A MOOC on Privacy by Design and the GDPR

Simone Fischer-Hübner, Leonardo Martucci, Lothar Fritsch, Tobias Pulls, Sebastian Herold, Leonardo Iwaya, Stefan Alfredsson, Albin Zuccato

A MOOC on Privacy by Design and the GDPR

Simone Fischer-Hübner [1], Leonardo A. Martucci [1], Lothar Fritsch [1],
Tobias Pulls [1], Sebastian Herold [1],
Leonardo H. Iwaya [1], Stefan Alfredsson,[1], and Albin Zuccato [2] *.

[1] Karlstad University, Sweden
[firstname.lastname]@kau.se
[2] Atea Sverige AB, Sweden
[firstname.lastname]@atea.se

Abstract. In this paper we describe how we designed a massive open online course (MOOC) on Privacy by Design with a focus on how to achieve compliance with the EU GDPR principles and requirements in IT engineering and management. This MOOC aims at educating both professionals and undergraduate students, i.e., target groups with distinct educational needs and requirements, within a single course structure. We discuss why developing and publishing such a course is a timely decision and fulfills the current needs of the professional and undergraduate education. The MOOC is organized in five modules, each of them with its own learning outcomes and activities. The modules focus on different aspects of the GDPR that data protection officers have to be knowledgeable about, ranging from the legal basics, to data protection impact assessment methods, and privacy-enhancing technologies. The modules were delivered using hypertext, digital content and three video production styles: slides with voice-over, talking heads and interviews. The main contribution of this work is the roadmap on how to design a highly relevant MOOC on privacy by design and the GDPR aimed at an heterogeneous audience.

1 Introduction

The General Data Protection Regulation (GDPR) is the EU regulation that aims to protect the "*fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*" and lays down "*rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*" [5] The regulation has a broad territorial scope and applies to the processing of personal data of people who reside in the EU, regardless of whether the processing of their data takes place in the EU or not. It gives the supervisory authorities discretion to apply administrative fines of up to €20M or 4% of a company's total worldwide annual turnover (of its preceding fiscal reporting year, whichever is higher).

* This work was partially funded by WISR 16, Web-based Courses for International positioning of Strategic Research Groups, a project in the NU 16 Programme for Web-based International Education of the Knowledge Foundation (KKS) of Sweden.

The GDPR was published in April 2016 and came into force on May 25^{th} 2018. During the two-year transition period between its adoption and enforcement national governments had to transpose the GDPR into laws and organizations had to adapt to the regulation. The GDPR requires organizations to appoint a data protection officers (DPO) to oversee that the processing of personal data is compliant with the regulation, according to the cases specified under Art. 37–39 GDPR. DPOs are designated on basis of their professional qualities, including expert knowledge in data protection law and to provide advice and monitor the process of a data protection impact assessments (DPIA) required according to Art. 35 GDPR, an activity that requires legal, technical and organizational expertise. Besides, it will also be expected that a DPO can advise organizations in regard to their obligations to implement data protection by design pursuant to Art. 25 GDPR. As a consequence, the GDPR created a sudden demand for qualified professionals on technical, organizational and legal data protection aspects.

In order to serve this sudden educational demand, we designed a course on the GDPR and Privacy by Design (PbD) principles and legal and technical requirements. We set as objective to educate professionals and full-time undergraduate students using a single course structure. Therefore, we implement the course as a massive open online course (MOOC) that supports the individual learning behaviors and needs of an heterogeneous audience.

In this paper we describe how we designed this MOOC and present our lessons learned. We explain the overarching course structure and its organization into five modules, introduce the learning outcomes, and discuss the implemented teaching and learning activities.

This paper is organized as follows. Section 2 provides an introduction to the PbD course. Its modules, content and learning outcomes are outlined in Section 3. The teaching methods and the characteristics of the produced course content are described in Section 4. Section 5 presents the related work. The PbD course is discussed in Section 6 and Section 7 concludes the paper.

