Curriculum on Data Protection

University of Education Freiburg

January 2025

Lucie Brzáková, Deborah Krzyzowski, with Bernd Remmele, and Zlatko Valentic

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents

1. Introduction

Digital technologies pervade every aspect of our private and public lives, and the capitalization of personal information online made privacy a valuable good –for corporations, the government, and for individuals[1]. Safeguarding personal data with data minimisation principles and data protection measures is the crucial concern in consequence.

DataPro is a project within the Erasmus Plus program of the European Union and recognizes the need to cultivate young citizens' understanding of the value of their data, their privacy rights, and measures for data protection. In the three years of project duration, the transdisciplinary partners will develop learning tools on data protection for students. This curriculum will dive into the three mentioned areas of data use and protection, and grants teachers and partners insight into the concepts operationalized in the educative tools.

The broader goal of the DataPro project is hence, to support teachers with a comprehensive educational framework that helps students in becoming active and autonomous digital agents. Conscientizing the students about the value of their data as a good, and the value of their own privacy for democracy are the underlying intentions behind teaching data protection methods. By educating students on the multifaceted nature of data usage and the critical importance of protecting personal information, DataPro seeks to cultivate a well-informed citizenry equipped to uphold and advocate for their data rights.

This Curriculum sets forth specific learning goals. These goals are to be realized with a series of competencies that enhance students' understanding of data protection complexities and the recognition of privacy as a human rights issue. Through a structured approach involving the collection, adaptation, and development of innovative learning tools, DataPro wants to integrate theoretical knowledge and practical understanding. This initiative not only focuses on disseminating these resources among schools and educational stakeholders, but it also emphasizes integration of students' and teachers' concerns and feedback. Another advantage of the learning tools is their

[1] See 'surveillance capitalism' in Zuboff, S. (2018) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Zuboff, Shoshana*. Available at: http://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019 (Accessed: 10 January 2025).

encouragement of students to become digital agents. In such role, they would be equipped to identify and protect themselves from digital threats. For example, false influence through digital disinformation or coordinated data attacks using social engineering tactics.The Curriculum is also considering previously researched learning hurdles like the desensitizing effect of everyday use of the internet on online privacy[2]. Based on the current English version of the Curriculum, the syllabi will be translated for the target groups of respective countries.

By integrating this curriculum into educational settings, we envision nurturing a generation that is not only aware of the importance of data protection but also skilled in implementing best practices. This foundational knowledge is expected to foster the students' societal attitudes towards data protection and privacy rights for the development of informed, responsible digital citizens.

2. Competencies in focus within DataPro

The Data Protection Curriculum informs teachers and partners about the essential knowledge young citizens need to navigate the complexities of data protection. Central question of the project is the competencies students need to securely tackle digital challenges. Young people grow up in an environment where data plays a central role, whether through social media, online learning, or digital communication. However, many lack awareness of the risks and rights associated with using digital technologies. The DataPro project aims to develop playful and creative learning tools for students to develop mechanism for safe management of their data.

As introduced in previous chapter, the envisioned areas of competence are based on the knowledge of data as a good; encompassing data processing mechanisms, capitalization of personal information online, algorithmic recommendation systems, and inferences from online behaviour to name a few. In upcoming section, the Curriculum presents a comprehensive scheme that sets the implications of data as a good into context for individuals and society. Given that data is the good in question, the scheme also includes relevant competencies students must acquire to successfully protect their data online.

[2] Krzyzowski, D. (2024) *Report on Quantitative Analysis of Survey Data*. Freiburg: University of Education Freiburg, p. 21-23.

The Curriculum orients itself on the DigComp Framework[3], while several feedback loops with education professionals were implemented in its development. Advice from consortium members, data protection experts, and especially teachers was obtained. This should ensure suitability of the educative tools for the target group being secondary school students.

Starting point of the Curriculum is casting light on the obscured economic value of personal data. Based on this crucial premise, the importance of privacy rights for healthy democracies, and data protection for individual autonomy of the citizens of such societies is stressed. The Curriculum integrates named three topic areas to ensure that students acquire the skills to protect their privacy and act responsibly in the digital space. The interrelated dynamics between these topics of data protection will be explained in Section 4., aided by visualization in a Competence Matrix (*Figure 1*).

3. Competencies Description

The DataPro competencies are structured along three topic areas that cover differing implications of digital data:

1. **Data as a Good**: the 'what' of the project. The object of protection is personal data online that is being commercialized and handled as an exchangeable good by online service providers, and online platforms.

