BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 6 • N° 25 • AUGUST 2020

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

THE DARK SIDE OF THE MOOC?

THE RISE OF EDTECH IN TIMES OF COVID-19: A DATA PROTECTION CHALLENGE FOR UNIVERSITIES

Jonas Botta, Postdoctoral Researcher at the German Research Institute for Public Administration and Reader in Human Rights Law at the Berlin School of Economics and Law

The dramatic spread of COVID-19 is causing a profound upheaval in education. Almost overnight, there has been an unprecedented need for educational technologies ("EdTech") to compensate for the loss of "face-to-face" teaching at schools and universities. Especially for universities, it makes sense to benefit from the numerous offers of e-learning platforms, mainly so-called Massive Open Online Courses (MOOCs). After all, the choice of topics for online courses is extremely diverse, from introductory courses in programming languages such as Java or Python to modules on the work of William Shakespeare and units on the legislative mechanisms in the EU Multi-Level System.

However, if, for instance, universities want to make EdTech such as MOOCs available to their students as soon as possible, they will not only have to deal with financial and educational but also legal challenges. The virtual seminar room gives rise to completely new questions regarding the privacy of students: Which data protection standards must EU universities observe within the scope of the General Data Protection Regulation if they want to process user data for teaching or research purposes? Which data protection provisions can be invoked by universities if they want to make online studies mandatory? Could universities possibly be liable for data protection violations by the MOOC providers? These are the questions this working paper aims to answer.

Key Words: (Joint) controllership, data processing for scientific research purposes, freely given consent, GDPR, e-learning platforms, Massive Open Online Courses (MOOCs)

Contents

Disclaimer 2

1. The Return of the MOOC 3

2. Realities in the Virtual Seminar Room: Big Data and Small Privacy? 4

3. Legal Framework of Data Processing in the Virtual Seminar Room 5

3.1 The Gretchen Question: Who is the Controller? 5

3.2 Universities and MOOC providers as joint controllers 6

3.2.1 Possibility of Controlling Influence through Individual Contract Design 6

3.2.2 Mere Causality? 7

3.3 Consequences 9

3.3.1 Arrangement in a Transparent Manner 9

3.3.2 Claims for Damages by Students 9

4. Data Protection Requirements for Universities 10

4.1 Privileged Data Processing for Scientific Research Purposes 10

4.2 Legal Basis for Mandatory Online Courses 12

4.2.1 Student Consent 12

4.2.2 Legal Basis in the Law of the Member States 13

4.3 Fully Automated Processing of Digital Examinations 13

Conclusion 14

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
An earlier version of this working paper was published as Jonas Botta, 'The Dark Side of the MOOC?: The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities' [2020] Privacy in Germany 93. Both are based on the findings from the author's doctoral thesis. See Jonas Botta, *Datenschutz bei E-Learning-Plattformen: Rechtliche Herausforderungen digitaler Hochschulbildung am Beispiel der Massive Open Online Courses (MOOCs)* (Frankfurter Studien zum Datenschutz 2020).

Disclaimer

1. The Return of the MOOC

Less than ten years ago, there was still substantial hype surrounding MOOCs. Their success seemed to signal the end of traditional university teaching in brick-and-mortar classrooms, making the best education available to anyone at any time with a simple mouse-click. The trigger for worldwide enthusiasm was the course "Introduction to Artificial Intelligence" at Stanford University in 2011, which was designed by two computer scientists, Peter Norvig and Sebastian Thrun. They not only digitised a conventional university lecture, but also integrated exercises and a discussion forum into their online course. Their concept was so successful that approximately 160,000 people registered and over 20,000 users successfully completed the course.[1] As a result, their "Introduction to Artificial Intelligence" had more graduates than students enrolled at Stanford at the time.[2]

The subsequent spread of MOOCs was described by commentators at the time as a revolution[3] or even a "tsunami"[4], and the emergence of online courses was seen as extremely disruptive. The New York Times even proclaimed the year 2012 as the year of the MOOC.[5] Above all, the potentially unlimited number of participants made this EdTech known globally. As a result, universities around the world joined the hype. Outside the sphere of education, companies were founded that made the digital infrastructure for the creation and deployment of MOOCs available. Eventually, the two private companies Coursera (the market leader with around 45m users)[6] and Udacity (co-founded by the "MOOC father" Thrun), along with the non-profit company edX (which was initiated as a joint venture between Harvard University and the Massachusetts Institute of Technology), were the winners in global competition. These companies have become more than mere service providers for the universities cooperating with them. They have established themselves as independent brands for digital education.

As is usually the case with hyped technologies, MOOCs could not meet all the expectations placed on them. The vision of the Bangladeshi fisherman who takes management courses at Harvard Business School has not been realized as a result of digital higher education, nor have empty lecture halls and extinct university buildings. But even if the number of graduates has fallen short of initial expectations,[7] the number of users is growing steadily[8].

After things recently became quiet around MOOCs, with the digitisation of the whole higher education system progressing slowly (though steadily), dramatic events came thick and fast in spring 2020. The reason, however, was not a new education policy agenda, but the outbreak of COVID-19. Around the world, schools and universities have been forced to shift their teaching online. Due to the short lead time, but also because of the popularity of online courses, this has been heralded the "return" of MOOCs.

