Co-funded by
the European Union

Curriculum on data protection

Bernd Remmele, Zlatko Valentic

University of Education Freiburg

Freiburg 2024

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

Introduction

In an era where digital technologies pervade every aspect of our lives, the safeguarding of personal data emerges as a crucial concern. DataPro, a pioneering educational initiative under the Erasmus Plus program of the European Union, recognizes the imperative need to encourage a deep understanding of data protection as a fundamental human right among the younger generation. This curriculum is designed to address the intricate landscape of data use and protection, aiming to empower students with the knowledge and tools necessary to navigate this complex field.

Our society is increasingly data-driven, with vast amounts of information being processed daily, impacting individual privacy and collective security. Set against this backdrop, the DataPro project offers a comprehensive educational framework to enlighten young minds about the significance of data privacy and the ethical considerations it entails. 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.

The curriculum sets forth a series of objectives and specific goals aimed at enhancing students' understanding of data protection complexities and its recognition as a vital 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 also emphasizes the active engagement of students and teachers in a dynamic learning process.

The anticipated impact of DataPro is profound. 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 enhanced privacy measures and influence broader societal attitudes towards data protection and privacy rights in our increasingly digital world.

Through its structured methodology and collaborative efforts under the auspices of the Erasmus Plus program, DataPro is committed to achieving these outcomes, thereby contributing significantly to the development of informed, responsible digital citizens. This curriculum serves as a beacon for educational innovation, guiding young individuals towards a future where they are capable and confident in protecting their data in an interconnected digital age.

1. Preamble

The Data Protection Curriculum, part of the DataPro project under the Erasmus Plus program of the European Union, aims to equip young people with the essential knowledge and skills to understand and navigate the complexities of data protection. The curriculum is based on a comprehensive competence matrix, divided into relevant educational fields. The following sections provide a detailed overview of the curriculum's structure.

In today's digital world, protecting personal data is of paramount importance. 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 a comprehensive educational solution that enables students to manage their data competently and securely.

The curriculum reflects topical fields, each covering specific competences and considering previously researched learning hurdles. Based on the curriculum, country-specific syllabi will be adapted for each target group. The training prototypes in WP3 will build on the theoretical foundations of these WP2 results.

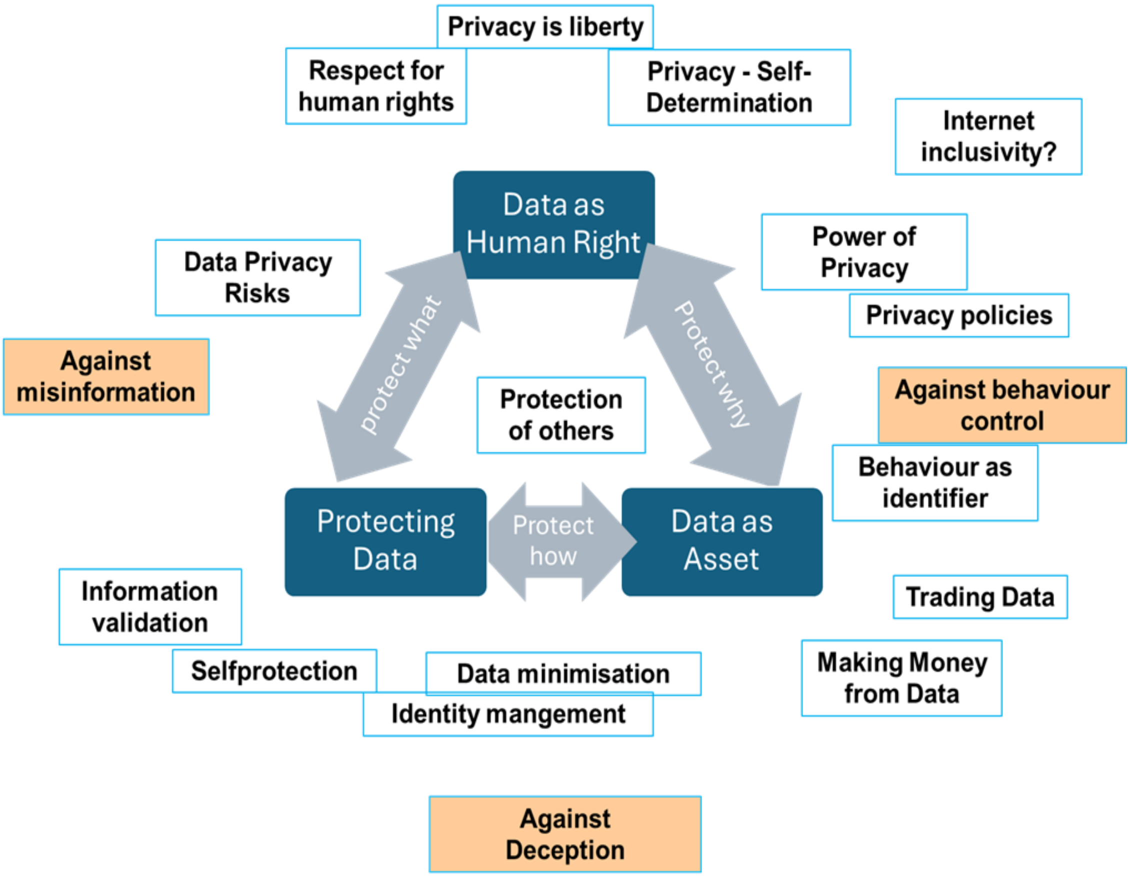
While the curriculum draws heavily from the DigComp Framework[1] its selective development included several feedback loops with consortium members and data protection experts, ensuring it is comprehensive and practical. It conveys on the one hand that data protection is both an individual right and a practice including risks for others as well as on the other hand that data have an often hidden economic value. The DataPro curriculum integrates these dimensions to ensure that students acquire the skills to protect their privacy and act responsibly in the digital space.