2 Designing the PbD Course

The course requirements were elicited by a core of data protection specialists from both academia and industry. This group was responsible to outline the learning outcomes of the course, structure it to address the needs of an heterogeneous audience constituted of professionals and undergraduate students, and reach out for a broad diverse and international audience.

Concerning the **intended audience and outreach**, the MOOC general model offers the desired tools for providing access to the course material to a large (and theoretically unbounded) audience. A MOOC also provides flexibility regarding the participants' individual learning pace, allowing them to decide upon their weekly effort devoted to the course, and adjust their attendance to their ongoing professional and academic commitments. The intended audience is undergraduate students and professionals with basic technical background in information technology (IT).

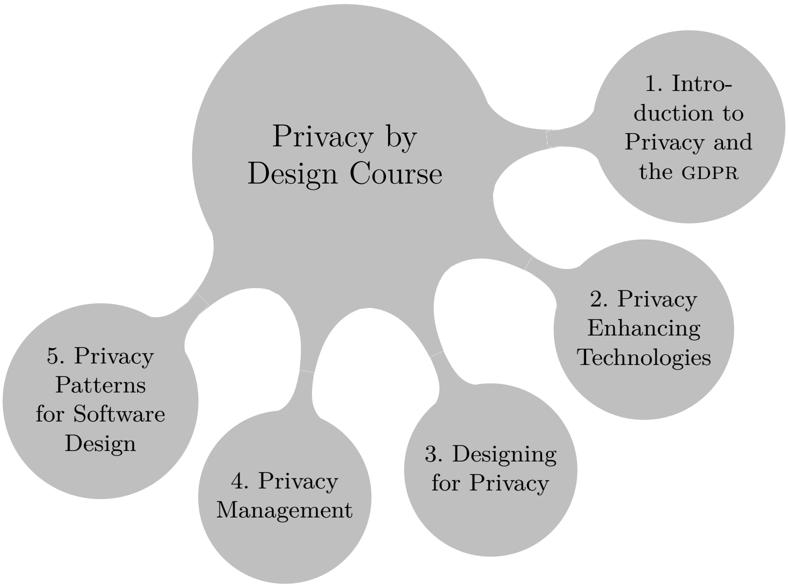
Privacy by Design Course
1. Introduction to Privacy and the GDPR
2. Privacy Enhancing Technologies
3. Designing for Privacy
4. Privacy Management
5. Privacy Patterns for Software Design

Fig. 1: The PbD course structure and its five modules.

The **course content** covers topics on PbD, the GDPR and its application. The topics covered were chosen based on the course responsible experts' considerations about relevant legal, technical and organizational needs of a professional to demonstrate knowledge and competence on tasks assigned to a DPO.

The **course structure** is build on modules. The division into modules has a threefold objective: (a) the course content is divided into specific topics within the scope of PbD and the GDPR. It allows the course participants to select which modules to attend or to prioritize; (b) the required effort per module is bounded to 40 hours. This requirement is key for course participants coming from industry, who can then better plan their work and study schedules, and in some cases claim the effort spent on the module as competence development; and (c) apply specific pedagogical tools and methods that better suits the course content and the learning outcomes defined for each module.

Fig. 1 illustrates the five course modules. Participants who are interested in all modules, are recommended a sequential learning path: "1. Introduction to Privacy and the GDPR", "2. Privacy Enhancing Technologies" (PETs), "3. Designing for Privacy", "4. Privacy Management", and "5. Privacy Patterns for Software Design". Modules 1–2 cover the introductory topics (privacy fundamentals, GDPR and PETs) that the course is built upon. Modules 3–4 refer to PbD and the general knowledge on tools and methods required by the GDPR. Module 5 covers privacy in the context of software design. At the start of modules 3–5, a summary of the first two modules is provided.

The structure of the course into those modules was decided to make the course also attractive to full-time students and to professionals from industry and public sector, who may attend the course part-time and are able to select the modules that augment and complement their expertise. For instance, an experienced software developer would probably benefit most from the PbD course by attending the first three and the fifth modules.