1 C. Osvaldo Rodriguez, 'MOOCs and the AI-Stanford like Courses: Two Successful and Distinct Course Formats for Massive Open Online Courses' (2012) <http://www.eurodl.org/materials/contrib/2012/Rodriguez.pdf> accessed 21 March 2020..
2 Cf. < https://registrar.stanford.edu/everyone/enrollment-statistics/enrollment-statistics-2011-12> accessed 21 March 2020.
3 Thomas L Friedman, 'Revolution Hits the Universities' *The New York Times Online* (26 January 2013) <https://www.nytimes.com/2013/01/27/opinion/sunday/friedman-revolution-hits-the-universities.html?_r=1&> accessed 21 March 2020.
4 David Brooks, 'The Campus Tsunami' *The New York Times Online* (3 May 2012) <https://www.nytimes.com/2012/05/04/opinion/brooks-the-campus-tsunami.html> accessed 21 March 2020.
5 Laura Pappano, 'The Year of the MOOC' *The New York Times* (4 November 2012) ED26.
6 See > https://www.classcentral.com/report/coursera-2019-year-review/< accessed 21 March 2020.
7 Elise Young, 'Educational Privacy in the Online Classroom: FERPA, MOOCs, and the Big Data Conundrum' (2015) 28 Harvard Journal of Law & Technology 549, 566.
8 Isaac Chuang and Andrew D Ho, 'HarvardX and MITx: Four Years of Open Online Courses' (Cambridge, MA 2016) 4.

2. Realities in the Virtual Seminar Room: Big Data and Small Privacy?

When introducing new digital teaching formats, universities not only have to consider financial and pedagogical challenges but also various data protection risks surrounding MOOCs.[9] This is because anyone who decides to attend a MOOC enters a virtual seminar room in which users not only broaden their own horizon, but also expose themselves to the gaze of an invisible observer. The software systems of the online courses can process every click the user makes to form a digital footprint.

From registration and participation to the successful completion or cancellation of an online course, the MOOC providers process immense amounts of data of its users. This includes information such as user name, e-mail address, country of origin, gender and date of birth, which the provider already collects when someone registers as a user and creates a personal profile. On top of that, comprehensive evidence of the exact activities of the individual course participants is generated. This is the major difference from conventional education databases.

For example, the clickstream of the first MOOC of the Massachusetts Institute of Technology recorded all 230m interactions of the approximately 155,000 registered participants.[10] The data on individual user behaviour provides information, for instance, on the number of registrations (all log-ins or log-outs of the user), the processing time required for the entire course, the web-pages viewed, the user's IP address and the frequency and duration of access to the materials.[11] In order to collect this user data, the providers make use of tracking tools such as Google Analytics and cookies, which they also pass on to third parties (e.g. Facebook, Google or Twitter) and allow them to place the information on their websites.

The providers also gain comprehensive information about the services provided online by the individual: examination results, grades, submitted work and evaluations by the lecturer or other participants. In order to officially certify the completion of a MOOC, the provider must also ensure that all input actually comes from the registered user and not from a third party. For this reason, on some platforms there are identity checks with the help of a webcam or copies of the identity card.[12]

A MOOC provider can access even more data if the user wants to make use of other services offered by the provider, such as the career service. In this case, users regularly provide information not only about their previous education, former and current employers, but also their salary in order to ensure that the provider finds them a job according to their individual wishes.[13] In addition to user profiles, the public discussion forums of the online courses are another data source. In these forums, not only is it usual to

9 There is no single definition of MOOCs. However, they are characterized mainly by the following identification features: a large number of short video and audio recordings, uploaded teaching material, a forum for exchange among users, as well as digital examinations.

10 Lori Breslow and others, 'Studying Learning in the Worldwide Classroom Research into edX's First MOOC' [2013] Research & Practice in Assessment 13, 14.

11 Jon P Daries and others, 'Privacy, anonymity, and big data in the social sciences' [2014] Communications of the ACM 56, 59; International Working Group on Data Protection in Telecommunications, 'Working Paper on E-Learning Platforms' (Washington, D.C. 2017) 1; Una-May O'Reilly and Kalyan Veeramachaneni, 'Technology for Mining the Big Data of MOOCs' [2014] Research & Practice in Assessment 29, 29.

12 Gabi Witthaus and others, 'Validation of Non-formal MOOC-based Learning: An Analysis of Assessment and Recognition Practices in Europe (OpenCred)' (Brussels 2016) <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96968/lfna27660enn.pdf>, 30 et seq.

13 Mario Martini and Jonas Botta, 'Undurchsichtige Datentransfers – gläserne Studierende?: Datenschutzrechtliche Schranken der Datenübermittlung in die USA am Beispiel von Massive Open Online Courses (MOOCs)' (2019) 110 Verwaltungsarchiv 235, 239.

introduce oneself personally,[14] but users also hold debates in which they express their political opinion or religious beliefs. Moreover, the provider's data access is not limited to the virtual seminar room. If users connect their profiles on the MOOC platform with their profiles on a social network, the provider can also access information stored there.

