

Data subject access requests as an interdisciplinary learning tool

Carlos Castillo, Gloria González Fuster, Dimitris Kotzinos & Noortje Marres

To cite this article: Carlos Castillo, Gloria González Fuster, Dimitris Kotzinos & Noortje Marres (2026) Data subject access requests as an interdisciplinary learning tool, Cogent Education, 13:1, 2686480, DOI: [10.1080/2331186X.2026.2686480](https://doi.org/10.1080/2331186X.2026.2686480)

To link to this article: <https://doi.org/10.1080/2331186X.2026.2686480>



© 2026 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 25 Aug 2026.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Data subject access requests as an interdisciplinary learning tool

Carlos Castillo^a , Gloria González Fuster^b , Dimitris Kotzinos^c  and Noortje Marres^d 

^aDepartment of Engineering at UPF, ICREA and Universitat Pompeu Fabra, Barcelona, Spain; ^bFaculty of Law and Criminology, Vrije Universiteit Brussel, Brussel, Belgium; ^cETIS Lab UMR 8051, CY Cergy Paris University, ENSEA, CNRS, Cergy, France; ^dCentre for Interdisciplinary Methodologies, University of Warwick, Warwick, UK

ABSTRACT

The General Data Protection Regulation (GDPR) gives data subjects the right to obtain a copy of their data, as well as information regarding the purposes of the processing, categories of personal data collected, recipients to whom this data has been disclosed, data retention periods and whether automated decision-making or profiling have been undertaken. This article describes our experience using data subject access requests (DSARs) as a learning tool in an international higher education setting. Our pedagogical practice centred around a group-based assignment in which students performed DSARs, recorded the fulfilment process, and examined the received data. This format enabled the deployment of DSARs for practice-based learning by students from different disciplinary backgrounds. In the three years during which we have used DSARs in this manner, we have established that they provide a starting point for fruitful discussions regarding the legal and technical aspects of personal data processing. The pedagogical value of DSARs derives from their ability to motivate the students to navigate the complexities of obtaining and understanding data about them held by various platforms. This radically transforms the discussion about data rights from potentially fairly abstract into a tangible, close and relevant exploration of complex categories and concepts.

IMPACT STATEMENT

The practice-based approach presented converts abstract concepts into tangible elements, and enables students to learn not only about their data protection rights, but also about the digital infrastructures the data protection regulation framework regulates, and the way they, as users, are known and influenced by these infrastructures.

ARTICLE HISTORY

Received 22 August 2025
Revised 2 June 2026
Accepted 4 June 2026

KEYWORDS

Interdisciplinary education;
technology regulation; data
protection; personal data;
data access rights

SUBJECTS

Social Sciences; Education;
Curriculum Studies;
Mathematics; Education -
Social Sciences; Teaching &
Learning - Education;
Classroom Practice

1. Introduction

'Data Subject Access Requests' (DSARs) are a fundamental component of data protection law. The General Data Protection Regulation (GDPR) and the United Kingdom (UK) Data Protection Act aim to increase the level of protection granted to individuals' personal data notably by strengthening the exercise of their right of access. DSARs, which lay audiences commonly equate with a request for a mere copy of the personal data about them held by someone else, constitute in reality a broader, richer right. The right does indeed go beyond the right to receive a copy of your personal data, encompassing access to other elements, such as the reasons for processing, the recipients to whom the data has been disclosed, whether automated decisions including profiling have been taken and information on the right to lodge a complaint with a data protection authority. Although the right of access has existed for several decades – being already a core element of early data protection thinking in the 1970s¹, it was reinforced in the last wave of European data protection reform, which expanded the list of elements that must be communicated to data subjects, and also detailed the general modalities applicable to the exercise of data subject rights. Illustrating its almost constitutional importance in Europe, the right of

access is explicitly mentioned in Article 8 of the Charter of Fundamental Rights of the European Union (EU), devoted to the fundamental right to personal data protection.

Any individual can submit a DSAR to a company or organisation that might be processing personal data about them, for free. Data controllers, defined as the entities that determine the purposes and means of the processing of personal data, are then obliged to confirm whether or not personal data processing is taking place. If that is the case, they have to provide the individual with a copy of the data, as well as with a series of pieces of information. The possibility of submitting DSARs for free and the obligation for data controllers to follow up create significant opportunities for their use, not only in research, but also for pedagogical purposes. Submitting DSARs in the context of teaching can enable learning about: 1) *the results of the DSAR process*; that is, what personal data do companies and organisations hold?; which form does the data have (is this a digital archive containing a number of files?); how expected, or unexpected, was such an outcome?; 2) *the DSAR process itself* – how do organisations interact with data subjects in today's digital societies, in particular when confronted with a request?; what variations exist in how different controllers handle the requests?; are there recurrent problems, or best practices?; and 3) *personal data infrastructures in digital societies* – what personal data do organisations routinely collect, how and with what purpose?

Teaching with DSARs is a pedagogical approach that addresses a specific knowledge gap: the disconnect between abstract legal rules and the messy, material reality of data processing. We see that this exercise constitutes an Authentic Learning activity (Herrington & Oliver, 2000), as it relies on a real-world scenario where students interact with actual organisations rather than simulations. Furthermore, we argue that this process connects with the theory of Legitimate Peripheral Participation (LPP) (Lave & Wenger, 1991). Under LPP, learning is understood as a trajectory moving from the edges of a community of practice toward the centre. In our context, the relevant communities of practice are those of data scientists and data protection law specialists. Typically, entry into these communities is gated by employment or internship. However, with these kinds of exercises, the 'licence' to act as a legitimate peripheral participant is conferred by the GDPR – or any other data protection rule – itself. By exercising their legal rights, students are granted legitimate entry to observe, query and analyse the professional practices of data controllers, effectively allowing them to participate in the data ecosystem even if from the periphery.

In this article, we report on a joint pedagogical exercise that we, professors at four different European universities, designed for various courses at the undergraduate and graduate level in computer science, in law and in Science, Technology and Society (STS). Students in all modules undertook the same assignments, with some variations as reported below. The assignment might be understood as promoting 'data literacy,' in particular if such data literacy is not reduced to an uncritical embrace of 'dataism' (Huw, 2022). Potentially serving a variety of data literacies, it was designed to facilitate practice-based learning about multiple aspects surrounding contemporary data practices. We asked students to work in small groups to jointly perform DSARs, track their fulfilment, analyse the output obtained and the process itself within their group, and reflect on their observations and findings within the group and together with the class, as well as together with students from at least one other University, and their instructors. Being a joint activity across institutions in four different countries and across different disciplines, the assignment featured both synchronous and asynchronous elements.

1.1. Learning objectives

The learning objectives of the activity were interdisciplinary, combining technical, legal and social learning, as follows:

1. *Learning about key notions underpinning data processing and data governance*, such as personal data, data access, data control. The assignment allows students to develop a practice-based understanding of abstract principles and rules – including legal rules they might have never directly read before – through a concrete exercise with which they immediately experience a direct, personal link (as it is about their personal data).
2. *Reflecting upon the legal, ethical, social and political aspects of data protection* in a digital society, including learning about data rights and thinking about the principles, values and transformative

ideals associated with these rights and the GDPR as a fundamental rights framework, perceiving the collective dimension of the issues at stake (what is at stake is about their personal data, but also about the data of others – their group, other groups, students in general, other individuals more broadly).

3. *Getting insights into the sociotechnical infrastructures in society*, including how platforms use data technologies such as profiling, the implications for the construction of personhood within digital platforms, and the implications of the application of digital data technologies for organisations and society, including elements of accuracy and accountability (the learning is also about contemporary data practices).

