JOURNAL OF LAW, TECHNOLOGY & THE INTERNET • VOL. 13 • NO. 1 • 2021 – 2022

IMPLEMENTING DATA PROTECTION BY DESIGN IN THE ED TECH CONTEXT: WHAT IS THE ROLE OF TECHNOLOGY PROVIDERS?

Liane Colonna[*]

This article explores the specific roles and responsibilities of technology providers when it comes to implementing Data Protection by Design ("DPbD") and Data Protection by Default ("DPbDf"). As an example, it looks at the Education Technology ("Ed Tech") sector and the complexities of the supply chains that exist therein to highlight that, in addition to the Higher Education ("HE") institutions that procure products and services for advancing teaching and learning, Ed Tech vendors may also have responsibility and liability for the processing of student's personal data. Ultimately, this paper asks whether there are any legal gaps, ambiguities, or normative conflicts to the extent that technology providers can have responsibility in contemporary data processing activities yet escape potential liability where it concerns issues of General Data Protection Regulation ("GDPR") compliance.

This paper argues that there is befuddlement concerning the determination of which parties are responsible for meeting DPbD and DPbDf obligations, as well as with regards to the extent of this responsibility. In some cases, an Ed Tech provider is a controller or processor in practice together with a HE institution, yet, in others it, may not have any legal responsibility to support the development of privacy and data-protection preserving systems, notwithstanding the fact it might be much more knowledgeable than a HE institution that has procured the Ed Tech product or service about the state-of-the-art of the technology. Even in cases where it is clear that an Ed Tech provider does have responsibility as a controller or processor, it is unclear how it should share DPbD obligations and coordinate actions with HE

[*] The support of the JPI More Years, Better Lives and the Swedish Research Council for Health, Working Life, and Welfare (grant number is 2017-02302) and The Wallenberg AI, Autonomous Systems and Software Program–Humanities and Society (WASP-HS), Ethical and Legal Challenges in Relationship to AI-driven Practices in Higher Education (MMW2020.0138), is gratefully acknowledged. I also owe gratitude to Professor Teresa Cerratto-Pargman and Fredrik Sandberg who have provided helpful comments on the manuscript, or parts thereof, at various stages in its development.

institutions, especially when the Ed Tech supplier may only be involved in a limited way or at a minor phase in the processing of student data.

There is an urgent need to recognize the complex, interdependent, and non-linear context of contemporary data processing where there exists many different controllers, processors, and other actors, processing personal data in different geographical locations and at different points in time for both central and peripheral purposes. Likewise, the complexity of the supply of software must also be emphasized, particularly in contexts such as the supply of educational technology where technology providers can play a key role in the preservation of privacy and data protection rights but may only have a tangential link to the universities that ultimately use their products and services. There is also a need for a more dynamic approach of considering responsibility regarding DPbD. Instead of thinking about responsibilities in terms of "purpose" and "means" the law should shift towards a focus on powers and capacities. The law should also clarify whether technology providers must notify controllers about changes to the state-of-the-art and, if so, to what extent.

CONTENTS

I. Introduction

In the European Union, data controllers bear primary responsibility for ensuring that processing activities are compliant with data protection law, including the requirements for Data Protection by Design (DPbD) and Data Protection by Default (DPbDf) set forth in Article 25 of the General Data Protection Regulation (GDPR).[1] However, in many instances, controllers are not necessarily the ones who are in a position to build privacy into systems at the very outset of their development and to ensure that this requirement is fulfilled through the product's lifecycle. This may be because a controller purchases a product downstream such as some pre-designed off-the-shelf solution or it might rely extensively on a data processor, limiting the capacity for a controller to exert influence in the design of a technological system. It might also be because the controller simply lacks the technical knowledge to, for example, stay up to date with the state-of-the-art.

Recital 78 of the GDPR recognizes the dilemma and states that technology providers[2] have a core role in securing DPbD and DPbDf.[3] The European Data Protection Board (EDPB) echoes this sentiment and explains that technology providers are "key enablers" for DPbD since they are more knowledgeable about the potential risks that the use of a system or service may involve, and are more likely to be up to date on technological developments.[4] Nevertheless, the notion of "technology provider" is rather broad and may not fall under the remit of data protection law in every situation, especially where a technology provider does not receive, process,

[1] Commission Regulation 2016/679, art. 25, 2016 O.J. (L 119); Commission Regulation 2016/679, art. 82, 2016 O.J. (L 119) 3 (noting that a controller may be exempted from liability, in whole or in part, "if it proves that it is not in any way responsible for the event giving rise to the damage").

[2] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) recital 78 ("Technology providers" is understood broadly to include entities that supply technology products or services. For example, they might supply the necessary technology services, software tools, devices, or infrastructure in a particular digitalized environment). *See* Center for Information Policy Leadership, *infra* note 5.

[3] *Id.* (stating "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations").

[4] Eur. Data Prot. Bd., *Guidelines 4/2019 on Article 25 Data Protection and Design V 2.0*, EUROPA ¶ 94 (Oct. 20, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf [hereinafter *Guidelines 4/2019*].

store or access any personal data but merely provides a product or service.[5] In these situations, it may be difficult for data controllers to exert influence over technology providers to demand a high level of data protection through, for example, contractual negotiations.

II. Data Protection by Design

In many ways, DPbD represents a new generation of legal strategies in the Digital Age where traditional forms of law have become outmoded. Taking a proactive approach to law, DPbD has a conscious orientation to the future insofar as it seeks to avoid privacy and data protection problems before they can occur.[6] Fundamentally, it involves the transformation of legal rules, namely those that appertain to privacy and data protection, into *both* organizations and systems.[7] Multiple parties are involved in its implementation such as engineers, managers, lawyers, policymakers, and executives within an organization and each group is expected to share responsibility for achieving privacy goals.[8]

With the adoption of the GDPR, Data Protection by Design (DPbD) became a legally binding obligation and placed data controllers at risk of substantial fines for noncompliance.[9] The actual language of Article 25 of the GDPR has been explained as "tautological" and "theoretical."[10] As such, recent guidance has emerged from data protection authorities[11] and academia,[12] helping to make the provision more concrete and understandable.

---

[5] Center for Information Policy Leadership [CIPL], *Comments by the Centre for Information Policy Leadership on the European Data Protection Board's "Guidelines 4/2019 on Article 25 Data Protection by Design and By Default" Adopted on 13 November 2019* 1, 6 (Jan.16, 2020), https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/cipl_response_to_edpb_privacy_by_design_guidelines.pdf.

[6] *See generally* Peter Seipel, *Nordic School of Proactive Law Conference June 2005 Closing Comments*, 49 SCANDINAVIAN STUD. L. 359, 360 (2006).

[7] Dag Wiese Schartum, *Making Privacy by Design Operative*, 24 INT'L J.L. & INFO. TECH. 151, 152–53 (2016).

[8] Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 402 (2013).

[9] Lina Jasmontaite et al., *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, 4 EUR. DATA PROT. L. REV. 168, 172 (2018).