The modules were assigned and developed by subgroups of this article's authors, which includes academic teachers and data protection specialists having technical, legal, industry and academic backgrounds, some of whom had been following the discussions around the GDPR and its development since the release of its first proposal in 2012. The modules were developed independently, having each a specific set of learning outcomes and delivered using a suitable set of pedagogic and presentation teaching techniques. Nonetheless, the overall course objective and course content was discussed and agreed upon in the team.

Most of the course content is **accessible** for those with (somewhat limited) physical or psychological impairment. All videos produced either are provided with scripts or have subtitles (or both). The platform used in the course lacks native text-to-speech capabilities but supports third-party solutions. They were not deployed in the initial deployment of the course.

The **course accreditation** is provided by the academic authors' home institution, which provides course examinations and grades in the form of European Credit Transfer and Accumulation (ECTS) credits for the participants enrolled in the course and on individual modules (1.5 ECTS/module).

The **assessment** of the participants is based on individual assignments and a short oral exam. Assignments are uploaded by the participants to the online course platform. Each module has its own assignment, and the expected effort to complete it is approximately eight hours. The oral exam has a twofold objective: assessment and checking for authorship. When uploading their assignments, the participants book their oral exams. Before the oral examination, the reports are checked for plagiarism and corrected. Oral exams are 10-minute interviews using an online communication platform with video feedback.

The PbD course contents were distributed following a **Creative Commons Attribution license**, which allows all course content to be shared and adapted as long as appropriate credit is given and changes are indicated.

3 Modules, Content and Learning Outcomes

In this section, we describe the course modules, content and learning outcomes.

3.1 The Course Modules and their Content

1. Introduction to Privacy and the GDPR covers the definition, history, and foundations of privacy, highlighting privacy challenges surrounding modern Information and Communication Technology. The primary focus of the module is on the legal European framework on privacy, data protection, and cyber security. It includes agreements for transfer of personal data outside of the EU. Selected European Court of Justice decisions are discussed. The content is divided into the following five areas of knowledge:

1. The fundamentals of privacy, including the right to privacy, basic principles, laws and history, and key court decisions.
2. Contemporary privacy issues, including mobile computing, smart metering, social networks, big data, and cloud computing.
3. The GDPR, including its background, scope, definitions, basic principles, lawfulness and consent, data subject rights and responsibilities, and rules for data controllers and data processors.
4. The ePrivacy draft regulation and its possible implications.
5. The mapping from GDPR legal privacy principles to PETs.

2. Privacy Enhancing Technologies (PETs) introduces security and privacy mechanisms and technologies and details how security and privacy mechanisms can be used to solve practical and theoretical problems, along with discussions of their advantages and disadvantages.

1. An introduction to PETs, computer and network security basics and tools, and terminology for security and privacy.
2. Secure communication protocols and architectures, including PGP, TLS, Certificate Authorities (CAs), digital certificates and secure messaging.
3. Anonymous communication protocols (mainly Mix networks and Tor).
4. Databases and privacy, including k-anonymity and differential privacy.
5. Other relevant PETs and security technologies, such as blockchains, anonymous credentials, and Transparency Enhancing Technologies (TETs).

3. Designing for Privacy introduces the foundations of privacy, data protection, and privacy enhancing technologies, and then focuses on the concepts of privacy by design and privacy impact assessments (PIAs) by exploring the relevant background, their relationship to the foundation and fundamental human rights, and by introducing relevant methods.

1. Fundamental concepts that summarize the GDPR and PETs.
2. The meaning behind designing for "privacy". Privacy in relation to data protection, PbD, privacy paradigms, technology in hostile states, privacy protection goals, data protection by design and by default [4].
3. Privacy and DPIA, PIA as a process, frameworks and PIA in practice.

4. Privacy Management deals with privacy management as part of an organization's information security management. It introduces approaches to privacy management, provides insight into a management approach and explains how privacy threats can be anticipated and mitigated.

1. Privacy management into the context of data protection, stakeholders, PETs, and privacy management approaches, e.g. PDCA (Plan–Do–Check–Act).
2. The concept of "managed privacy", including privacy management as a data processing administration task.
3. PIA and privacy risk analysis as integral part of privacy management, including threats to privacy and sources of risk information.
4. The concept of privacy controls and properties, selection and risk mitigation..