Even in its early days, the data volume of a single MOOC amounted to around 20 gigabytes.[15] This corresponds to several million pages of paper.[16] Today's educational data sets, created when digital learning opportunities are used, are therefore larger and more complex than ever before. We are talking about Big Data.[17] However, the technical possibilities have clearly not been exhausted yet. In order to be able to react to the individual learning motivation of MOOC participants in real time, it is conceivable, for example, to implement face recognition software that would allow the attention and emotional state of users to be determined immediately.[18]

3. Legal Framework of Data Processing in the Virtual Seminar Room

As a result of the complex and extensive data collections resulting from MOOC use, online courses are proving to be an education-specific manifestation of the Big Data age. It is often solely up to the controllers, whether their technology turns out to be an essential step on the way to Humboldt's educational ideal of "equal education for all" or an Orwellian dystopia of "transparent users".[19]

This raises the crucial question of who are the controllers in the virtual seminar room: the universities or the MOOC providers (1) or even both (2)? The answer to this question determines the extent to which universities must comply with data protection provisions (3). This is because EU data protection law primarily obliges the controller(s) of a data processing operation (see Article 24, Recital 74 GDPR).

3.1 The Gretchen Question: Who is the Controller?

A controller is any body which alone or jointly with others determines the purposes and means of the processing of personal data (Article 4 (7) GDPR). The decisive factor in determining responsibility is therefore the essential power to decide on the "why" and the "how" of the data processing.[20] Some universities have created their own digital infrastructure to enable their students to access MOOCs – examples for university operated platforms are openHPI in Potsdam (Germany) or iMooX in Graz (Austria). It is then solely their responsibility to decide which personal data of their students they want to process and for which purposes.

14 Daries and others (n 11) 58.
15 Andrew D Ho and others, 'HarvardX and MITx: The First Year of Open Online Courses' (Cambridge, MA 2014) 5.
16 Young (n 7) 551.
17 ibid, 549; cf. Martini and Botta (n 13) 241.
18 Face recognition software is already being used for this purpose in education: For example, two online courses at the PSB Paris School of Business use Nestor to analyze user attention. See Amar Toor, 'This French school is using facial recognition to find out when students aren't paying attention: Nestor software will be used for two remote classes at a Paris business school later this year' *The Verge* (26 May 2017) <https://www.theverge.com/2017/5/26/15679806/ai-education-facial-recognition-nestor-france> accessed 21 March 2020.
19 Cf. Martini and Botta (n 13) 237.
20 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor", WP 169' (Brussels 16 February 2010) 13.

Even if universities only refer their students to the offers of commercial MOOC providers such as Coursera or Udacity, they could be responsible for the data processing on their platforms. This is because the MOOC providers could merely be the processors of the universities. A processor only acts on behalf of the controller and does not make any major decisions about the purpose and means of data processing (Article 4 (8) GDPR). This does not imply that the processor is subordinate to the controller, but it is up to the controller to give the processor room for manoeuvre.[21]

The aforementioned MOOC providers collect and use the personal data of their users for their own purposes, for example to personalize and develop their services, but also to pass them on to third parties, and with their own means such as cookies, evaluation software, analysis algorithms etc. They are not simply processors of their university partners, since they not only exercise de facto control over user data, but also pursue their own economic interests in data processing, which go beyond the mere fulfilment of contractual obligations with the universities.[22] Under these circumstances, the MOOC providers are controllers according to Article 4 (7) GDPR – and the universities that cooperate with them?

3.2 Universities and MOOC providers as joint controllers

Even if universities do not operate their own MOOC platforms, but only require or encourage their students to participate in courses offered by commercial providers, they cannot assume that they will not be held responsible for data processing in the virtual seminar room. On the contrary, they may also be liable for data protection violations by the MOOC providers.

The reason for this is the concept of joint controllership (Article 4 (7) and Article 26 (1) sentence 1 GDPR). In times of increasingly complex forms of cooperation in the processing context, this concept intends to prevent the data subjects from falling behind, as they can no longer be sure who is responsible for processing the personal data relating to them and to what extent. Joint controllership implies that each party involved has a controlling influence on the purposes of and the means of data processing.[23]

3.2.1 Possibility of Controlling Influence through Individual Contract Design

The possibility of controlling influence is to be determined on the basis of the factual circumstances and not solely on the basis of formal provisions, which may result from the contractual relationship between the MOOC provider and the university.[24] Nevertheless, the existence of an official relationship in the form of a contract between provider and university is an important indication of joint controllership.[25] With regard to the processing objectives, such as the evaluation of performance and identification of users or the transfer of data to the universities, a common interest of the latter with the provider can generally be assumed. However, the higher education institutions would also have to be able to exert a controlling influence on the processing purposes and means.

