 EN (2020) <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/how-families-handled-emergency-remote-schooling-during-covid-19-lockdown-spring-2020> last accessed 31. August 2021.

platforms provided by tech giants due to data protection concerns. Further, cybersecurity concerns relating to the increased attack surface as a direct result of the shift to online education is addressed. Section III elaborates the obligations arising from the GDPR and NIS Directive for the different actors involved in the German e-learning set-up. Focussing on the challenges of varying implementations, this section concludes on the divergences in accountability across the German states.

2 E-Learning in Germany

2.1 Obstacles in transition to e-Learning

A variety of factors influence the ad-hoc shift to distance teaching and learning. Instead of exploring all factors that hindered the smooth transition to e-learning in Germany, two central questions are discussed: the digital education ecosystem, and concerns about data protection and IT security. This section thus leaves aside teachers' habitus[8] and computer literacy as well as sociological and psychological concerns against the use of digital technology in daily educational routines.[9] The role of Germany as a federalist state and the emphasis on data protection even prior to the GDPR are briefly addressed.

2.1.1 Prenote: Education Policy in the Federalist System

Independency in matters of cultural and educational policy means that each of Germany's 16 states administers its own education system. Accordingly, there is neither a uniform approach to e-learning nor a shared e-learning solution. As regulations and restrictions vary from state to state, the German federal regulations have been blamed to restrict the adoption of distance teaching tools that are successfully used in education elsewhere.[10] Although this does not relate predominantly to the federalist system, there is some truth in this. Obviously diverging approaches may lead to confusion; legal certainty is challenged when state regulators address issues in a different manner. In that regard, section III of this paper outlines some of the consequences and challenges for schools in practice.

2.1.2 The Digital Education Ecosystem

The technological obstacles in transitioning to e-learning are highlighted from macro to micro level, addressing digital infrastructure as such, connectivity and digital equipment of schools and digital competence of teachers and pupils alike.

---

[8] Carolyn Blume, German Teachers' digital habitus and their pandemic pedagogy, [2020] Postdigit Sci Educ. 879-905.
[9] See for instance Michael Kerres, Against all odds: education in Germany coping with Covid-19, [2020] Postdigit Sci Educ. 1-5.
[10] Ibid.

Digital technology can still not be taken for granted in German classrooms: deficits range from weak internet connections to overall deficits in network infrastructure, IT services and equipment.[11] In 2018, the German government approved the creation of a billion-euro digital infrastructure fund to help boost internet connectivity throughout the country. This fund comes after the annual national IT summit in 2017 revealed the intermittent broadband network coverage.[12] According to the 2016 Akamai 'state of the internet' report, Germany ranked 25th in Europe in terms of average internet connection speed.[13] For almost one third of internet users in Germany, their broadband speed was less than half of what their contracts promised.[14] There is a stark discrepancy between regions, especially rural vs. city.[15] In some rural areas less than 10% of households reached the government's target bandwidth capacity.[16]

In line with Germany in general being in 'the digital slow lane'[17] goes Germany's struggle with digitalization in schools. Before the COVID-19 crisis, six computers were available for every 10 pupils at German schools.[18] When schools were forced to close during the pandemic, it became obvious that only a few could meet the technical criteria required for online teaching. To elaborate the reasons for outdated infrastructure and equipment goes beyond the scope of the paper. Some critics blame federalism: Due to the cultural sovereignty of the Länder, the federal government cannot provide financial means for technology in education institutions. A digital education initiative of the federal government addressed this weakness in its "DigitalPakt Schule" of 2019.[19] For this initiative, it was necessary to change the German Basic Law[20], which now allows the federal government to invest € 5 billion to improve digital infrastructure over the following five

---

[11] Peter Hille, 'Could Germany's digital education initiative threaten states' rights?' (*Deutsche Welle,* 15 March 2019) <https://www.dw.com/en/could-germanys-digital-education-initiative-threaten-states-rights/a-47923536> last accessed 31 August 2021.

[12] Rolf Wenkel, 'Germany in the digital slow lane' (*Deutsche Welle,* 09 June 2017) <https://www.dw.com/en/germany-in-the-digital-slow-lane/a-39187166> last accessed 31 August 2021.

[13] Akamai, ‚akamai's [state of the internet] Q4 2016 report', 32 <https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-connectivity-report.pdf> last accessed 31 August 2021.

[14] Elizabeth Schumacher, ‚Germany, land of woefully slow internt' (*Deutsche Welle,* 17 January 2018) < https://www.dw.com/en/germany-land-of-woefully-slow-internet/a-42195241> last accessed 31 August 2021.

[15] See Arthur Sullivan, 'Faster internet needed in new era for German farmers' (*Deutsche Welle,* 23 January 2018) < https://www.dw.com/en/faster-internet-needed-in-new-era-for-german-farmers/a-42272917> last accessed 31 August 2021.

[16] Rolf Wenkel, 'Germany in the digital slow lane' (*Deutsche Welle,* 09 June 2017) <https://www.dw.com/en/germany-in-the-digital-slow-lane/a-39187166> last accessed 31 August 2021.

[17] Ibid.

[18] Hille (n5).

[19] For more inforamtion see the dedictated website of the Federal Ministry of Education and Science (Bundesministerium für Bildung und Forschung) https://www.digitalpaktschule.de.

