



Co-funded by the
European Union



DIRECT

Digital Responsibility
Education and Training

DR CONCEPTUAL FRAMEWORK REPORT

Deliverable D 2.1

Revision: 2.1

Revision date: 8.9.2026

Author(s): Henriette Blom, Nikolaus Obwegeser,
Marie Peskova

Name of Organisation: BFH

Place: Bern, Switzerland

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.



Deliverable Factsheet

Project number:	101185365-DIRECT-ERASMUS-EDU-2024-PI-ALL-INNO-EDU-ENTERP
Project acronym:	DIRECT
Project Title:	Digital Responsibility Education and Training
Work Package:	WP2
Work Package Leader:	BFH
Title of Deliverable:	D 2.1: DR Conceptual Framework Report
Dissemination Level:	PU/SEN
Editor(s):	Henriette Blom, Nikolaus Obwegeser, Marie Peskova
Reviewer(s):	Pantelis Papadopoulos, Elli Papageorgiou, Maria Ganopoulou

Version History

Version	Date	Comments
0.9	10.03.2026	For internal review
0.9	30.03.2026	Received comments from internal reviewers
1.0	15.04.2026	Final deliverable shared internally
1.0	11.05.2026	Feedback and Amendments received during consortium meeting (Bern)
1.1	10.06.2026	Revised version shared internally
2.0	17.06.2026	Final revision internally approved
2.1	8.09.2026	Revised after PO comments



Table of Contents

1 Introduction	5
1.1 Purpose and scope	5
1.2 Positioning work package 2 in DIRECT	5
2 Background and synthesis for conceptual framework development.....	6
2.1 Definition of Digital Responsibility.....	6
2.2 Related concepts.....	7
2.3 Analysis of DR principles	8
3 Digital Responsibility Competence Framework.....	11
3.1 The dimensions and levels.....	11
4 Mapping DR principles to ESCO.....	14
4.1 Principle: Make it fair	17
4.1.1. Promote inclusion.....	17
4.1.1.1 Participatory co-design with underrepresented communities.....	17
4.1.1.2 Designing for the digital divide	17
4.1.1.3 Inclusive language, representation, and culturally responsive defaults.....	18
4.1.2. Promote the principles of democracy and the rule of law	18
4.1.2.1 Process and contestability in automated decision-making	18
4.1.2.2 Information integrity against manipulation (prebunking).....	18
4.1.2.3 Designing for democratic participation and deliberation	19
4.1.3 ICT accessibility standards.....	19
4.1.3.1 Standards-conformance evaluation	19
4.1.3.2 Accessible-by-default authoring	20
4.1.3.3 Assistive-technology and disabled-user testing	20
4.1.4 Promote human rights implementation	20
4.1.4.1 Human Rights Impact Assessment	20
4.1.4.2 Privacy- and data-protection-by-design	21
4.1.4.3 Access to remedy and expression safeguards in content governance.....	21
4.2 Principle: Make it good.....	22
4.2.1 Protect the environment from the impact of digital technologies.....	22
4.2.1.1 Measure and reduce the energy and carbon footprint of software and digital services	22
4.2.1.2 Extend ICT hardware lifespan through repair, refurbishment and circular procurement	22
4.2.1.3 Apply eco-design principles to digital products and services	23
4.2.2 Operate open source software	23
4.2.2.1 Evaluate open-source alternatives against proprietary solutions for a specific business need	23
4.2.2.2 Assess and comply with open source license obligations before adoption and distribution.....	24
4.2.2.3 Manage open source dependencies and supply-chain risk in operational use.....	24



4.2.3 Corporate sustainability	24
4.2.3.1 Conduct a double materiality assessment to prioritize sustainability issues	24
4.2.3.2 Apply a recognized sustainability reporting framework to disclose performance	25
4.2.3.3 Set science-based targets and integrate them into operational decision-making	25
4.2.4 Data ethics	26
4.2.4.1 Apply pseudonymisation and anonymisation techniques to protect personal data	26
4.2.4.2 Identify and mitigate bias and fairness risks in datasets and algorithmic outputs	26
4.2.4.3 Design meaningful transparency and consent mechanisms for data subjects	27
4.3 Principle: Make it safe	27
4.3.1 Protect personal data and privacy	27
4.3.1.1 Practice data minimization when sharing personal information online	27
4.3.1.2 Recognize and respond to identity and credential threats	28
4.3.1.3 Configure privacy-protective settings on devices, accounts, and apps	28
4.3.2 Information governance compliance	28
4.3.2.1: Classify information by sensitivity before handling or sharing it	28
4.3.2.2. Apply retention and disposal rules to documents and data	29
4.3.2.3: Maintain transparent records of information processing activities (ROPA)	29
4.3.3 Risk management	29
4.3.3.1: Identify digital risks using a structured threat-modeling approach	30
4.3.3.2 Assess and prioritize digital risks using likelihood-impact analysis	30
4.3.3.3 Decide on risk treatment using a deliberate strategy choice	30
4.3.4 Manage IT security compliances	31
4.3.4.1 Map controls against a recognized security framework	31
4.3.4.2 Sustain compliance through evidence collection and audit-readiness routines	31
4.3.4.3 Manage non-conformities through corrective and preventive action	32
4.4 Principle: Make it understandable	32
4.4.1 Accept own accountability	32
4.4.1.1 Personal After-Action Review	32
4.4.1.2 Credible Error Acknowledgment in Digital Communication	33
4.4.1.3 Recognising Self-Serving Attribution in One's Own Reasoning	33
4.4.2 Assume responsibility	34
4.4.2.1 Implementation Intentions for Accepted Commitments	34
4.4.2.2 Explicit Scope-Setting and Handoff Agreements	34
4.4.2.3 Voluntary Stewardship of Shared Digital Resources	35
4.4.3 Ensure information transparency	35
4.4.3.1 Provenance and Source Documentation	35
4.4.3.2 Disclosing Uncertainty and Limitations	36
4.4.3.3 Disclosing Conflicts of Interest and Communicator Stakes	36
4.4.4 Provide information	36
4.4.4.1 Audience-Adapted Framing and Plain Language	36
4.4.4.2 Proactive Sharing and Information Push	37
4.4.4.3 Structuring Information for Findability and Quick Uptake	37



5 Methodology.....	38
5.1 Research approach.....	38
5.1.1 Problem identification and motivation	39
5.1.2 Definition of Objectives of a solution	39
5.1.3 Design and development of the DR Competence Framework.....	40
5.1.4 Demonstration.....	41
5.1.5 Evaluation.....	41
5.1.6 Communication	42
6 Next steps	42
References	44



1 Introduction

1.1 Purpose and scope

The report for Work Package (WP) 2, D.2.1 of the DIRECT project, encompasses the conceptual framework for Digital Responsibility (DR). Its purpose is to provide a robust structure for DR education that is conceptually precise, educationally usable, and compatible with European competence-oriented approaches. The framework is intended to serve as the conceptual basis for later work on learning pathways, the skills analytics engine, and the learning platform.

The report implements the overall objectives of WP2 and aims to:

- To conduct a detailed analysis of the several different dimensions that DR contains.
- To provide guidelines regarding the development of skills in the context of DR.
- To discover the associated skills for each DR dimension.

More specifically, this deliverable provides a detailed analysis on the principles of DR, its practices so far, and why these practices are occasionally flawed. It includes guidelines for the correct practice of DR under different circumstances and dimensions, building on established frameworks such as the European multilingual classification, European Skills, Competences, Qualifications and Occupations (ESCO), while also developing the baseline for validating that DR is correctly applied to an organization. As a core element of DIRECT, this report defines the skills-competency mapping framework for each dimension of DR, represented as a classification schema of skills that comprise the knowledge pool for effectively applying DR.

The remainder of this report is structured as follows. Section 2 introduces the scientific background and definition of DR based on extant research. Building on this, Section 3 presents the final framework dimensions. Section 4 establishes the operationalization of the framework by means of mapping relevant skills from ESCO to each principle. Further, providing detailed descriptions and examples for each skill. Section 5 provides a detailed overview of the methodology applied to develop the DR framework, before Section 6 closes the report with an outline of next steps in the DIRECT project.

1.2 Positioning work package 2 in DIRECT

The DIRECT project is structured into six interrelated WPs, each addressing a specific aspect of the project objectives. Together, these WPs contribute to the development of a comprehensive approach to DR. This report focuses on WP2, which plays a key role in establishing the conceptual foundation for the project. In the proposal, the first goal of WP2

is to conceptualize a framework for DR. Second, analyze ethical challenges associated with digital technologies. Third, to map required skills to DR framework dimensions.

The resulting DR framework of WP2 provides important input for WP3, WP4, and WP5. WP3 focuses on designing learning pathways for DR, while WP4 is dedicated to developing the skills analytics engine and WP5 on the learning platform. By delivering both a conceptual framework and a structured overview of relevant skills, WP2 ensures that the later project stages are based on a clear, evidence-informed, and practice-oriented understanding of DR.

The positioning of WP2 within DIRECT has several implications for framework design. First, the framework must be analytically rigorous enough to guide curriculum design and competence development. Second, it must be flexible enough to travel across HE, VET, and labour-market settings. Third, it should align with the project's wider commitments to low-barrier access, inclusion, interoperability with existing European frameworks, and support for the twin green and digital transition. The proposal explicitly links DIRECT to DigComp, LifeComp, GreenComp, ESCO, and broader EU priorities concerning social fairness, sustainable competitiveness, and resilience.

2 Background and synthesis for conceptual framework development

2.1 Definition of Digital Responsibility

DR has emerged as a response to the fact that digitalization generates not only opportunities, but also social, ethical, ecological, and political consequences that cannot be addressed through compliance alone (Obwegeser et al., 2026). Recent research in the field of information systems, particularly the studies by Trier et al. (2023) and Recker et al. (2025) conceptualize DR as multilevel frameworks spanning individual, organizational, societal and international levels.

Trier et al. (2023) draws on political and organizational white papers and academic literature on corporate responsibility and digital ethics which propose norms and principles that should guide the design of information systems and the behaviour of key stakeholders. This further led to the identification 8 DR principles, which is defined as foundational value-based requirements that motivates actors to attain responsible digital transformation (Trier et al., 2023). Recker et al. (2025) further sharpen the concept by arguing that DR rests on accountability for digital outcomes, obligation to foster desirable outcomes and mitigate undesirable ones, and dependability as a continuing commitment over time.