21 Cf. European Data Protection Supervisor, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' (Brussels 7 November 2019) 16 et seq.
22 Martini and Botta (n 13) 250; cf. Article 29 Data Protection Working Party (n 20) 25.
23 Mario Martini, 'Art. 26' in Boris P Paal and Daniel A Pauly (eds), *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz: Kommentar* (Beck'sche Kompakt-Kommentare, 2nd edn C. H. Beck 2018) Rn. 19.
24 Article 29 Data Protection Working Party (n 20) 8 et seq.
25 Martini and Botta (n 13) 251.

In principle, universities have the possibility to negotiate individual contract conditions with the provider or, if necessary, to achieve a better negotiation result with other providers. In this way, the respective co-operation partner can ensure control over the processing of user data. The decisive factor is, therefore, whether an individual contract has been drawn up in the respective case or whether the university could ultimately only agree to or reject a standard form contract issued by the provider.[26]

An individual contract design can be expressed in particular by specific quality requirements for the course offer.[27] For example, if universities want to recognise the examination results obtained in the MOOCs as their own academic achievements and award points for this according to the European Credit Transfer and Accumulation System, they must ensure that the online courses meet the respective requirements. The more content requirements a university has for online courses, the greater its potential influence on data processing by the MOOC provider. In this case, it is, in principle, insignificant that only the provider processes the personal user data. Such a division of labour is permissible.[28] In any case, the joint controllership of a university is limited to the processing procedures of the provider that are necessary for the recognition of performance.[29]

3.2.2 Mere Causality?

Even if the university refrains from influencing the processing of personal user data by means of an individual contract, it is still partly responsible for the latter if it induces its students to take a MOOC. However, is a mere causality sufficient to establish joint controllership under Article 4 (7) and Article 26 (1) sentence 1 GDPR?

3.2.2.1 Lessons from the CJEU's Judgment in the "Facebook Fan Page" Case

In recent years, a similar question has kept German administrative jurisprudence busy: Is a company allowed to administer a Facebook fan page without being responsible for ensuring that the social network complies with applicable data protection laws, even though it receives extensive (anonymised) visitor statistics thanks to Facebook Insights[30] and can potentially control these statistics through parameterisation[31]?[32]

The starting point of the legal dispute was an order issued by the Independent Data Protection Centre for the Land of Schleswig-Holstein in 2011 against the Wirtschaftsakademie Schleswig-Holstein[33] to deactivate its Facebook fan page due to data protection violations of the social network.[34] Following the

26 Cf. Mario Martini and Saskia Fritzsche, 'Mitverantwortung in sozialen Netzwerken: Fanpage-Betreiber in der datenschutzrechtlichen Grauzone' [21/2015] Neue Zeitschrift für Verwaltungsrecht Extra 1, 4 et seq.
27 Martini and Botta (n 13) 251.
28 Cf. Thomas Petri, 'Datenschutzrechtliche Verantwortlichkeit im Internet: Überblick und Bewertung der aktuellen Rechtsprechung' [2015] Zeitschrift für Datenschutz 103, 104 et seq.
29 Cf. Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW e. V.* [2019] ECLI:EU:C:2019:629, para 74 (‚Fashion ID v Verbraucherzentrale').
30 In particular through the installation of cookies on the computer of the fan page visitor.
31 For example, according to the age, gender, relationship status or professional situation of fan page visitors.
32 See also Nicolas Blanc, 'Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law?' (2018) 4 European Data Protection Law Review 120; Charlotte Ducuing, Jessica Schroers and Els Kindt, 'The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership – A Challenge for Supervisory Authorities Competences' (2018) 4 European Data Protection Law Review 547.
33 A private-law company operating in the field of education.
34 Martini and Fritzsche (n 26) 3 et seq.

decision of the Administrative Court (***Verwaltungsgericht***) to revoke the order,[35] the Higher Administrative Court (***Oberverwaltungsgericht***) ruled that although the Wirtschaftsakademie sets up and operates a fan page indispensable for Facebook to be able to collect personal data from visitors via this page, Facebook alone decides "whether", "why" and "how" data is processed.[36] In short: the fan page operator is not "master of data".[37]

The same can also be said for universities, which only encourage their students to attend courses, but have no influence on the processing of user data by the MOOC provider. But the legal dispute had not yet come to an end. In 2016, the Federal Administrative Court (***Bundesverwaltungsgericht***) referred the question of the fan page operator's responsibility under data protection law to the CJEU.[38]

In June 2018, the CJEU concluded that the fan page operator and Facebook would indeed be joint controllers.[39] Until this ruling, it had generally been held that a mere causality for data processing without any actual influence was not sufficient to establish joint controllership.[40] The CJEU, however, did not consider a joint controllership based on the creation of a ***fan page*** alone, but rather set out additional qualifying requirements for it. It is of particular importance that the fan page administrator can at least exert a certain influence on the data collection by means of the individual filter settings.[41] However, such a parameterisation is more than just a mere causality for data processing, it, at least, represents factual influence. The CJEU's reasoning[42] on the existence of joint controllership can also be applied to the relationship between a MOOC provider and its university partners.[43]