5. Privacy Patterns for Software Design deals with privacy aspects during software design. It focuses on architectural tactics and patterns as reusable conceptual solutions to recurring privacy problems. It outlines how are these concepts used in agile development in order to engineer privacy into software.

1. An introduction to software architecture and design.
2. Privacy design strategies and as quality attribute of software systems.
3. Privacy design patterns and applying them in agile development.
4. Privacy anti and dark patterns.

3.2 The Learning Outcomes

The learning outcomes were specified following the principle of constructive alignment [2] which aims at aligning learning outcomes, learning activities and examination [9]. The SOLO (structure of observed learning outcome) taxonomy [3] was used to express the expectations concerning the participants' level of understanding after concluding a module. The learning outcomes range from uni-structural to extended abstract level of the SOLO taxonomy.

Every module has its own set of learning goals. The first two modules (on fundamentals of privacy, the GDPR, and PETs) provide the underlying building blocks for the learning material that follows.

The **Introduction to Privacy and the** GDPR module learning goals are:

- *Give an account* of basic legal privacy concepts, regulations and principles, and of major court decisions at national and European level.
- *Analyze* privacy challenges and the risks of ICT and applications.
- *Map* legal privacy principles to technical privacy concepts.

The **Privacy Enhancing Technologies** module learning goals are:

- *Give an account* of the basic security and privacy enhancing technologies.
- *Relate* security and privacy goals to mechanisms and technologies.
- *Explain* when and how to apply different privacy enhancing technologies.

The **Designing for Privacy** module learning goals are:

- *Give an account* of the concepts of privacy, data protection, privacy enhancing technologies, privacy by design, and privacy impact assessment.
- *Relate* privacy by design to privacy, data protection, privacy enhancing technologies, and fundamental human rights.
- *Explain* how privacy by design and privacy impact assessments are used.

The first learning objective of Designing for Privacy ("[g]ive an account of the concepts of privacy. . . ") refers to the modules 1–2 and content introduced in module 3 (PIAs). This learning goal is included in the goals of the modules 4–5. At the beginning of modules 4–5 on a summary of the modules 1–3 is provided, and a summary of the modules 1–2 is given at the start of module 3.

The **Privacy Management** module learning goals are:

- *Give an account* of approaches for managing information privacy.
- *Apply* methods for managing information privacy.
- *Analyze* risks to information privacy.

Table 1: Amount of minutes of novel audio & video material per module.

Module	Intro. Privacy and the GDPR	PETs	Designing for Privacy	Privacy Mngmt.	Privacy Patterns	TOTAL
Video	184	135	106	—	115	540
Audio	—	—	24	—	—	24

- *Compare and select* privacy controls and methods.

The **Privacy Patterns for Software Design** module learning goals are:

- *List* relevant privacy patterns.
- *Apply* appropriate architectural tactics for privacy and privacy patterns in a given systems context and for a given set of privacy requirements.
- *Explain* the key principles of architectural tactics for privacy patterns.
- *Analyze* the usage/occurrence of privacy patterns in a given system context.

4 Teaching Methods and Course Deployment

The teaching methods are adapted to the course contents and the MOOC model. The techniques used to deliver the modules are hypertext, digital content and three video production styles: slides with voice-over, talking heads and interviews. The videos' length is in the range between four and twenty five minutes.

All modules were delivered using video and slides especially designed for the PbD course, with the exception of the "Privacy Management" module. All videos have the option for subtitles (provided by the video hosting platform). All course slides are available in their source file format (MS PowerPoint) and in `pdf` format under the CC BY 4.0 (attribution) license. The amount of minutes of novel audio & video material present in each module is shown in Table 1. The videos length range of the n=65 produced videos is [1:24, 24:35] minutes, with (AVG=7:40, SD=4:17) and $\tilde{n}$=6:30, IQR=4:09 (Q1=4:51, Q3=9:00).