Trier et al. (2023) defines DR as efforts of stakeholders such as individuals, corporations, and public institutions “to contribute to a sustainable, more inclusive, fair, and value-based



digital society (...) beyond the legal minimum.” Recker et al. (2025) further conceptualize DR as a multidimensional construct built around three core tenets: accountability for both beneficial and harmful outcomes, the obligation to enable positive outcomes while safeguarding against negative ones, and dependability, understood as a continuous commitment to these duties over time. Taken together, these perspectives position DR as a proactive, value-driven approach to the design, deployment, and governance of digital technologies, emphasizing long-term accountability and societal impact rather than reactive or compliance-oriented responses.

For the purposes of DIRECT, this implies that DR should not be reduced to privacy, cybersecurity, or AI ethics in isolation. Rather, DR concerns the responsible design, development, deployment, use, and governance of digital technologies in ways that are fair, beneficial, safe, and intelligible. This broader framing is consistent with the project’s ambition to promote the responsible use of digital technologies for the benefit of society and the environment through education and training.

Combining these emerging perspectives to an operational definition for DIRECT, we therefore define DR competency as the *capacity of individuals to design, develop, use, and govern digital technologies in accordance with ethical principles and with regard to their social, ecological, and economic consequences*. This definition preserves the guiding ambition of DR while making explicit its relevance for education: responsibility is treated not as an institutional obligation, but also as a learnable capability.

2.2 Related concepts

DR overlaps with several adjacent concepts, but it is not identical to any one of them. Corporate Digital Responsibility (DCR) focuses more specifically on the responsibilities of firms and has developed into a visible stream in management and IS research (Trier et al., 2023). Digital ethics is broader and concerns the moral evaluation of digital technologies and practices (Whiting & Pritchard, 2017). AI ethics is a more specific subdomain focused on the design and governance of AI systems (Huang et al., 2022). Responsible digital transformation adds a process perspective by asking how digital transformation can generate value without reproducing social or environmental harms (Pappas et al., 2023).

For DIRECT, DR is best treated as an integrative umbrella concept. It draws normative orientation from digital ethics, governance concerns from CDR, and a transformation perspective from responsible digital transformation. This is educationally useful because learners need more than rules tied to a single technology. They need the capacity to reason across contexts in which privacy, fairness, sustainability, accountability, participation, and transparency interact. Further, while some DR literature differentiates between actor levels,

an educational framework should not hard-code those levels into its core architecture. The same learner may act as citizen, student, employee, developer, manager, or decision-maker depending on context. A DR competence framework for education therefore benefits from a role-agnostic structure in which the principles remain stable, while applications vary across settings.

2.3 Analysis of DR principles

The conceptual core of the DR framework is derived from a comparative synthesis of DR, digital ethics, and AI ethics frameworks. As part of the design and development of the DR framework, a systematic analysis of existing DR-, digital ethics-, and AI ethics-oriented frameworks and tools was conducted. The purpose of this analysis was to identify commonly articulated principles, review their conceptual overlap, and understand how different frameworks operationalize responsibility across varying scopes and technological contexts. Table 1 shows a selection of frameworks and tools that were reviewed.

The analysis covered a diverse set of frameworks originating from academic research, industry practice, and policy-oriented initiatives. These frameworks differ in scope, ranging from comprehensive DR approaches to more narrowly focused digital ethics or AI ethics tools, and in their intended audiences, such as organizational leaders, engineers, or policymakers. Despite these differences, the comparative analysis revealed a high degree of convergence at the level of underlying principles. A detailed methodology description is provided in the section “Methodology” of this document.

Table 1: Overview of DR frameworks

Framework / tools	Scope	Principles	References
DR cube	DR	Accountability, Data Privacy, Fairness, Functionality, Norms & Values, Participation, Sustainability, Transparency	(Trier et al., 2023)
Multidimensional canvas	DR	Accountability, Dependability, Obligation	(Recker et al., 2025)
Digital Ethics Compass	Digital Ethics	Avoid manipulation, Avoid inequality, Control, Humancentric, Understandability	(Dansk Design Center, n.d.)
Digital Ethics Canvas	Digital Ethics	Beneficence, Empowerment, Fairness, Non-maleficence, Privacy, Sustainability	(Hardebolle et al., 2023)
PaRA analysis	Digital Ethics	Autonomy, Beneficence, Justice, Non-maleficence, Transparency	(Nemat et al., 2023)
Digital Ethics Guidelines	Digital Ethics	Accountability, Autonomy, Avoid Harm, Control, Fairness, Transparency	(Swiss Post, 2024)



PwC	AI ethics	(1) Interpretability and explainability (2) Sustainability (3) Robustness (4) Bias and fairness (5) Security (6) Privacy (7) Safety	(PwC, 2024)
Trustworthy AI	AI ethics	(1) Human agency and oversight (2) Technical robustness and safety (3) Privacy and data governance (4) Transparency (5) Diversity, non-discrimination and fairness (6) Societal and environmental well-being (7) Accountability	(European Commission, 2019)
OECD AI principles	AI ethics	(1) Inclusive growth, Sustainable development, and well-being, (2) Human centered values and fairness (3) Transparency and explainability (4) Robustness, security and safety (5) Accountability	(Organisation for Economic Co-operation and Development [OECD], n.d.)
Responsible Technology Playbook	AI ethics	(1) Diversity, Equity & Inclusion, (2) Sustainability (3) Data and AI (4) Privacy (5) Security, (6) Inclusive design & accessibility	(Thoughtworks, 2023)

Our research identified strong convergence across the reviewed literature and policy-oriented frameworks. Recurring themes include fairness and inclusion, societal and environmental benefit, privacy and security, and transparency and accountability. This convergence matters because it suggests that a parsimonious framework can capture the core of DR without fragmenting the concept into narrow technology-specific sub-frameworks. At the same time, principles alone are not yet an educational structure and need to be translated into learnable domains of judgement and action.

To bridge this gap, the recurring principles were therefore clustered into four higher-order categories: *Make it Fair*, *Make it Good*, *Make it Safe*, *Make it Understandable*. The high-level labels are intentionally simple so that they can easily travel across educational contexts. However, they should not be read as slogans. They represent integrative competence domains, as described in the following sections.

First, the principle of *Make it Fair* addresses justice, inclusion, accessibility, participation, and respect for rights in digital contexts. It focuses on whether digital technologies distribute benefits and burdens equitably, whether they include or exclude particular groups, and whether they uphold democratic and human rights values. In DR education, this principle provides a lens for learners to examine when utilizing digital technology. For example, how digital systems may reinforce bias, marginalize users, or create unequal access to opportunities and services. It is therefore closely related to the project's emphasis on inclusion, equality, and social fairness in responsible digitalization.

Second, the principle of *Make it Good* focuses on the beneficial purposes and outcomes of digitalization. It asks not only whether digital technologies avoid harm, but whether they

actively contribute to societal well-being, sustainability, and meaningful value creation. This principle is particularly important in DIRECT because the proposal explicitly links DR education to the twin green and digital transition, responsible innovation, and the broader societal benefits of digital technologies.

Third, the principle of *Make it Safe* concerns privacy, security, robustness, and the prevention of digital harm. It reflects the fact that responsible digitalization requires more than good intentions: digital systems must be governed and operated in ways that protect persons, organizations, and society from misuse, failure, and avoidable risk. In DIRECT, this principle is relevant because the project seeks to strengthen learners' ability to manage the dilemmas of responsible digitalization in practical settings.

Finally, the principle of *Make it Understandable* addresses transparency, explainability, communication, and accountability. Responsible digitalization requires that relevant stakeholders understand what a digital system does, why a decision was made, what assumptions are embedded in a process, and who is responsible for consequences. This principle is therefore essential for trust, contestability, and informed participation in digital environments.

Together, these four domains provide a coherent and teachable architecture for DR education. This structure also aligns with recent research, showing that digital rights and responsibility in education require more than legal literacy; they require capability development around privacy, security, critical reflection, and responsible participation (Gallego-Arrufat et al., 2024). Table 2 provides an overview of the selected frameworks and principles, further how these are mapped with the overarching higher-level principles.



Table 2: Mapping extant frameworks to DR competence framework principles

Make it fair	Make it Good	Make it Safe	Make it understandable	Reference
Norms & Values, Fairness, Participation	Sustainability, Functionality	Data privacy	Transparency, Accountability	(Trier et al., 2023)
	Dependability, Obligation		Accountability	(Recker et al., 2025)
Avoid manipulation, Avoid inequality,	Humancentric	Control	Understandability	(Dansk Design Center, n.d.)
Empowerment, Fairness	Beneficence, Non-maleficence, Sustainability	Privacy		(Hardebolle et al., 2023)
Autonomy, Justice,	Non-maleficence, Beneficence		Transparency	(Nemat et al., 2023)
Autonomy, Fairness,	Avoid Harm	Control	Accountability, Transparency	(Swiss Post, 2024)
Bias and fairness	Sustainability, Robustness	Security, Privacy, Safety	Interpretability and explainability	(PwC, 2024)
Diversity, non-discrimination and fairness	Societal and environmental well-being	Human agency and oversight, technical robustness and safety, Privacy and data governance	Transparency, Accountability	(European Commission, 2019)
Human centred values and fairness	Inclusive growth, Sustainable development, and well-being,	Robustness, security and safety	Transparency and explainability, Accountability	(OECD, n.d.)
Diversity, Equity & Inclusion, Inclusive design & accessibility	Sustainability	Privacy, Security	Data and AI	(Thoughtworks, 2023)

3 Digital Responsibility Competence Framework

3.1 The dimensions and levels

Figure 1 illustrates the DR competence framework. The framework consists of two main sections, named the “WHAT?” and the “HOW?”. By differentiating between these two parts, the framework aims to simplify its practical use and interpretation. The first section defines the foundational principles of DR, while the second section outlines how these principles can be translated into teaching and learning practices.