[20] The German Basic Law irrevocably states that Germany is a federal republic. Education policy is considered as the core of state sovereignty.

years.[21] The funds will be used to invest in faster internet and IT equipment. However, with state and local authorities also involved in the procedure, this will take some time. Also, investing in the hardware alone will not be sufficient. In addition, teachers need to be trained to use digital devices and provide teaching in a remote setting.[22] IT literacy of teachers remains a concern that is finally addressed in public.[23] In addition, pupils need to be equipped with hardware since in particular younger pupils do not own a computer. [24] Sharing equipment with other family members triggers competition among siblings and parents.[25]

2.1.3 Data Protection Concerns as a Restraining Factor for Using Established Video-conferencing Software

The perception that personal data may not adequately protected is deeply rooted in German society. Concerns exist as to what the key industry players – in most cases U.S. tech companies - do with the data. The principle of data minimization, i.e., that a provider should only process and store data that is strictly needed for the performance of the service, is given a lot of weight in Germany. Obviously, any distance learning platforms or supporting tools, e.g., video conferencing systems collect a variety of personal data: they require as a minimum username and email address to manage identification, accounts and log-ins. Further data that may be processed include the pupil's real name as well as the custodians' names. The platforms might use images, audio and/or text messaging; they may log who connects when and for what purpose and to which service. Meta data such as the IP address, cookies, or other online identifiers constitute personal data, if they relate to an identifiable person. From content uploaded by individuals, conclusions can be drawn regarding his personality. Chat messages may reveal sensitive data etc. Considering the wide interpretation of the concept of personal data, also visual images including the surrounding of an individual (home, etc.) may amount to personal data. Not only personal data of the pupil or his custodians may be processed: when third parties walk across the camera, third party data is processed by automated means. The same applies to audio files containing the spoken words of individuals. Spoken words as well as images render a person identifiable.

---

[21] The fund saw an additional boost in 2020, see Hille (n5).
[22] Hille (n5).
[23] Dpa, 'Digitalisierung: SPD-Chefin will unfähigen Lehrern helfen' (*heise online,* 12 December 2020) < https://www.heise.de/news/Digitalisierung-SPD-Chefin-will-unfaehigen-Lehrern-helfen-4987859.html> last accessed 31 August 2021.
[24] According to the 2020 KIM-Studie, less than half of pupils aged 6 to 13 own a smartphone, and 18 % a desktop computer or laptop; see Medienpädagogischer Forschungsverbund Südwest, 'KIM-Studie 2020', 12, <https://www.mpfs.de/fileadmin/files/Studien/KIM/2020/KIM-Studie2020_WEB_final.pdf> last accessed 31 August 2021..
[25] Cf. KIM-Studie 2020, 5.

2.1.3.1 Lawful Data Processing under the GDPR

Considering the vast amount of personal data concerned, the first hurdle for any education entity is the lawfulness of data processing under the GDPR. The GDPR sets the applicable framework for the legitimate processing of personal data and applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the EU, Art. 3(1) GDPR. Pursuant to Art. 3(2) GDPR, the GDPR further applies to controllers or processors not established in the EU, if processing activities relate to the offering of goods or services; or monitoring of behaviour of data subjects as far as this takes place within the EU.

Lawful data processing requires either consent for the processing or a lawful purpose. Consent in the sense of Art. 6 (1) lit. a GDPR as a 'catch-all' for processing personal data is difficult in the case of online education as consent may be withdrawn and thus, challenge the delivery of education services. In contrast, a lawful purpose prevents this dilemma. Pursuant to Art. 6 (1) lit. c GDPR, a legal obligation can be a lawful purpose. Accordingly, where a state law explicitly foresees the deployment of a learning platform,[26] processing is necessary for the compliance with a legal obligation to which the controller is subject in the sense of Art. 6(1) lit. c.[27]

Further, a lawful purpose may also be the maintenance of the continuity of remote education. Irrespective of whether a national law governs the use of distance learning platforms, the processing may be necessary for the performance of a task carried out in the public interest (Art. 6(1) lit. e) since education is of vital interest for society.

2.1.3.2 Transfer of Personal Data to Third Countries

Instead of assessing the various data protection challenges for distance learning, the following example shall highlight one of the most problematic features: the transfer of personal data to third countries. This data processing highlights many concerns related to distance teaching and learning, namely the fear of losing control of data and data being subject to a regime that does not provide equivalent data protection. Although the assumption that 'teachers are strictly banned from using cloud services, social platforms, micro-blogs, or document sharing tools that are hosted outside of the EU, because of these technologies' lack of (full) compliance with EU standards for privacy and data protection, telemetric practices, and the imponderables of data leaving EU territory'[28] is too generalized, there is some truth in it. When the necessity to switch to distance teaching and learning became obvious, almost immediately the joint body of the German data protection authorities issued a warning on using common video conference systems like

[26] As in § 28 SächsSchulG (School Law of Saxonia).
[27] Most German states lack an explicit legal basis in their domestic law.
[28] Kerres (n9).

Microsoft Teams, Skype, Zoom, Google Meet, GotoMeeting and Cisco WebEx.[29] The warning was based on personal data of the participants of video conferences being processed outside EU territory. If videoconferencing was to be implemented, the 'initiator' (who in most cases would also be the controller) was asked to assess whether own service based on open source software could be used rather than the aforementioned systems.[30] In any case, compliance with EU data protection law should be guaranteed.

Similar concerns had been raised in the past regarding the communication via WhatsApp within a school context. DPAs advised that WhatsApp must not be used by teachers as a communication means with pupils due to the transfer of data to the US.[31] In that line, the Ministry of culture of Baden-Württemberg inter alia requested schools to refrain from using WhatsApp and Skype because of 'non-compliance with data protection law'.[32]

Notably, the providers of video conference systems have to comply with the high level of data protection provided by the GDPR even when they are established outside the EU and process data of data subjects located in the EU.[33] In any case, the transfer of personal data to a third country is only permissible if the conditions laid down in Chapter V GDPR are complied with. Compliance is achieved, when the third country in question ensures an adequate level of protection of personal data. This requires, in general, either an adequacy decision by the Commission on the level of protection (Art. 45 GDPR), the provision of appropriate safeguards by the controller or processor (Art. 46 GDPR), or the existence of binding corporate rules (Art. 47 GDPR). Following the CJEU Schrems II[34] ruling, transfer of

[29] Datenschutzkonferenz, Orientierungshilfe Videokonferenzsysteme (23 October2020) <https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/oh-videokonferenzsysteme_final.pdf> last accessed 31 August 2021.

[30] See for instance Berliner Beauftragte für Datenschutz und Informationsfreiheit, Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen (3 July 2020), <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf> accessed 24 August 2021.