[10] *See* Pwel Kamocki & Andreas Witt, *Privacy by Design and Language Resources*, *in* PROCEEDINGS OF THE 12TH CONFERENCE ON LANGUAGE RESOURCES AND EVALUATION 3423 (Nicoletta Calzolari et al. eds., 2020), http://www.lrec-conf.org/proceedings/lrec2020/index.html.

[11] *See Guidelines 4/2019*, *supra* note 4, at ¶ 5.

[12] *See e.g.,* Ari Ezra Waldman, *Privacy's Law of Design*, 9 UC IRVINE L. REV. 1239, 1286 (2019); Jasmontaite et al., *supra* note 9, at 172, 174; Lee A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 1 OSLO L. REV. 105, 117 (2017).

Article 25 clearly states that organizations must "implement appropriate technical and organizational measures... which are designed to implement data protection principles..., in an effective manner and to integrate the necessary safeguards into [data] processing."[13] The Article also clarifies that in so doing, organizations must take several factors into account: the-state-of the-art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.[14] Recital 78 provides a list of potential measures that may assist a data controller with its compliance burden.[15] These measures include "minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, and enabling the controller to create and improve security features."[16]

Furthermore, Article 25 mandates the use of Privacy by Default (PbDf).[17] PbDf "means that in the default setting the user is already protected against privacy risks" and "this affects the choice of the designer which parts are wired-in and which are configurable."[18] Jasmontaite explains, "[w]hile the concepts are interrelated, (DPbD) refers to the existence of embedded safeguards and mechanisms throughout the lifecycle of the application, service or product that protect the right to data protection, whereas (DPbDD) refers to the activation and application of such safeguards as default setting."[19] Likewise, ENISA states, "(DPbD) refers to the design and existence of embedded safeguards and mechanisms that protect the right to data protection throughout the lifecycle of the application, service or product, as discussed above," whereas "(DPbDD) refers to the implementation of such safeguards as a default setting."[20] This means in practice "that boxes should be pre-checked for the most privacy friendly option, or the option that allows the collection of the least amount of personal data, and that it should be made clear to the user what personal data is being collected, and what it may be used for."[21]

---

[13] Commission Regulation 2016/679, 2016 O.J. (L 119) recital 78.
[14] *Id*.
[15] *Id*.
[16] Waldman, s*upra* note 12, at 1256.
[17] Commission Regulation 2016/679, 2016 O.J. (L 119) recital 78.
[18] George Danezis et al., *Privacy and Data Protection by Design—From Privacy to Engineering*, ENISA 11 (Dec. 2014), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/@@download/fullReport.
[19] Jasmontaite et al., *supra* note 9, at 168.
[20] *Id.*
[21] *Deceived by Design*, FORBRUKERRÅDET 9 (June 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (citing European Data Protection Supervisor, *Preliminary Opinion on Privacy by Design*, EUROPA 7 (May 2018), https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf).

Sanctions for failing to implement DPbD and DPbDf may come hand in hand with a breach of one of the data protection principles, implying a kind of data protection double jeopardy. Waldman makes the point that the core of Article 25 is the requirement to take technical and organizational steps designed to implement data protection principles but since these principles are covered in other parts of the GDPR, Article 25's version of DPbD effectively turns into "a catch-all provision with no specific requirements of its own."[22] Likewise, Jasmontaite *et al.* state: "DPbD and DPbDf constitute a meta requirement system embedding the (GDPR) principles in every personal data processing operation."[23] Stalla-Bourdillo *et al.* succinctly explain: "DPbD is the backbone of the GDPR, as complying with Article 25 should lead to complying with the data protection principles, as detailed by Article 5, and to enable all data subject rights, as listed in Articles 12–22."[24]

III. The Complexity of the Ed Tech Supply Chain

Higher education ("HE") institutions are increasingly adopting Ed Tech products.[25] Educational technology can be defined as "a complex, integrated process, involving people, procedures, ideas, devices and organization, for analyzing problems and devising, implementing, evaluating and managing solutions to those problems, involved in all aspects of human learning."[26] Ed Tech has evolved rapidly in recent years, especially because of the COVID-19 pandemic.[27] For better or worse,[28] institutions have replaced clunky desktop computers with mobile technologies, virtual and augmented realities, simulations and immersive environments, social networking, cloud computing, Ed Tech robots, Internet of Things-based devices, machine

---

[22] Waldman, *supra* note 12, at 1256.
[23] Jasmontaite et al., s*upra* note 9, at 189.
[24] *See* Sophie Stalla-Bourdillon et al., *Data Protection by Process How to Operationalize Data Protection by Design for Machine Learning*, FUTURE PRIV. F. (2019), https://fpf.org/wp-content/uploads/2019/12/WhitePaper_DataProtectionByProcess.pdf.
[25] *See generally* OFF. OF EDUC. TECH., REIMAGINING THE ROLE OF TECHNOLOGY IN HIGHER EDUCATION (2017), https://tech.ed.gov/files/2017/01/Higher-Ed-NETP.pdf.
[26] ASS'N FOR EDUC. COMMC'NS & TECH., THE DEFINITION OF EDUCATIONAL TECHNOLOGY 19 (1977); *see also* ALAN JANUSZEWSKI, EDUCATIONAL TECHNOLOGY: THE DEVELOPMENT OF A CONCEPT 78 (2001); RONGHUAI HUANG ET AL., *Introduction to Educational Technology*, *in* EDUCATIONAL TECHNOLOGY: A PRIMER FOR THE 21ST CENTURY 3 (2019) ("Educational technology refers to the use of tools, technologies, processes, procedures, resources, and strategies to improve learning experiences in a variety of settings, such as formal learning, informal learning, non-formal learning, lifelong learning, learning on demand, workplace learning, and just-in-time learning.").
[27] *Remote Learning During COVID-19: Lessons from Today, Principles for Tomorrow*, THE WORLD BANK, https://www.worldbank.org/en/topic/edutech/brief/how-countries-are-using-edtech-to-support-remote-learning-during-the-covid-19-pandemic (last visited Mar. 18, 2022).
[28] *See e.g.*, Justin Reich, *Ed Tech's Failure During the Pandemic, and What Comes After*, 102 PHI DELTA KAPPAN 20 (2021).

learning, blockchain tools, and more.[29] This section briefly explains the complexity of the Ed Tech supply chain, highlighting that many different actors are involved, including hardware and software providers, internet providers, subcontractors, *etc.*, as well as, of course, the HE institutions that ultimately employ the tools.