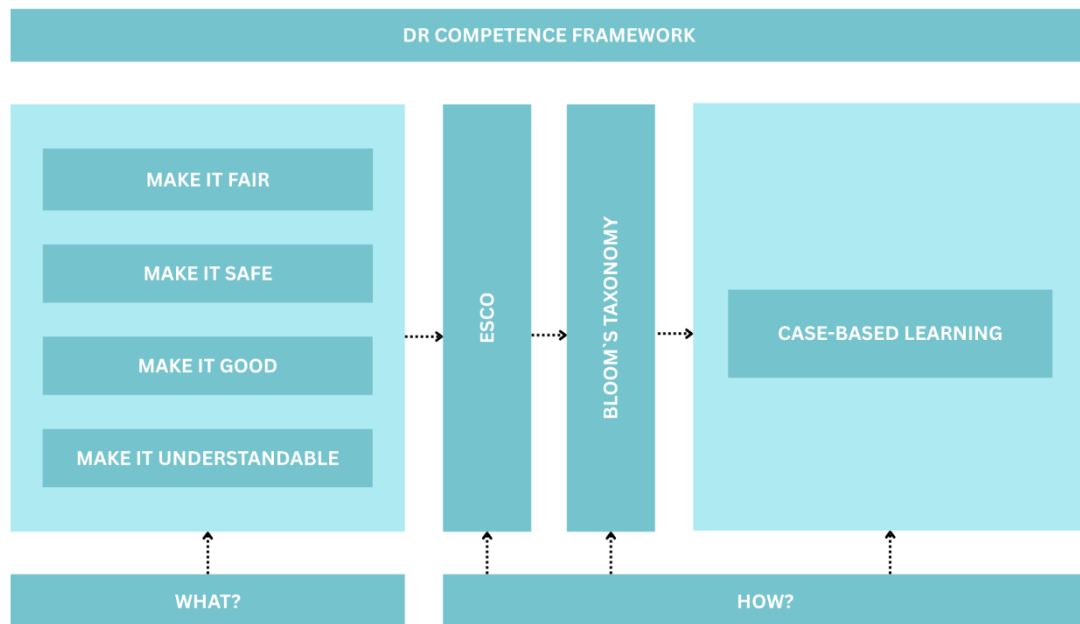


Figure 1: The DR Competence Framework

The first section: “WHAT?” consists of the four overarching guiding principles: *Make it Fair*, *Make it Good*, *Make it Safe*, *Make it understandable*. These principles can also be understood as higher-level categories that group related DR principles as explained in section 2.3, thereby providing a coherent structure for organizing the principles identified across existing frameworks and tools. Clustering the principles into these four categories allows for systematic organization while maintaining a clear theoretical grounding of the framework. Although DR can be analysed at personal, organizational, societal, and international levels (Trier et al., 2023; Recker et al., 2025), education benefits from a principle- based structure that remains stable across roles and contexts. This is particularly suitable for DIRECT, because the project addresses educators and learners in HE, VET, and labour- market settings and seeks to support both broad awareness and context-specific application.

The four principles also makes it possible to retain a common normative language across settings while still adapting cases, tasks, and assessment criteria to specific contexts such as data use, AI deployment, automation, digital platforms, or behavioural design. The framework should therefore be understood as a structure frame for DR education. It does not aim to replace richer actor-level analyses in the DR literature but to provide a baseline

architecture that can support curriculum design, learning progression, and competence mapping.

The next section consists of the category named “HOW?”, which aims to provide a pathway for how these principles can be taught. The first part is “ESCO”, which is the EU classification scheme for skills, competences and occupations. Through a mapping process, further explained in section 4, relevant skills and competences were identified and aligned with each of the four guiding principles. This mapping ensures that the framework is anchored in recognized professional skill structures and supports alignment between educational outcomes and labour-market expectations.

The second component of the “HOW?” section points to Bloom’s Taxonomy, which provides a pedagogical structure for defining levels of cognitive complexity in learning (Bloom et al., 1956). Bloom’s Taxonomy organizes learning objectives into hierarchical categories, remembering, understanding, applying, analysing, evaluating, and creating, thereby supporting the development of learning pathways. Based on the DR competence framework, Bloom’s Taxonomy is used in WP3 of DIRECT to structure learning outcomes associated with each principle, ensuring that learners progress from foundational awareness to advanced, context-sensitive application and critical reflection. This approach supports both the scaffolding of learning and the design of assessment strategies that capture different levels of competence development.

As an educational structure, the DR framework can be used at three connected levels. First, it will support curriculum design by providing a high-level architecture for modules, cases, and learning pathways (WP3). Second, it can support learning outcomes and assessment by translating each principle into observable competences, enabling the design of targeted assessment practices and tools. Third, it supports interoperability with European reference frameworks such as ESCO, DigComp, DigCompEdu, LifeComp, and GreenComp. The framework is particularly well suited to case-based and dilemma-oriented learning, as is part of WP3 developments within DIRECT. DR problems rarely have one single correct answer. They involve tensions among values, stakeholders, and contextual constraints. Educational design should therefore not merely transmit rules, but develop learners’ capacity for critical reflection, perspective-taking, justification, and responsible action. This is also consistent with the proposal’s emphasis on concrete ethical dilemmas, innovative pedagogies, and reflective skill development. Finally, the framework is deliberately open to role-specific elaboration. In HE, it can guide integration into disciplinary curricula. In VET, it can support practice-oriented competence development. In labour-market contexts, it can inform professional upskilling and organizational learning. Its value lies in combining conceptual stability with contextual flexibility.



4 Mapping DR principles to ESCO

To support the development of learning materials in DIRECT, the four guiding principles are mapped to relevant skills and competences from ESCO, the European multilingual classification of Skills, Competences, Qualifications and Occupations. ESCO works as a dictionary to describe, identify and classify professional occupations and skills relevant for the EU labor market and education and training. Those concepts and the relationships between them can be understood by electronic systems, which allow different online platforms to use ESCO for services like matching jobseekers to jobs based on their skills, suggesting trainings to people who want to reskill or upskill etc. In this report, we follow the ESCO classification in the sense that we (i) do not further distinguish between skills and competences, and (ii) reuse the exact preferred labels proposed by ESCO to ensure consistency and compliance (European Commission, n.d.).

Ethical and responsibility-related principles are often formulated at a high level of abstraction, which makes it difficult to operationalize in educational practice. By connecting the four principles *Make it Fair*, *Make it Good*, *Make it Safe*, and *Make it Understandable* to ESCO, they are translated into concrete, observable, and assessable learning outcomes. This makes it possible to move from normative statements about what “should” guide digital practice to clearly defined competencies that learners can develop, demonstrate, and be evaluated on. In this way, the linkage provides a bridge between conceptual frameworks of DR and the practical requirements of curriculum design, learning activities, and assessment.

On that note, it is important to consider the nature and structure of the ESCO classification. ESCO is organized into broad occupational profiles and transversal skill categories, covering knowledge, skills, and competences across many domains, but it does not contain a single, clearly defined category for DR. This means that DR-related competences must be identified by combining and interpreting skills from multiple parts of the taxonomy. Consequently, the mapping presented in Table 3 offers a structured and coherent selection of ESCO skills aligned with the four principles. It does not claim to represent a final or exhaustive set of DR competences, but rather a pragmatic and well-founded selection within the current ESCO framework. As interpretations of DR evolve and ESCO is further developed, this mapping may be refined and extended in future work.



Table 3: Mapping DR principles to relevant ESCO skills

Principle	ESCO Skill	Description
Make it fair	Promote inclusion	Promote and respect diversity, and advocate for equal treatment of genders, ethnicities, and minority groups in organizations in order to prevent discrimination and ensure inclusion and a positive environment.
	Promote the principles of democracy and the rule of law	Take an active role in promoting the principles of democracy, social justice, and the rule of law. Confront discrimination based on ethnic, cultural or sexual identity or orientation as well as social, educational, or economic background, by assessing and voicing the implications for different groups of any planned action, including legislation, policies, or programmes.
	ICT accessibility standards	The recommendations for making ICT content and applications more accessible to a wider range of people, mostly with disabilities, such as blindness and low vision, deafness and hearing loss, and cognitive limitations. It includes standards such as Web Content Accessibility Guidelines (WCAG).
	Promote human rights implementation	Promote the implementation of programs which stipulate agreements, binding or non-binding, concerning human rights in order to further improve efforts to decrease discrimination, violence, unjust imprisonment or other human rights violations. As well as to increase efforts to improve tolerance and peace, and better treatment of human rights cases.
Make it good	Protect the environment from the impact of the digital technologies	Be aware of the environmental impact of digital technologies and their use.
	Operate open source software	Knowing the main Open Source models, licensing schemes, and the coding practices commonly adopted in the production of Open Source software.
	Corporate sustainability	A business practice to conduct long-term sustainable growth by seeking environmental, economic, and social strategies as its three main pillars.



	Data ethics	Assess processes such as collecting, analysing and disseminating structured and unstructured data that might negatively impact the society.
Make it safe	Protect personal data and privacy	Protect personal data and privacy in digital environments. Understand how to use and share personally identifiable information while being able to protect oneself and others from damage. Understand that digital services use a “Privacy policy” to inform how personal data is used.
	Information governance compliance	The policies regarding processes and procedures for the use of information, the balance between information availability and information security and IPR (Intellectual Property Rights) and personal data protection.
	Risk management	The process of identifying, assessing, and prioritising of all types of risks and where they could come from, such as natural causes, legal changes, or uncertainty in any given context, and the methods for dealing with risks effectively.
	Manage IT security compliances	Guide application and fulfilment of relevant industry standards, best practices and legal requirements for information security.
Make it understandable	Accept own accountability	Accept accountability for one`s own professional activities and recognize the limits of one`s own scope of practice and competencies.
	Assume responsibility	Accept responsibility and accountability for one's own professional decisions and actions, or those delegated to others.
	Ensure information transparency	Ensure that required or requested information is provided clearly and completely, in a manner which does not explicitly withhold information, to the public or requesting parties.
	Provide information	Ensure quality and correctness of provided information, depending on the type of audience and context.

In the following section, each ESCO skill is linked with good practices derived from literature (incl. academic studies, industry reports, standards and policy documents). These good practices represent a selection of widely used and accepted practices, reported in literature, that serve as examples on how to make each ESCO teachable and



practically applicable. However, they do not represent an exhaustive list of practices per ESCO, nor are they “best” practices.