[31] Even before GDPR, see Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit, 12. Tätigkeitsbericht zum Datenschutz: Öffentlicher Bereich (2017), 404 <https://www.tlfdi.de/mam/tlfdi/presse/12._tb_oeffent._webversion_tlfdi_.pdf> last accessed 31 August 2021.

[32] Kultusministerium Baden-Württemberg, Kommunikationsplattformen am Beispiel WhatsApp, <https://it.kultus-bw.de/,Lde/1653651> last accessed 31 August 2021. Beside issues relating to the transfer of data to non-EU or EEA states, concerns were expressed towards issues of joint controllership.

[33] Cf. Art. 3(2) GDPR. Where the provider is established in the US, as it is the case with most of the aforementioned providers, they also have to comply with domestic law at their place of establishment.

[34] CJEU, C-311/18 *Facebook Ireland v Schrems (Schrems II)* ECLI:EU:C:2020:559.

personal data is no longer possible under Art. 45 GDPR since the EU-US privacy shield has been declared void.[35]

Schrems II also created considerable uncertainty towards the use of standard contractual clauses (SCCs) for data transfer between EU and non-EU countries.[36] The implementation of SCCs is a means to provide safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. SCCs provide an optional set of clauses that controllers and processors may use to execute contracts in compliance with the GDPR. Sample SCCs published by the European Commission existed in the past under Directive 95/46/EC[37]; in the wake of the Schrems II judgement, the Commission published a modernised SCCs version under Art. 46(1) and (2)(c) GDPR. [38] These new SCCs provide for EU regulatory jurisdiction over the controllers and processors with respect to the EU personal data transferred. The new SCCs provide for a mandatory data transfer impact assessment to be carried out and requires the parties to warrant, prior to any data transfer, that they have no reason to believe that the laws and practices in the destination country prevent the importer from fulfilling his obligations under the SCCs. This means in essence that the level of data protection equivalent to the GDPR for the data in question is guaranteed. Considering that U.S. laws, in particular section 702 FISA[39] granting government access to data for surveillance purposes, do not meet the essentially equivalent standards, the EDPB noted that in such scenarios, only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data.[40] Accordingly, legitimate transfer requires supplementary measures such as encryption or pseudonymisation,[41] which would have to be implemented for the lawful use of video conference systems or other systems that foresee the transfer of data to, for example, the United States.

---

[35] See with regard to remote teaching platforms Chiara Angiolini, Rossana Ducato, Alexandra Giannopoulou, and Giulia Schneider, Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education, Opinio Juris in Comparatione 1 (2020), 45, 57 et seq.

[36] For the use of SCCs in the context of remote teaching platforms see ibid, 58 et seq.

[37] As regards EU data controller to non-EU or EEA data processor: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (consolidated version) [2010] OJ L39/5-18.

[38] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. At the same time the Commission introduced SCCs for DPAs under Art. 28(7) GDPR, see Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council [2021] OJ L199/18-30.

[39] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq. (FISA).

[40] EDPB, Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0 (adopted on 18 June 2021) 17.

[41] Ibid, 22.

Prior to the EDPB Recommendation 01/2020 in that regard, the joint body of the German data protection authorities had already declared that controllers using video conference systems by providers established outside the EU, must be able to demonstrate that they verified that the processor adheres to data protection principles enshrined in the GDPR.[42] The threshold is thus set high. Considering that schools are under municipality authority, a lack of expertise to set up SCCs at this government level and the perceived liability risk for education institutions seem to be the root cause why this route is not pursued for distance teaching.

Adding to the concerns are the providers of the systems themselves when they make false claims regarding data security. For instance, the highly popular online collaboration tool 'zoom' that provides video conferencing capabilities was exposed to 'lie' about end-to-end-encryption.[43] The fear to lose control over personal data even when there are SCCs in place is omnipresent. The benefit of relying on a working system for most institutions do not outweigh the data protection concerns meaning that the video conference systems of U.S. providers are hardly used.

As a consequence, the Berlin DPA for instance provides a regularly updated evaluation of video conferencing systems in terms of compliance with EU data protection law.[44] As of August 2021, Cisco Webex Meetings, freely available Jitsi services, Google Meet, GoTo Meeting, Microsoft Teams, Skype, Skype for Business, TeamViewer Meeting and Zoom are considered non-compliant.

In sum, concerns regarding to data transfer to servers located outside of the EU mean that software applications that potentially could make data available outside the EU are avoided and hence, education entities rather refrain from interactive video conferencing.[45]

2.1.4 Cybersecurity Concerns in Relation to E-Learning

Protection of personal data is intrinsically tied to network and information systems (NIS) security. NIS security and privacy interact in a complex fashion. Many IT security incidents

---

[42] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Orientierungshilfe Videokonferenzsysteme (23 October 2020) 7 <https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf> last accessed 31 August 2021.

[43] Jon Brodkin, Zoom Lied to Users About End-to-end Encryption for Years, FTC Says (ars technical, 9 November 2020) <https://arstechnica.com/tech-policy/2020/11/zoom-lied-to-users-about-end-to-end-encryption-for-years-ftc-says/> last accessed 31 August 2021.

[44] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten (Version 2.0 18 February 2021) <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf> last accessed 31 August 2021.

[45] With the exception of some Universities or private institutions.

ultimately lead to personal data breaches. In the context of distance learning, IT security incidents are also likely to interfere with the right to equal access to education, and thus IT security includes a fundamental rights component as well.

Traditionally, in NIS security, one distinguishes between three dimensions: i.e. *confidentiality, integrity and availability* (the CIA triad) of NIS. A secure information system always requires all three dimensions to a certain extent. Confidentiality means that access to information should be restricted to only those who need access to it. Integrity relates to a guarantee of accurate, and reliable information, that is protected from unauthorised modification, destruction and loss. Finally, availability means that access to information is guaranteed to authorised persons as and when necessary.