3.2.2.2 Joint Controllership as a Result of a (de facto) Obligatory MOOC Assignment

The mere use of a MOOC platform by the university does not cause joint controllership in the sense of Article 4 (7) and Article 26 (1) sentence 1 GDPR.[44] However, the situation is different if the universities obtain user data from the provider and encourage the persons concerned to take an online course.[45]

Admittedly, even in this case they cannot determine the specific processing method of the platform operator, as the latter exercises sole data sovereignty. But by obliging certain persons (at least indirectly) to complete one or more MOOCs, the universities are setting the direct prerequisite for the provider to collect the user data of precisely these persons.[46] This is a scenario that distinguishes the relationship between a university and its students from the relationship between the administrator of a fan page and fan page

35 *Verwaltungsgericht Schleswig*, case VG 8 a 14/12 [2013] (not final).
36 *Oberverwaltungsgericht Schleswig*, case OVG 4 LB 20/13 [2013] (annulled).
37 ibid.
38 *Bundesverwaltungsgericht,* case BVerwG 1 C 28.14 [2016].
39 Case C-210/16 *Unabhängiges Landeszentrum for Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2017] ECLI:EU:C:2017:796, para 44 ('ULD v Wirtschaftsakademie'). As a result of this judgment, the Federal Administrative Court annulled the appeal judgment of 4 September 2014 before it and referred the case back to the Higher Administrative Court of Schleswig-Holstein. See *Bundesverwaltungsgericht*, case BVerwG 6 C 15.18 [2019].
40 Martini and Fritzsche (n 26) 5; Winfried Veil, 'Art. 26' in Sibylle Gierschmann and others (eds), *Datenschutz-Grundverordnung: Kommentar* (Bundesanzeiger Verlag 2018) Rn. 36.
41 C-210/16 *ULD v Wirtschaftsakademie* (n 39) paras 35 et seqq.
42 It should be noted that the questions were raised under the Directive 95/46/EC. However, the definition of controller has not changed in the GDPR.
43 Cf. Ducuing, Schroers and Kindt (n 32) 550.
44 Cf. ibid para. 35.
45 Martini and Botta (n 13) 252 et seq. Where several operators are jointly responsible for the same processing, it is not required of each of them to have access to the personal data concerned. Cf. C-210/16 *ULD v Wirtschaftsakademie* (n 39) para 38.
46 Cf. C-210/16 *ULD v Wirtschaftsakademie* (n 39) paras 35 et seqq.

visitors, since fan page visitors are basically free to access the social network. Universities can exert pressure on those concerned, not only by declaring the courses to be mandatory for their students, but also by providing clear incentives – such as less time spent, or a larger range of courses, or by creating factual circumstances that force students to study online (see above).

If the administrator of a fan page can already be assumed to be part of a joint controllership, then – under the above-mentioned conditions – this is a fortiori the case for the MOOC provider's university partners, whose factual influence is considerably greater. This broad understanding of the concept of "controller" is also required by a comprehensive protection of data subjects, which is the aim of EU data protection law.[47] In particular, joint controllership does not presuppose that the MOOC provider and its university partners have an equal influence on data processing.[48] However, universities do not have to accept responsibility for processing operations for which they neither determine the purposes nor the means, for example if the MOOC provider sells the user data to third parties.[49]

3.3 Consequences

A joint controllership of the provider and a university has various legal consequences, but mainly causes the need for a transparent agreement on joint data processing (aa.) and a joint liability of the parties involved (bb.).

3.3.1 Arrangement in a Transparent Manner

If the provider and the university are jointly responsible, they must conclude an agreement as to which of them fulfils which obligation arising under the GDPR (Article 26 (1) sentence 2). Although there is no specific provision on the form of this agreement, its absence can lead to a fine of up to 10m Euro or 2 % of the annual worldwide turnover, in accordance with Article 83 (4) (a) GDPR, which is why it should at least be in writing. However, it should be noted that public universities are not subject to administrative fines per se. This is because the EU legislator has left it open to the Member States whether their supervisory authorities may also impose fines on public bodies (Article 83 (7) GDPR). The German state legislators, for example, have generally ruled this out. Despite the possibility of fines, however, the agreement is not constitutive for joint controllership, but results from it.[50]

The agreement must be transparent and truthful (Article 26 (1) sentence 2 and (2) sentence 1 GDPR). In order to avoid a fine, the provider and its university partner must make their agreement as precise, easily accessible and easily understandable as possible, as well as written in clear and plain language and, if necessary, use additional visual elements (cf. Recital 58 sentence 1 of the GDPR).

3.3.2 Claims for Damages by Students

Since the agreement only applies to the internal relationship between joint controllers, affected students are not restricted in asserting their rights against each party individually (Article 26 (3) GDPR). The party

47 Cf. ibid para 42.
48 Cf. ibid para 43; Case C-25/17 *Tietosuojavaltuutettu v Jehovah's Witnesses* [2018] ECLI:EU:C:2018:551, para 66.
49 Cf. C-40/17 *Fashion ID v Verbraucherzentrale* (n 29) para 74.
50 Jürgen Hartung, 'Art. 26' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: Kommentar* (2nd edn C.H. Beck 2018) Rn. 20; Martini (n 23) Rn. 22.

concerned may also assert a claim for damages against all co-responsible parties (Article 82 (4) GDPR). For the universities, this means that, in the case of joint controllership, they may be liable to the students for data protection violations by the MOOC provider. They would then have to take recourse against the provider accordingly.