Section 2 provides some background on the GDPR and DSARs. Section 3 describes our methods and interdisciplinary approach. Section 4 presents key results, and Section 5 summarises the lessons learned through this exercise. Section 6 concludes with some limitations and implications of this work.

2. Background: data subject access request (DSAR)

The data subjects' right to submit an access request is a key element of the GDPR; the right is established in the GDPR's Article 15 and its exercise is regulated also by the general requirements applying to data subject rights as described in GDPR's Article 12. Upon receiving a DSAR, a data controller must react without undue delay, and in any event respond to the data subject within one month of receipt of the request. The data controller should first, verify if it holds personal data related to the data subject. If that is the case, the controller should provide them with a copy of all personal data undergoing processing, as well as information stating the purposes for which the personal data is processed, the categories of personal data processed, the recipients of the personal data (or categories of recipients) and the planned retention period (or the criteria for determining that period). Additionally, the data controller must inform the data subjects of their rights, including the rights to rectification and erasure, their right to object to certain types of data processing, how to lodge a complaint, what is the origin of this data (when not provided by the subjects themselves) and whether there is any automated decision-making performed on the basis of this data, including profiling, as well as disclose the logic involved. If data have been transferred to a third country, the data subject must be informed of the relevant appropriate safeguards.

Compliance with DSARs obligations has been the subject of socio-legal research, sometimes carried out precisely by submitting access requests (René et al., 2018). An empirical study published in 2018 (Ausloos & Dewitte, 2018) relying on 60 DSARs (submitted before the GDPR) found that, by and large, these requests were not adequately accommodated by the recipient organisations, which demonstrated 'often flagrant lack of awareness, organisation, motivation, and harmonisation' (p. 20). After the GDPR, persistent shortcomings in compliance with the right of access have continued to be decried (Hase et al., 2024). A 2023 overview of academic research relying on the use of DSARs showed, in general, low levels of compliance (Habu & Henderson, 2023). Limited compliance has also been recorded in relation to the so-called 'right to explanation' partially enshrined in Article 15 of the GDPR (Serveto, 2020).

In recent years, some measures to deal with data access requests have been put in place by most large providers of online services, such as social networking or content streaming services, which now often provide some kind of 'download your data' feature. These provisions, however, can have significant shortcomings: participants in a 2019 focus group study indicated various problems (Veys, XXXX), including lack of tools for filtering, searching and visualising the data contained in personal data files made available for download to platform users. Importantly, these 'data download' tools in most cases contain merely a copy of some of the user's data, but do not include all the personal data undergoing processing, and typically fail to provide other important required elements described in Article 15 of the GDPR.

The usage of some level of automation be it to submit or to manage large volumes of DSARs has notably prompted researchers to explore authentication issues in relation to verifying the identity of the individual submitting the request, and the related possible misuse of DSARs by 'malevolent attackers' (Di Martino et al., 2022).

The use of DSARs for research purposes has unexplored potential (Marres et al., 2019) but it has, at times, encountered resistance. In December 2021, Jonathan Mayer, leading a team of computer science researchers at Princeton University and Radboud University working on a study about ‘Privacy Law Implementation’, had to publicly apologise after receiving numerous complaints and being subject to online backlash. The study the team had launched claimed to investigate the implementation of the GDPR and of the California Consumer Privacy Act (CCPA) by submitting to websites data access requests, which were sent through an automated system. Accused of creating an inappropriate burden on website operators, email system operators and privacy professionals (Ausloos & Dewitte, 2018), Mayer stopped the research and announced the deletion of all obtained data³.

Since the 1970s, DSARs have also been used by activists, with a variety of purposes and often in synchronised ways that multiply their potential and impact. Already in 1976, for instance, following an announcement by the Reader’s Digest of the creation of a mailing list that would have presumably listed all of the households in Sweden, Swedish data subjects were encouraged to submit access requests to the magazine, resulting in 7000 data access requests submitted in a single week (New Scientist, 1976). Research has highlighted that a DSAR can motivate discussions and activism around online privacy, as receiving comprehensive records of one’s own online activities elicits a wide range of emotional responses, from feeling ‘creeped out’ to experiencing confusion, shock and anger (Borem et al., 2024).

The use of DSARs in educational settings is not unprecedented. At the end of the 1990s, researchers at the University of Oslo developed a ‘free internet based program in order to make efficient use of some of the core access rights’ under Norwegian data protection law, which provided background information but also generated access requests, as well as advice for the recipients on how to respond (Schartum, 2001). The tool was described as ‘particularly suitable as an educational tool for colleges and universities,’ including ‘for students in disciplines other than the law’ such as ‘computer science and public administration students’ (Schartum, 2001). Since 2010, the French Association of Data Protection Officers (*Association Française des Correspondants à la protection des Données à caractère Personnel* (AFCDP)) publishes an ‘index’ concerning the evaluation of compliance with the right of access, based on DSARs submitted by participants of a specialised educational programme⁴.

From the background analysis, it becomes clear that in order to fully contextualise the educational value of DSARs, we must look beyond procedural compliance and see if these exercises can throw light on the nature of the data itself, or the different types of data at stake and the relationship between controllers and data subjects. A critical distinction exists between ‘provided’ data (volunteered by the user) and ‘derived’ or ‘inferred’ data (created by the controller *via* analytics). While the latter is often the most valuable for the digital economy – driving profiling and the ‘construction of person-hood’ mentioned in sociotechnical critiques (Cheney-Lippold, 2011) – it is also the most difficult to uncover. Legal scholars note that the ‘right to explanation’ regarding these inferences remains contested and technically opaque (Wachter & Mittelstadt, 2019). This opacity creates a knowledge gap where data subjects are often unaware of the algorithmic identities constructed about them, necessitating a pedagogical approach that digs beneath the surface of simple data files (objective O3).

Furthermore, the DSAR mechanism is at the very core of power asymmetries characterising digital societies. The relationship between data controllers and data subjects can be envisaged as mediated by a ‘black box,’ where the logic of processing is invisible to those it affects. This friction highlights the collective dimension of data protection: while the right is exercised individually, the opaque infrastructures it reveals (or fails to reveal) point to broader systemic issues of accountability and control (Shoshana Zuboff, 2019). Understanding this friction is essential for reflecting on the ethical and political values underpinning the GDPR (objective O2).

3. Methodology

The practice-based educational activity using DSARs described here was developed in the context of a Connected Learning Community facilitated by EUTOPIA – a partnership originally formed by ten European universities and co-funded by the European Union, through the European Universities Initiative. This partnership facilitated the matching across universities to form the learning community, which was named Fairness, Accountability, Transparency and Ethics of Data Processing (FATE).

The four authors of this article are course instructors in four different universities within this partnership, and drew on their complementary expertise in computer science, data protection law and STS to co-create and execute the joint activity.

3.1. General information sheet

At the beginning of the activity, participating students were given a *general information sheet* stating the following:

The general objective of this joint activity is to learn about personal data requests, their limitations and their potential. Specific objectives depend on each course and may include: documenting the process of a personal data request and its obstacles, understanding compliance with the GDPR and potentially other applicable regulations about personal data requests, in particular in an educational setting, understanding the inferences that are made by online service providers, reflecting about the quality and relevance of the data and thoroughly understanding how the obtained data is organised in terms of data types and references.