4.1 Principle: Make it fair

4.1.1. Promote inclusion

This skill concerns the ability to recognize diversity in digital settings and to ensure that digital practices, tools, and services do not disadvantage people based on gender, ethnicity, age, disability, language, or socio-economic background. In a DR context, promoting inclusion means actively shaping digital environments so that they support equal participation rather than reproduce exclusion. This includes sensitivity to representation, usability, access, and participation.

4.1.1.1 Participatory co-design with underrepresented communities

Participatory co-design treats members of underrepresented communities as partners in shaping a product from the outset, rather than as people consulted once the important decisions have already been made. This practice is well established and applied across both research and technology development (Halskov & Hansen, 2015; Lopez et al., 2019). While participatory design could be seen as means for reducing exclusion, it is only effective if it redistributes authority (Harrington et al., 2019). Relevant questions would be who defines the problem, whose knowledge is treated as legitimate, who has influence over design choices, and who can contest or redirect the project. From this perspective, inclusion in digital technology design is not achieved simply by consulting users or inviting underrepresented groups into workshops. It depends on whether participatory processes change the power relations through which technologies are imagined, built, and evaluated. Thus, promoting inclusion is not achieved by consulting marginalized groups after a design is fixed, but by sharing decisions with them while those decisions are still open.

4.1.1.2 Designing for the digital divide

Designing for the digital divide is an inclusion practice that involves creating digital services usable under uneven conditions. Who benefits from digital services is shaped by several determinants, such as access, skills and use (Scheerder et al., 2017). Hollimon et al. (2025) extend this point in a more design-oriented direction by arguing that digital exclusion cannot be understood only as a question of access, because meaningful participation also depends on availability, adequacy, and affordability. In design terms, this means considering whether users have reliable infrastructure, whether connection quality is sufficient for the service, and whether the ongoing costs of data, devices, and connectivity make use realistic. A digital service built only for stable connection, recent devices, and high data use may therefore exclude users whose access is limited, slow, or expensive.

4.1.1.3 Inclusive language, representation, and culturally responsive defaults

This practice concerns the words, images, examples, and default settings an interface presents, and whether they reflect a varied user base or quietly assume a narrow standard person. Friedman and Nissenbaum (1996) established that bias in computing systems should be considered in the early stages the design process. More recent work shows the stakes in concrete terms, with unexamined data and design choices producing measurably different treatment for different demographic groups (Buolamwini & Gebru, 2018). Representation is far from cosmetic, because the defaults a system ships with announce who it expects its users to be. An interface that pictures only one kind of user, or whose forms cannot hold a person's name or gender, signals exclusion whatever the intention behind it. Reworking a fitness app that assumes a young, able-bodied man as its default, by changing its imagery, pronoun handling, and pre-filled fields, removes a barrier that is easy to miss from the inside but plainly felt by the people it shuts out.

4.1.2. Promote the principles of democracy and the rule of law

This skill refers to upholding democratic values, social justice, and lawful conduct when designing, implementing, or using digital technologies. In practice, it involves recognizing that digital systems influence participation, freedom of expression, procedural fairness, and access to rights. Within DR education, this skill helps learners understand that digitalization is not value-neutral and that technologies can either strengthen or weaken democratic institutions and public trust.

4.1.2.1 Process and contestability in automated decision-making

Contestability is a practice that ensures people affected by automated decisions have a way to challenge them. In digital systems that use AI or automated decision-making, exclusion can occur when users are treated as passive subjects of a system whose outputs they cannot question. A contestable system instead gives users notice that an automated decision has been made, provides enough information to understand the basis of the decision, and creates a process for expressing their point of view, requesting human review, and disputing the outcome. Under Article 22 of the EU General Data Protection Regulation (GDPR), a person has the right not to be subject to a decision based solely on automated processing, including profiling, where that decision produces legal effects or similarly significant impacts (Regulation (EU) 2016/679, Art. 22). Kaminski and Urban (2021) imply that contestability works best when it is built into a system rather than bolted on afterwards. The rule of law depends on decisions being reviewable and non-arbitrary, and that principle does not lapse when a decision is handed to software.

4.1.2.2 Information integrity against manipulation (prebunking)

Information-integrity work aims to build resistance to manipulation before people encounter it, drawing on inoculation theory: people are shown weakened versions of common manipulation techniques, with explanations, so they recognise the same moves

later. The evidence behind it is strong and the method has been applied at scale, with cross-cultural field studies and large public interventions such as the Bad News game and short prebunking videos, several developed with governments and platforms, improving people's ability to separate manipulation from honest content (Roozenbeek et al., 2020). Teaching people to recognise the tactic of fake-expert framing, then checking whether they catch it in unfamiliar headlines, strengthens the conditions for democratic debate without dictating its content.

4.1.2.3 Designing for democratic participation and deliberation

This practice builds digital spaces for collective reasoning at the level of the polity, structured, inclusive, and resistant to manipulation, which sets it apart from co-designing a single product. Such tools have moved from the margins into ordinary governance. The OECD (2020) documents a wave of deliberative and participatory processes adopted by public authorities around the world, together with a maturing set of design and quality standards for running them well. Studies of platforms already in use give the practice an empirical footing; analysis of large deployments such as Decidim shows how particular interface and process choices raise or lower the quality of online deliberation (Aragón et al., 2017). Democracy is not only a matter of protecting rights but of providing real avenues for participation. A municipal consultation that maps thousands of contributions to surface where agreement actually lies, publishes its agenda openly, and guards against coordinated brigading turns broad public input into something a decision can be built on, rather than a forum that simply rewards the loudest voices.

4.1.3 ICT accessibility standards

This skill concerns the ability to apply standards and design principles that make digital content, systems, and services usable for people with diverse physical, sensory, and cognitive abilities. In DR terms, accessibility is not merely a technical add-on; it is a fairness requirement because inaccessible systems systematically exclude users from education, employment, and public life. The skill therefore connects ethical inclusion to concrete design and implementation choices.

4.1.3.1 Standards-conformance evaluation

Conformance evaluation is the methodical assessment of a digital product against recognised accessibility standards, mainly WCAG 2.2 and, in Europe, EN 301 549, following a defined procedure instead of informal spot-checks. These standards are the global baseline for disability access, now formalised internationally and written into law through instruments such as the European Accessibility Act, and the W3C's Website Accessibility Conformance Evaluation Methodology gives evaluators a repeatable process (W3C, 2023). How the evaluation is carried out turns out to be decisive. Vigo et al. (2013) showed that automated checkers, used alone, cover at most half of the relevant success criteria and catch only a fraction of real violations, so a clean automated scan can disguise serious barriers. Conformance becomes meaningful only when automated tooling, expert

inspection, and assistive-technology checks are used together. Auditing a university portal by running a scanner, hand-verifying each flagged criterion, and testing with a keyboard and a screen reader yields a defensible account of where it really stands.

4.1.3.2 Accessible-by-default authoring

Accessible-by-default authoring puts accessibility into content at the moment it is created, through semantic structure, proper headings, alternative text, captions and transcripts, a sensible focus order, and adequate contrast, instead of repairing these things later. The annual WebAIM Million analysis of the top one million home pages finds detectable WCAG failures on the great majority of them, dominated year after year by the same authoring-level mistakes, low-contrast text and missing alternative text foremost among them (WebAIM, 2026). A way to prevent these defects is to accessibility into authoring and procurement routines so that it is never left as an afterthought. Standards are far cheaper to meet, and met far more consistently, when they are applied at the beginning.

4.1.3.3 Assistive-technology and disabled-user testing

Testing with assistive technology and with disabled people checks how a product behaves in actual use, on the premise that meeting a standard and being usable are not the same thing. The gap between the two is documented rather than assumed. Power et al. (2012) found that only around half of the problems blind users genuinely ran into were covered by WCAG success criteria, which means a conformant product can still leave real obstacles in place. Usability testing with disabled participants is the accepted way to find those obstacles, and it has been used to validate accessibility guidelines themselves (Rømen & Svanæs, 2012). Standards set a floor, and honouring their purpose means confirming that people can finish real tasks, not merely that requirements have been ticked off. A moderated session in which screen-reader users try to complete a checkout flow regularly exposes dead-ends that passed both automated scans and expert review, the kind of failure conformance testing alone was never going to surface.

4.1.4 Promote human rights implementation

This skill refers to supporting and operationalizing human-rights principles in digital environments. It includes awareness that rights such as privacy, non-discrimination, access to information, freedom of expression, and protection from harm can be directly affected by digital systems and data practices. In DR education, this skill helps learners move from abstract ethical concern to rights-based evaluation of technologies and policies.

4.1.4.1 Human Rights Impact Assessment

A Human Rights Impact Assessment is a structured examination, undertaken before and during deployment, of the full range of rights a digital product or AI system might affect,

identifying the most serious risks and the measures needed to address them. The practice puts an authoritative framework into operation: the UN Guiding Principles on Business and Human Rights set human-rights due diligence as the expected standard for business conduct, technology firms included (United Nations, 2011). Methodologies now adapt that framework specifically to digital activities, supplying repeatable guidance and tools for technology settings (Danish Institute for Human Rights, 2020). Promoting human rights implementation means accounting for the whole spectrum of rights in play, from privacy and non-discrimination through to assembly and expression, rather than examining a single decision or a single right in isolation. Working through a facial-analysis feature for a hiring platform, scoping which rights it touches, consulting the groups it could affect, and recording either the mitigations or a decision not to release it, is the disciplined inquiry the method exists to support.

4.1.4.2 Privacy- and data-protection-by-design

Privacy by design builds protection into a system from the start, through data minimisation, purpose limitation, protective defaults, and structured risk assessment, treating privacy as part of the architecture rather than a feature added late. It is at once a settled framework and a legal obligation. Cavoukian's (2011) seven foundational principles articulated the approach, and the EU General Data Protection Regulation now requires data protection by design and by default (Regulation (EU) 2016/679, Art. 25). Gürses et al. (2011) show that this is workable engineering rather than aspiration, translating the idea into concrete system-design strategies. Privacy is itself a human right, and respecting it in practice depends on choices made while a system is being built, not on assurances issued afterwards. A analytics feature that records only aggregate counts, discards identifiers at the point of collection, and is documented through a data-protection impact assessment before launch protects that right by construction, which is considerably more dependable than a promise to handle personal data carefully once it has already been gathered.