At the outset, it is important to acknowledge that universities often have scarce resources in terms of budgets and staff time to select Ed Tech products and services. Universities also face organizational, political, and bureaucratic hurdles during the procurement process.[30] Thus, even though it would be strategic for universities to engage key stakeholders, such as teachers, administrators, and students, in dialogue with each other and vendors in order to ensure the suitability of Ed Tech products, research suggests this rarely happens.[31] Generally, Chief Technology Officers (CTOs) assume primary roles in selecting and acquiring ed-tech products.[32]

There is a vast array of Ed Tech available on the market and under development. Broadly, the technology helps teachers effectively produce and manage resources and release notices and manage students; helps students obtain resources and participate in learning activities; helps teachers and students interact in real time; and helps teachers, students, and universities understand students' learning performance and make timely interventions.[33] Polonetsky and Tene categorize Ed Tech innovation into four categories: 1) *administrative technologies,* which help to more effectively manage schools; 2) *delivery systems,* which help to augment traditional learning tools, and data management solutions; 3) *measurement tools,* which deploy big data analytics to measure the performance of students, teachers, and schools; and 4) *optimization programs,* which enable personalized and adaptive learning.[34] If learning management systems and video conferencing represent older digital education technologies, then adaptative tutors and virtual reality represent emerging techniques.[35]

---

[29] *See generally* HUANG ET AL., *supra* note 26.
[30] Jennifer R. Morrison et al., *From the Market to the Classroom: How Ed-Tech Products Are Procured by School Districts Interacting with Vendors*, 67 EDUC. TECH. RSCH. DEV. 389, 393 (2019).
[31] *Id*. at 394.
[32] *Id*. at 395.
[33] Smart Learning Institute of Beijing Normal University, *Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents*, UNESCO (2020), https://iite.unesco.org/wp-content/uploads/2020/06/Personal-Data-and-Privacy-Protection-in-Online-Learning-Guidance-for-Students-Teachers-and-Parents-V1.0.pdf.
[34] Jules Polonetsky & Omer Tene, *Who Is Reading Whom Now: Privacy in Education from Books to Moocs*, 17 VAND. J. ENT. & TECH. L. 927, 934 (2015).
[35] Reich, *supra* note 28, at 21.

The fact that many of the new and emerging Ed Tech technologies are driven by big data and AI has created concerns over the power shift from universities to the suppliers of Ed Tech. Critics of Ed Tech, including educational and privacy advocacy groups, are concerned that student data is being improperly shared with private vendors, risking student privacy rights and data protection.[36] For example, one concern is that student data concerning sensitive information like learning disabilities might be shared with a third-party vendor who then uses the information for monetization or manipulation.[37] Ostensibly, placing responsibility on Ed Tech companies for DPbD and DPbDf could alleviate some of these concerns and help to rebalance power relationships.

From a legal perspective, however, it is unclear whether Ed Tech companies are obligated to meet the requirements of DPbD and DPbDf as set forth in Article 25 of the GDPR. Two key questions relevant to understanding whether an Ed Tech company is bound by the law are: how and to what extent do Ed Tech companies' products and services process personal data? Which actors are involved in the supply chain that play a role in the design of the Ed Tech product or service? Because the answer to these questions will vary depending on the product or service, a hypothetical example below introduces the complexity of data processing operations. The example involves learning analytics, broadly understood as "the measurement, collection, analysis, and reporting of data about learners and their contexts, for the purposes of understanding and optimizing learning and the environments in which it occurs."[38]

The hypothetical example herein involves a HE institution that uses a predictive learning analytics (PLA) app called Course Cues to identify learners who may not complete a course.[39] The objective of the app is to provide useful information to teachers to help them identify at-risk students so that they can intervene and provide academic support for the student. More broadly, the app helps to increase retention of students.[40] The app works by utilizing AI to identify students who may fail to submit their next teacher marked assessment

---

[36] *See* Joe Jerome, *Privacy is key: Holding EdTech accountable*, HEINRICH BÖLL STIFTUNG (Apr. 15, 2021), https://us.boell.org/en/2021/03/31/privacy-key-holding-edtech-accountable.
[37] Yoni Har Carmel, *Regulating "Big Data Education" in Europe: Lessons Learned from the US*, INTERNET POL'Y REV. (Mar. 31, 2016), https://policyreview.info/articles/analysis/regulating-big-data-education-europe-lessons-learned-us.
[38] George Siemens, *Learning Analytics: The Emergence of a Discipline*, 57 AM. BEHAV. SCIENTIST 1380, 1382 (2013).
[39] *Cf.* Christothea Herodotou et al., *A Large-Scale Implementation of Predictive Learning Analytics in Higher Education: The Teachers' Role and Perspective*, 67 EDUC. TECH. RSCH. DEV. 1273 (2019).
[40] *Cf. id.* at 1276, 1278.

(TMA).[41] Using predictions about whether a student will submit their next TMA, the system is also able to provide information about whether a student will complete a course.[42] The app mines static data like demographics, and behavioral data like students' interactions within the virtual learning environment hosting a course like Moodle and subsequently transforms the data into a generated risk level with supporting information for each student.[43] In this specific hypothetical example, the software vendor behind Course Cues has chosen not to release the product as a deployed system, but rather as an application service, where it sells the usage of its product rather than the product itself.[44]

As noted above, the scarcity of resources has led the HE institution to delegate responsibility for procuring applications, like Course Cues, to its CTO who enters into a contract with the third-party Ed Tech service provider in order to gain access to the application.[45] In return, Course Cues gains access to valuable student data.[46] The terms of the service agreement are likely opaque and not readily or publicly accessible, although in Scandinavian countries (*e.g.* Sweden), this may not be the case where openness and transparency are vital parts of public administration.[47] Another possible consideration is that Course Cues scrapes students' profiles for information to build secondary tools and services.

The supply chain of a service like Course Cues is highly complex, increasingly distributed, and diverse.[48] The fact that providers can build commercial software offerings like Course Cues, using a variety of open-source components also creates complexity in this context to the extent that the inclusion of open-source components into a product or service may limit

---

[41] *Cf. id.* at 1278.
[42] *Cf. id.*
[43] Kimberly E. Arnold & Matthew D. Pistilli, *Course Signals at Purdue: Using Learning Analytics to Increase Student Success*, LAK '12: PROCEEDINGS OF THE 2ND INTERNATIONAL CONFERENCE ON LEARNING ANALYTICS AND KNOWLEDGE 267–70 (2012); Herodotou et al., *supra* note 39, at 1278.
[44] *See* Slinger Jansen et al., *Providing Transparency in the Business of Software: A Modeling Technique for Software Supply Networks*, *in* 243 THE INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING BOOK SERIES: ESTABLISHING THE FOUNDATION OF COLLABORATIVE NETWORKS 677, 679 (Luis M. Camarinha-Matos et al. eds., 2007).
[45] *See* Jeff Harris & Rick Skinner, *Recasting the Role of the Higher Ed CIO/CTO*, HARRIS SEARCH ASSOC., https://harrisandassociates.com/pub/publications/publications/recasting-the-role-of-the-higher-ed-ciocto/ (last visited Mar. 15, 2022).
[46] *See* Herodotou et al., *supra* note 39, at 1275.
[47] *See* REGERINGSFORMEN [RF] [CONSTITUTION] (SWED.), TRYCKFRIHETSFÖRORDNINGEN [TF] [CONSTITUTION] (SWED.), YTTRANDEFRIHETSGRUNDLAGEN [YGL] [CONSTITUTION] (SWED.), SUCCESSIONSORDNINGEN [SO] [CONSTITUTION] (SWED.).
[48] Petri Helo & Yuqiuge Hao, *Artificial Intelligence in Operations Management and Supply Chain Management: An Exploratory Case Study*, PROD. PLAN. & CONTROL 1, 1 (2021), https://www.tandfonline.com/doi/full/10.1080/09537287.2021.1882690.

the possibilities for DPbD or DPbDf.[49] Besides the end user, students and teachers, and the Ed Tech provider, many other actors are involved in the supply chain of a service like Course Cues. Put differently, the development of AI-based Ed Tech software involves a large number of technical resources as well as stakeholders like front-ed developers, back-end developers, data-base managers, cloud vendors, *etc*.[50] Brinkkemper and Finkelstein explain: "software products and services are no longer monolithical systems developed in-house, but consist of complex hardware and software system federations produced and sold by different organizations."[51] As a result of the increased complexity, participants acting within the supply chain face greater difficulty in managing reasonability and liability as well as risk, more broadly.[52] In short, due to emergence of computer networks and modern software development practices, software supply chains have witnessed significant changes in recent years.[53] Long gone are the days of stand-alone software. These are the days of large and complex system-of-systems.[54]

IV. Responsibility for DPbD and DPbDf in the Ed Tech Context

a. Responsibility as a Controller or Joint Controller?