4. Data Protection Requirements for Universities

As (joint) controllers, the universities are obliged to respect the protection of their students' personal data. Which data protection provisions apply depends in particular on the purpose for which the universities process the data.

4.1 Privileged Data Processing for Scientific Research Purposes

"In the internal organization of the higher scientific institutions {...} {everything} is based on preserving the principle of considering science as something not yet fully found and never fully discovered, and to ceaselessly seeking it as such",[51] the educational reformer Wilhelm von Humboldt put it over 200 years ago. This never-ending search for new knowledge results in a comprehensive demand for information of universities and scientists, which can potentially collide with the privacy of the individual if it or at least its personal data becomes the object of research. The use of digital educational applications also provides universities with new access to knowledge for their students and third parties, as well as unexpected insights into their learning behaviour. Universities gain access to this digital tree of knowledge when they themselves operate learning platforms or when the course provider forwards user data to them. Never before has education been as transparent as in the times of Learning Analytics and Educational Data Mining.

However, the pursuit of knowledge not only potentially interferes with the data sovereignty of those affected, but also leads to an area of personal and autonomous responsibility of the individual scientist that is free from state interference. This is because public universities are not only bound by the data protection rights of their students and third parties (Article 8 CFR), but can also invoke the freedom of science, which is also a fundamental right (Article 13 CFR). The EU legislator solved this particular conflict between the two fundamental rights by privileging data processing for scientific research purposes within the scope of Article 89 (1) GDPR in contrast to other processing purposes.

4.1.1 Data Processing for Research Purposes

The processing purpose of scientific research includes, for example, technological development and demonstration, fundamental research, applied research and privately funded research (Recital 159 sentence 2 of the GDPR). Although the EU legislator did not define the concept of research itself in more

51 Translated from the German original quote "[B]ei der inneren Organisation der höheren wissenschaftlichen Anstalten [...] [beruht alles] darauf, das Princip zu erhalten, die Wissenschaft als etwas noch nicht ganz Gefundenes und nie ganz Aufzufindendes zu betrachten, und unablässig sie als solche zu suchen" by Wilhelm von Humboldt, 'Über die innere und äussere Organisation der höheren wissenschaftlichen Anstalten in Berlin' in Der Präsident der Humboldt-Universität zu Berlin (ed), *Gründungstexte: Festgabe zum 200-jährigen Jubiläum der Humboldt-Universität zu Berlin* (Humboldt-Universität 2010) 231.

detail, it can generally be understood as an activity aimed at acquiring new knowledge in a methodical, systematic and verifiable manner.[52] If a university processes user data from the MOOCs it supervises, for instance within the framework of an educational science study on what indicates a dropout in digital self-study, this is done for scientific research purposes within the meaning of Recital 159 sentence 2 of the GDPR.

There are a number of privileges for data processing for scientific research purposes within the meaning of Article 89 (1) GDPR, which universities can invoke when they process user data from MOOCs. For example, if the principle of purpose limitation applies in data protection law, according to which a controller may only collect personal data for specified, explicit and legitimate purposes and may not process it for a purpose that is incompatible with the purpose for which it was collected (first part of Article 5 (1) (b) GDPR), this will not apply in the area of research (second part of Article 5 (1) (b) GDPR). There are also less stringent requirements with regard to the certainty of consent (Recital 33 sentence 2 of the GDPR). It is sufficient if the users of online courses consent to their personal data being processed for certain areas of scientific research - for example, a specific project on digital higher education (broad consent). In this case, consent is not required for each individual processing operation.

In addition, the data subject rights are limited. To illustrate the point, the MOOC user has a right to erasure ("right to be forgotten") in accordance with Article 17 (1) and (2) GDPR; however, this does not apply if the processing was carried out for the purposes of scientific research, and it would otherwise be impossible or at least considerably more difficult for the university to achieve the objectives pursued by the processing (Article 17 (3) (d) GDPR). If a university has processed user data – for example, to use it for several research projects – it does not have to delete it when the initial purpose is fulfilled.

4.1.2 Data Processing for Teaching Purposes

However, if a university recognises the services provided online as official academic achievements or checks the identity of users, this cannot be subsumed under the pursuit of new knowledge. The data processing required for this falls exclusively within the scope of academic teaching.

With the concept of scientific research purposes in mind, one may think that data processing for teaching purposes according to Article 89 (1) GDPR is also privileged. This is because science is the generic term for research and teaching.[53] The fact that the concept of processing data for scientific research purposes is to be interpreted broadly is also explicitly stated by the EU legislator in Recital 159 sentence 2 of the GDPR ("should be interpreted in a broad manner"). However, the designation of research purposes as scientific was not intended to include academic teaching, but rather to ensure that not every Big Data analysis is already carried out for a privileged research purpose because it is based on a mathematical method[54].