4.1.4.3 Access to remedy and expression safeguards in content governance

This practice builds notice, appeal, and proportionate redress into the way platforms govern content, so that someone whose post or account is actioned receives an explanation and a genuine route to challenge it. It has become the working benchmark for rights-respecting moderation. The Santa Clara Principles, endorsed by major platforms and increasingly reflected in law such as the EU Digital Services Act, set out standards for reporting numbers, giving notice, and offering appeals that protect users' expression and their interest in fair process (Santa Clara Principles, 2021). Suzor et al. (2019) provide the scholarly counterpart, examining what transparency and procedural fairness in commercial moderation must involve before they count as meaningful. The third pillar of the human-rights framework, access to remedy, is applied here to private systems that now shape public speech. An



appeals process that tells a user which specific rule was breached, preserves the disputed content, and guarantees human review within a stated time gives substance to the right to be heard, instead of leaving a removal effectively final.

4.2 Principle: Make it good

4.2.1 Protect the environment from the impact of digital technologies

This skill concerns awareness of the environmental footprint of digital infrastructures, devices, software, and patterns of use. In a DR framework, it emphasizes that digitalization has material consequences, including energy consumption, emissions, extraction of raw materials, and e-waste. Educationally, the skill develops the ability to make environmentally responsible choices when selecting, using, or designing digital technologies.

4.2.1.1 Measure and reduce the energy and carbon footprint of software and digital services

The treatment of software carbon measurement as a core competency is increasingly supported by the emerging consensus that environmental impacts need to be assessed at the level of individual digital services, rather than only at the broader data-centre level. For example, the Software Carbon Intensity (SCI) specification, developed by the Green Software Foundation, defines a per-functional-unit carbon rate covering operational electricity, regional grid intensity, and embodied hardware emissions (ISO/IEC, 2024). Freitag et al. (2021) supply the scientific urgency, showing through peer-reviewed analysis that ICT's share of global greenhouse gas emissions has been systematically understated and plausibly reaches between 2.1 and 3.9 percent. In practice, a development team might apply the SCI formula to compare two implementations of an image-processing API and choose the architecture with the lower carbon rate per request.

4.2.1.2 Extend ICT hardware lifespan through repair, refurbishment and circular procurement

Hardware lifespan extension is among the most consequential interventions in the environmental footprint of digital technology, because the embodied carbon of devices typically exceeds their lifetime operational footprint several times over. Within the European market it has also become a legal obligation: the Circular Economy Action Plan identified electronics and ICT as one of the priority sectors for circularity, and the Right to Repair Directive, places binding repair duties on manufacturers (European Commission, 2020). The Joint Research Centre quantifies the stakes, estimating that lengthening smartphone use by a single year across the EU would yield emissions savings on the order of removing two million vehicles from European roads, while flagging electronics as a fat-growing waste

stream (Joint Research Centre, 2022). Consider a procurement officer who replaces routine new-laptop purchases with refurbished devices under multi-year warranty, supported by internal repair contracts and end-of-life return schemes.

4.2.1.3 Apply eco-design principles to digital products and services

Eco-design brings sustainability into the design of websites, applications, and APIs. It focuses on the environmental impacts that come from how digital services are built and used, not only on whether the underlying infrastructure becomes greener. The French *Référentiel général d'écoconception de services numériques* (RGESN) offers auditable criteria across the lifecycle of a digital service and can be used by the French public sector as well as other projects that want a reference framework (Arcep et al., 2024). A similar non-country-specific framework is the W3C Web Sustainability Guidelines, which provide sustainability criteria for digital products and services (Siegman, 2023). For example, offering a video-only option when audio is mainly used as background music can reduce unnecessary data transfer and energy use. In practice, a product team could apply this approach by auditing a digital service against selected RGESN or W3C Web Sustainability Guidelines criteria and deciding to remove autoplay audio from the homepage.

4.2.2 Operate open source software

This skill refers to understanding and working with open-source models, licenses, and collaborative development practices. In a DR perspective, open source can contribute to public value, transparency, interoperability, and reduced dependency on proprietary vendors, although it also requires responsible governance and maintenance. The competence is relevant because it supports learners in evaluating when openness in software and infrastructure promotes societal benefit and responsible innovation.

4.2.2.1 Evaluate open-source alternatives against proprietary solutions for a specific business need

Structured evaluation of open source against proprietary solutions has shifted from optional exercise to baseline procurement competency, since nearly all contemporary software embeds open source (Black Duck, 2025). Virtually every meaningful technology decision therefore involves an open-source-versus-proprietary comparison. Peer-reviewed evaluation methodologies, including OpenBRR, QSOS and the more recent OSSpal, remain the academic reference for scoring functionality fit, maintenance activity and total cost of ownership. In practice, these findings result e.g. in a procurement team weighing a commercial CRM platform against a community-supported alternative using OSSpal criteria, with explicit attention to community responsiveness and exit risk.

4.2.2.2 Assess and comply with open source license obligations before adoption and distribution

Open source licenses define the legal conditions under which a FOSS component can be incorporated into a distributed product, and their assessment has matured into a formal international quality standard. ISO/IEC 5230:2020, derived from the Linux Foundation's OpenChain Specification, sets out the requirements for a compliant programme and has been adopted several companies (ISO/IEC, 2021). A development team might detect a copyleft library entering via a transitive dependency, incompatible with their proprietary distribution model, and either swap the component or restructure release boundaries to comply.

4.2.2.3 Manage open source dependencies and supply-chain risk in operational use

After several high-impact incidents (e.g. SolarWinds, Codecov and Log4Shell), managing dependencies and their supply-chain exposure has moved from internal hygiene to regulated activity. In the United States, The Secure Software Development Framework, oblige software supplied to federal agencies to include provenance verification, Software Bill of Materials generation in SPDX or CycloneDX format, and continuous vulnerability monitoring (Souppaya et al., 2022). The companion technical reference is the OpenSSF Supply-chain Levels for Software Artifacts (SLSA) framework, originally proposed by Google and now stewarded by the Linux Foundation, which sets out a four-level model for verifiable build provenance and tamper resistance (Open Source Security Foundation, 2023). A DevOps team might integrate SLSA-compliant build attestations and SBOM generation into a CI/CD pipeline, automatically blocking deployments that fail provenance checks. Supply-chain hygiene closes a gap that license compliance alone cannot address: even a legally pristine component can carry critical CVEs or tampered build artefacts, and this practice is the operational safeguard against that residual risk.

4.2.3 Corporate sustainability

This skill concerns integrating environmental, social, and economic sustainability into organizational strategy and operations. Applied to digitalization, it means evaluating whether digital initiatives support long-term societal value rather than only short-term efficiency or profit. In the DR framework, the skill is relevant because organizations increasingly shape the societal effects of digital technologies through procurement, design choices, data practices, and platform models.

4.2.3.1 Conduct a double materiality assessment to prioritize sustainability issues

Double materiality, in its dual reading of how sustainability matters affect the undertaking and how the undertaking affects people and the environment, is the conceptual entry point for any organization reporting under the EU Corporate Sustainability Reporting Directive. EFRAG's Materiality Assessment Implementation Guidance (IG 1), supplies the stepwise procedure and the FAQs that operationalize the requirement (EFRAG, 2024). KPMG's (2024) Survey of Sustainability Reporting, based on a coding of 5,800 companies across 58 jurisdictions, documents that half of G250 companies and 45 percent of European companies have adopted double materiality, a rise from a small minority two years earlier. As an illustration, a manufacturer might map climate risk, water stress and labor conditions across tier-one suppliers, then locate each topic on a matrix of financial and impact materiality to set disclosure priorities.

4.2.3.2 Apply a recognized sustainability reporting framework to disclose performance

Using a recognized sustainability reporting framework is a practice for making corporate sustainability work comparable and verifiable. Instead of writing a general narrative about sustainability, organizations use standards such as GRI, ESRS, or ISSB to decide what information to report and how to report it. This matters because sustainability performance can only be compared across companies, sectors, and countries when organizations use shared indicators. KPMG (2024) shows that this is already a common practice: many large companies use the GRI Standards, most of the largest global companies publish ESG information, and adoption of ISSB and ESRS is increasing. In practice, a company preparing an ESRS report might select required datapoints on climate impacts, workforce conditions, and governance, then use GRI or ISSB mappings where relevant to avoid duplicate reporting. This turns sustainability reporting into a teachable practice: identifying the right framework, selecting the required indicators, collecting evidence, and reporting performance in a standardized way.

4.2.3.3 Set science-based targets and integrate them into operational decision-making

Headline commitments to net zero or carbon neutrality only become accountable when translated into measurable, time-bound targets aligned with the Paris Agreement, and science-based target setting has become the dominant methodology for doing so. The Science Based Targets initiative (2026) reports that close to 10,000 companies held validated targets by the end of 2025, and that committed or validated firms account for 41 percent of global market capitalization. Faria and Labutong (2020), describes the four principal target-setting methods (Absolute Contraction, Sectoral Decarbonization Approach, GHG Emissions per Unit of Value Added, and C-FACT) that underpin the SBTi Corporate Net-Zero Standard. A logistics firm setting a 1.5°C-aligned absolute-contraction

Scope 1 and 2 target might then cascade it into procurement criteria, fleet renewal schedules and executive performance contracts.

4.2.4 Data ethics

This skill concerns the ability to assess how data are collected, analysed, shared, and used, and to judge the wider societal implications of those practices. It goes beyond legal compliance by requiring reflection on fairness, proportionality, consent, harm, benefit, and power asymmetries. In DR education, data ethics is central because many digital dilemmas involve tensions between innovation, efficiency, and the responsible handling of data.