This general information sheet also outlined the time slots for two important milestones: an initial *talk* on DSARs by a legal expert on the GDPR (one of the authors of this article), and a final student *presentation* of the results to be given in a joint session. These two events were the only synchronous activities in the joint activity, with joint participation by classes from different universities facilitated *via* videoconferencing; everything else took place asynchronously.

3.2. Detailed description

Students in the different modules were also given a *course-specific information sheet* that was adapted for each university to fit each of the different classes and students' levels of expertise. This information sheet provided detailed instructions for performing and analysing data access requests, and detailed a series of intermediate steps, which basically cover a cycle of (1) forming groups, (2) selecting services, (3) anticipating, (4) requesting, (5) redacting and (6) analysing (and possibly visualising) the data.

To ensure group-based learning, the activity was designed to be conducted in teams of 4–5 students per team, and the first step in the activity was accordingly to form small groups.

Second, each student, either individually or as a group decision, was asked to select an online service used by them on (at least) a weekly basis. Examples were provided: a social networking site, a content sharing site, a job search site, a gaming site, an e-commerce platform. Students were asked to consider that the class and/or the instructors would learn that they are users of the online service they chose, and would be asked to disclose to their team portions of the data that the service was processing about them. Next, students were asked to coordinate with the rest of their team in reviewing and finalising this selection. To facilitate comparative analysis, the instruction stipulated that the group interacts with one or two online services at most. This means that all the students within a group did not need to interact with the same service, but they could do so if they chose.

In the third step, students were asked to anticipate what type of data they expected to receive from the selected service, as a way to encourage reflection and comparison. To this end, they were asked to create an inventory, a review that should be as comprehensive as realistically possible, of all the data elements, including categories, types of actions and details of activity traces, that the students expect will be present in the response from each of the different online services to which they had chosen to address their data access request.

Fourth, each student was asked to individually perform two different types of data requests to his/her chosen online service. One request was to be made through a *standard interface* provided by the website/app/platform in question, such as a button to 'download all of your data'. The other request was to be a formal personal data request, making explicit reference to the GDPR, and sent in written form, such as an e-mail (or in some cases through an online form, which some groups of students also made use of). To facilitate analysis, students were asked to keep track of all their interactions with the selected services, including each message sent to or received from the organisation about their requests, recording the date and time of each interaction.

Fifth, upon receipt of personal data, each student was asked to examine the received data package and remove or redact any information they did not wish to share with the rest of their team and/or the instructors.

Sixth, students were asked to analyse the data received and reflect on the process of making data access requests (and visualise it in some cases). To enable this, students were asked to share the data or descriptions of the data with their team, and compare what data they received, and by what means, both across services and within the same service. Students were asked to pay particular attention to data missing in some cases but present in others, irrelevant data, incorrect data and inferences made by the services (and to consider in which cases there was consent for, or awareness of, such inferences).

Students at VUB followed different instructions, as in their case the submission of a DSAR was suggested as an individual activity for all the students of the involved class, while only a sub-group of them actively took part in the EUTOPIA activity. For them, specific reflective tasks were given each year, resulting in the first year in a podcast, and in the second year in a video. The evaluation/grading of the task was done following the course context within each university; details are included in [Appendix 2](#).

3.3. Pedagogical dimensions of the methodological design

The methodology described above was structured around three specific pedagogical dimensions intended to deepen student engagement with the material:

3.3.1. Inquiry-based learning and scaffolding

The transition from Step 3 (Anticipation) to Step 4 (Request) and Step 6 (Analysis) follows an *Inquiry-Based Learning* (IBL) cycle. Rather than presenting the GDPR as a set of static answers, the methodology scaffolds the students' entry into the topic through active questioning. The initial 'course-specific information sheet' provides just enough structure to allow students to navigate the complex reality of raw data files without being overwhelmed. By framing the DSAR as an experimental query rather than a bureaucratic task, students are positioned actively against legal knowledge and its mix with society and technology.

3.3.2. Metacognition through anticipation

Step 3, which asks students to create an 'inventory' of expected data before receiving it, is a specific design choice to trigger *metacognitive conflict*. Research in critical data studies suggests that users often possess a 'folk theory' of algorithms that differs significantly from reality. By forcing students to articulate their expectations explicitly, the methodology sets up a 'moment of surprise' when the actual data arrives. This discrepancy between the anticipated (mental model) and the actual (material evidence) serves as a powerful learning trigger, forcing students to re-evaluate their understanding of datafication.

3.3.3. Collaborative constructivism

The requirement to work in teams and cross-compare results (Step 6) relies on *Social Constructivism* (Vygotsky, 1978). In the context of algorithmic profiling, an individual data set is often unintelligible in isolation. For example, the logic of a platform's categorisation or other inferences only become visible and even understandable through *difference* – by comparing why one student received a certain ad category while another did not. The pedagogical decision to pool data within groups allows students to socially construct a more complete picture of the data situation than any individual could achieve alone, transforming personal data into a shared educational resource.

3.4. Methodological design and educational frameworks

We align the 'messiness' of this exercise – specifically the external delays and platform unpredictability – with *Experiential Learning Theory*. Rather than viewing the (potentially) month-long waiting period as a logistical flaw, we treat it as the 'Concrete Experience' necessary for deeper learning and as a period of reflection on what is expected. As reference (Kolb, 1984) argues, knowledge is created through the transformation of experience; therefore, the frustration of waiting and the emotional impact of seeing one's

own data are vital points. By validating these emotional reactions during the reflection phase, we help students process why they feel safer sharing, e.g. data from the Spotify music service than data from the Tinder dating app, fostering a visceral understanding of privacy boundaries that textbook definitions cannot achieve.

On the other hand, the exercise's configurable design, where students choose between service comparisons or user experience analysis, is rooted in *Inquiry-Based Learning (IBL)*, although some of the elements of the exercise are already described by the instructors. We try to shift the instructor's role from lecturer to facilitator, we allow students to choose their own data, analyse their parameters and formulate their own questions. This approach is particularly effective for addressing data literacy inequities, such as the difficulty of reading/understanding JSON or other 'uncommon' data files. Following the scaffolding principles described in previous work (Hmelo-Silver et al., 2007), we engage in 'just-in-time' teaching – providing tools that help students better understand their data exactly when students need them. This, and working in a group setting, turns potential inequity into a shared problem-solving activity, ensuring students build some additional technical capacity without being overwhelmed.

Finally, this methodology serves as a practice for *Digital Citizenship*, moving beyond internet safety to ethical participation. We implement a strict 'analyse individual / share aggregate' protocol to prevent unwanted effects, where personal data might inappropriately bleed into the classroom setting. This aligns with a definition of digital citizenship that balances rights with responsibilities (Ribble, 2015). By requiring students to protect their peers' raw data while sharing sanitised insights, we are not just teaching privacy regulations; we are actively training them to be responsible data stewards who understand the ethical implications of transparency while they still manage to 'get the job done'.

3.5. Personal data processing

In relation to personal data protection, the issue of consent is sometimes raised. Consent to the processing of personal data is generally not the best legal basis for grounding such processing in the context of educational activities, due to the inevitable imbalance between the instructor and the students (see Recital 43 of the GDPR).

In the context of the described activities, what was deliberately put into place is a by design plan to minimise, and actually prevent, the possible processing of personal data. A key element of this strategy is the presentation and discussion of group results, as opposed to the sharing of personal data obtained through access requests, as stated above. This way, each student (as data subject exercising their access request) can make sure their personal data is not processed by any other person—it is the findings of the exercise that are shared. Other additional elements put in place to mitigate risks for students included oral instructions recalling the need to not share personal data during the class discussions, and that instructors took notes to provide feedback at the group level, and not at the individual level.