52 Hans D Jarass, *Charta der Grundrechte der Europäischen Union* (3rd edn C.H. Beck 2016) Art. 13 Rn. 6; Bernhard Kempen, 'Art. 13' in Klaus Stern and Michael Sachs (eds), *Europäische Grundrechte-Charta: Kommentar* (C.H. Beck 2016) Rn. 15.

53 Norbert Bernsdorff, ‚Art. 13' in Jürgen Meyer and Sven Hölscheidt (eds), *Charta der Grundrechte der Europäischen Union* (5th edn Nomos Verlag 2019) Rn. 14; Jarass (n 52) Rn. 6; Matthias Ruffert, 'Art. 13 GRCh' in Christian Calliess and Matthias Ruffert (eds), *EUV/AEUV: Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar* (5th edn C.H. Beck 2016) Rn. 5.

54 Benedikt Buchner and Marie-Theres Tinnefeld, 'Art. 89' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: Kommentar* (2nd edn C.H. Beck 2018) Rn. 12; Holger Greve, 'Art. 89' in Martin Eßer, Philipp Kramer and Kai von Lewinski (eds), *Auernhammer DSGVO/BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze, Kommentar* (6th edn Carl Heymanns Verlag 2018) Rn. 6.

If the EU legislator had wished to privilege data processing for teaching purposes, he could have made a distinction in Article 89 (1) GDPR within the concept of scientific purposes or should at least have expressly listed academic teaching in Recital 159 sentence 2 of the GDPR. Furthermore, the fact that the terms "research" and "teaching" are not used synonymously in EU law is due, in particular, to the fundamental right of freedom of science, which explicitly distinguishes between scientific research and academic freedom (Article 13 sentences 1 and 2 CFR), the latter being applicable to digital university teaching[55]. It follows that only research and not teaching purposes are privileged under data protection law.[56]

If the universities therefore process personal user data for academic teaching purposes, only the general provisions of the GDPR apply.

4.2 Legal Basis for Mandatory Online Courses

In principle, the European data protection law prohibits any processing of personal data without a legal basis. This is acknowledged by Article 8 (2) sentence 1 CFR, according to which data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or another legitimate basis laid down by law.

It follows that the prohibition is subject to permission. The general elements of authorisation under the GDPR are anchored in Article 6 (1). Apart from consent (aa.) there are several legal bases (bb.). The following section will examine the extent to which a university can invoke one of these processing bases when it introduces MOOCs that are required for its students.

4.2.1 Student Consent

The possibility of consenting to the processing of personal data relating to an individual is an original expression of the informational self-determination of the individual and as such is central to, albeit equally important as the other legal bases of the GDPR (Article 6 (1) (a)).[57] Consent is therefore a primary legal basis for the processing of MOOC user data.

The users must declare their consent freely (Article 4 (11) GDPR), i.e. they must be given genuine freedom of choice as to whether or not to consent to the processing of data (Recital 42 sentence 5 of the GDPR). This is continually the most controversial requirement of the element of authorisation in Article 6 (1) (a) GDPR. This is because freely given consent is precluded if there is a "clear imbalance" between the person responsible and the person affected (Recital 43 sentence 1 of the GDPR).[58] A clear imbalance exists primarily when the data subject is dependent on the controller, which creates a power asymmetry between the two.[59]

55 Cf. Jarass (n 52) Rn. 8; Ruffert (n 53) Rn. 9.
56 However, Golla and Matthé show that such a privilege would have been justified under primary law. See Sebastian J Golla and Luisa Matthé, 'Das neue Datenschutzrecht und die Hochschullehre' (2019) 51 Wissenschaftsrecht 206, 207 et seq.
57 Jan P Albrecht, 'Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung: Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog' [2016] Computer und Recht 88, 91.
58 Benedikt Buchner and Jürgen Kühling, 'Art. 7' in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: Kommentar* (2nd edn C.H. Beck 2018) Rn. 42.
59 Stefan Ernst, 'Die Einwilligung nach der Datenschutzgrundverordnung: Anmerkungen zur Definition nach Art. 4 Nr. 11 DS-GVO' [2017] Zeitschrift für Datenschutz 110, 111 et seq.; Sibylle Gierschmann, 'Art. 7' in Sibylle Gierschmann and others (eds), *Datenschutz-Grundverordnung: Kommentar* (Bundesanzeiger Verlag 2018) Rn. 27.

Whether it is optional or – as a result of the coronavirus pandemic – obligatory for students to use MOOCs can therefore have far-reaching consequences for the university. If a required course can only be taken online and the degree cannot be obtained without the course in question, there is a clear imbalance between the university and the students, with the result that the consent of those affected is considered involuntary (cf. Recital 43 sentence 1 of the GDPR).

Even if it is officially at the discretion of the students, whether they attend a mandatory course online or in person, voluntary consent may be lacking if this freedom of choice actually exists only for some of the students due to spatial or personnel capacities of the university. In this case, there is at least a de facto obligation to take part in an online course. This scenario is not unlikely at present, due to curfews, ill teaching staff, or the like.