All lectures are complemented with mandatory and optional reading material and self-assessment online quizzes. The optional reading material provides the literature and resources for further self-studies for the course participants that are interested on a given topic. In addition, all lectures from the modules "Introduction to Privacy and the GDPR" and "Privacy Patterns for Software Design" include transcripts. A discussion forum is embedded in the MOOC platform.

Introduction to Privacy and the GDPR uses two video production styles: alternate talking head and slides with voice-over, and interviews. The module content covers legal and social privacy debates. Alternating a talking head with slides with voice-over video style was deemed an appropriate format to deliver this module's content because it allows the audience to follow the lecturer's face and expressions when voicing her viewpoints, which conveys relevant information. Twelve lectures were produced using this video production style.

The video interviews featured legal and technical experts from a German Data Protection Authority,[3] the DPO from the main authors' home institution, and a specialist from the industry. The overall topic of the interviews is on challenges and solutions for applying the legal requirements, especially the GDPR, in practice. This module featured six interviews. In addition, this module uses two existing anecdotal videos as support material.

Privacy Enhancing Technologies uses three video production styles: slides with voice-over, alternate talking head and slides with voice-over, and interviews. The module content covers technical aspects. Slides with voice-over offers a fitting alternative for technical subjects as animations help to illustrate how security and privacy protocols, tools and mechanisms work. Seventeen lectures were produced using this video production style.

Alternate talking heads and slides are used in the two videos on TETs. TETs is a subject with a strong human-computer interaction aspect connected to its technical aspects. Therefore, we judged that lecturer's face and expressions may improve the teaching quality for these two videos. This module feature an interview with an specialist in Tor from the University College London and four external videos: three presentations from specialists in selected subjects and one animation on Mix-Nets.

Designing for Privacy uses two video production styles: slides with voice-over and interviews. The module content covers technical aspects. Three interviews were recorded in audio format only. The lectures on Tor and PbD principles were delivered following the flipped classroom paradigm [8], as these topics requires a deeper analysis and criticism than the rest of module's content. These lectures reflect on the provided reading material and are supported by an external video (of Ann Cavoukian on the PbD principles).

Privacy Management uses a hypertext-based approach with elements of blended learning [7] and follows the flipped classroom paradigm. It discusses, illustrates and reviews the mandatory reading material. This module is supported by three external videos.

Privacy Patterns for Software Design uses three video production styles: slides with voice-over, alternate talking head and slides with voice-over, and interviews. Slides with voice-over were were used to cover to main module contents. The other video styles were used as support material for short introductions on the GDPR and PETs. The main module contents are delivered following the flipped classroom paradigm.

A summary of the number of videos in each module, sorted according to the production style used, is presented in Table 2.

4.1 Course Deployment

The PbD course is deployed using Canvas, an open-source Learning Management System (LMS) and MOOC platform. It is locally deployed and managed.[4] A

[3] The Unabhängiges Landeszentrum für Datenschutz (ULD), Schleswig-Holstein.

[4] Released under the AGPLv3 license (`https://github.com/instructure/canvas-lms`).

Table 2: The video production styles used in the PbD course modules. The TOTAL row corresponds to the unique entries to each category. External videos include presentation from external experts, anecdotes, and animations.

Module	Talking head and slides with voice-over	Slides with voice-over	Interviews	External Videos
Intro. Privacy	12	—	8	2
PETs	2	17	1	4
Design. Privacy	1	13	8	1
Privacy Mngmt.	—	—	—	3
Privacy Patterns	1	9	1	1
TOTAL (unique)	14	35	16	8

discussion forum and sharing of hand-in-assignments (the latter only to the "Privacy Management" module) are elements from the platform that are present in the courses. These tools aim at increasing student participation and interaction, and also help to reduce the drop-out rate, as shown by Anderson et al. [1].

The videos are hosted by YouTube (`www.youtube.com`), but not publicly indexed, i.e., they do not return as result of searches and can only be reached with a specific link to the video. The PbD course is available at `https://kau.se/cs/pbd`.