4. Activity results

The activity using DSARs as a pedagogical tool ran during different terms at the different universities. It was integrated into the following four diverse modules: one undergraduate computer science module related to fairness and transparency in data processing; a graduate module on 'Data Protection and New Digital Tools,' part of the MA of 'Political Ideas in the Digital Age (PIDA)'; a module on Privacy and Data Protection Law of the Masters of Law of the Faculty of Law and Criminology; a STS module taught as part of an interdisciplinary postgraduate degree on data visualisation. Students in all modules undertook the same assignments, but because the modules ran in different terms, each edition of the joint activity included two or three universities paired according to the overlaps in their teaching schedules. As described in Table 1, to date, the joint activity has been done six times. Over 30 groups, comprising more than 150 students, have taken part.

The rest of this section is organised as follows. First, we describe which services were chosen by students (§4.1). Second, we summarise the way and times in which they fulfilled the requests (§4.2). Third, we point out some elements of the students' analysis of the received data (§4.3).

Table 1. Courses and semesters in which the activity took place (/F = fall, /S = spring).

Course (level)	University	'22/F	'23/S	'23/F	'24/S	'24/F	'25/S	'25/F	'26/S
Fairness, Accountability, Transparency and Ethics of Data Processing (Undergraduate)	UPF		√		√		√		√
Data Visualisation: Science, Culture and Public Policy; Digital Sociology (Master)	WU		√		√		√		√
Data Protection and Digital Tools (Master)	CY	√		√		√		√	
Privacy and Data Protection Law (Master)	VUB	√		√		√		√	

4.1. Services chosen

A broad array of platforms/services were selected by the students for the DSAR. These included social media platforms, online banking services, public transport services and a university app. Service selection seems to be guided by two main criteria: whether more than one student in the group used the service in question in their daily lives, and whether students felt comfortable sharing some of the personal data received during the exercises with their fellow students.

We include a list of the services chosen by the students across the different editions of the activity:

- Social networking platforms: Discord, BeReal, WhatsApp, Twitter/X, LinkedIn, Instagram, Snapchat and Weibo.
- Online banking platforms: Monzo, WeChat Pay, Apple Pay and Revolut.
- Streaming and video sharing: Spotify, YouTube, Bilibili, TikTok, Netflix and Prime Video.
- Mobility and maps: Uber, Google Maps, Trainline and Navigo⁵.
- Shopping sites: Amazon, Uber Eats and IZLY⁶.
- Dating apps: Hinge and Tinder.
- Healthcare: La Meva Salut⁷ Doctolib⁸
- Other platforms: Indeed Job Search, OpenAI/ChatGPT, Firefox browser, Reach PLC media and My-'WU'.

4.2. Fulfilment process

Student presentations highlighted the following reflections regarding the different modalities for making a DSAR, as well as the response type and response time from services.

The GDPR does not require people to disclose why they ask for the data, but some requests, particularly those done by e-mail to smaller platforms, were answered in puzzling ways. Some platforms asked what the data subject needed the data for. Some platforms scrambled to find the data.

Many students requesting the data by e-mail were answered simply with the address of the online dashboard from where they could download their data. Some received no reply, others received automated replies. In one case, a student received an email that was intended for a different student in the same group who performed a similar request.

Most requests were answered within the one-month time limit. Many students received replies in one week, especially if the request concerned one of the large multinational technological companies. Smaller organisations were rather ignorant of the process and in one case they returned only the account information of the student without any of the transactions involved.

Overall students noted that the ease and transparency of the DSAR process varied greatly between organisations: while some offered an online template for making a DSAR, in other cases, one student noted, 'access opportunities are difficult and hidden.' Students noted that digitally native services such as Spotify made available greater volumes of data to their users, while retail, transport services, and other 'brick-and-mortar' organisations provided lower volumes of information, but through a more personalised medium, namely email.

Table 2 depicts an example of a timeline of events recorded by one of the groups when performing three DSARs from three different platforms (in this case Apple, Monzo and WeChat).

4.3. Data received

Requests made using the 'download your data' feature in many cases contained merely a copy of some personal data, but failed to contain more descriptive details such as the purposes for the data processing or instructions on how to lodge a complaint with a data protection authority.

Table 2. Recording of key dates of the DSAR from one of the groups, 2023 (University 2).

Apple	Monzo	WeChat
22 Feb. Request data <i>via</i> the official Apple website	24 Feb. Access transaction data on Monzo ✓	22 Feb. Request WeChat wallet data from the platform ✓
23 Feb. Offline inquiry/request in an Apple store	02 Mar. Request data <i>via</i> email, was requested to provide a proof of identity	02 Mar. Request data <i>via</i> email
27 Feb. Data acquired, but not the expected data ×	06 Mar. Get information needed	03 Mar. Receive instructions for individual's data requesting process
02 Mar. Request data <i>via</i> email, but no response up to now ×	07 Mar. Receive an email confirming the request ✓	

The obtained data revealed different levels of complexity. Most data sets contained multiple files, and in the case of DSARs submitted to online platforms like Spotify and YouTube, multiple directories and sometimes a 'start here' file in HTML that users could open directly. When digging deeper into the contents, the students sometimes found codes that they struggled to interpret. Students reflected on the extent to which data formats revealed expectations about user characteristics: some services returned machine readable '.json' files, while others provided '.csv' or plain text files, revealing different assumptions about the levels of digital literacy expected of data subjects.

Students also reflected on the type of data they received, taking a special interest in data pertaining to inferred attributes such as generational categories, consumer preferences and car ownership. They considered the divergences in ontological status of these attributes: while some are based on device detection (e.g. recording that a streaming service was accessed from a car's stereo) others appear to involve inference (e.g. determining that a user is interested in fashion).

Students also considered the quality of the data received, particularly data about inferences. These were often found to be inaccurate (one student was incorrectly assigned the category 'pet owner,' another was labelled as having 'affinity for electric vehicles'). A student requesting data from a music streaming website was amused to find out that the service had incorrectly inferred that she/he was interested in aquariums, particularly those with goldfish.

Students were, in general, surprised about the amount and detail of the data contained in the provided files, and the third parties their data had been given access to. Some observed that the volume and quality of data received from the same platform varied from student to student, noting that this was likely connected to the different privacy settings selected by the students in question, as well as the length of time they had been using the service and the country the student initiated the use of the platform from. For the latter, students coming to Europe from non-EU countries reported differences in the provided data for the time before and after residing in the EU.

Students also reflected on interpretability and discoverability: some of the received data is more memorable than others, comparing 'songs played' to account information in the case of Spotify. Google's search history includes information about advertising, something the user would not be likely to record themselves.

Many student groups considered the type of organisation, and how this affected their capacity to respond to data access requests: a payment provider, they noted, is only an intermediary, so payments are recorded but not the products/services purchased. They reflected on inequality implications, as smaller organisations would be more likely to lack the resources to process DSARs.

For some students, it was not clear which forms of personal data access qualify as data access requests. They asked: 'is requesting a "bill" (transaction overview) from WeChat a data access request?' 'Does DSAR mean receiving information beyond what is routinely available through the web interface?'

Appendix 1 (Figure A1) shows artwork created by one student of the data visualisation course depicting the data request process. Most of the visualisations were created to depict the process, rather than the outcome.

5. Lessons learned

This section presents some of the lessons learned by students and instructors while conducting these activities. First, we present some lessons learned about the activity itself (§5.1). Then, we present lessons learned per objective (§5.2). Finally, we present discipline-specific lessons learned (§5.3).