A lack of NIS security fundamentally touches upon trust in NIS services. A number of incidents that occurred in distance learning scenarios relying on NIS impacted the trust of users, or in particular parents and teachers. An example for a lack in *confidentiality and integrity* is Zoom's statement in relation to the encryption standard used. Zoom stated that it offered end-to-end, 256-bit encryption, when in fact a lower level of security was provided.[46] Zoom maintained the cryptographic keys allowing the provider to access and modify the content of its customers' zoom meetings. Zoom's security weaknesses were taken advantage off when individuals broke into private meetings or intruded virtual classrooms, not only overhearing conversations but also adding content (this phenomenon is now known as Zoom bombing or Zoom raiding) including indecent or inappropriate content.[47]

A lack in *confidentiality and integrity* can also be established, when users of a state-run e-learning platform (here: Mebis) were able to forward users to random URLS by uploading malicious scripts.[48] Where NIS are not kept up and running, *availability* is interfered with. Educational resources have been subject to an increased number of DDoS attacks. In fact, Kasperky reported an increase by 550% from January 2019 to January 2020.[49] The platform most commonly used as lure was Zoom followed by Moodle.[50] However, a lack of

[46] Federal Trade Commission, FTC Requires Zoom to Enhance its Security Practices as Part of Settlement (9 November 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement.

[47] For instance, pupils of a primary school were suddenly 'flooded' with defamatory videos during a group chat of their class, seehim/AFP, Lernplattform gehackt, Videos mit zweifelhaftem Material eingespielt (Spiegel online, 20 January 2021) <https://www.spiegel.de/panorama/bildung/kelheim-in-bayern-lernplattform-gehackt-videos-eingespielt-a-2d95f9c5-bcd3-4b64-8f69-85b0947500ee> last accessed 31 August 2021.

[48] Volker Breigleb, Hacker finden Sicherheitslücken in Lernplattform Mebis (heise online, 21 August 2020) <https://www.heise.de/news/Hacker-finden-Sicherheitsluecken-in-Lernplattform-Mebis-4876001.html> last accessed 31 August 2021.

[49] Kaspersky, Digital Education: The cyberrisks of the online classroom (Securelist by Kaspersky, 04 September 2020) <https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/> last accessed 31 August 2021.

[50] Ibid.

availability must not necessarily be the result of a malicious attack. It seems that several reported incidents related to limited server capacity meaning that only a limited number of pupils was able to access an e-learning platform at a given time.[51]

2.1.4.1 IT Security as a Necessity to Guarantee Access to Education

When online learning platforms can no longer be accessed and for e.g., remote teaching sessions cannot be attended, equal access to education can no longer be guaranteed. In particular, children with a weak internet connection are being left behind. Since equal access to education and equal educational opportunities are a fundamental right, this triggers at least ethical discussions where access is interfered with.[52] In that regard, it is important to evaluate to which end these incidents could have been foreseen and avoided by the respective provider of the e-learning platform. It is necessary to distinguish between platforms introduced pre-pandemic as mere supporting platforms in class and for homework, and platforms specifically set up to cope with a situation where on-site classes are not possible. For the former, their service level agreements most likely assumed a small fraction of their traffic dedicated to distributing content to students in their home. As regards the latter, increased traffic was clearly foreseeable.

While the above incidents have technical issues at their core, social engineering attacks such as phishing, i.e., the attempt by an attacker to lure the victim to provide its credentials to a malicious login page, can be observed as well.[53] In the cooperate world, such attacks are usually seen as preventable by educating employees. However, also in the context of employees in a professional context,[54] awareness training and education often fail, and might even cause unintended harms.[55] Accordingly, one can assume that in context of children and adolescents, such measures are likely to be ineffective and technical measures which are less dependent from user action are needed.

---

[51] MDR, Probleme beim digitalen Lernen: Bildungsministerium will Kapazität für „Schul-Cloud" erweitern (mdr, 17 December 2020) <https://www.mdr.de/nachrichten/thueringen/corona-unterricht-home-schooling-schul-cloud-100.html> last accessed 31 August 2021; BR, Lernplattform Mebis fällt zum Lockdown-Start aus (br24, 16 December 2020) <https://www.br.de/nachrichten/bayern/lernplattform-mebis-faellt-zum-lockdown-start-aus,SJJuVFX> last accessed 31 August 2021

[52] Cf. Art. 14 (2) EU Charter of Fundamental Rights.

[53] (n49).

[54] M Alsharnouby., F Alaca and S Chiasson, Why phishing still works: User strategies for combating phishing attacks [2015] *International Journal of Human-Computer Studies*, 69-82, 82.

[55] Y T Chua, S Parkin, M Edwards, D Oliveira, S Schiffner, G Tyson and A Hutchings, Identifying unintended harms of cybersecurity countermeasures, in: IEEE, *2019 APWG Symposium on Electronic Crime Research (eCrime).*

In sum, IT security serves several purposes in online education. A further layer is added where providers of digital learning systems fall within the scope of application of the NIS Directive, which will be discussed in section III. 2.

2.2 **Selected E-Learning Solutions in Germany**

Since education is within the exclusive competence of the German states, each state has its own e-learning agenda independent from that of other states. The solutions provided differ in many aspects. The following section highlights selected exemplary solutions deployed in Germany and tries to categorise them regarding organisational level, and whether the provision of the service is in the hand of the public entity or outsourced.[56] The latter is inter alia relevant to determine accountability under GDPR and obligations under the NIS Directive.

2.2.1 Centralised vs. decentralised Approach

2.2.1.1 Centralised Organisation

Some e-learning solutions are provided by the competent ministry of the respective state. Exemplary for such a centralised state-run solution is the Bavarian MEBIS (short for Medien, Bildung, Service [media, education, service]. The MEBIS platform is operated by the Bavarian ministry of culture. It builds upon the prior used BayernMoodle, which already indicates the software at base.