The GDPR places the responsibility of ensuring DPbD and DPbDf, and all other requirements of the regulation, on a data controller.[55] The provisions in Chapter III of the GDPR—concerning the rights of the data subject—are not only squarely directed at the controller, but also make it the controller's responsibility to compensate any person who has suffered damage as a result of an infringement or by processing data in violation of the regulation.[56] Besides defining the scope of accountability and the degree of eventual liability, the identification of a data controller enables communications from data subjects and data protection authorities to data

---

[49] Kapil Singi et al., *Trusted Software Supply Chain*, IEEE/ACM INT'L CONF. ON AUTOMATED SOFTWARE ENGINEERING 1212, 1212 (2019), https://ieeexplore.ieee.org/document/8952169; Bert-Jaap Koops, *Open-Source Intelligence and Privacy by Design*, 29 COMPUT. L. SEC. REV. 676 (2013).

[50] ALL PARTY PARLIAMENTARY GROUP, AI in Education: Designing fair and robust AI-based assessments systems, Big Innovation Centre (2020).

[51] Jansen et al., *supra* note 44, at 677.

[52] *Id.*

[53] Singi et al., *supra* note 49, at 1212.

[54] Audrey J. Dorofee et al., *A Systemic Approach for Assessing Software Supply-Chain Risk*, CARNEGIE MELLON UNIV. 2 (Feb. 2003), https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_297385.pdf.

[55] Tomas Sander, *Why You Should Implement Privacy by Design Before GDPR's First Birthday*, INFOSECURITY MAG. (Feb. 7, 2019), https://www.infosecurity-magazine.com/opinions/implement-privacy-design/.

[56] Commission Regulation 2016/679, art. 12–23, 2016 O.J. (L 119) (further noting that processors can also be liable but only if they did not comply with the instructions given to it by the controller).

controllers.[57] The Court of Justice of the European Union (CJEU) has held that data controllers must ensure, within the framework of their responsibilities, powers and capabilities, that their data processing meets all of the guarantees laid down by law to ensure the effective and complete protection of data subjects, in particular, of their right to privacy.[58] Blume puts it simply: "data protection stands and falls with the controller."[59]

A data controller is an entity that "determines the purposes and means of the processing of personal data."[60] In other words, the data controller is responsible for determining respectively the why and the how of certain processing activities.[61] According to the predecessor of the EDPB, the Article 29 Working Party,[62] "[b]eing a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes."[63]

---

[57] Briseida Sofia Jiménez-Gómez, *Risks of Blockchain for Data Protection: A European Approach*, 36 SANTA CLARA HIGH TECH. L.J. 281, 311 (2020) ("The importance of identifying a data controller is two-fold. First, it defines the degree of responsibility for participants, consequently, the scope of accountability and the degree of eventual liability. Second, it enables communications from data subjects and data protection authorities to data controllers."); *see also* Eur. Data Prot. Bd., *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR Version 2.0*, EUROPA 3 (July 7, 2021), https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (stating "[th]e concepts of controller, joint controller and processor play a crucial role in the application of the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice.") [hereinafter *Guidelines 07/2020*].

[58] In *Google Spain*, the CJEU found that the notion of controller is one that should be interpreted broadly to ensure "the effective and complete protection of data subjects." In that case, the Court found that Google Spain was a data controller which processes personal data in a manner that "can be distinguished from and is additional" to that of the original publisher because its "data processing [...] affects the data subject's rights additionally." In reaching this conclusion, the Court found that it is not necessary that the controller actually has access to the data that is being processed to qualify as a controller. *See* C-131/12 Google Spain SL and Google v. Agencia Espanola de Proteccion de Datos (AEPD) 2014 QB 1022: (2014) 3 WLR 659 (ECJ, 13 May 2014) ¶¶ 34, 35, 38, 83 (Google Spain).

[59] Peter Blume, *An Alternative Model for Data Protection Law: Changing the Roles of Controller and Processor*, 5 INT'L DATA PRIV. 292, 292 (2015).

[60] Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 7 (defining a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.").

[61] *See* Article 29 Data Prot. Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, EUROPA 13 (Feb. 16, 2010), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[62] *Id.*

[63] *Id.* at 8.

Mahieu *et al.* and Ivanova suggest that at least three criteria exist to establish a controller as independent.[64] First, the controller must carry out distinct data processing operations.[65] Second, each of the respective data processing operations should affect separately the data subject(s).[66] Third, there should not exist a legal relationship between the controllers as this may make them joint controllers or processors.[67]

In addition to controllers, the GDPR recognizes that there are instances where "joint controllers" exist "[w]here two or more controllers jointly determine the purposes and means of processing."[68] Joint controllers must determine "in a transparent manner" their respective responsibilities as well as provide information to the data subject in a proactive manner.[69] A joint controllership can result from "a common decision taken by two or more entities" or it can result from "converging decisions by two or more entities regarding the purposes and essential means."[70] An important criterion to identify converging decisions is "whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, *i.e.* inextricably linked."[71] The EDPB concludes: "The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand."[72] It is further key to remember that for a joint controllership to exist, it is not necessary that separate parties determine the purposes and means equally.[73]

In *Fashion ID*, the CJEU concluded that the Fashion ID company was a joint controller because it had embedded on its website the Facebook 'Like' social plugin and thereby exerted "a decisive influence" over the collection and transmission of the personal data of visitors (*e.g.* the user's IP address and

---

[64] *See* Yordanka Ivanova, *Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World*, SSRN 1, 20 (May 21, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3584207 (citing René Mahieu et al., *Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe*, 10 JIPITEC 85, 86 (2019)).
[65] *Id*.
[66] *Id*.
[67] *Id.* at 61.
[68] Commission Regulation 2016/679, art. 26, 2016 O.J. (L 119) 1.
[69] *Id*.
[70] *Guidelines 07/2020*, *supra* note 57, at 18; *see also* Brendan Van Alsenoy, *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, 7 JIPITEC 271, 280 (2016) ("If the parties do not pursue the same objectives ("purpose"), or do not rely upon the same means for achieving their respective objectives, their relationship is likely to be one of 'separate controllers' rather than 'joint controllers'.").
[71] *Guidelines 07/2020*, *supra* note 57, at 18
[72] *Id*.
[73] *See* Ivanova, *supra* note 64, at 6.