4.2.4.1 Apply pseudonymisation and anonymisation techniques to protect personal data

Pseudonymisation and anonymisation are protective practices that involve transforming personal data so that individuals can no longer be readily identified from it. The European Union Agency for Cybersecurity points out that no single technique works for all scenarios, since the right choice depends on factors such as data protection level, utility, scalability and recovery (ENISA, 2019). Rocher, Hendrickx and de Montjoye (2019) extend this point in a more critical direction by showing that even heavily sampled datasets can be re-identified with high accuracy, estimating that 99.98 percent of Americans could be correctly identified from any dataset using just fifteen demographic attributes. In practical terms, this means selecting techniques appropriate to the sensitivity of the data, testing their resistance to re-identification, and recognising that what counts as adequate anonymisation may need revisiting as new attack methods emerge. A dataset released under weak pseudonymisation may therefore expose the individuals it was intended to protect.

4.2.4.2 Identify and mitigate bias and fairness risks in datasets and algorithmic outputs

Bias and fairness in datasets and algorithmic outputs are no longer purely ethical concerns. EU AI Act obliges providers to examine training, validation and testing data for biases that could harm fundamental rights or produce prohibited discrimination, and to document the mitigations applied (European Parliament & Council, 2024b). Hardt and Narayanan's (2023) formalise statistical and causal fairness measures, disparate-impact analysis and the trade-offs between competing fairness criteria. The community-standard documentation artefacts, Datasheets for Datasets (Gebru et al., 2021) and Model Cards (Mitchell et al., 2019), provide the practical scaffolding for transparency about provenance and subgroup performance, and are now embedded in EU AI Act technical documentation requirements.



An ML team might audit a hiring model's false-negative rate across gender and ethnicity, then apply reweighting or threshold adjustment to reduce disparate impact.

4.2.4.3 Design meaningful transparency and consent mechanisms for data subjects

Transparency and consent design is the point at which abstract data-subject rights either come alive or quietly fail, which is why the European regulator has moved to codify the boundary between meaningful consent and dark-pattern manipulation. The European Data Protection Board's (2023) Guidelines enumerate prohibited deceptive design categories such as overloading, skipping and leaving users in the dark. Nouwens et al. (2020), whose CHI study of the top 10,000 UK websites found that fewer than twelve percent of consent management platforms satisfied minimum legal requirements, and that minor interface changes such as relocating the opt-out button shifted consent rates by twenty-two to twenty-three percentage points. By way of illustration, a product team might redesign a cookie banner so that accept and reject options share visual prominence and equal granularity.

4.3 Principle: Make it safe

4.3.1 Protect personal data and privacy

This skill refers to understanding how personal data are generated, processed, shared, and stored, and to acting in ways that protect privacy in digital environments. In DR education, privacy is not merely a matter of rule-following; it is a competence involving judgement about what data should be collected, who should access them, and how individuals can be protected from harm, manipulation, or surveillance.

4.3.1.1 Practice data minimization when sharing personal information online

Data minimization requires individuals and organizations to disclose, collect, or retain only the personal information strictly necessary for a specific purpose. Thereby reducing harm if the information is later exposed. The practice is established as a binding obligation by the EU, which further requires application by default under Article 25 (European Parliament and Council, 2016). Empirical work by Biega et al. (2020) demonstrates that personalization systems can preserve service quality while collecting substantially less personal data, supporting the operational feasibility of the principle. A typical individual-level application of this practice is the decision to share minimal data. For example, only an email address, rather than a full set of contact details and a date of birth, when registering for a newsletter.

4.3.1.2 Recognize and respond to identity and credential threats

Recognizing and responding to identity and credential threats encompasses the detection of phishing, smishing, impersonation, and account takeover attempts, followed by appropriate action such as verifying through a second channel, refusing to act on suspicious requests, reporting the incident, and rotating compromised credentials. Verizon's (2025) Data Breach Investigations Report identified credential abuse as the leading initial access vector across 12,195 confirmed breaches, while the European Union Agency for Cybersecurity (2025) reported phishing as the dominant intrusion vector at 60 percent of observed incidents, with AI-assisted variants accounting for over 80 percent of social engineering activity. An example application is a person who, upon receiving an unexpected SMS requesting bank verification, refrains from clicking, contacts the bank directly, and reports the message to the national anti-fraud service.

4.3.1.3 Configure privacy-protective settings on devices, accounts, and apps

Configuring privacy-protective settings on devices, accounts, and applications involves the active review and adjustment of defaults that govern app permissions, advertising personalization, location sharing, cookie preferences, and social media visibility. The relevance of this practice rests on evidence that platform defaults are systematically permissive. Bourdouden and Lindqvist (2024) found that default configurations frequently failed to match user expectations and that available instructions for adjustment were vague or incomplete. Liu et al. (2016) demonstrated with 84 Android users that targeted privacy nudges prompted measurable permission restrictions which users retained over time, indicating that proactive configuration reduces unwanted data flows without undermining usability. An example is the user who, upon installing a new application, denies access to contacts and precise location until those permissions are demonstrably required for an intended function.

4.3.2 Information governance compliance

This skill concerns the policies, procedures, and controls that govern the responsible use of information, including availability, security, intellectual property, and personal data protection. In DR terms, this skill supports safe digitalization by ensuring that information is handled consistently, lawfully, and in line with organizational and societal expectations. It is especially relevant where large volumes of data flow across systems, departments, and platforms.

4.3.2.1: Classify information by sensitivity before handling or sharing it

Classification of information by sensitivity requires the application of a consistent labelling scheme, typically distinguishing public, internal, confidential, and restricted material, so that downstream rules for handling, access, storage, retention, and disposal can follow automatically. Bertino and Sandhu (2005) argue that data-sensitivity classification is the foundational input on which coherent access-control and protection policy depends. A typical example is the marking of a draft financial report as Confidential, Internal Only, which automatically restricts its distribution of channels and storage locations under the organization's policy.

4.3.2.2. Apply retention and disposal rules to documents and data

Applying retention and disposal rules requires knowing what information must be kept, for how long, and how it must be securely destroyed at the end of its lifecycle, avoiding both over-retention and premature deletion. Empirical work commissioned by Blancco Technology Group and Kroll Ontrack (2016) found recoverable residual data on 78 percent of 200 used drives purchased through eBay and Craigslist, with only 10 percent properly wiped, illustrating the failure modes that disciplined disposal prevents. A representative example is the cryptographic erasure of a decommissioned employee laptop, documented with a certificate of destruction, before the device is returned to the supplier.

4.3.2.3: Maintain transparent records of information processing activities (ROPA)

This practice means keeping a clear record of how an organization uses personal data. The record should show where the personal data comes from, why it is used, who it is shared with, whether it is transferred to other countries, how long it is kept, and what security measures protect it. Under Article 30 of the GDPR, organizations are generally required to keep these records as part of their accountability duties (European Parliament and Council, 2016). The Irish Data Protection Commission also explains that a ROPA is an important practical tool and is often one of the first documents regulators ask for during an investigation (Irish Data Protection Commission, 2023). Beyond legal compliance, keeping this kind of record helps organizations understand what data they hold and how it is used. For example, a small consultancy might keep a spreadsheet listing its main data uses, such as payroll, marketing, and client work, including the purpose, legal basis, data categories, retention period, and parties the data is shared with.

4.3.3 Risk management

This skill refers to identifying, assessing, prioritizing, and addressing risks that may arise in connection with digital systems, services, or decisions. Within a DR framework, the key point is that digital risks are not limited to cybersecurity; they can also include reputational,

ethical, legal, societal, and environmental harms. Learners therefore need the ability to anticipate consequences and make proportionate mitigation decisions.

4.3.3.1: Identify digital risks using a structured threat-modeling approach

Structured threat modeling identifies digital risks systematically by analyzing a system's representation against a known taxonomy of threat categories, most commonly STRIDE, which encompasses spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The practice was institutionalized within Microsoft's Security Development Lifecycle (Microsoft, n.d.). An illustrative example is a development team building a new web application identifying that an authentication endpoint is vulnerable to credential stuffing under the spoofing category, and prioritizing rate limiting and multi-factor authentication accordingly.

4.3.3.2 Assess and prioritize digital risks using likelihood-impact analysis

Likelihood-impact analysis is a way to rank digital risks by looking at two things: how likely the risk is to happen and how serious the damage would be if it happened. These two scores are often placed in a simple risk matrix, such as a five-by-five table, to help decide which risks need attention first. This method is widely used in information security risk assessment and is described in NIST (NIST, 2012) and ISO/IEC (ISO, 2022c). However, this method is not perfect. Some scholars argue that risk matrices can be too simple and may give a false sense of accuracy. Cox (2008) criticizes the mathematical weaknesses of risk matrices, while Hubbard and Seiersen (2023) argue that more quantitative methods, such as probability estimates and Monte Carlo simulation, can give better results. For this reason, the practice should be taught as a common and useful method, while also recognizing its limits. For example, a small business might rate “ransomware encrypting the file server” as both likely to happen and highly damaging. This would place it near the top of the risk list, meaning it should be addressed before lower-priority risks. The practice helps turn a list of possible threats into a clear order of priorities for action.

4.3.3.3 Decide on risk treatment using a deliberate strategy choice

Risk treatment requires a deliberate choice among four standard strategies, namely mitigate, accept, transfer, or avoid, documented together with the rationale, the responsible owner, and an assessment of the residual exposure that remains after action. The taxonomy is established in ISO 31000:2018 (ISO, 2018b) and carried into the information security domain by ISO/IEC 27005:2022 (ISO, 2022c), with NIST CSF 2.0 (NIST, 2024) echoing the same four-option framing. Hubbard and Seiersen (2023) extend this to security specifically by advocating treatments evaluated against quantified costs and expected loss reductions



rather than chosen ad hoc. An example of the practice is an organization that, having applied technical controls, decides to transfer the residual cyber liability through an insurance policy, with the chief information security officer recorded as the owner of the residual risk acceptance.

4.3.4 Manage IT security compliances

This skill concerns the implementation and oversight of relevant standards, legal requirements, and best practices for information security. In the DR context, it links safety to governance: secure systems are not produced only through technical controls, but also through sustained compliance, documentation, accountability, and organizational routines. For education, this skill develops learners' capacity to recognize how security obligations are translated into practice.