4.2 Enrollment and Participants

The course opened in two stages. In mid-January 2018 it was available for enrolled students and in March 2018 it opened for the general (non-enrolled) public. We initially set a limit for 100 enrolled students/module (to accommodate for the limitations on examining student essays). The exception is "Introduction to Privacy and the GDPR" which was planned to accommodate additional participants. The total number of students enrolled per module shown in Table 3.

4.3 Examination

The PbD course has quizzes for formative self-assessment [10] in all its modules. The quizzes are either multiple choice of true/false statements. As pointed out in Section 2, the assessment of the participants is based on individual assignments and a short oral exam. In this section, we discuss the content of the assignments.

Table 3: Number of students enrolled in each module.

Module	Intro. Privacy and the GDPR	PETs	Designing for Privacy	Privacy Mngmt.	Privacy Patterns	TOTAL (unique)
Enrolled	115	100	99	96	99	146
Completed	15	10	8	7	9	22

In **Introduction to Privacy and the** GDPR the assignment is the design of valid consent forms including privacy policy statements. The task is twofold: (*i*) to evaluate the consent forms used for social login with Facebook according to the legal requirements of the GDPR, taking into consideration the Guidelines of the Art. 29 Data Protection Working Party on Consent. [5] The goal is to point out the legal requirements of the GDPR, such as for consent (Art. 7 GDPR) and data protection by default (Art. 25 GDPR), are not met. And (*ii*) to discuss how user interfaces could be designed to be GDPR compliant. This exercise has a high practical relevance, as most consent forms (as in January 2018) are not yet fully GDPR compliant. This exercise also relates to basic privacy principles (Art. 5 GDPR) connected to the design of policy and consent forms.

In PETs the assignment evaluates the extended abstract level of understanding of a participant into two out of four selected topics. Additional literature is provided in form of academic papers, online manuals and reports. The assignment was designed in two parts: (*i*) to discuss the benefits and limitations of a PET (Tor or Let's Encrypt) and (*ii*) to analyze the properties and privacy guarantees offered when aiming for anonymizing the contents of database or to analyze and assess the privacy properties of a crypto currency (Bitcoin).

In **Designing for Privacy** the assignment focus on the deeper learning objectives of the module, namely having to analyze or evaluate one out of five selected topics discussed in the module, such as comparing and motivating preferences for one PIA framework over another, or arguing for why a particular type of security technology in a setting is a reasonable measure that should be taken for the data protection by design requirement in the GDPR being fulfilled.

The **Privacy Management** assignment is twofold: (*i*) a written essay on the handling of legacy data under the light of the GDPR and report on data protection and user consent aspects, and (*ii*) using a mobile dating application as a case study, and perform a partial privacy risk assessment.

In **Privacy Patterns for Software Design** the assignment covers applying privacy design strategies and privacy patterns. The course participants are asked to describe a system and the personal data processed in it. They are asked to elaborate on several privacy design strategies that could be applied in this context and explain potentially applicable patterns implementing them.

The first round of examinations for the enrolled students ended in June 2018. The total number that completed the course modules is shown in Table 3. Three participants completed all five modules and four only one module.

5 Related Work

To the best of our knowledge, one of the first academic courses for data protection professionals that implemented an interdisciplinary perspective was introduced at the Hochschule Ulm in 1988. The program evolved into a certification course program for professionals in data protection [6]. Its curriculum has three parts:

[5] Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/679, `http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849`

legal, information security and privacy management. It is a three weeks full-time regular course. The technical aspects of this course, however, do not include PETs (only general IT security).

There are private offerings for GDPR courses.[6] [7] [8] They are shorter than our PbD and GDPR course and/or focus only on the GDPR principles and core obligations of DPOs (such as privacy management), while not sufficiently addressing technical aspects that are important for the PbD process, such as PETs.

The International Association of Privacy Professionals (IAPP) lists institutes that offer privacy-related courses.[9] In its list, the majority are offered by law schools. To the best of our knowledge, there is no other MOOC on PbD and the GDPR targeting both undergraduate students and professionals.