browser string) to the third party service provider, Facebook.[74] The CJEU further concluded that the purposes of processing were jointly determined to the extent that the processing operations were performed "in the economic interests" of both Fashion ID and Facebook.[75] Essentially, the Court came to the conclusion that using third party services that collect and transmit personal data gives rise to a joint controllership, so long as both controllers have economic interests in the processing.[76] Here, it is worth emphasizing that while the Court found Fashion ID is responsible for the collection and transmission of the personal data collected on its webpage, it was not responsible for the subsequent processing that Facebook carried out.[77]

Mahieu *et al.* and Lindroos-Hovinheimo describe the approach taken by the Court in *Fashion ID* to determining a joint controllership as "phase-oriented"[78] or a "step-by-step" approach.[79] This is because the CJEU limited its determination of the existence of the joint controllership to only the set of operations in which Fashion ID and Facebook were both involved (*e.g.* collection and transmission of data).[80] In other words, it examined the data processing chain and decoupled the processing operations from the processing system as a whole in an effort to attribute Fashion ID and Facebook as joint controllers.[81]

In the Ed Tech context, a controllership or joint-controllership may exist even if an individual or entity does not have any access to the data in

---

[74] *Guidelines 07/2020*, *supra* note 57, at 20.
[75] Case C-40/17, Fashion ID v. Verbraucherzentrale, 2019 E.C.R. 629.
[76] Case C-40/17, Fashion ID v. Verbraucherzentrale, 2019 E.C.R. 629; Article 29 Data Prot. Working Party, *supra* note 61, at 19 ("[h]ere, it is worth mentioning that such a decision is at odds with the Article 29 working party which has concluded: "First of all, the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers.").
[77] *See* Case C-40/17, Fashion ID v. Verbraucherzentrale, 2019 E.C.R. 629.
[78] Mahieu et al., *supra* note 64, at 85.
[79] Susanna Lindroos-Hovinheimo, *Who controls our data? The legal reasoning of the European Court of Justice in* Wirtchaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v. Jehovan todistajat, 28 INFO. & COMMC'NS TECH. L. 225, 234 (2019).
[80] René Mahieu & Joris van Hoboken, *Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?*, EUR. L. BLOG (Sept. 30, 2019), https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/ [https://perma.cc/Y93V-YZGW]; *see also* Case C-40/17, Fashion ID GmbH & Co. KG v. Facebook Ir. Ltd., ECLI:EU:C:2018:1039, ¶107 (Dec. 19, 2018) (explaining, "I consider that the liability of the Defendant [Fashion ID] has to be limited to the stage of the data processing in which it is engaged and that it cannot spill over into any potential subsequent stages of data processing, if such processing occurs outside the control and, it would appear, also without the knowledge of the Defendant.").
[81] Orla Lynskey, *Delivering Data Protection: The Next Chapter*, 21 GERMAN L.J. 80, 82–83 (2020).

question.[82] In this case, if an Ed Tech provider has influence over the "means" of processing for their own economic benefit then they may be classified as a controller.[83] Ivanova points to the "know-how" and "information and technology capabilities" of many technology providers and suggests that they have a "decisive influence" over the "means" of processing.[84] Likewise Chen *et al.* note that the architectural designers of systems or the collaborating or independent developers of certain components may fall within the scope of a controllership as they are the ones defining in technical terms how personal data are collected and for what potential purposes.[85]

When it comes to the imposition of DPbD and DPbDf responsibility onto technology providers through the finding of a joint controllership, the phase-oriented approach applied by the CJEU is problematic to the extent that it fails to recognize the "complex, interdependent and non-linear context of contemporary data processing."[86] Ivanova explains, "distinguishing the phases and types of data processing operations may turn out to be particularly difficult in certain circumstances or outright inadequate."[87] In particular, this may be quite irrelevant when all operations actually pursue a common objective or are part of an integrated service or product involving many different actors.[88] Ivanova contends that, because the "phase-oriented approach focuses only on the set of operations or phases of processing, it

---

[82] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388, ¶ 38 (June 8, 2018); *see also* Case C-25/17, Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta, ECLI:EU:C:2018:551, ¶¶ 69–75 (July 10, 2018) (finding that a religious community was a controller jointly with its members even if the community did not have access to the data); *Guidelines 07/2020*, *supra* note 57, at 9–11.

[83] Ivanova, *supra* note 64, at 15; *see also* Case C-210/16, Wirtschaftsakademie at ¶¶ 36–38 (Jun. 5, 2018) (holding that a joint-controllership was found to exist because personal data was being processed through statistics of visitors to a fan page to not only enable Facebook to improve its system of advertising but also to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity, emphasizing that while each entity pursued its own interests both parties nevertheless participated in the determination of the purposes (and means) of the processing of personal data with respect to the visitors of the fan page).

[84] Ivanova, *supra* note 64, at 5.

[85] Jiahong Chen et al., *Who is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption*, 10 INT'L. DATA PRIV. L. 279, 284–85 (2020).

[86] Ivanova, *supra* note 64, at 16; *see also* Christopher Millard et al., *At This Rate, Everyone Will be a [Joint] Controller of Personal Data!*, 9 INT'L DATA J. 217, 217 ("[T]he fervour with which the label 'joint controller' is being applied to entities with even the most tenuous of connections to each other and to particular processing activities, risks undermining severely the essential nexus between responsibility and control. The end result is likely to be a growing disconnect between legal theory and what actually happens in practice, most likely accompanied by a reduction, not an enhancement, in the availability of meaningful protection for data subjects.").

[87] Ivanova, *supra* note 64, at 16; *see also* Mahieu & van Hoboken, *supra* note 80.

[88] Ivanova, *supra* note 64, at 16.

inherently entrenches the Court's analysis in examining only the joint 'means' of processing, but disregarding the common overarching objective(s) which may ultimately connect the various data processing phases along the full data value chain."[89] To put it differently, by focusing on the stage of processing where a controller is directly involved, and not the preceding or subsequent stages is to lose the forest from the trees; this approach fails to understand that "the effects on and the risks for the rights and freedoms of individuals of such complex systems, are–as a whole–much bigger than the mere sum of the risks connected to the individual processing phases."[90] Mahieu *et al.* conclude that the result of the phase-oriented approach to data protection taken in *Fashion ID* is that the data controllers are unable to meaningfully discharge responsibilities, particularly since there are insufficient methodological approaches to divide up complex data processing operations into different phases.[91]

Instead of the phase-oriented approach in allocating responsibility, Ivanova suggests using the "'responsibilities, powers and capacities'" criterion established in *Google Spain*.[92] She explains that this approach is preferable since all requirements for DPbD "would be thus placed directly on the service provider within whose 'powers and capacities' solely remain the provision of a GDPR compliant service."[93] She further explains that this would include "designing the appropriate arrangement for the allocation of data protection responsibilities which users of the service must only accept and implement accordingly."[94]

The "responsibilities, powers and capacities" approach is sensible since it recognizes that there are often multiple entities involved in modern data processing activities as well as focuses on the entity that has the most influence over the processing. Another benefit is that it avoids the mucky territory of divorcing data processing functions in a contextual and structural void which may lead to liability for an entity that has little or no control over the offensive data processing. In other words, instead of potentially arbitrarily delimiting stages of data processing, it takes a more holistic, balanced, and common-sense approach that may include considerations like the complete life cycle of personal data processing as well as who is best positioned to safeguard the rights of the data subject. In some situations, a technology provider will merely facilitate the necessary infrastructures for data processing whereas in others, it will be in a far better position than the data controller to control the way that personal data are handled and to design the system in the

[89] *Id*.
[90] Mahieu & van Hoboken, *supra* note 80.
[91] Mahieu & van Hoboken, *supra* note 80; *see also* Ivanova, *supra* note 64, at 19.
[92] Ivanova, *supra* note 64, at 18.
[93] *Id*. at 18.
[94] *Id*.

most privacy preserving manner.[95] In the latter case, it makes more sense to hold them accountable under the GDPR.