4.3.4.1 Map controls against a recognized security framework

Mapping organizational controls against a recognized security framework provides a structured method for evaluating which controls are implemented, partially implemented, or absent, generating a gap analysis that establishes the basis for subsequent compliance work. The leading frameworks for this purpose are the NIST Cybersecurity Framework 2.0, organized around six functions including Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024), and the CIS Critical Security Controls version 8.1 (Center for Internet Security [CIS], 2024), which CIS reports is used by thousands of practitioners worldwide and which has been cited by several U.S. states as evidence of reasonable security. The mechanism is built into the design of CSF 2.0, which guides organizations to construct current-state and target-state Organizational Profiles whose gap defines the work program. A representative example is a mid-size firm mapping its existing controls against CSF 2.0 and identifying that incident response procedures under the Respond function are documented but not exercised, generating a specific remediation action.

4.3.4.2 Sustain compliance through evidence collection and audit-readiness routines

Sustaining compliance through evidence collection and audit-readiness routines requires the continuous gathering and preservation of records, such as logs, signed policies, training completions, configuration screenshots, and ticket histories, that demonstrate the operational reality of declared controls. ISO/IEC 27001:2022 (ISO, 2022a) requires planned internal audits, with certification dependent on the organization's ability to produce objective evidence over a three-year cycle. ISO 19011:2018 (ISO, 2018a) supplies the methodological foundation by establishing the evidence-based approach as a named audit principle, requiring that audit conclusions rest on verifiable records collected through defined procedures. Equivalent expectations govern SOC 2, PCI DSS, and FedRAMP



programmes, and the proliferation of compliance automation platforms reflects the practical scale of the requirement. An example application is the automated weekly export of access reviews from an identity management system into a compliance evidence repository, time-stamped and retained against the next audit cycle.

4.3.4.3 Manage non-conformities through corrective and preventive action

Managing non-conformities through corrective and preventive action (CAPA) requires a structured response to deviations, incidents, and audit findings, consisting of immediate correction, root cause analysis, corrective action to prevent recurrence, consideration of preventive action elsewhere, and effectiveness verification. The practice is mandated across the major management system standards, including ISO 9001 Clause 10.2 (ISO, 2015), ISO/IEC 27001 (ISO, 2022a), and the U.S. Food and Drug Administration's Quality System Regulation (Quality System Regulation, 1996), making it one of the most widely practiced compliance activities globally. The discipline that distinguishes CAPA from superficial correction is the explicit search for causes, typically conducted through methods such as the Five Whys, the Ishikawa diagram, or Pareto analysis. A representative example is a security team responding to a phishing-related breach by not only resetting the affected credentials but also identifying that the underlying cause was the absence of multi-factor authentication for a specific application class, leading to organization-wide enforcement.

4.4 Principle: Make it understandable

4.4.1 Accept own accountability

This skill concerns recognizing and accepting responsibility for one's own decisions, actions, and professional limits in digital contexts. In a DR perspective, it prevents responsibility from being displaced onto "the system," the organization, or the technology itself. Learners need to understand that digital tools may support decisions, but they do not remove human accountability.

4.4.1.1 Personal After-Action Review

A personal after-action review (AAR) is a structured, individual reflection protocol applied after a discrete task or event. The individual examines what was intended, what occurred, what caused the gap, and what they will do differently next time. This practice operationalizes accountability as a self-directed cognitive habit rather than a reactive social gesture. Consider a professional who uses an AI tool to draft a client-facing report and later



discovers that one section contained an unsupported claim. Using the AAR protocol, they examine what they intended to achieve, what actually occurred, why the error was not caught, and what they will do differently next time. They may identify that they relied too heavily on the AI output, failed to verify factual claims against primary sources, or did not clearly separate generated text from reviewed analysis. The practice is directly constitutive of the competency because it systematizes the retrospective examination of one's own contribution to outcomes. Tannenbaum and Cerasoli (2013) found that individual debriefs consistently improve performance by promoting structured reflection and goal-setting. The AAR protocol has been in continuous use across the U.S. Army, medical, and aviation communities for decades, and its application in professional development contexts is well established (Tannenbaum & Cerasoli, 2013).

4.4.1.2 Credible Error Acknowledgment in Digital Communication

Credible error acknowledgment is the practice of writing accountability statements that meet the structural requirements of an effective apology: naming the specific impact, accepting unambiguous ownership of the failure, and proposing a corrective step. Research on trust restoration consistently shows that vague or passive formulations fail to repair relational trust, whereas specific ownership language does (Lewicki et al., 2016; Schweitzer et al. 2006). In a professional digital responsibility context, this might involve a team member sending a written correction after sharing inaccurate data in a report, stating precisely what was wrong, what consequence it had, and what action they have taken. This practice is distinct from generic apology behavior because it focuses on the linguistic and structural choices that determine whether an acknowledgment is perceived as credible rather than performative. Lewicki et al. (2016) demonstrated that acknowledgment of responsibility and an offer of repair were the most critical elements for perceived credibility.

4.4.1.3 Recognising Self-Serving Attribution in One's Own Reasoning

A persistent obstacle to accepting accountability is the self-serving attribution bias, which leads individuals to credit successes to their own effort or ability while attributing failures to external circumstances. Recognizing this pattern in one's own reasoning is a trainable meta-cognitive skill that directly supports the competency. A finance professional who attributes a forecasting error to market volatility while crediting a successful prediction to their analytical rigor is demonstrating self-serving attribution. Understanding this bias requires familiarity with the three dimensions of attribution theory: locus, stability, and controllability (Weiner, 1986). Weiner's attributional theory of motivation provides the foundational framework, showing that the explanations people construct for their own outcomes shape their subsequent behaviour and responsibility-taking. Miller and Ross (1975) provided early empirical evidence that this bias is systematic and widespread. Awareness of self-serving attribution is a recognised element of reflective practice in management education,



precisely because naming and interrupting the pattern is a prerequisite for genuine retrospective accountability.

4.4.2 Assume responsibility

This skill refers to taking responsibility not only for one's own direct actions, but also for delegated tasks, downstream consequences, and the responsible execution of professional duties in digital settings. In educational terms, it broadens accountability from passive recognition to active stewardship. It is especially important where digital decisions are distributed across teams, vendors, and platforms.

4.4.2.1 Implementation Intentions for Accepted Commitments

When individuals accept responsibility for a task, the translation from intention to action is far from guaranteed. Implementation intentions address this gap by converting a stated commitment into a specific if-then plan: if situation X occurs, I will perform action Y. This practice is more granular and behaviourally specific than general goal-setting. A team member who has agreed to coordinate stakeholder feedback might form the plan: if I receive a deliverable without comments by Thursday, I will follow up with the responsible colleague directly. This level of specificity creates a reliable link between situational cues and goal-relevant behaviour. Gollwitzer and Sheeran (2006) shows that if-then planning substantially increases goal attainment across a wide range of domains and self-regulatory challenges. A more recent study tests confirmed these effects across cognitive, affective, and behavioral outcomes, with effect sizes largest when plans followed a contingent if-then format (Sheeran et al., 2024). Implementation intentions are particularly effective when the risk of failing to follow through is high, making this practice well-suited to professional responsibility contexts.

4.4.2.2 Explicit Scope-Setting and Handoff Agreements

Assuming responsibility requires not only a willingness to act but also a shared understanding of what one is and is not responsible for. Explicit scope-setting is the practice of negotiating and documenting the boundaries of one's duties before work begins, using structured tools such as a RACI matrix, a working agreement, or a handoff checklist. Without such clarity, overlapping or ambiguous responsibilities are a frequent cause of coordination failure in teams (Salas et al. 2005). In a cross-functional project where two departments both assume the other is responsible for client communication, the resulting gap can be prevented by a RACI entry assigning a single accountable owner at the outset. Salas et al. (2005) review of 20 years of teamwork research identified shared mental models and clear role differentiation as foundational coordinating mechanisms for effective team performance. The RACI matrix is one of the most widely adopted tools for externalising these



shared role models in professional practice, referenced in major project management frameworks including PMBOK and the IPMA Individual Competence Baseline.

4.4.2.3 Voluntary Stewardship of Shared Digital Resources

Assuming responsibility extends beyond the tasks one has been formally assigned. Voluntary stewardship is the practice of identifying and acting on responsibilities that have not been allocated to anyone, particularly in shared digital environments such as team wikis, shared inboxes, or collaborative code repositories. A team member who notices that a data governance procedure document is outdated and takes ownership of updating it, without being asked, is exercising this form of responsibility. The practice draws on the concept of organisational citizenship behaviour (OCB), defined by Organ (1988) as discretionary individual behaviour that is not formally rewarded but that contributes positively to the functioning of the organisation. Organ's framework helps explain why voluntary stewardship is not simply exceeding one's job description but is instead a recognisable and socially significant form of responsibility assumption. Research consistently links OCB to higher levels of organisational effectiveness, knowledge sharing, and team cohesion (Organ, 1988; Dekas et al. 2013). This practice is especially relevant in digital work contexts, where shared resources depend on collective maintenance rather than formal assignment.

4.4.3 Ensure information transparency

This skill concerns making relevant information accessible, clear, and complete for those affected by digital systems or decisions. Transparency in DR does not mean disclosing everything indiscriminately; it means providing meaningful information so that stakeholders can understand key processes, implications, and grounds for action. In education, this competence helps learners distinguish between formal disclosure and genuine intelligibility.

4.4.3.1 Provenance and Source Documentation

Information transparency requires that the origin and chain of custody of information be made visible to those who use it. Provenance documentation is the practice of recording the source, date, version, and lineage of a piece of information so that others can assess its quality, trace its origin, and reproduce the reasoning that depended on it. A policy analyst who cites a dataset in a briefing note and includes the date of access, the issuing body, and the version number is applying this practice. This corresponds directly to what the World Wide Web Consortium formalized in its PROV standard (W3C, 2013), which characterizes provenance as essential documentation for establishing the origin, quality, trust, and authorship of data. The W3C PROV specifications have been adopted in scientific research,

open data, and software development as the technical norm for provenance representation. Source documentation is a structural requirement for ensuring that information can be evaluated independently of the claims derived from it, which is the core concern of the competency.