5.1. Lessons learned about the activity itself

The *Experiential Learning* and *Authentic Learning* aspects of this activity indeed requires us to deal with the ‘messiness’ of interactions with external actors. Hence, students need to be given enough time for this activity. First, they need time to form groups and have an initial meeting to agree on the platforms they will do the data request from, particularly if they are asked to make sure that at least two students in each group query the same platform. Second, they need time to wait for the requests to be fulfilled, and while the GDPR specifies a one-month period and in practice many requests are answered within a few days, students may need to do some back-and-forth with the data controller in some cases, particularly smaller organisations. Third, they need time to do the analysis and/or visualisation, depending on the complexity of the requested deliverable.

Regarding the choice of platforms, we observed that most groups selected streaming platforms, as those would reveal music/movie tastes, but nothing considered more sensitive by the students. However, in some cases students chose dating apps and online banking sites, which arguably hold more sensitive data – this may point out at different privacy choices regarding their group of peers and their instructor. The work was delivered to instructors and peers through documents and oral presentations in which students provided overviews of their project design, the data collection process and their findings and reflective insights. They did not share their entire data and instead choose specific examples to showcase. Students shared a selection of the collected data among participants in their small peer group, but they did not share their data packages with instructors or with other students in their course. The whole context of the activity foregrounds concerns on data privacy, but nevertheless we believe we should continue to stress in future editions that each student should analyse their own data individually and share their analysis results with the rest of the group, but not their data. Based on the discussion in class, they already seem to be largely doing this.

There was also considerable variability in the comparative frameworks chosen by different groups: while some chose to compare different services in the same category (e.g. two streaming platforms) in terms of response times, ease of data access and data volumes, other groups chose to compare user experiences. This indicates a degree of configurability of the research design for this exercise, which is arguably expected in IBL, and this we consider a strength of this exercise.

We observed that the formats in which the data were provided, while challenging to navigate in some cases, were mostly legible by students across disciplines. In other words, data formats were partially transparent and partially opaque across the board, but in varying degrees. For natively digital services, there was often a ‘start here’ file in HTML or PDF that all students could open directly on their computers. There are also various online tools to, for instance, display a file in a machine-readable format such as JSON⁹ in an indented presentation that is easier to read. Developers commonly refer to these tools as ‘pretty print’ tools. However, especially in the case of online platforms, there were often also obscure data files, and particularly data elements, that students could not interpret.

5.2. Lessons learned per objective

5.2.1. Learning about categories/concepts (O1)

We did not perform a formal evaluation of their learning of concepts, such as a written exam, although students in one university wrote a project report after the group presentations had taken place. However, the overall emphasis in the assignment-based activity is on practice-based learning. In such an approach, collaborative project development, supported by in class discussions, enables *Experiential Learning*, i.e. ‘learning through doing’: students develop their understanding of high-level concepts such as personal data and data access rights by exploring how they apply in relation to their own digital practices, and learn about the potential, benefits and challenges of data rights by examining their (imperfect) operationalisation in personal data access provisions scripted into online services and platform architectures. The structured presentation format enables students to demonstrate their understanding through the communication of the research process and its results.

These group presentations also provided the lecturers with the opportunity to review student learning and to identify common elements and striking aspects of the research design, findings and reflective

insights. During group project presentations and subsequent group discussions in class, lecturers took observation and interpretation notes. Based on these notes taken in 2023 and 2024 during group presentations by students at UPF and WU- and supported by a review of the student presentation slides that several groups provided to us on a voluntary basis – we can report the following qualitative insights.

5.2.2. Reflecting on the personal data economy (O2)

While students were obviously aware that platforms and services collect data from them, the group assignment enabled them to grasp the specific features of this process. As one 2024 WU student put it: ‘Spotify knows my car, what devices I own and what generation I belong to.’ A 2024 UPF group reported a similar finding: my Spotify profile mentions ‘In car listening ... it knows I was listening in my Volvo.’ Other groups too commented on the depth of data storage. A 2024 WU group noted: ‘Selfie verification is stored in Hinge!’ By contrast, students who had investigated a Chinese social media platform, emphasised in their presentation the relatively superficiality of the data they had received: ‘the only data provided was CV copies, message history and a very small amount of demographic data, no inferences and no mention of third parties.’

Students indicated that they did not have beforehand a robust understanding of the categories of data collected from them. They did expect the data to contain the main business objects (e.g. the list of songs streamed), and some identifying information (e.g. name and e-mail address), but as discussed the data packages also contained other elements at high levels of granularity, such as inferences about their potential interest in specific products and services that were not specifically related to the platform that they queried.

By conducting DAR as a group, students were able to detect by comparison relevant features of personal data management as well as the gap between their own expectations and the evidence of personal data capture by digital services – in the process engaging in a joint construction of meaning. One group (2024, WU) compared the data profiles of long-time Spotify users with recent subscribers, with the former including comparatively more individual-specific details. They also observed that different privacy settings seemed to affect whether Spotify data profiles included inferences or not. Another group equally noted that ‘if you change the privacy settings, you receive more data.’ Regarding the inferences in Spotify personal data, one group commented on the relative lack of accuracy: ‘Spotify data includes inferences, but many of these are inaccurate, as in the case of the wrongly identified pet owner.’

Several student groups noted the relative ease of downloading personal data profiles *via* the online dashboards of platform services as compared to the requesting personal data *via* email. online services. In 2024 A UPF group noted that ‘Requesting data via email takes a lot more time to receive data,’ while another UPF group summed up the situation succinctly as ‘easy - automatic; hard - via email.’ A WU group observed in 2023 regarding a major platform (YouTube/Google): ‘The email address provided did not exist in one case. in another case, we kept receiving an automated response in reply to our emails.’ The assignment then lead students to discover for themselves how digital services have responded to the GDPR by installing generic web-based forms without facilitating more personal, such as email-based interaction with data subjects.

Conducting DSAR enabled students to reflect on what qualifies as personal data, and what does not. One group compared payment services (WeChat, Monzo and Applepay) and asked ‘requesting a bill from WeChat, is this a personal data access requests?’ Conducting international comparisons of this type, also enabled them to explore how different legal and regulatory regimes affect the collection of personal data. As one group noted: ‘WeChat collects data across functions – from messaging to social media to e-commerce and health code while in the UK the law prevents this kind of mixed function.’ By contrast, a 2024 presentation from WU of ApplePay found that no personal data was provided, as Apple Pay indicates that ‘What you buy, where you bought it, and how much you paid is sensitive information. Apple doesn’t store, sell, or use any of that information.’

Students also offered insightful reflections on the relation between personal data access and data literacy: while some services – like the Spanish supermarket Bonpreu – offered ‘all info in one PDF’, others like Spotify provided access to more detailed information in the form of JSON files. This UPF group

(2024) inferred that the infrastructures of personal data access created by tech companies seem to be biased toward the computationally literate. They noted that more revealing details, such as inferences, tend to be included in JSON files. In the case of one social networking platform (BeReal) to which users are supposed to upload one photo per day, the platform was found to record not only that the user uploaded a photo, but also how many previous takes of that photo the user made before uploading the final one. Another UPF (2024) group offered this general conclusion: '[Personal] [d]ata not understandable for non-experts.'

5.2.3. DSAR as an instrument for user-centred evaluation of technologies (O3)

The above discussion also makes it clear that, when the data contained inferences, particularly inferences about interests, several student groups were able to judge the quality of such inferences, and it was evident that some of these inferences were incorrect. This can only be judged by each data subject, which suggests that it is a good idea that each person examines carefully their own data.