Regardless of whether the "responsibilities, powers and capacities" approach is adopted over the "phase oriented" approach, there is still the significant issue of how to allocate responsibility and liability between joint controllers, particularly if a technology provider only has a tangential connection to the personal data processing activities and is involved only during a short phase of processing. The CJEU has been emphatic that joint data controllers do not necessarily have equal responsibility in respect of the processing of personal data.[96] For example, in *Wirtschaftsakademie*, the Court explicitly stated that joint data controllers may have "different degrees" of involvement and responsibility which requires specific assessments, paying attention to all of the relevant circumstances of the particular case.[97] That said, the Court failed to offer any guidance as to how to apportion the shares of responsibility, particularly in situations where joint controllers do not clearly arrange their responsibility.[98]

It is possible that the use of Article 26 of the GDPR may have a role to play in this context which permits the use of contracts to allocate spheres of responsibility.[99] The existence of a contract allocating responsibility will likely be relevant to any analysis of the circumstances of a particular case, even if it must be acknowledged that under existing legal doctrine, in many instances a (joint) controllership can result from technical or organizational configurations rather than an explicit legal arrangement between concerned parties.[100] Also, practical challenges to drafting these agreements will be high given the difficulty of deciphering who is responsible for what in the context of modern data processing activities. Standardization to demonstrate compliance with best available practices may also prove to be relevant in assessing each controller's level of responsibility.

b. Responsibility as a Processor

---

[95] DAVID MCAULEY ET AL., COMMENTS ON THE EUROPEAN DATA PROTECTION BOARD'S GUIDELINES 4/2019 ON ARTICLE 25 DATA PROTECTION BY DESIGN AND BY DEFAULT, ¶¶ 5, 13 (2020).

[96] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Facebook Ir. Ltd., ECLI:EU:C:2018:388, ¶ 43 (June 5, 2018) ("operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case"); *see also* Case C-25/17, Tietosuojavaltuutettu v. Jehovan todistajat-uskonnollinen yhdyskunta, ECLI:EU:C:2018:551, ¶¶ 65–66, 75 (July 10, 2018).

[97] *Id.*

[98] Mahieu et al., *supra* note 64, at 85.

[99] Commission Regulation 2016/679, art. 26, 2016 O.J. (L 119).

[100] Chen et al., *supra* note 85, at 282.

A data processor is an entity that "processes personal data on behalf of the controller."[101] According to the EDPB, in order to qualify as a processor, the entity must be separate from the controller and it must process personal data on the controller's behalf.[102] That said, the EDPB has stated that "practical aspects of implementation . . . can be left to the processor."[103]

While controllers are primarily responsible for compliance with all of the provisions of the GDPR, processors are required to process the data according to the controller's instructions and comply with the set of obligations provided in Article 28. For example, processors must only process personal data on instructions from a controller, unless otherwise required by law.[104] Additionally, a processor must enter into a binding contract with the controller.[105] Processors must also provide "sufficient guarantees to implement appropriate technical and organizational measures" in order to protect personal data against loss or unlawful processing.[106] While the GDPR lists the elements that the processing agreement must include, it should also include "more specific, concrete information as to how the requirements will be met.[107] Data processors must also only engage with other processors after they have obtained "prior specific or general written authorisation (sic) of the [data] controller."[108] Finally, it is important to note that the GDPR sets forth a "cumulative" liability regime, such that, "(i)n situations involving more than one controller or processor, every controller or processor involved in the processing may in principle be held liable for the entire damage, provided the damage results from its failure to comply with an obligation to which it is subject (article 82[4])."[109]

If an Ed Tech provider is classified as a processor because it processes personal data on behalf of a controller, then it will bear some responsibility to implement DPbD. While Article 25 does not mention data processors specifically, Article 28 does specify that a controller must only use processors that provide: "sufficient guarantees to implement appropriate technical and

---

[101] Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 8.
[102] *Guidelines 07/2020*, *supra* note 57, at 3.
[103] *Id.*
[104] Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119); *see also* Case C-119/12, Probst v. mr.nexnet GmbH, 2012 E.C.R. 748, ¶ 25.
[105] Commission Regulation 2016/679, art. 4, 2016 O.J. (L 119) 8; Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119) 3.
[106] Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119) 1, 3 ("[w]here processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.").
[107] *Guidelines 07/2020, supra* note 57, at 4.
[108] Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119) 1.
[109] Van Alsenoy, *supra* note 70, at 282.

organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."[110] While it is unclear whether a data processor must actively assist a data controller to meet its DPbD obligations, at a minimum it appears the processor must guarantee that it meets the requirements of the GDPR.[111] In other words, controllers must select processors which provide sufficient guarantees to meet GDPR requirements, ostensibly including DPbD.

c. Responsibility as a Technology Provider

There is no definition of a technology provider in the GDPR. That said, the proposed EU AI Regulation defines a "provider" as "a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge."[112] It further defines "small-scale provider," "importer," "distributor," and "operator." Recital 60 explicitly acknowledges "the complexity of the artificial intelligence value chain" and encourages "relevant third parties" like "the ones involved in the sale and the supply of software, software tools and components, pre-trained models and data, or providers of network services" to cooperate to meet legal obligations.[113] The fact that EU AI Regulation acknowledges a broad range of operators in the chain of supply of AI and seeks to regulate the various actors is an implicit recognition that the GDPR, directed only at data subjects, controllers, and processors, is insufficient on its own to effectively regulate AI.

A central question that arises is whether technology providers have control over the processing. In many instances, it is the controller who is poised to define the purposes of processing, leaving technology providers largely unaware of both the "nature, scope, context and purposes of processing" as well as any risks to the data subject that may arise from the processing activities. A good example of this concerns developers, understood as "the parties that develop software, architect services and operate the cloud infrastructure."[114] Developers write the code that controls core software, but they are unlikely to qualify as a controller "because they only make available the software to the user."[115] That is, they do not control the software use, nor

---

[110] Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119) 1.
[111] *See* Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119) 3.
[112] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts, 2021 O.J. (C 206) 1, 39, 40.
[113] *Id.* at 32; Commission Regulation 2016/679, art. 32, 2016 O.J. (L 119) 1.
[114] Seda Gürses & Joris van Hoboken*, Privacy after the Agile Turn*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 579, 581 (Jules Polonetsky, Omer Tene & Evan Selinger eds., 2018).
[115] Jiménez-Gómez, *supra* note 57, at 313.

the data that it stores.[116] Nevertheless, they are in a key position to enable DPbD and DPbDf since they have the capacity to build a technological system that can completely stop certain actions as well as privilege certain stakeholders and values at the expense of others.[117] As discussed above, this could give rise to an argument that they have control over the "means" of processing and therefore constitute controllers, subject to meeting all of the requirements of the GDPR.