MEBIS provides the following services:

- 'Infoportal': content provision on media education and media literacy as well support pages.
- 'Mediathek': media library containing more than 60.000 digital media files including content by public broadcasting services.
- 'Prüfungsarchiv': an archive providing access to previous final examinations and comparative exams.
- 'Lernplattform': a virtual learning environment based on the open-source learning management system (LMS) moodle. This is the central part of MEBIS. As MEBIS Lernplattform, it features a platform for teacher to create assignments and provide materials; it further includes a chat function and the possibility for teachers to create interactive content with H5P.[57]

---

[56] For an overview see Sven Rieken, Lernplattformen: Ein typisch deutsches Chaos (zdf heute, 15 January 2021) <https://www.zdf.de/nachrichten/politik/corona-schule-lernplattformen-100.html> last accessed 31 August 2021.

[57] H5P is also an open-source product making it easy for everyone to create, share and reuse interactive HTML5 content.

- 'teachSHARE': a platform with access restricted to teachers allowing them to exchange online content along themselves.
- 'Tafel': a browser-based software to make notes and serve as a virtual blackboard. Teachers may draft notes on the blackboard and share it with pupils.

Rhineland-Palatinate follows the Bavarian approach and launched Schulcampus RLP[58] in March 2021. This platform also integrates the prior existing moodle@RLP into a comprehensive service platform and hosts inter alia a digital media library, teaching plans and materials regarding media education and media literacy. A centralised solution must not necessarily be an in-house product. Other than the platforms integrating moodle and other open source or 'home-made' products, some states including Bremen opted to acquire licences from the commercial provider itslearning AS. Bremen signed a contract as early as 2015 following a European-wide tender in order to use itslearning as a supporting means for in-class education.[59]

Itslearning provides a platform for communication and cooperation and demonstrates features such as inter alia a content library, teacher communities, and reporting tools. The platform is specially adapted for schools with different assignment tools available. With itslearning being the only platform in Bremen, even prior to the COVID-19 crisis every pupil and teacher possessed a user account. Similarly, Saxony is operating LernSAX since 2011. It is based on the WebWeaver suite,[60] a commercially licensed, closed source platform that is offered as a SaaS solution by the German based company DigiOnline GmbH.

To the knowledge of the author, the key technical difference between itslearning and LernSAX is that the former is based on a public cloud solution, where all infrastructure is shared by the costumers of the platform, while the latter is based on a hybrid solution, where local storage in the schools is connected with a public cloud solution for sharing. Obviously, the solutions have in common that they were created to support in-class teaching; they were created to serve as an accessory and not foreseen to provide for direct distance teaching via video-conferencing.

---

[58] The platform is available at https://www.schulcampus-rlp.de.

[59] Freie Hansestadt Bremen, Landesinstitut für Schule, Unsere landesweite Lernplattform, <https://www.lis.bremen.de/medien/itslearning-32095> last accessed 31 August 2021.
The same applies to Berlin, which acquired licences for itslearning to reduce traffic directed at the domestic 'Lernraum Berlin'. The first licence encompasses 50,000 users, in the 2nd half of 2021 100,000 users may use the service. DPA, Schulen können Lernplattform „itslearning" kostenfrei nutzen (Berlin.de, 11 February 2021) <https://www.berlin.de/aktuelles/berlin/6441166-958092-schulen-koennen-lernplattform-itslearnin.html> last accessed 31 August 2021.

[60] For information on WebWeaver suite see https://www.webweaver.de/.

2.2.1.2 Decentralised Organisation

Unlike the afore-mentioned approaches, the state of Baden-Wurttemberg, for example, does not provide a centrally administrated platform. Instead, the ministry of culture advised schools to install and run their own moodle or bigbluebutton instances, and use the instant messenger Threema for communication.[61] Also, several Jitsi instances are used by 100,000 users.[62] Jitsi[63] is a video conferencing software that is open source under the apache license 2.0.[64] In order to use Jitsi, schools have to file a request with the school district's media center. In December 2020, the additional rollout of itslearning has been announced.[65] According to the ministry of culture, the ministry provides the means for using the aforementioned video conferencing solutions; in order to use the software, schools must address their competent media centre which is part of public administration of the municipality.[66] If one consults the websites of the local media centres, some provide direct access to e-learning platform such as moodle,[67] or guidance for the usage of the video conferencing solutions. In several cases, this guidance is drafted by local teachers.[68] There is strong fragmentation at local level with some municipalities providing central access to moodle and others even refraining from requesting a particular means or even giving a recommendation as to the use of a particular means. The only common approach at local level is the provision of a link to the central media library SESAM which inter alia hosts content of the public broadcasting institution of the state for use by teachers.

2.2.2 The Service Provision: Public or Private?

Further differences between the various solutions relate to the provider of the service: namely, whether the e-learning solution is run by the respective public body in charge, or whether this task is outsourced to a private sector company, which then in turn acts as

---

[61] Ministerium für Kultus, Jugend und Sport Baden-Württemberg, Instant Messenger Threema erhält Zuschlag als Teil der Digitalen Bildungsplattform (24 September 2020) <https://km-bw.de/,Lde/startseite/service/2020+09+24+Instant+Messenger+Threema> last accessed 31 August 2021.

[62] Sven Rieken, Lernplattformen: Ein typisch deutsches Chaos (zdf heute, 15 January 2021) <https://www.zdf.de/nachrichten/politik/corona-schule-lernplattformen-100.html> last accessed 31 August 2021.

[63] See https://jitsi.org.

[64] See http://www.apache.org/licenses/.

[65] Ministerium für Kultus, Jugend und Sport Baden-Württemberg, itslearning erhält Zuschlag als Lernmanagementsystem für die Digitale Bildungsplattform (09 December 2020) <https://km-bw.de/,Lde/startseite/service/2020+12+09++itslearning+erhaelt+Zuschlag+als+Lernmanagementsystem+fuer+die+Digitale+Bildungsplattform> last accessed 31 August 2021.

[66] Landesmedienzentrum Baden-Württemberg, Informationen für Schulen zur Videokonferenz-Software Jitsi (28 May 2020) <https://www.lmz-bw.de/newsroom/newsroom/detailseite/informationen-fuer-schulen-zur-videokonferenz-software-jitsi/> last accessed 31 August 2021.

[67] Cf. for instance https://moodle.mzhd.de/moodle/blocks/exa2fa/login/.