On the other hand, working as a group made it possible for students to reflect on the 'double function' of personal data requests, as in the case of a WU (2023) group presentation on LinkedIn data collection and analysis which included career inferences and inferred interests. They noted that 'you gain insight into the data they hold on you, but at the same time you also gain insight in the type of analysis the organisation performs.' A student in a different group (WU, 2024) offered a similar insight: 'we saw this with Spotify.' They queried whether inferences – such as 'loves cats,' 'belongs to GenZ' – tell us more about the person, the services, both?

The exercise also enabled that to think critically about the assumed empirical validity of personal data collection by online services and platforms. A WU group in 2024 challenged the assumed authenticity of the information contained in their personal data profile. They observed about Instagram: 'the personal data included topic tags, so we could use this data to answer the question: who are we according to Instagram?' However, they observed that this data inevitably was the result of obfuscation, as they remembered deleting content and blocking accounts. Challenging the empirical status of personal data, this group asked the students listening to the presentation: 'Do you feel inclined to evaluate if its true?'

It was also clear in some cases that platforms that seem to be monolithic from the user perspective actually demonstrate more variation and implement their analytic capacities internally in different ways for different purposes. For instance, in the case of Amazon, depending on the particular part of the store being queried, the obtained data was different and/or organised differently.

5.3. Discipline-specific and interdisciplinary learnings

University courses at all levels, but particularly undergraduate, rarely provide the opportunity to interact with students from other disciplines. The complementarity between the ways in which different students approached the exercise were evident, which helped us drive the message that issues at the intersection of technology, law and ethics cannot be studied on a disciplinary island. It also seems to build confidence about the possibility of meaningful exchange and mutual learning across disciplinary boundaries.

In addition to the lessons learned per objective described in the previous section, below we identify some lessons learned that are to an extent discipline-specific.

5.3.1. Computer science students

Computer science students tended to compare the structure and contents of the data files at a deeper level than other students. There were some disparities between the data received, e.g. some files that were present in a data package were absent in another. Sometimes those disparities were attributed to having created an account at a different time, or from a different country, in the case of students who created their account before moving to the country where they are currently attending university. In other cases, these disparities did not have any apparent explanation.

5.3.2. Social science students

Social/political science students engaged with the exercise worried about the technical aspects of the returned results, but also with questions about the social elements of the DSARs. Graduate students

come from diverse scientific backgrounds, which added another interesting element in the discussion. They are also coming from diverse countries all over the world, which provided the ability to explore the differences in the returned data (after a DSAR) when an account started in a different country (especially outside of the EU). They also worked on commenting different aspects of the process and the difference between smaller, local companies and larger, multinational tech companies and the way they handle the DSARs.

5.3.3. Law students

For law students studying data protection law, it is interesting to be confronted directly with the question of whether the services that they use, or the institutions that have data about them generally, appear to comply or not with the studied legal obligations. Typically, students realise that compliance levels are not perfect, be it for instance in terms of compliance with transparency obligations or with the responses to the requests as such. This, in turn, leads to several other important questions, and most notably questions about access to remedies and enforcement. In relation to access to remedies, students are triggered to wonder what data subjects can do to demand compliance, and which kind of additional steps might need to be taken into account in that case (e.g. collecting evidence in an appropriate manner). Regarding enforcement, students are led to think about whether enforcement is sufficient and how it could be improved.

5.3.4. STS students

Students demonstrated awareness of the data access requests opening up multi-actor constellations, involving digital infrastructure, data practices, users of varying literacy levels, service models and so on. Several of their presentations investigated how the implementation of DSARs varies widely across platforms, and in some cases offered some interesting insights gained into the platform and data protection practices of their own university. They noticed how in small organisations DSARs were handled by a single individual (not a team of individuals), and that they were reviewed individually and handled in a manual manner. This was contrasted with large online platforms queried, where data access procedures included some level of automation.

5.3.5. Interdisciplinary learning

Notwithstanding the disciplinary variations in approach among the student bodies noted above, there was significant continuity among the presentations, with similar research designs and insights presented by student groups in the different universities. Some of this overlap was facilitated by the relatively detailed project brief and standardised deliverable (the expected content of student presentations was specified on a slide-by-slide level), which means that students in the different universities could anticipate the other presentations to a high degree. The degree of similarity, overlap and resonance between presentations prepared without any prior communications between university groups was nevertheless impressive. As already suggested, in educational contexts where interdisciplinary exchange is still relatively rare, our exercise offers valuable opportunities for building trust in cross-disciplinary exchange and communication.

6. Conclusions

6.1. Key recommendations

The practice-based approach to data rights adopted in our exercise enables students to learn not only about their data protection rights, but also, at the same time, about the digital infrastructures the data protection regulation framework regulates, and the way they, as users, are known and influenced by these infrastructures. In addition, by making data access requests, students learn relevant skills that may help them educate others in how to exercise data protection rights and how to understand the results of the DSARs, placing them in a good position to teach this to others and be a reference for others.

Although the activity can only be carried out in a jurisdiction where similar data subject rights are granted, it is important to highlight that across Europe it can also be deployed in courses comprising

significant levels of international students, as the nationality of the data subjects does not matter for GDPR purposes.

Making the exercise work in practice, in any case, requires taking into account a series of considerations. From an educational perspective, we emphasise the following important aspects:

- As a first step, it is crucial that at least basic information is provided to students. Indeed, the design of the exercise needs to be preceded by a lecture and a discussion on what is a DSAR and what it means to submit a DSAR. It was observed that students kept mistaking a DSAR for a simple request for some data and were not insisting on requesting the full spectrum of information they were entitled to obtain. Nevertheless, information should and cannot be exhaustive, attempting to preempt any problems they might encounter, as encountering such problems is typically part of the experience of submitting a DSAR.
- DSARs take time. Although some data might be easily obtained quickly, submitting an actual request might be followed by weeks of wait, which is part of the exercise. The exercise thus requires some time to be completed fully and correctly. This needs to be carefully planned to allow the students the time to make the DSAR, wait, potentially send reminders, hopefully receive relevant results and analyse them.
- Privacy and data protection issues that might emerge require thinking in advance about the implications of specific data requests, including decisions regarding eventual sharing (be it with their team, the whole class, or even with other classes or instructors). In the context of the exercise, there are risks that students over-share, consciously or not (e.g. by inadvertently including some data in a screenshot), or feel pressured into providing data that might be interpreted in different ways by different people. It is thus crucial to encourage students to proactively consider these implications, but also to stress it is not necessary to share the received data with others. To cope with this, we allowed students to process their data individually and share and compare with the group their results, in order to reach a common understanding and common conclusions at the end. Additionally, instructors must ensure there is no unnecessary data processing, for instance by not recording student presentations.
- Interdisciplinary exchange matters. Discussion with the participation of students from different disciplines and from different countries is always invaluable. It functions in general as an invitation for students to consider which dimensions of data processing they might be missing. Often, exchanges illustrate common concerns and practices, allowing students to move from the anecdotal (e.g., thinking they had difficulties receiving a reply due to the idiosyncrasies of their national administration) to the structural and systemic.

6.2. Challenges, tensions, risks and limitations

Using DSARs in an educational setting triggers certain challenges, tensions and risks and doing so in an interdisciplinary, inter-institutional and international manner can reinforce some difficulties.