2. **Privacy as a Human Right**: the 'why' of the project. The societal importance of protecting the good in question because of the vital role individual privacy plays for the exercise of fundamental rights in democracies.

3. **Data Protection**: the 'how' of the project. After user-oriented sensibilization for aforementioned topics of data capitalization and online privacy, practical measures for students to protect their data can be introduced. These measures are means for more autonomy online and self-efficacy in exercising one's rights.

Specific competencies needed to navigate these interrelated topic clusters are covered in the upcoming section.

[3] EU Science Hub and European Commission (2022) *DigComp Framework*. Available at: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en.

3.1 Data as a Good

'Data as a good' is the premise behind the pressing importance of education on data protection. Privacy has been a point of political debate since governments and the press documented information about their citizens[4], yet algorithmic advertising and data harvesting for insurance made data an exchangeable currency for free online services. DataPro seeks to explain such mechanisms of the data industry to encourage students to benefit from the value of their data. Recognition of the economic value of data is possible when students acquire the following competencies:

Competencies Cluster A.	Practical Measures
A.1 **Translate Data into an Asset**	***Treating Data like an Online Currency*** Understand the value of their personal data, like how they value money. This includes recognising when and which data is processed by online services, understanding how personal data may be monetised, knowing the risks of the exploitation of personal data, and making informed decisions about sharing their data. ***Monetisation Awareness*** Learn about the main ways companies make money from personal and aggregated data, such as through advertising platforms and improving targeted advertising (including political ads). Be aware that many free communication services (like social media) and online content are paid for by advertising or the sale of user data. This economic model relies on monetising personal data.
A.2 **Distinguish Security Risks of Data Sharing**	***Public Sharing*** Understand that anything shared publicly online (e.g., images, videos, sounds) can be used to train AI systems, which may include

[4] For the historical development of the discourse on privacy rights, refer to Warren, S.D. and Brandeis, L.D. (1890) 'The Right to Privacy', *Harvard Law Review*, 4(5), pp. 193–220. Available at: https://doi.org/10.2307/1321160.

	undesirable tracking functions. Be cautious about the extent of your public data sharing. ***Data Minimisation Practice*** Regularly question the necessity of keeping and sharing personal data. Adopt practices such as only providing essential information and using disposable email addresses or phone numbers when appropriate. ***Security Measures*** Be aware of common social engineering attacks (phishing) through various communication channels to prevent the fraudulent acquisition of (digital) assets.
A.3 **Evaluate Intentions behind Data Monetization**	***Critical Evaluation*** Regularly ask who is behind the information found on the internet, especially on social media. Identify who might have an interest in creating echo chambers (bubbles). ***Quality Awareness*** Understand that misinformation can be highly convincing, especially with the use of advanced technologies like AI which can create sophisticated visualisations. Always question the quality and source of information.
A.4 **Awareness of Behaviour Control**	***Mechanism Awareness*** Be aware that many digital platforms use psychological tactics such as nudging, gamification, and manipulation to influence user behaviour. Recognise these tactics to avoid being unduly influenced. Recognise that usage patterns and connected devices can be used to optimise online services and targeted advertising. This involves tracking user behaviour to deliver personalised content.

	Control Measures Learn strategies to control and limit the extent of behavioural tracking, such as adjusting privacy settings and using privacy-enhancing technologies. Develop strategies to diminish these influences, such as setting personal limits on usage and critically evaluating the content being consumed.

3.2 Privacy as a Human Right

From a general education perspective, the dimension of 'Privacy as a Human Right' stresses the significance of private life, and informational self-determination both for individuals and democracies. The *Universal Declaration of Human Rights* protects every individual's "privacy, family, home or correspondence" from any kind of "arbitrary interference"[5]. As a negative example, these rights are seriously infringed through illegitimate use of spyware by governments as the case of *Pegasus* confirmed[6]. Privacy as a human right helps students to contextualize their own online privacy within their life as a member of a (European) democracy. The special status of privacy, and a private life protected from state and corporate interference should also conscientize about the value of individual autonomy for the whole of society. Privacy is therefore a core pillar for other values of democracy, like freedom of expression and informational self-determination. Only in the absence of control, be it by the government, institutions, or powers of the private sector, may individuals form autonomous opinions and express them in democratic discourse. Privacy can therefore be conceptualized as the absence of recordable knowledge about the individual, a status in which they may experience obscurity of their selves from officials and authorities[7].