[68] Cf. For instance https://www.kmz-sbk.de/videokonferenz-server/.

service provider. From the above examples, itslearning, learnSAX, and the use of Threema fall under the private model, while the various moodle and jitsi instances fall under the public model.

2.2.2.1 Public Provision

A central part of most state-operated e-learning platforms are moodle-based integrations. Moodle[69] in itself is an open-source software published under the gnu general public license version 3,[70] under which anyone can run (and modify) a moodle instance. However, setting up and maintaining a moodle instance requires infrastructure and expertise, both generally lacking at the level of the actual user (i.e., individual schools). Under such circumstances both expertise and infrastructure can be outsourced to a cloud service under a Software as a Service (SaaS) model.

SaaS is a software licencing and delivery model where the software with the business logic is centrally hosted and maintained by a service provider. Users are accessing the software using a thin client, i.e., a client software that does not run any business logic, such as a browser. Moodle is offering such services directly, but as an Australian-based project, using their services, would raise the same concerns as using similar US-based services. Hence many states refrain from SaaS and run their moodle instances themselves.[71]

The provision of software must not be confused with the hosting of content. When MEBIS for instance features further applications such as the media library or the virtual blackboard, these applications are not only provided by the state of Bavaria but also hosted on servers of the IT-Dienstleistungszentrum (Center for the provision of IT services) of the state of Bavaria, a public authority under the auspice of the Bavarian state ministry of finance and homeland.[72]

Baden-Wurttemberg with its decentralised approach regarding organisation, also uses servers that are operated and owned by the state. Accordingly, Bigbluebutton is hosted on state-owned servers.[73] As regards Jitsi, however, hosting services are either provided by

[69] More information about Moodle can be accessed via the Moodle website at https://moodle.com.
[70] https://www.gnu.org/licenses/gpl-3.0.en.html.
[71] See above moodle@RLP and the BayernMoodle.
[72] For more on the IT-Dienstleistungszentrum des Freistaats Bayern, see https://www.ldbv.bayern.de/digitalisierung/itdlz.html.
[73] Ministerium für Kultus, Jugend und Sport Baden-Württemberg, Erweiterung der Serverkapazitäten von BigBlueButton (24 February 2021) < https://km-bw.de/,Len/startseite/service/2021-02-24-serverkapazitaeten-big-blue-button-erhoeht> last accessed 31 August 2021.

the respective media center (i.e. state) or external service providers (i.e. private third parties).[74]

2.2.2.2 Private Provision

The state of Saxony has been operating the commercially licensed, closed source platform LernSAX since 2011. LernSAX is based on the WebWeaver suite[75], and is offered as a SaaS solution by the German based, small company DigiOnline GmbH. Technical information is scarce, but the infrastructure seems to be based on a combination of public and private clouds, i.e., some of the cloud infrastructure is placed at the customer's premises while other parts are shared with all DigiOnline costumer. According to DigiOnline, data of German schools is hosted in Germany.

Similar to LernSax, itslearning is also a commercially licensed, closed source platform offered as a SaaS solution. Itslearning is provided by Itsleaning GmbH[76], part of the globally active Finnish cooperation Sanoma[77]. As with LernSax, there is not much information available regarding the technology, but the infrastructure seems to be based on a pure cloud solution with minimal hardware locally in schools.

3 Accountability and Legal Obligations arising from the GDPR and NIS Directive

Due to the fragmented approach to e-learning and e-learning solutions in Germany, different roles can be attributed to the different actors under the GDPR. The following section briefly outlines the main obligations for data controllers and data processors, before the challenges posed by the different organisational frameworks for e-learning are addressed. In that regard, the legal uncertainty stemming from the overall fragmentation and a potential shift of accountability towards the weakest link are focussed on. Furthermore, since e-learning requires security of the underlying infrastructure, this

---

[74] Landesmedienzentrum Baden-Württemberg, Informationen für Schulen zur Videokonferenz-Software Jitsi (28 May 2020) < https://www.lmz-bw.de/aktuelles/aktuelle-meldungen/detailseite/informationen-fuer-schulen-zur-videokonferenz-software-jitsi/> last accessed 31 August 2021.

[75] See https://www.webweaver.de/. Regarding the privacy by design implemented in Webweaver School see Webweaver, Wie unterstützt Webweaver School den Datenschutz (Priavy by desing)? <https://www.webweaver.de/wws/9.php#/wws/privacy_by_design.php?sid=27980258220660131861780108019690> last accessed 31 August 2021.

[76] https://itslearning.com/de/.

[77] See http://www.sanoma.com. In 2021, the net sales of Sanoma amounted to approx. EUR 1.25bn; the number of employees amounted to 5,000. Sanoma declares itself as 'the leading European publisher of education materials and services for students, teachers and schools in primary, secondary and vocational education'.

section also analyses whether the NIS Directive imposes any additional obligations upon the service providers involved.

3.1 Accountability and Legal Obligations under GDPR – A Determination of the Role of Actors Involved: Who is Who?

As outlined above, e-learning tools may collect, and consequently process a variety of personal data in the sense of Art. 4(1) GDPR. The extent to which a data processing organisation or natural person is subject to obligations under data protection law depends on whether they are considered as data controller or data processor.

For the afore described scenarios, the distinction is not as obvious as it may seem at first glance. Instead of focusing in detail on the exact determination of the actors involved, this section rather seeks to outline how accountability shifts depending on the set-up.

Considering the many different actors involved (individual teachers, schools, local/regional municipalities, ministries), the question arises as to who can be held accountable as data controller.[78] According to Art. 4(7) GDPR '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 EU or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law. In contrast, natural or legal persons, public authorities, agencies, or other bodies which process personal data on behalf of the controller are data processors (Art. 4(8) GDPR). Controllers bear primary responsibility for ensuring that processing activities are compliant with EU data protection law.