6.2.1. Overwhelming data controllers

First, when a relatively large group of students is invited to submit DSARs, there might be a risk that a large number of students would decide to submit the request to the same data controller. Depending on the data controller, and especially if they are a small company or organisation, receiving at the same time a large number of requests could hinder their ability to react – or they could be tempted to use the fact that they received numerous requests to try to justify delays. This should in principle not be a problem if the instructors guide and frame the selection of controllers as described above, limiting the number of requests submitted to each controller. A specific challenge – and a related dilemma – might surface in relation to submitting requests to institutions close to the students and the instructor, such as, for instance, their own university. While this can have a specific pedagogical value, as discussing data practices by their university can be of great interest for students, it might eventually generate tensions, especially if numerous requests are regularly submitted in the context of the activity. Instructors should think about this in advance and assess possible implications and mitigation strategies.

6.2.2. Challenges regarding the disclosure or not of the purpose of the request

Second, it is possible to debate whether students should – perhaps at some point of the procedure – disclose the fact that they are submitting the request in the context of an educational activity. If they do so, there is a risk that this might alter the reaction by the data controller. If they do not do so, there is a risk that the data controller might nevertheless at some point realise this, perhaps during an exchange with the student, and use the fact that this information was hidden as an argument to contest the genuine nature of the request. Data protection law does not require DSARs to serve a particular purpose, and does not in any case allow data controllers to derogate from their obligations merely because the request would have been submitted in the context of an educational activity. Nevertheless, ethical considerations might require weighing carefully the pros and cons of providing the information to the data controller, at least perhaps in some cases and at some later stage of the procedure (for instance at the end of the exercise), for their information.

6.2.3. No answer or very limited data and information are a real possibility

The set up of the exercise embraces the fact that after submitting a DSAR, in practice, the student might obtain no reaction at all, or at least within the time frame of the exercise; equally, it could be that they receive some data or some information, but that the obtained data and information are very limited. This might be regarded as an interesting finding for the students, but it limits what can be learned from the data and the information. The fact that students work in teams reduces the risk of them having no access to any data, as they could eventually work with the group's results. In any case, instructors should not penalise students not receiving a reply or receiving less information, and for instance encourage instead a deeper study of publicly available information, such as in data protection notices – as an alternative transparency tool.

6.2.4. Student engagement across countries requires special attention

Beyond disciplinary borders, students from different classes and institutions can feel a significant distance with the other students, and perhaps be less comfortable in the language used for exchanging (in our case, English) or with public speaking. Making them feel comfortable but also sustaining their attention can be especially challenging when exchanges are taking place online. A measure to be considered is to create mixed groups or at least foresee time for exchange in a set up different than in front of a whole unknown class, lowering possible barriers hindering questions and comments.

In terms of limitations, it is fundamental to keep in mind that the design of the activity is not directed toward research, and the activity does therefore not allow to draw any conclusions on the state of DSARs compliance as such.

Notes

1. For an early explanation of the importance of the right of access in European data protection law, see reference (Braibant, 1976).
2. See, for instance, O'Malley arguing that 'As a person working in the privacy community, it is beyond frustrating that small teams can drain the resources of thousands of professionals around the world for the purpose of their own research' (O'Malley, 2021)
3. See formal announcements: <https://privacystudy.cs.princeton.edu/>
4. <https://afcdp.net/index-du-droit-d-acces/>
5. Paris area public transport, more at <https://www.iledefrance-mobilites.fr/>
6. Food purchasing app for students in France, more at <https://www.izly.fr>
7. Catalan public healthcare portal, <https://lamevasalut.gencat.cat/>
8. French app for booking doctors' appointments, more at <https://www.doctolib.fr>
9. ECMA-404 The JSON Data Interchange Standard. See, e.g. <https://json.org/>

Acknowledgements

We are thankful to all of our students for their participation. This research was partially supported by the Connected Learning Communities program at EUTOPIA MORE, co-funded by the European Union under Grant Agreement No. 101089699.

Author contributions

CRedit: **Carlos Castillo**: Conceptualization, Investigation, Project administration, Writing – original draft, Writing – review & editing; **Gloria González Fuster**: Conceptualization, Investigation, Writing – original draft, Writing – review & editing; **Dimitris Kotzinos**: Conceptualization, Investigation, Writing – original draft, Writing – review & editing; **Noortje Marres**: Conceptualization, Investigation, Writing – original draft, Writing – review & editing.

Disclosure statement

The authors report there are no competing interests to declare.

Funding

This research was partially supported by the Connected Learning Communities program at EUTOPIA MORE, co-funded by the European Union under Grant Agreement No. 101089699.

ORCID

Carlos Castillo  <http://orcid.org/0000-0003-4544-0416>
 Gloria González Fuster  <http://orcid.org/0000-0002-3452-3737>
 Dimitris Kotzinos  <http://orcid.org/0000-0002-3678-4092>
 Noortje Marres  <http://orcid.org/0000-0002-8237-6946>

Data availability

Data sharing is not applicable to this article. No datasets were created or analysed in this qualitative study.

References

- Ausloos, J., & Dewitte, P. (2018). Shattering one-way mirrors—data subject access rights in practice. *International Data Privacy Law*, 8(1), 4–28. <https://doi.org/10.1093/idpl/ipy001>
- Borem, A., Pan, E., Obielodan, O., Roubinowitz, A., Dovichi, L., Mazurek, M. L., & Ur, B. (2024). Data subjects' reactions to exercising their right of access. *33rd USENIX security symposium (USENIX security)*, 24 (pp. 2865–2882). USENIX.
- Braibant, G. (1976). The citizen's right of access to his personal file. *Proceedings of the OECD seminar, 24th to 26th June 1974, organisation for economic cooperation and development (OECD) (Policy issues in data protection and privacy concepts and perspectives)* (pp. 147–158). OECD.
- Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture & Society*, 28(6), 164–181. <https://doi.org/10.1177/0263276411424420>
- Di Martino, M., Meers, I., Quax, P., Andries, K., & Lamotte, W. (2022). Revisiting identification issues in GDPR 'Right of Access' policies: A technical and longitudinal analysis. *Proceedings on Privacy Enhancing Technologies*, 2022(2), 95–113. <https://doi.org/10.2478/popets-2022-0037>
- Habu, A. A., & Henderson, T. (2023). Data subject rights as a research methodology: A systematic literature review. *Journal of Responsible Technology*, 16, 100070. <https://doi.org/10.1016/j.jrt.2023.100070>
- Hase, V., Ausloos, J., Boeschoten, L., Pfiffner, N., Janssen, H., Araujo, T., Carrière, T., de Vreese, C., Haßler, J., Loecherbach, F., Kmetty, Z., Möller, J., Ohme, J., Schmidbauer, E., Struminskaya, B., Trilling, D., Welbers, K., & Haim, M. (2024). Fulfilling data access obligations: How could (and should) platforms facilitate data donation studies? *Internet Policy Review*, 13(3), 1–37. <https://doi.org/10.14763/2024.3.1793>
- Herrington, J., & Oliver, R. (2000). 2000. An instructional design framework for authentic learning environments. *Educational Technology Research and Development*, 48(3), 23–48. <https://doi.org/10.1007/BF02319856>
- Hmelo-Silver, C. E., Duncan, R. G., & Chinn, C. A. (2007). Scaffolding and achievement in problem-based and inquiry learning: A response to Kirschner, Sweller, and Clark (2006). *Educational Psychologist*, 42(2), 99–107. <https://doi.org/10.1080/00461520701263368>
- Huw, C. D. (2022). Rescuing data literacy from dataism. In M. Currie, J. Knox, & C. McGregor (Eds.), *Data justice and the right to the city* (pp. 146–164). Edinburgh University Press.
- Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.
- Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge university press.
- Marres, N., Spencer, M., & González-Fuster, G. (2019). Rights as methodology: Next steps in data-intensive research at the intersections of technology, law and society. *Centre for interdisciplinary methodologies (CIM) blog* (2019). University of Warwick.