6 Discussion

The course was released in January 2018 to participants enrolled to it through the official channels and opened to the general public in March 2018. The difference between the two groups is that the enrolled students have their written assignments graded and receive ECTS credits upon the successful completion of the course. At the time of writing, not enough student feedback is available for meaningful quantitative conclusions to be reached. Nonetheless, in this section we discuss some insights from the feedback obtained so far and from the background of the students enrolled in the PbD course.

Target group: an objective of the course is to teach skills that are needed by DPOs to undergraduate students and professionals, including those with major legal background and IT professionals who aim for GDPR compliance. The PbD course curriculum blends the legal, technical and managerial skills. It was designed for an audience with basic IT knowledge, with an equivalent of a semester of upper education studies in computer science or other technical subjects related to IT, or equivalent work experience. The first cohort of enrolled students is mainly composed of IT professionals, DPOs, and undergraduates.

On-line teaching styles: the modularized structure of the course allowed for experimentation with multiple presentation styles within the course, as seen in Section 4. The content of the modules is delivered using various audio&video styles, and even a hypertext only module. The flipped classroom paradigm is present in three out of five modules. In our course evaluation, we plan to assess the impact of our pedagogic choices using the students' feedback as input data.

The interaction with students was, so far, low compared to teaching in classroom. This was expected in a self-paced, with student interaction happening only via the platform's forum or by email, which is the general case for MOOCs.

Limited student feedback was obtained from: (*a*) online feedback forms distributed by the university and (*b*) informally after examination and grading.

[6] IT Governance. https://www.itgovernance.co.uk/

[7] GDPR Firebrand Training. http://www.firebrandtraining.co.uk/courses/

[8] Olive Group. https://gdprcourse.com/

[9] https://iapp.org/resources/article/colleges-with-privacy-curricula/

All feedback was provided voluntarily. So far, it is positive, with participants pointing out their personal and professional needs for such course. All but one course participants favor video lectures over text only material, and short videos (up to 10 minutes) were preferred rather than to long videos. The results from the online feedback forms are available at: `https://www3.kau.se/kurstorget/`. Feedback is nonetheless limited, with a small subset of participants completing the (anonymous) feedback forms. Praise on the course material was received from the industry, public sector agencies, and colleagues from universities in Sweden, Germany, Italy and Switzerland.

7 Conclusions

With the PbD course, we produced and deployed the first open, free, online course on interdisciplinary aspects of privacy, PbD and the GDPR. The course includes legal, technological and IT management perspectives. It is designed to capacitate IT professionals and undergraduate IT students with knowledge required by DPOs. It enables self-paced studies both in and out an academic program.

By opening the course to the general public we not only reach a much broader audience but also opened another channel to collect feedback to our teaching material and methods. By providing the PbD course in the GDPR transition year, we expect to provide an invaluable support not only to all course participants but to the whole society.

References

1. Anderson, A., Huttenlocher, D., Kleinberg, J., Leskovec, J.: Engaging with massive online courses. In: Proc. of the 23^{rd} Int. Conf. on World Wide Web. ACM (2014)
2. Biggs, J., Tang, C.: Teaching For Quality Learning at University. McGraw-Hill Education (2011)
3. Biggs, J.B., Collis, K.F.: Evaluating the quality of learning: The SOLO taxonomy (Structure of the Observed Learning Outcome). Academic Press (1982)
4. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J., Métayer, D., Tirtea, R., Schiffner, S.: Privacy and data protection by design. Tech. rep., Enisa (2014)
5. European Commission: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union (2016)
6. Kongehl, G.: Das Ulmer Modell. Datenschutz und Datensicherheit 31(5) (2007)
7. MacDonald, J.: Blended learning and online tutoring: Planning learner support and activity design. Gower Publishing, Ltd. (2008)
8. Mazur, E.: Peer Instruction: A User's Manual. Series in Educational Innovation, Prentice Hall, Upper Saddle River (1997)
9. Moon, J.: Linking levels, learning outcomes and assessment criteria. In: Ministerial Conf. of the European Higher Education Area (EHEA). vol. 12 (2005)
10. Scriven, M.: The methodology of evaluation. In: Perspectives of Curriculum Evaluation, AERA Monograph Series on Curriculum Evaluation. Rand McNally (1967)