While Recital 78 extends the DPbD concept to technology providers, it does not require them to comply.[118] That said, it does place a responsibility, albeit non-binding, on a data controller to work with technology providers that have taken privacy and data protection into account during system development.[119] Note that the effect of Recital 78 is to place pressure on technology developers to take DPbD into account to increase their attractiveness in the market. Here, the EDPB stresses the competitive advantage technology providers and processors can gain by ensuring they not only implement DPbD themselves but can advise controllers on how best to do so.[120]

Despite the lack of a binding legal obligation, the EDPB argues that technology providers should play an active role in ensuring that the "state of the art" criterion is met.[121] This is because technology providers may be in a better position to identify the potential risks that the use of a product or service may entail. In other words, it suggests that technology providers assist data controllers stay up to date on technological progress. Particularly if a controller purchases or procures a service or product downstream. EDPB contends that "(c)ontrollers should include this requirement as a contractual clause."[122]

The concept of "state of the art" exists within various EU acquis, such as environmental protection and product safety.[123] In the GDPR, reference to

---

[116] *Id.*
[117] *See id.* (discussing the macro-level control of developers over blockchain design in compliance with GDPR privacy considerations); *see generally* Roger Brownsword, *Code, Control, and Choice: Why East is East and West is West*, 25 LEGAL STUD. 1 (2005) (discussing regulation through code, also called "techno-regulation").
[118] Commission Regulation 2016/679, 2016 O.J. (L 119) recital 78.
[119] *Id.*
[120] *Guidelines 4/2019*, *supra* note 4, at 4.
[121] *Id.* at ¶ 96 (stating, "Producers and processors should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures they have in place. Controllers should include this requirement as a contractual clause to make sure they are kept up to date").
[122] *Id.*
[123] *Id.* at ¶ 18.

the "state of the art" is not only in Article 32, for security measures, but also in Article 25. The EDPB guidelines explain that the concept of "state of the art" is "a dynamic concept that cannot be statically defined at a fixed point in time" and "imposes an obligation on controllers, when determining the appropriate technical and organizational measures, to take account of the current progress in technology that is available in the market."[124] In a footnote, the EDPB guidelines identify "state of the art" as "the technology level of a service or technology or product that exists in the market and is most effective in achieving the objectives identified."[125] This implies a certain level of maturity, an ability to ensure effective implementation and an objective character.[126]

Next, technology providers may have an obligation to notify data controllers of changes to the "state of the art" that may affect the effectiveness of the measures in place to mitigate against privacy and data protection infringements. While this obligation may be non-binding under the GDPR if a technology provider is not a controller or processor, it is possible that to incorporate the obligation into a contract.[127] It is important to note that while the GDPR clearly regulates the contractual relationship of the controller and the processor in Article 28, it makes no mention of the obligation of technology providers to notify controllers of any changes to the "state of the art."[128]

Once again, the complexity of the supply of software must be emphasized. If one considers the hypothetical app Course Cues, described above, it becomes apparent that the app involves linked software, hardware, and service organizations all cooperating to satisfy the market demand for the app. Unlike a physical good, the app is also malleable after its release and delivery, giving raise to the need for significant maintenance.[129] However, there is often a lack of information, communication, and feedback between different actors in the software supply chain about how software should be maintained.[130]

---

[124] *Id.* at ¶¶ 19–20.
[125] *Id.* at 8 n.8.
[126] Athena Bourka, Eur. Union Agency for Cybersecurity (ENISA) (EU), Presentation at the Computers Privacy and Data Protection 2021: Enforcing Rights in a Changing World, panel organized by the Swedish Institute of Law and Informatics: Data Protection by design and by Default in the Post-Covid World (Jan. 27, 2021).
[127] *See* The Norwegian Tax Administration, *Re: Public consultation reply to the EDPB's "Guidelines 4/2019 on article 25 Data Protection by Design and by Default,"* EUROPA (Jan. 16. 2020), https://edpb.europa.eu/sites/edpb/files/webform/public_ consultation_reply/edpb_opinion_on_ data_protection_ by_design_16_jan_2020_final_on_template.pdf.
[128] *See id.*
[129] Jansen et al., *supra* note 44, at 677.
[130] *Id.* at 677–78.

While there theoretically should be a transparent view of all changes throughout the software development lifecycle, effective coordination between relevant actors can be challenging, especially where geographically distributed teams work on software development.[131] From a practical perspective, this would certainly complicate placing a rigid legal demand on Ed-Tech providers to notify controllers about changes to the "start of the art." Here, it can be argued, pointing to Article 28(3)(f),[132] that any obligation to support the controller in understanding the "state of the art" must be strictly limited to the information that is available to the technology provider.[133] It can also be argued that there should be a legally defined relationship between the actors insofar as it may be impossible to regulate informal and ad hoc relationships that exist within a software supply chain, especially when one takes into consideration the use of open-source code.

d. Critical Perspectives

In many ways, it makes sense to hold an Ed Tech provider responsible for DPbD since they are in a position to develop a system that supports data protection principles, values, and rules. As Tsormpatzoudi *et al.* explain: data controllers only operate at the very end of the supply chain which may be too late for the obligations of DPbD and for DPbD to be effective.[134] However, it is virtually impossible to predict all potential privacy and data protection harms *ex ante*. Technologies are situated in society and interact with humans who can use them in unimaginable ways. Indeed, the multistability of technologies, a concept proposed by Ihde that refers to the unpredictable uses of technology different from the originally intended ones, is well explored.[135] When it comes to Ed Tech, the end users – teachers and students – are generally not be the same person as an Ed Tech's client (the university represented by a CTO). This complicates DPbD since Ed Tech companies are far removed from teachers and students who might find new and unexpected uses for the technology that that neither the school nor the technology provider imagined.