[5] See Article 12 in United Nations (1948) *Universal Declaration of Human Rights*. United Nations. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[6] United Nations General Assembly (2022) *The right to privacy in the digital age*. Report of the Office of the United Nations High Commissioner for Human Rights* A/HRC/51/17. Human Rights Council, pp. 2. Available at: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

[7] Compare to the conceptualization of privacy as obscurity in Selinger, E. and Hartzog, W. (2016) 'Obscurity and Privacy', *Spaces for the Future: A Companion to Philosophy of Technology* [Preprint]. Available at: https://scholarship.law.bu.edu/faculty_scholarship/3099.

Competencies Cluster B.	Practical Measures
B.1 **Understand the Scope of Liberty**	***Recognizing Freedom*** Recognize the importance of privacy for your freedom. By protecting your privacy, you safeguard your ability to express opinions freely and live without unnecessary interference. Be mindful that when others can observe or control your behavior, your personal freedom may be at risk.
B.2 **Understand Self-Determination**	***Data Control*** Remember, you have the right to control what data about you is collected, processed, and used. Exercising this right helps you maintain your personal autonomy and stay in charge of your digital identity. ***Automation Protection*** Be aware that data protection includes the right not to be subjected to fully automated decision-making processes that can significantly affect individuals. ***Misuse Prevention*** Protection of personal data helps guard against unwanted surveillance, identity theft, discrimination, and other forms of misuse of personal data. Be aware of common social engineering attacks (phishing) through various communication channels to prevent the fraudulent acquisition of (digital) assets.
B.3 **Knowledge on Privacy Rights (GDPR)**	***Data Rights and Consent Necessity*** Know your rights against companies using your data, including the right to access data held about you, rectify inaccuracies, erase data (Right to Be Forgotten), and lodge complaints with authorities.

	Understand that companies generally need to obtain your consent to handle your personal data. Regularly evaluate whether it is necessary to give such consent. ***Consent Evaluation*** Frequently assess the necessity of giving consent for data usage to ensure that your personal information is not exploited unnecessarily.
B.4 **Human Rights' Awareness**	***Digital Responsibility*** Be aware of your responsibility to safeguard human dignity, freedom, democracy, and equality while acting on the internet. This involves respecting the privacy and data rights of others and advocating for responsible data practices.
B.5 **Assess Risks to Individual Privacy**	***Risk Levels*** Understand that there are varying levels of privacy risk associated with different data practices. Some data processes, particularly those involving AI, carry higher risks. ***AI Risks*** Be aware that AI-based processes and services can pose different levels of risk to privacy, often due to their ability to process large amounts of data and infer sensitive information.
B.6 **Assessing the Internet's Potential**	***Recognize Internet Duality*** One should be aware that the internet creates new opportunities for participation in society for vulnerable groups, but it can also contribute to the isolation of those who do not use it.
B.7 **Review Privacy Policies**	***Policy Evaluation*** Develop the ability to review and judge the privacy policies of apps and services critically. This includes understanding what data is collected, how it is used, and the rights you have regarding your data.

3.3 Data Protection Measures

'Protecting Data' is the overall learning aim of the Curriculum. This dimension builds upon the understanding of topic clusters 1: Data as a Good, and 2: Privacy as a Human Right. Competencies within cluster 3. refer to practical data protection and cyber security measures that may be taken by individuals on an everyday basis.

Competencies Cluster C.	Practical Measures
C.1 **Identity Management**	***Usage Awareness*** Regularly question how and where to use and share personally identifiable information securely. Understand the risks associated with sharing personal data. ***Anonymity Measures*** Use measures to hide your identity online, such as VPNs, encrypted communication tools, and privacy-focused browsers.
C.2 **Ensuring Data Security**	***Security Measures*** Employ standard security practices, such as using different strong passwords for different online services, enabling multi-factor authentication, using biometric locks, performing regular software updates, and installing protection software. ***Secure Identification*** Learn to secure your electronic identification through methods like strong, unique passwords and two-factor authentication.
C.3 **Examine Online Trackability**	***Tracking Management*** Implement measures to limit and manage the tracking of your activities on the internet, including the use of browser extensions that block trackers and cookies. ***Communication Controls*** Know and use measures to stop receiving unwanted messages or emails, such as spam filters and email rules.
C.4 **Information Validation**	***Source Checking*** Be prepared to consult multiple sources to verify information. This helps in recognising and understanding different points of view or biases behind particular information and data sources.