- O'Malley, C. (2021). *DSAR probing 'attack' from Princeton researchers*. <https://medium.com/lucid-privacy-group/dsar-probing-attack-from-princeton-researchers-553f0d50cd29>. Medium (2021).
- René, L. P., Mahieu, H., Asghari, & M., van Eeten. (2018). Collectively exercising the right of access: Individual effort, societal effect. *Internet Policy Review*, 7(3), 1–23. <https://doi.org/10.14763/2018.3.927>
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.
- Schartum, D. W. (2001). Technology to improve exercise of privacy rights: A Norwegian example. *Privacy Law and Policy Reporter*, 7(8), 153–155. <https://classic.austlii.edu.au/au/journals/PrivLawPRpr/2001/2.html>
- Serveto, M. M. (2020). Exercising GDPR data subjects' rights: Empirical research on the right to explanation of news recommender systems. *The European Data Protection Law Review*, 6(2020), 593. <https://doi.org/10.21552/edpl/2020/4/17>
- Shoshana Zuboff. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
- news Scientist. (1976). *Swedes gag on readers' digest data bank*. New Scientist.
- Veys, S. Daniel Serrano, Madison Stamos, Margot Herman, Nathan Reiting, Michelle L Mazurek, and Blase Ur. (2021). Pursuing usable and useful data downloads under { GDPR/CCPA } access rights via { co-design}. *Seventeenth symposium on usable privacy and security (SOUPS 2021)* (pp. 217–242). USENIX.
- Vygotsky, L. (1978). Social constructivism. *Mind in society*. Harvard.
- Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review* 2019, 2, 494–620. <https://doi.org/10.7916/cblr.v2019i2.3424>

Appendix 1



Artwork

Figure A1 shows artwork made by one of the students, illustrating the request process.

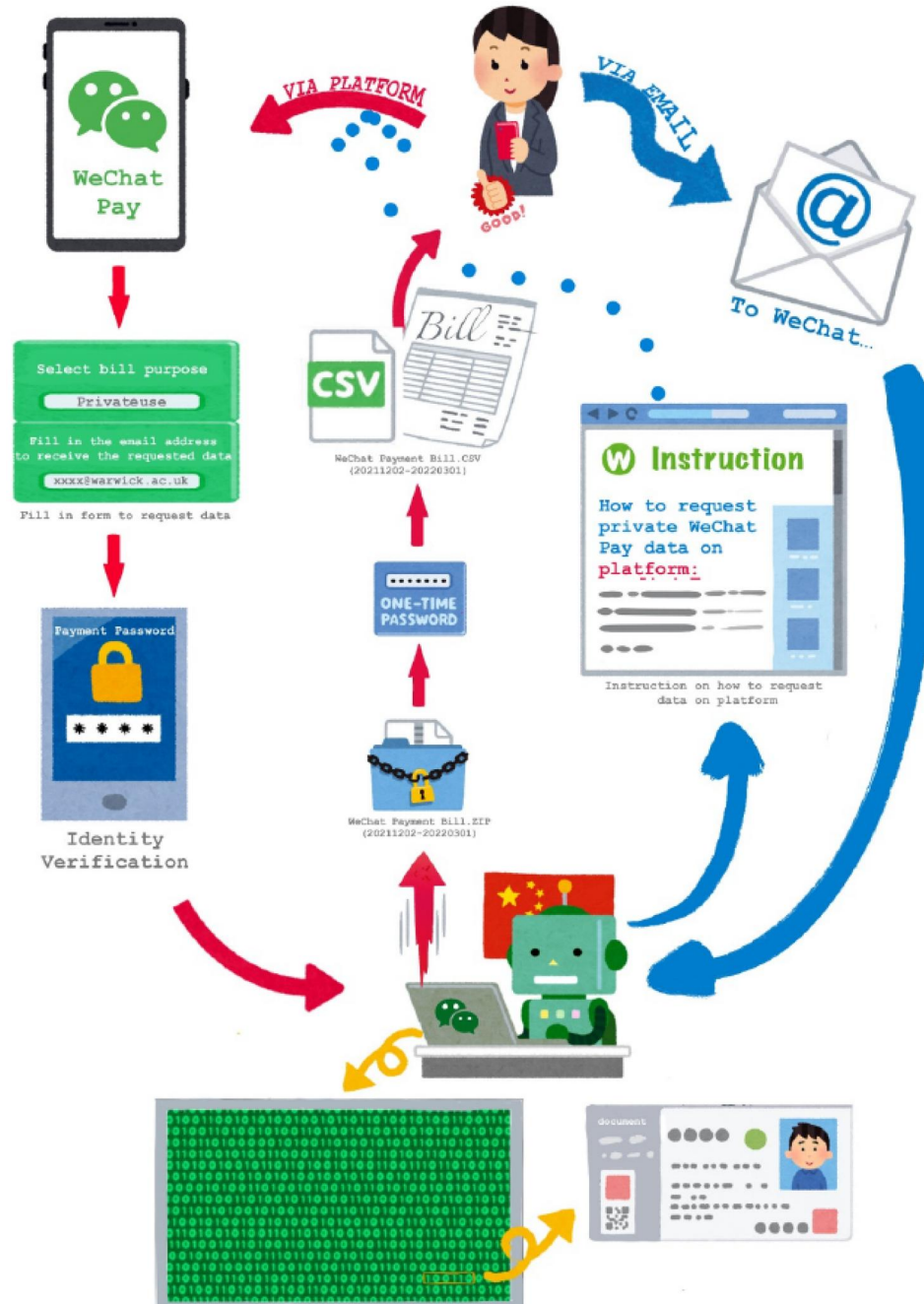


Figure A1.

Appendix 2

Evaluation

This section contains course-specific details on how the activity was evaluated.

2.1. Delivery format and grading

The course-specific information sheets described how students should deliver their work and how their work would be graded. All groups were asked to prepare slides for a 10 min-presentation. Additionally, students taking the module on data visualisation at WU were asked to prepare a visualisation of the DSAR process or outcome. The classes at WU and CY were also asked to prepare a report (of about 1500 words at WU and up to 6-pages per group at CY). The grading was different depending on the delivery format. At UPF, where only slides had to be produced, this was weighted at about 5% of the students' final grade. At CY and WU, where slides and a report had to be produced, this was weighted at about 20% of their final grade.

2.2. Alternative task for law students

The involvement of VUB students took into account that, due to administrative reasons, their participation had to remain voluntary, and that it could not be taken into account for the official grading of the course. In light of this, what was proposed – in addition to a general invitation to all course students to submit DSARs and several accompanying sessions to critically discuss their experiences – as to participate in two distinct accompanying tasks, that motivated students could voluntarily join. In the first year, a team explored the legal issues around the use of DSARs as an educational tool, based on their knowledge of the GDPR and produced a short podcast that is now available online.¹ In the second year, a team focused on using DSARs to explore how companies were processing data about their mobility, and produced a video that aims to reach non-GDPR experts as well.² To reward their contribution, microcredits were awarded to participating students.

¹ <https://eutopia-university.eu/english-version/education/eutopia-learning-communités/fairness-accountability-and-transparency-in-data-processing>

² 'Demystifying the GDPR: A Journey Through the Right of Access.' Available online: <https://www.youtube.com/watch?v=wEHwuAWgpBA>