In recognition of the iterative and dynamic nature of the design process (which does not necessarily have a clear beginning and endpoint),[136] the GDPR requires controllers to implement DPbD measures and safeguards both

---

[131] Singi et al., *supra* note 49, at 1212.
[132] *See* Commission Regulation 2016/679, art. 28, 2016 O.J. (L 119) 3(f).
[133] *See* CIPL, *supra* note 5.
[134] Pagona Tsormpatzoudi et al., *Privacy by Design: From Research and Policy to Practice–the Challenge of Multi-Disciplinarity*, *in* APF 2015: PRIVACY TECHNOLOGIES AND POLICY 199, 207 (Bettina Berendt et al. eds., 2016).
[135] *See generally* DON IHDE, TECHNOLOGY AND THE LIFEWORLD: FROM GARDEN TO EARTH 1–22 (1993); MIREILLE HILDEBRANDT, PROFILING AND THE RULE OF LAW 1–17 (2009).
[136] Waldman, *supra* note 12, at 1241.

at the time of determining the means of processing and at the time of processing itself.[137] The controller must also regularly review the effectiveness of the chosen measures and safeguards.[138] In other words, in order to meet the DPbD requirements, measures and safeguards should be adopted at the conception phase (the time of determination of purposes and means), and considered throughout the whole processing stage (up until erasure or anonymization of the data).[139]

The fact that technological consequences are hard to foresee from the design perspective suggests that is may be appropriate for lawmakers to limit the extent of liability held by Ed Tech providers. In many cases, it will be impossible to understand and foresee privacy and data protection threats during the Research and Development stage or even after a Privacy Impact Assessment (PIA) is conducted.[140] Even after a technology, infrastructure, system, service, or device has been deployed or put to use, the uncertainty or unawareness of all the privacy threats and implications of the technology in question may remain.[141]

While technology providers should try to make systems adaptable to different kinds of risks that arise in various processing environments, the reality is that this may not always be possible from a design perspective, even after a PIA. Even the Spanish data protection authority (AEPD) acknowledges that the use of off-the-shelf third-party components may limit the possibility of configurability.[142] Asking technology to configure the products in a privacy-aware way without full knowledge of the context of use, or any knowledge of particular set of specifications, is almost like asking them to see in the dark. Besides, the technical limitations may be unduly costly, particularly for smaller companies.

V. Conclusion

Blume contends that data protection is founded on a fiction "that the data controller is in control and is able to meet the obligations set out in the law."[143] He suggests that this model rejects the kind of data processing that

---

[137] Commission Regulation 2016/679, art. 25, 2016 O.J. (L 119).
[138] *Guidelines 4/2019*, *supra* note 4, at ¶ 37 (explaining that "once the processing has started the controller has a continued obligation to maintain DPbDD, *i.e.* the continued effective implementation of the principles in order to protect the rights, staying up to date on the state of the art, reassessing the level of risk, etc.").
[139] *See* Kamocki & Witt, *supra* note 10.
[140] *See* Demetrius Klitou, *Privacy by Design and Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century*, 5 LEGISPRUDENCE 297 (2011).
[141] *See id.*
[142] Agencia esanola de proteccion de datos (AEPD) [Spanish Data Protection Agency], A GUIDE TO PRIVACY BY DESIGN (October 2019).
[143] Blume, *supra* note 59, at 292.

occurs in modern life due to the complexity of current ICT.[144] Criticizing the unrealistic obligations on controllers set forth in the GDPR, he states: "It is undesirable and clashing with general legal culture and tradition to have rules that communicate obligations that cannot be met by those who are obliged to do so."[145]

Blume is not alone in his concerns about the controller/processor dichotomy and its application in the contemporary technological and economic reality.[146] Gürses and van Hoboken have argued that recent developments in software production have major implications for data protection, and in particular, understanding to what extent organizations operating in the software supply chain have data protection obligations.[147] Pointing to the shift from shrink-wrap software to software as a service, and the rise of the mobile internet, cloud computing and agile software development processes, they argue that software is becoming more modular (meaning that most applications, websites and other software are built out of service modules of third party software).[148] The essential point is: "In the current networked world, almost no system in which personal data is processed stands on its own."[149]

Edwards et. al. explain how data processing has changed since the EU data protection law's beginning. [150] They note, first, the shift from unitary control over the means and the purposes of processing towards shared control in complex data ecosystems; and second, the shift from centralized to distributed infrastructure and organization.[151] They contend that the current technological reality is complex and diverse, and data processing operations can easily be intermingled which, in light of recent caselaw, calls into question the suitability of existing doctrine of controllership.[152]

The CJEU has expanded the concept of data controller, contending that a broad interpretation of the concept is necessary to ensure the principle of

---

[144] *Id.*
[145] *Id.*
[146] *See* Seda Gürses & Joris van Hoboken*, supra* note 114, at 579; Brendan Van Alsenoy, *Allocating Responsibility Among Controllers, Processors, and "Everything In Between": The Definition of Actors and Roles in Directive 95/46/EC*, 28 COMPUT. L. & SEC. REV. 25, 35 (2012).
[147] Gürses & van Hoboken, *supra* note 114, at 592.
[148] Mahieu et al., *supra* note 64, at 88.
[149] *Id.* at 85.
[150] Lilian Edwards et al., *Data Subjects as Data Controllers: A Fashion(able) Concept?*, INTERNET POL'Y REV. (June 13, 2019), https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400.
[151] *Id.*
[152] *Id.*

"the effective and complete protection of data subjects."[153] Consequently, the demarcation between the concepts of controller, processor, and technology provider is unclear, as well as the respective liabilities of each of those actors, causing significant legal confusion and uncertainty of adequate legal protection for the data subject. The issue is exacerbated in areas with complex technical configurations that involve a variety of stakeholders, like in the Ed Tech sector where AI is increasingly embedded in all kinds of devices and services.

To highlight gaps and ambiguities in the current legal framework, this article has sought to understand the scope of Article 25 from the perspective of all system designers acting within the chain of supply of an Ed Tech product or service. It has examined the role of technology providers and concluded that in many circumstances they may be considered a (joint) data controller or a processer, particularly if the court or DPA takes a "microscopic view" of data processing operations that is focused on individual data processing operations within the system and the value chain. That said, if a technology provider does not process any personal data nor have any influence over the "means" of processing for their own economic benefit, then a finding of a controllership is unlikely. Regardless of whether a technology provider is found to be a controller or processor, it may have obligations to assist a data controller to stay up to date on the state of the art under Article 25, although the scope of this obligation is unclear.

In conclusion, there is a need to recognize the complex, interdependent and non-linear context of contemporary data processing where there exist many different controllers, processors and other actors processing personal data in different geographical locations and at different points in time for both central and peripheral purposes. Likewise, the complexity of the supply of software must also be emphasized, particularly in contexts like in the supply of educational technology where technology providers can play a key role in the preservation of privacy and data protection rights but may only have a tangential link to the universities that ultimately use their products and services.

Finally, the GDPR, directed only at data subjects, controllers, and processors, is insufficient on its own to regulate AI effectively. There are many different actors involved in the design, development, procurement, and use of AI systems like those being deployed in HE settings and new approaches are needed to ensure that these systems respect the fundamental

[153] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388 (citing Case C-131/12, Google Spain and Google, ECLI:EU:C:2014:317).

right to privacy and data protection.[154] Here, there is no doubt a need for a more dynamic approach towards considering responsibility regarding DPbD and DPbDf not least where it concerns technology providers. Instead of thinking about responsibilities in terms of "purpose" and "means" the law should shift towards a focus on powers and capacities. Clarification concerning whether and to what extent technology providers must inform controllers about changes to the state of the art is also needed.

[154] *See also* Virginia Dignum, *Responsibility and Artificial Intelligence, in* THE OXFORD HANDBOOK OF ETHICS OF AI (Markus D. Dubber et al. eds., 2020).