	Bias Recognition Learn to identify potential biases in information, understanding that every data source can have an inherent bias based on its origin or purpose.
C.5 **Mutual Data Protection**	***Data Sharing Consideration*** Regularly question whether personally identifiable information of others is being shared and whether it could be misused. ***Legal Awareness*** Be aware that sharing information about others can have serious legal consequences. Always seek consent before sharing someone else's personal data.

4. Relationships between Competencies

The competencies needed for self-determined and responsible use of online services can be sorted into the three presented topic clusters. The clusters are interdependently connected. *Data as a Good* and *Privacy as a Human Right* overlap in weighing the (legitimate) interest of data-driven companies against one's privacy. The Curriculum addresses the balance between corporate interests in data utilisation and individual privacy rights. This shall help learners understand the broader implications of data economics, like information asymmetries and power imbalances between society, corporations and the state[8].

Data Protection Measures and *Privacy as a Human Right* overlap in the pragmatics of how to protect individual data while considering the privacy rights of others. This means that the Curriculum not only envisions teaching individuals how to safeguard their own data but also instils a respect for the data privacy of others. Mutual practice of care about personal data conceptualizes privacy as an interdependent good in democracies rather than a simple personal preference. The recognition of interdependency helps students to understand that not caring for their own privacy also leads to an

[8] See for example van de Waerdt, P.J. (2020) 'Information asymmetries: recognizing the limits of the GDPR on the data-driven market', *Computer Law & Security Review*, 38, p. 105436. Available at: https://doi.org/10.1016/j.clsr.2020.105436.

erosion of privacy right in broader society, and that upkeeping online privacy for themselves and others strengthens democracy.

The tautology is completed by the relationship between *Data Protection Measures*, and *Data as a Good*. These dimensions overlap in the pragmatics of how to utilise one's data in the light of information asymmetries. This intersection focuses on the practical skills needed to manage and leverage personal data responsibly and effectively in various contexts.

The dynamics and dependencies between the dimensions of data protection education are visualised in the following Competence Matrix (*Figure 1*.). The Curriculum does not discriminate in importance of competencies from one dimension over competencies from another dimension. Every competency, and its interplay with other competencies are considered equally fundamental for self-efficacy and freedom of individuals in an information society. These essential skills, and the underlying understanding of the three dimensions of data protection, are deemed necessary for individuals to navigate the digitally interconnected world effectively and responsibly.

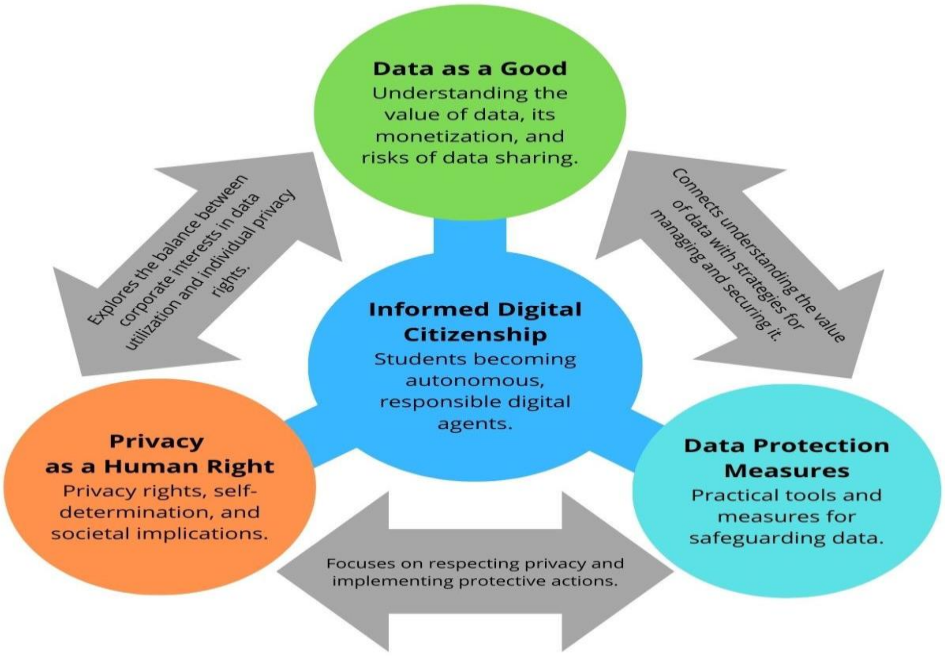
Data as a Good
Understanding the value of data, its monetization, and risks of data sharing.
Explores the balance between corporate interests in data utilization and individual privacy rights.
Connects understanding the value of data with strategies for managing and securing it.
Informed Digital Citizenship
Students becoming autonomous, responsible digital agents.
Privacy as a Human Right
Privacy rights, self-determination, and societal implications.
Data Protection Measures
Practical tools and measures for safeguarding data.
Focuses on respecting privacy and implementing protective actions.