Taking the example of the centrally organised approach of Bavaria, the ministry of culture that provides the platform as a service, also determines the means and purpose of data processing and can thus be considered a data controller. When the IT service centre of Bavaria hosts the learning platforms centrally, the centre may be processing data on behalf of the ministry of culture and be thus considered as a data processor. It can be assumed that individual schools and teachers (or even pupils) are not involved in the data processing since they neither determine nor control the processing activities; Teachers as well as the pupils are mere data subjects. The attribution and determination of roles is rather clear cut. However, the scenario becomes more complicated where there is no central state administrated platform, but schools are free to install and run their own moodle or bigbluebutton instances like in Baden-Wurttemberg. As outlined above, the local school district's media centre may provide direct access to a moodle instance and provide direct or indirect (via guidance) access to video conferencing tools. In this case, the individual

[78] Regarding the untangling of powers and responsibilities of actors involved in remote teaching see (n35), 49 et seq.

school may determine the means of processing for learning purposes itself and thus, become a data controller with regard to the respective application. Where an individual institution and the school district's media centre take a joint decision as to the means and purposes of a certain application, they may qualify as joint controllers in the sense of Art. 26 GDPR. Of course, not all processing operations involving more than one entity give rise to joint controllership. However, when two entities complement each other and are essential for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of processing, joint controllership can be established.[79] Following the CJEU's ruling in the Fashion ID case[80], the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data is likely to amount to a joint decision on the means of that processing by those entities. Considering that schools are free to use online teaching means, and if they decide to do so, the media centre determines the means by providing a pre-selection of applications or an application that runs on its own servers, this amounts to joint controllership. Individual schools (as well as the media centres) are then data controllers in the sense of Art. 4(7) GDPR for the processing of personal data on the learning platform or video-conferencing system, meaning that they are subject to an extensive catalogue of obligations under GDPR. For instance, they must conduct a data protection impact assessment (Art. 35 GDPR), implement appropriate security measures (Art. 32), keep records of processing activities (Art. 18), are subject to reporting obligations (Arts. 33 and 34) or must potentially appoint a DPO (Art. 37 GDPR).

Comparing the Baden-Wurttemberg and Bavarian approach, a further difference exist in that Baden-Wurttemberg foresees the use of servers of an external host provider to host content, i.e. personal data. An external provider may process data on behalf of the joint controllers (media centre and individual school). This again raises the issues addressed in the background section: is the third-party data processor in a position to guarantee compliance with EU data protection law? This issue does not occur where servers are hosted locally (or even on EU territory) by the state. Any data processing carried out by a third-party data processor acting on the school's, media centre's or ministry's behalf, must be governed by a contract or other legal act. Regularly, so called data processing agreements are concluded with the service provider. These processing agreements must include concrete information as to how the requirements of Art. 28 GDPR will be met and consider the specific tasks and responsibilities of the processor in the context of the data processing as well as the risk to the rights and freedoms of the data subjects. German states that employ itslearning have for instance concluded such data processing agreements. However, where a state only bears the licence fee for a third-party e-learning instance, the individual school as data controller or jointly with a media centre will have to conclude such an agreement.

[79] EDPB, Guidelines 07/2020 on the Concept of Controller and Processor in the GDPR (Version 1.0, 02 September 2020) 18.
[80] Case C-40/17 *Fashion ID* ECLI:EU:2018:1039.

In conclusion, the attribution of the different roles in data processing varies when individual institutions are free to decide alone or jointly with the local media centre on using a certain application. In said case it must be identified whether the media centre only processes data on behalf of the individual institution for instance by integrating an open source software solution or whether they decide jointly on the means and purpose of processing, especially in the case of using a third party service. When the individual institution becomes a data controller, a variety of challenges arise in connection with the obligations imposed upon data controllers including the conclusion of processing agreements with third party providers. An individual school, however, is likely to lack the expertise as to GDPR compliance in terms of processing agreements or data processing in general. Where third-party service providers are involved, one also needs to consider that technology companies want to keep their data analytics and algorithms proprietary which can make it difficult to see what information is being collected, and how it is being used. Without external expertise, the individual institution is unlikely to be in a position to grasp the dimension of data processing. This is very much different from where a ministry is the data controller and processes personal data on state-owned local servers.

3.2 Obligations Arising under the NIS Directive: Improving the Overall Security?

As a Directive the NIS Directive is not directly applicable and needs to be transposed into national law by the Member States. In terms of simplification, the following section will refer to the respective articles of the NIS Directive instead of those of the German implementing acts.

The Directive applies to and distinguishes between operators of essential services of a type referred to in Annex II of the NIS Directive, and providers of digital services of a type listed in Annex III of the NIS Directive.[81] Of relevance in the context of distance learning are digital services. These encompass cloud computing services, search engines and online marketplaces. Cloud computing service means a digital service that enables access to a scalable and elastic pool of shareable computing resources (Art. 4(19) NIS Directive).[82] E-Learning platforms display these three properties and can therefore be identified as a cloud service. The NIS Directive however only applies, when such service is provided by a 'legal

[81] Cf. Art. 4(4) and (5) NIS Directive.

[82] Recital 17 NISD: For the purposes of this Directive, the term 'cloud computing services' covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services. The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term 'elastic pool' is used to describe those computing resources that are provisioned and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term 'shareable' is used to describe those computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

person' (Art. 4(6) NIS Directive). This excludes public administrations, since recital 45 clarifies that the NIS Directive only applies to 'those public administrations which are identified as operators of essential services'. As a consequence, the NIS Directive is not applicable where the e-learning solution is provided by a public authority that is part of the public administration, e.g., as it is the case in Bavaria.

Where the NIS Directive applies, service providers are inter alia subject to reporting obligations in case of security incidents (Art. 16(3) NIS Directive) and security mechanisms (Art. 16(1) NIS Directive). However, recital 53 exempts micro and small enterprises from these requirements. This means for the e-learning tools offered by third-party service providers as SaaS, that being subject to obligations under the NIS Directive depends on their size – resulting in more obligations for large companies in contrast to the relatively small provider of LearnSax[83]. But also, where the incident reporting obligation exists in general, incidents are likely to remain unreported due to the requirement that reporting is only mandatory where the incident has a substantial impact on the service.