[1] https://joint-research-centre.ec.europa.eu/digcomp/digcomp-framework_en

Co-funded by the European Union

2. Competence Description

In the following section, the curriculum is described using the provided graphic, which serves as a visual representation of the competence matrix. The DataPro Curriculum is structured in three overlapping fields: ***Data Protecting***, ***Privacy as a Right***, and ***Data as a Good***. It reflects the requirements of an active, autonomous, and responsible member of a democratic, data/information-driven market society.



The curriculum focuses on three interrelated topics:

- ‘Protecting Data’ is the most obvious part as it refers to the practicalities of data protection and cyber security as understood in many guidelines.
- ‘Data as Human Right’ – from a general education perspective – refers to the significance of informational self-determination as a human right.

Co-funded by the European Union

- ‘Data as Asset’ takes an economical stance, on the one hand, to explain how the data industry works, and on the other, how individuals can benefit from the value of their data.

Thus overall the competencies can be clarified by answering the following three questions: A. How can I protect my private data (and my trust in information)? B. What makes data protection a human right? C. What makes data valuable (economically)?

The three foci are not separate dimensions, they overlap heavily. Data Protecting and Privacy as a Right overlap in the pragmatics of how to protect 'what' and the consideration of the privacy rights of others. This means that the curriculum not only teaches individuals how to safeguard their own data but also instills a respect for the data privacy of others.

Privacy as a Right and Data as a Good 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, helping learners understand the broader implications of data economics.

Data Protecting and Data as a Good overlap in the pragmatics of how to utilise one's data. This field focuses on the practical skills needed to manage and leverage personal data responsibly and effectively in various contexts.

The DataPro Curriculum does not have competence levels because the list of competencies provided is considered fundamental for an information society. These essential skills and understandings are deemed necessary for individuals to function effectively and responsibly in a digitally interconnected world.

Competences to recognize and handle malevolent behaviour on the internet are specifically highlighted.

Co-funded by
the European Union

A. How to protect my private data (and my trust in information)?

To protect your private data and maintain trust in information, consider the following learning objectives, which focus on empowering students to navigate the digital world more securely and responsibly.