***Figure 1:* Competence Matrix.** The diagram shows the three topic clusters ("Data as a Good," "Privacy as a Human Right," and "Data Protection Measures") forming a triangle. At the centre is the overarching goal, "Informed Digital Citizenship," connected to all dimensions to signify its integration and reliance on their interplay.

5. Broader Learning Outcomes

Among the overall goal of educating students to make informed decisions as digital citizens, an indirect learning outcome should be the recognition of malevolent behaviour online. This might include cyber security attacks like phishing or ransomware. Further, attacks on democratic freedom and discourse might be harder to distinguish as in the form of disinformation campaigns. Such issues are not a central topic of the Curriculum yet are seen as subordinated advantages when mastering the DataPro competencies. Hence, knowing how online platforms profit from their users' attention, both positive and negative, presupposes the awareness of *Data as a Good*. Such knowledge might help students to critically examine sensational headings and manipulated information, equipping them with tools to identify and tackle misinformation online. Connecting competencies from cluster A: *Data as a Good*, to cluster B: *Privacy as a Human Right* therefore fosters democratic awareness and resilience to attacks like disinformation.

Knowing the mechanisms of data trading and implementing data minimisation practice helps students to protect themselves from behaviour control. Behaviour control mechanisms are omnipresent on online platforms, in e.g. algorithmic advertising, and algorithms that seek to capitalize attention through increasing screen time on the service. The interdependency between cluster A: *Data as a Good* and cluster C: *Data Protection Measures* is supporting the students' autonomy and self-determination online.

When it comes to cyber security, cluster B: *Privacy as a Human Right*, and cluster C: *Data Protection Measures* intersect. Making the interconnection between the value of online privacy, and practical measures to protect it helps students to build resistance to deceptive practices. Negative examples for the lack of online privacy would be the exploitation of personal information by e.g., authoritative states or organized crime. Strengthening students against deception means throughout understanding of privacy risks and hands-on ways to keep their online privacy with the help of competencies from cluster C.

6. Conclusion for Educators

To relay to learners a critical awareness of digital technologies, encouraging their beneficial an effective use, teaching the competencies from clusters A, B, and C are crucial. Based on the DigComp Framework[9], following key takeaways from the Curriculum shall be points of orientation for educators:

Protecting Devices and Digital Content:

- Educate learners on safeguarding digital devices from threats like malware and physical damage, using antivirus software, regular updates, and secure passwords.
- Teach learners to identify and respond to threats such as phishing, ransomware, identity theft, and cyberbullying.

Understanding Safety and Security Measures:

- Instruct on safe browsing habits, two-factor authentication, and using secure networks like VPNs.
- Emphasize the importance of protecting personal data, understanding what to share online, and managing strong, unique passwords.

Protecting Personal Data and Privacy:

- Highlight the importance of avoiding sharing sensitive information on insecure websites and understanding privacy policies of digital services.
- Teach how to set privacy settings on social media and other platforms.

Safe Use and Sharing of Personal Information:

- Educate on securely sharing personal information, encrypting sensitive data, and recognizing the potential harm from improper data use.

[9] EU Science Hub and European Commission (2022) *DigComp Framework*. Available at: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en.

Understanding Privacy Policies:

- Explain the significance of privacy policies in digital services and teach learners to read and understand them for informed decision-making.

Avoiding Health Risks:

- Instruct on mitigating health risks from prolonged digital device use, such as eye strain, poor posture, and mental health impacts.

Protecting Against Digital Dangers:

- Educate on identifying, avoiding, and reporting cyberbullying, online predators, and other harmful behaviors.

Promoting Social Well-being and Inclusion:

- Highlight the positive aspects of digital technologies in fostering social connections and inclusive practices.

Environmental Impact Awareness:

- Teach the environmental implications of digital technologies, including electronic waste and energy consumption.

Monitoring and Safeguarding Well-being:

- Actively monitor online activities to ensure well-being and intervene when necessary to prevent harmful behaviors.

Be prepared to take immediate action against threats to learners' well-being, such as cyberbullying.

Enable learners to value their data like money

- One important aspect that is not addressed in the DigiCompEdu based Framework, namely in the current activities, is the value of data as an asset.