The notion of substantial is defined in Art. 16 NIS Directive and the parameters are further specified in a Commission Implementing Regulation.[84] Art. 4 Commission Implementing Regulation[85] for instance provides that an incident shall be considered as having a substantial impact where at least one of the following situations has taken place: (a) the service provided by a digital service provider was unavailable for more than 5,000,000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes; (b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100,000 users in the Union; (c) the incident has created a risk to public safety, public security or of loss of life; (d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1,000,000. Although user-hours may be of relevance where larger states are concerned or a disruption for several days occurred, the measurement of the number of users impacted remains one of the most important variables in determining significance.[86] In that regard recital 9

[83] LearnSax is a small business in the sense of Art. 2(2) Commission Recommendation 2003/361/EC annex whereas itsLearning GmbH with a presumably dominant influence by the mother cooperation passes the threshold.

[84] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L26/48.

[85] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L26/48.

[86] Cf. ENISA, Incident Notification for DSPs in the context of the NIS Directive (2017), 23.

Commission Implementing Regulation determines that the users of digital services should encompass natural and legal persons who are customers of or are subscribers to [...] a cloud computing service. This raises the question whether teachers and pupils can be considered customers or subscribers. ENISA identified the following measurement units for subscribers: corporate subscribers, non-subscribers (visitors), reliant services and individual subscribers/accounts.[87] One may argue that schools are corporate subscribers in the case of Baden-Wurttemberg and have multiple accounts per client set by different individuals, whereas in the case of a central platform like Mebis, pupils and teachers are individual subscribers. Considering that the Commission Implementing Regulation sets thresholds for DSPs, decentralisation of remote learning obviously results in less mandatory reporting obligations. This in turn raises concerns, because for the individual users it does not make a difference who provides the service. Further, the general public may find it difficult to understand why a security incident for instance in the state of Saxony may never be reportable (small provider and number of pupils not reaching reporting threshold).

4 Conclusion

The process of setting up an environment for every student to be able to learn on the same day encounters many obstacles. Some of these are owed to insufficient infrastructure and lacking capacities, while others are of a legal nature.

The case of Germany, with its educational system where exclusive competence is granted to the 16 German states for their jurisdiction resulting in 16 potentially diverging legal frameworks, perfectly highlights several of the legal obstacles of switching to e-learning solutions. The decentralised organised state solutions raise questions with regard to accountability under GDPR. The attribution of the role of (joint) controller becomes difficult with many actors involved. Adding to this is the lack of consistency even within some states. The fragmentation leads to confusion and an overburden concerning GDPR compliance on the smallest actor involved, the individual institution, if clear guidance with standards is lacking. Individual institutions together with municipalities must for instance draw risk assessments and set up processing agreements, whilst potentially lacking the legal expertise. When guidance for using Jitsi is drawn by local teachers, this presents a strong indication that neither guidance is provided for the use of the software nor for using it in a GDPR-compliant manner.[88]

Under the NIS Directive, there is also a different treatment of the actors involved, which primarily depends on the size of the actor. In terms of security and incident reporting, which are central elements of the NIS Directive, fragmentation results in diverging

[87] Ibid.

[88] For GDPR compliance in the design of an e-learning platform see Evangelia Vanezi, Dimitrios Kouzapas et al., GDPR Compliance in the Design of the INFORM e-Learning Platform: A Case Study, (2019) 13th International Conference on Research Challenges in Information Science (RCIS).

reporting obligations: decentralised solutions are likely to impair no such obligations, whereas a central organisation means that the threshold to fall within the scope of application of the NIS Directive can be reached. Obligations also vary depending on whether the entity concerned is from the private or public sector. The different treatment of actors offering the same service may be justified in light of an increased attack surface, but not in terms of who offers the service.

Although seemingly most incidents that occurred so far where connected to insufficient infrastructure, with growing digitalisation the overall attack surface increases. The reported increase in attacks[89] is very much likely to stay. With fake login pages for moodle or phishing emails related to educational platforms, cybercriminals are trying to get hold of login credentials.[90] Thus, excluding some entities from incident reporting contravenes the aim of increased cyber resilience.

The ratio of the NIS Directive is not only to increase the overall resilience of NIS within the EU, but also the identification of threats and the sharing of the lessons learned. On this note, this leads to the question to which end the digital infrastructure for distance learning needs to be considered as vital for the functioning of the society also beyond the current pandemic situation. The example of Germany shows that the local solutions may not take sufficiently into account data security which in turn threatens data protection. Centralised solutions with clear attribution of accountability provide a more solid framework for personal data protection and data security. Introducing a uniform and consistent approach at state level as conducted in Bavaria or Rhineland-Palatinate is laudable start.

The NIS 2.0 proposal[91] targets some of the weaknesses identified in terms of NIS security. The proposal inter alia extends the scope of reportable incidents to incidents that have the potential to cause substantial operational disruption.[92] Further new sectors will be added including public administration, and several existing sectors are amended. In the context of e-learning, amendments in the digital infrastructure sector mean that also content delivery networks (which obviously include digital media libraries) are encompassed. Further, Art. 2 NIS 2.0 proposal foresees that 'this Directive applies to public and private entities of a type referred to as essential entities in Annex I and…not…to entities that qualify as micro and small enterprises…'.[93] Accordingly, the distinction between public authorities and private entities providing digital services is lifted and cloud-based solutions

[89] Kasperky, Digital Education: The Cyberrisks of the Online Classroom (Kaspersky Securelist, 04 September 2020) <https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/> last accessed 31 August 2021.
[90] Ibid.
[91] European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.
[92] Art. 20(3) NIS 2.0 proposal.
[93] Annex I enlists as essential entities, *inter alia,* cloud computing service providers and content delivery networks under the category of digital infrastructure.

provided by public authorities will fall under the Directive depending on the size of the providing entity.[94] This will at least eliminated the unjustified different treatment of public and private service providers.

Funding Acknowledgement: This research was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

[94] The NIS 2.0 proposal introduces a classification of services based on the importance of the service provided. Whether a service provider falls within the scope of the Directive is determined by the stand-alone criterion of size, which is applied across all Member States.