4.2.2 Legal Basis in the Law of the Member States

Instead of student consent under Article 6 (1) (a) GDPR, however, universities may base their data processing on Article 6 (1) (e) GDPR. According to this article, the processing must be necessary for the performance of a task carried out in the public interest, or in the exercise of official authority by the controller. Whether a task – such as teaching – is in the public interest is primarily determined by the law of the Member States. In Germany, for example, this legal basis results from the higher education laws of the German federal states, the Länder.

4.3 Fully Automated Processing of Digital Examinations

If a university wants to evaluate exam results[60] obtained in MOOCs or even recognise them as official academic achievements, the question of technical best practice arises. In principle, it would be conceivable for the university to use a fully automated evaluation or recognition procedure instead of an individual case examination by a university employee. This could, however, lead to a conflict with the prohibition of automated individual decision-making (Article 22 (1) GDPR).

In the long term, the provision could become one of the most important data subject rights for students.[61] In accordance with this provision, algorithm-based decisions that have a legal effect on the person concerned or at least significantly affect them in a similar way are generally prohibited. Students would be significantly affected by the decision at least if they fail the online course.

However, in order to be able to implement a computer-based evaluation or recognition system, the university has the option of obtaining the explicit consent of its users (Article 22 (2) (c) GDPR). It must then also enable the users to call in a human decision-maker in individual cases and have the automated decision reviewed (Article 22 (3) GDPR). Furthermore, the university must always carry out a data protection impact assessment before introducing automated decision-making systems (Article 35 (3) (a) GDPR).

60 Also electronically performed examinations are personal data. Cf. C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, para 62.

61 Mireille Hildebrandt, 'Learning as a Machine: Crossovers Between Humans and Machines' (2017) 4 Journal of Learning Analytics 6, 19.

Conclusion

The current crisis in university teaching is creating a new opportunity to experiment with innovative teaching formats and to permanently establish digital services at universities as a serious supplement to attending courses. MOOCs can be an important component of such a digitisation strategy. However, when universities integrate MOOCs in their curriculum, they not only open up a wide range of courses from all over the world to their students, but also expose them to data protection threats.

On the part of university management, there is not always sufficient awareness of these risks. Especially when the universities do not themselves provide the digital infrastructure for online education, but cooperate with commercial MOOC providers, the concerns seem to dwindle. In the absence of far-reaching possibilities for influencing data processing, universities are quick to assume that they could evade any responsibility for possible data protection violations. However, if they influence user data processing by means of individual contracts or oblige their students (de facto) to take MOOCs with a commercial provider, they become joint controllers along with that provider (Article 4 (7) and Article 26 (1) sentence 1 GDPR). Therefore, even universities without their own MOOC platform are obliged to respect their students' right to the protection of personal data. They must ensure that they themselves, or third parties, only process the user data lawfully.

If universities want to offer MOOCs to their students on a legitimate basis, they must develop strategies for using them in a GDPR-compliant manner. Then EdTech and data protection can be promoted together. This would also be in line with the spirit of Wilhelm von Humboldt, who correctly recognised more than 150 years ago that "freedom is the first and indispensable condition for education".[62]

62 Translated from the German original quote "Freiheit die erste und unerlässliche Bedingung" by Wilhelm von Humboldt, *Ideen zu einem Versuch, die Gränzen der Wirksamkeit des Staats zu bestimmen* (1851) 9.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri and Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommunications operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou and Paul de Hert (13 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

N°16 Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an *interim* period of no regulation at all) (June 2019) by Vagelis Papakonstantinou and Paul de Hert (25 pages)

N°17 Data Localisation: Deconstructing myths and suggesting a workable model for the future. The cases of China and the EU (September 2019) by Author: Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (31 pages)

N°18 Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination (January 2020) by Dr Monique Mann and Professor Tobias Matzner (18 pages)

N°19 Access to the Internet in the EU: a policy priority, a fundamental, a human right or a concern for eGovernment? (February 2020) by Lina Jasmontaite and Paul de Hert (23 pages)

N°20 The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? (March 2020) by Elena Gil González, Paul De Hert & Vagelis Papakonstantinou (31 pages)

N°21 Article 8 ECHR compliant and foreseeable surveillance: the ECtHR's expanded legality requirement copied by the CJEU. A discussion of European surveillance case law (April 2020) by Paul De Hert & Gianclaudio Malgieri (42 pages)

N°22 The "Ethification" of Privacy and Data Protection Law in the European Union. The Case of Artificial Intelligence (May 2020) by Niels van Dijk and Simone Casiraghi (23 pages)

N°23 Logic and Key Points of China's Cybersecurity Review Measures (June 2020) by Yanqing Hong, Senior Fellow, Law and Development Institute, Peking University of China, Edited by Vagelis Papakonstantinou, Brussels Privacy Hub (9 pages)

N°24 Individuation: re-imagining data privacy laws to protect against digital harms (July 2020) by Anna Johnston (22 pages)

N°25 The Dark Side of the MOOC? The Rise of EdTech in Times of COVID-19: A Data Protection Challenge for Universities (August 2020) by Jonas Botta (16 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

VUB BRUSSELS PRIVACY HUB