A.1 Identity Management:

a) *Secure Identification*: Learn to secure your electronic identification through methods like strong, unique passwords and two-factor authentication.

b) *Usage Awareness*: Regularly question how and where to use and share personally identifiable information securely. Understand the risks associated with sharing personal data.

c) *Anonymity Measures*: Use measures to hide your identity online, such as VPNs, encrypted communication tools, and privacy-focused browsers.

A.2 Selfprotection:

a) *Communication Controls*: Know and use measures to stop receiving unwanted messages or emails, such as spam filters and email rules.

b) *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.

c) *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.

A.3 Against Misinformation:

a) *Critical Evaluation*: Regularly ask who is behind the information found on the internet, especially on social media. Identify who might have an interest in

Co-funded by the European Union

spreading fake news, such as social bots, hate speech propagators, or those creating echo chambers (bubbles).

b) *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 Information Validation:

a) *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.

b) *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.

A.5 Protection of Others:

a) *Data Sharing Consideration*: Regularly question whether personally identifiable information of others is being shared and whether it could be misused.

b) *Legal Awareness*: Be aware that sharing information about others can have serious legal consequences. Always seek consent before sharing someone else's personal data.

A.6 Data Minimisation:

a.) *Necessity Questioning*: 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.

A.6 Against Deception:

a.) *Security Measures*: Be aware of common social engineering attacks (phishing) through various communication channels to prevent the fraudulent acquisition of (digital) assets.

B. What makes data protection a human right?

In concern of Data protection as a human right consider the following learning objectives, which focus on stundent’s understanding of data protection and its implications:

B.1 Privacy is Liberty:

a.) *Freedom*: Privacy is essential for liberty as it allows individuals to express their opinions freely and live without undue interference. If others can observe or control behavior, personal freedom is compromised.

B.2 Privacy - Self-Determination:

a) *Data Control*: Everyone has the right to decide what data about them is collected, processed, and used. This right to self-determination is crucial for maintaining personal autonomy.

b) *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.

c) *Misuse Prevention*: Protection of personal data helps guard against unwanted surveillance, identity theft, discrimination, and other forms of misuse of personal data.

B.3 Power of Privacy:

a) *Data Rights*: 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.

b) *Consent Necessity*: Understand that companies generally need to obtain your consent to handle your personal data. Regularly evaluate whether it is necessary to give such consent.

c) *Consent Evaluation*: Frequently assess the necessity of giving consent for data usage to ensure that your personal information is not exploited unnecessarily.

B.4 Respect for Human Rights:

a.) *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 Data Privacy Risks:

a) *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.

b) *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 Internet Inclusivity:

a.) *Awareness of 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 Privacy Policies:

a.) *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.

C. What makes data valuable (economically)?

As Data has significant economic value affecting also students, consider the following learning objectives, which rather focus on a general economic understanding:

C.1 Making Money from Data:

a) *Revenue Models*: 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).

b) *Service Economics*: Recognise that most free internet services are provided by profit-oriented companies, which often monetise user data to generate revenue.

C.2 Behaviour as Identifier:

a) *Data Usage*: 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.

b) *Control Strategies*: Learn strategies to control and limit the extent of behavioural tracking, such as adjusting privacy settings and using privacy-enhancing technologies.

C.3 Against Behaviour Control:

a) *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.

b) *Control Measures*: Develop strategies to diminish these influences, such as setting personal limits on usage and critically evaluating the content being consumed.

C.4 Trading Data:

a) *Monetisation Awareness*: 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.

b) *Public Sharing*: Understand that anything shared publicly online (e.g., images, videos, sounds) can be used to train AI systems, which may include undesirable tracking functions. Be cautious about the extent of your public data sharing.

Co-funded by the European Union

3. Conclusion for Educators and their Competences

To relay to learners a critical awareness of digital technologies, encouraging their benefical an effective use, the following competences based DigiCompEdu Framework[2] are crucial:

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.

[2] Digital Competence Framework for Educators (source: https://joint-research-centre.ec.europa.eu/digcompedu_en)

Co-funded by the European Union

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. Therefore, we would like to add: **Valuing Data as an Asset.**

Learners should be taught to understand the value of their personal data, similar to how they value money. This includes recognising the importance of protecting their data, understanding how it can be monetised or exploited, and making informed decisions about sharing their data.