4.4.3.2 Disclosing Uncertainty and Limitations

Being transparent about information means more than saying where it came from. It also means explaining how sure you are, what is still unknown, and where the evidence stops. For example, if an organization uses an AI tool to help screen job applications, it should not only say that AI is being used. It should also explain what the tool is meant to do, how reliable its results are, what data it was tested on, and where its results may be less accurate or biased. This helps people understand the limits of the system and question its outcomes when needed. Bhatt et al. (2021) ground this practice, arguing that explaining a model's behavior is insufficient unless stakeholders also receive information about where the model may lack the knowledge to perform reliably.

4.4.3.3 Disclosing Conflicts of Interest and Communicator Stakes

Evaluating information requires knowing not only what it claims and how certain it is, but also who is making the claim and whether they have a stake in how it is received. Disclosing conflicts of interest is the practice of explicitly naming one's financial interests, organisational affiliations, role, or involvement of tools and processes that a reasonable recipient would need in order to assess the information. A consultant presenting market research, for instance, should disclose any commercial relationship with the company being evaluated. Resnik (2023) provides the normative framework for this practice in professional and scientific contexts. Conflict-of-interest disclosure is institutionally mandated in biomedical research, financial services, journalism, and legal practice across most professional jurisdictions. Its underlying rationale is that transparency about the communicator's position is inseparable from the credibility of the information itself.

4.4.4 Provide information

This skill refers to supplying information that is accurate, appropriate to the audience, and fit for the relevant context. In a DR framework, it is closely related to responsible communication: stakeholders need information that is not only available, but also correct, comprehensible, and usable for decision-making. This skill matters because poor communication can itself become a source of digital harm, confusion, or mistrust.

4.4.4.1 Audience-Adapted Framing and Plain Language

Providing information effectively requires that content be shaped to match the prior knowledge, needs, and context of its intended recipients. Audience-adapted framing is the practice of analysing the audience before communicating and adjusting vocabulary, conceptual entry points, reading level, and examples accordingly. A data scientist presenting findings to a non-technical steering committee, for instance, replaces statistical terminology with plain-language equivalents and uses concrete numerical examples rather than methodological descriptions. Clark (1996) provides the theoretical foundation through his concept of common ground and recipient design: speakers construct utterances based on a shared model of what the listener already knows, and effective communication requires building an accurate model of that knowledge state before deciding how to frame a message. This practice connects directly to the competency because information that is technically accurate but pitched above or below the recipient's level of understanding fails in its purpose. Plain language and audience adaptation are also institutionally mandated across many professional and public-sector communication contexts, reinforcing their status as a recognised professional practice.

4.4.4.2 Proactive Sharing and Information Push

Providing information is not only a matter of responding accurately when asked; it also involves the active judgment of who needs to know something and whether they have been told. Proactive sharing is the practice of anticipating others' information needs and distributing relevant content without waiting to be prompted, including status updates, decisions with downstream consequences, and findings that another person or team would need to act effectively. A project lead who completes an internal review and immediately brings a relevant finding to the attention of a downstream colleague, before that colleague thinks to enquire, is applying this practice. Wegner's (1987) transactive memory theory provides the conceptual basis: in high-performing groups, members develop shared awareness of who knows what and route information accordingly. Research consistently shows that teams with effective information-routing behaviors substantially outperform those without (Wegner, 1987; Choi, Lee, & Yoo, 2010). Proactive sharing is the behavioral expression of the competency at the level of ongoing work practice, rather than a one-time communication event.

4.4.4.3 Structuring Information for Findability and Quick Uptake

The act of providing information is only complete when the recipient can locate and use what has been shared. Structuring for findability is the practice of organizing content so that its core message is accessible without requiring recipients to read in full: placing the key point first, using descriptive headings, creating a scannable hierarchy, and adding appropriate metadata. A policy analyst who submits a briefing with the recommendation in the opening paragraph, supported by clearly headed sections, enables a decision-maker to



act efficiently even under time pressure. The bottom-line-up-front (BLUF) principle originates in U.S. Army Regulation 25-50 and is standard in military and government communication for precisely this reason. Redish (2012) synthesized decades of usability research into practical document-design principles, demonstrating that readers scan before they read and that structural choices determine whether information is ultimately found and used. Information that is accurate but structurally inaccessible is not effectively provided, making this practice integral to the competency.

5 Methodology

5.1 Research approach

The development of the framework followed a Design Science Research (DSR) logic. DSR is appropriate because the project requires a practically usable artefact, namely a DR competence framework for education, that is grounded in theory and open to iterative refinement. The framework is therefore best understood as a designed artefact produced through the combination of conceptual synthesis, project requirements, and progressive evaluation. The process of conceptualizing the DR Competence Framework followed a Peffers et al. (2007) DSR process, Figure 2, which structures design research into six activities: (1) problem identification and motivation, (2) definition of objectives of a solution, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication in an iterative sequence.

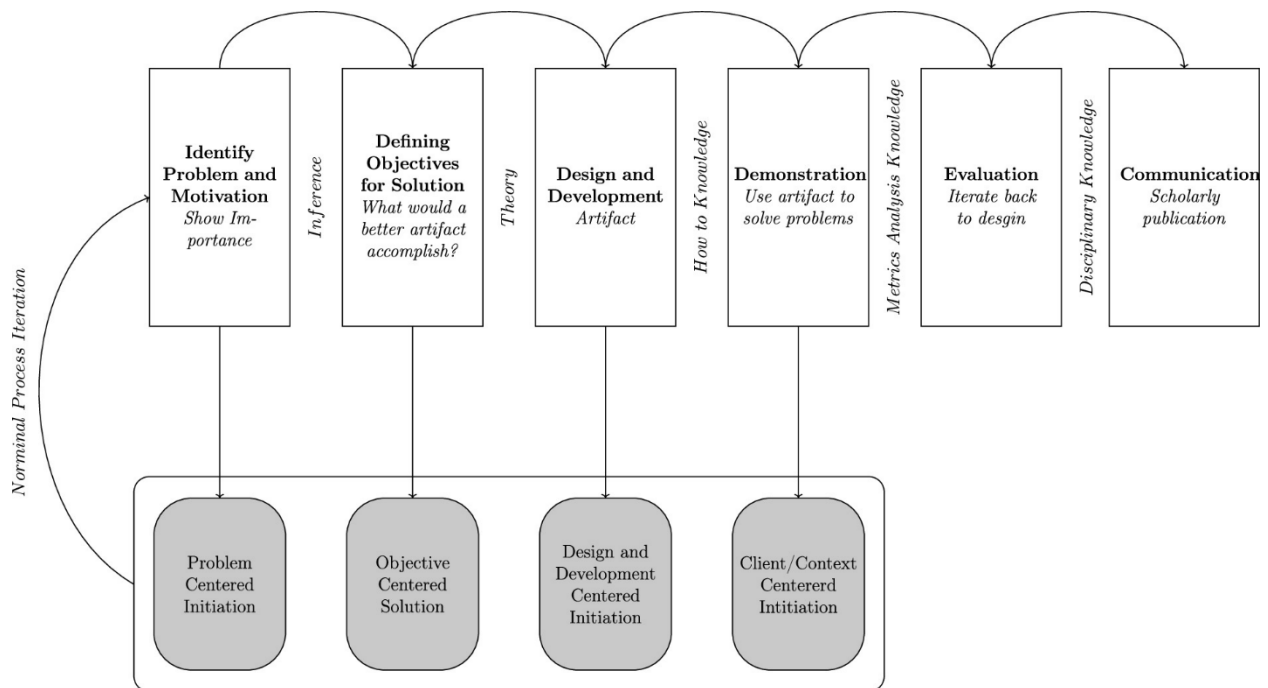


Figure 2: DSR process illustrated by Brinker (2024), based on Peffers et al. (2007)

5.1.1 Problem identification and motivation

The first step of the DSR process was problem identification. This was conducted through a combination of literature review and empirical input from practice. First, an extensive review of academic literature on DR was undertaken to examine existing principles, conceptualizations, and implementation approaches. In parallel with the literature analysis, real-world DR dilemmas were collected from project consortium members. Both the literature and the initial empirical outreach among the consortium converge on the view that digitalization creates ethical dilemmas that are cross-sectoral, practically relevant, and insufficiently addressed through compliance or purely technical skills alone. Furthermore, existing work does not explicitly articulate the skills and competencies required for effective implementation. Existing approaches tend either to remain highly abstract or to focus on narrower areas such as AI ethics, digital rights, or data governance. DIRECT therefore requires a framework that is broad enough to encompass DR as a whole while concrete enough to guide education and training.

5.1.2 Definition of Objectives of a solution

The second step is to translate the identified problems into concrete and justified design objectives (Peffers et al., 2007). These objectives are supposed to guide the development of the research artifact. For the DR Competence Framework, the objectives were derived directly from the conceptual and empirical shortcomings identified in the preceding phase. To conceptualize the framework, the objectives of the solution are derived directly from the conceptual and empirical shortcomings identified in the preceding phase. Given the fragmented, largely normative, and context-insensitive nature of existing DR approaches,

the primary objective is to develop an integrative framework that systematically structures the principles, dimensions, and practices of DR in an organizational context. The framework is intended to move beyond abstract ethical guidelines by providing actionable guidance that supports consistent and transparent application across different organizational settings.

In addition, the solution seeks to explicitly address the human and organizational capabilities required for the effective implementation of DR. To this end, an objective of the artifact is the development of a skills–competency mapping framework that aligns specific DR dimensions with the knowledge, skills, and competencies required to enact them. By systematically linking DR principles to competencies, the solution supports organizations in identifying capability gaps, guiding training initiatives, and allocating responsibilities in a more informed manner.

Collectively, these objectives define the functional and conceptual requirements for the designed artifact and provide a clear link between the identified problem space and the subsequent design and development activities. In accordance with the DSR approach, the explicit articulation of solution objectives ensures traceability between problem identification, artifact construction, and later evaluation, thereby strengthening both the rigor and relevance of the research.

5.1.3 Design and development of the DR Competence Framework

The design and development activity represents the core phase of the DSR approach, in which the objectives defined in the preceding stage are translated into a concrete research artifact. The framework was developed through several iterations within the DR Team at BFH. Initially based on Trier et al. (2023)'s framework, 8 DR principles were mapped against the European Skills, Competences, Qualifications, and Occupations (ESCO) classification. This step was necessary to move from a conceptual and normative understanding of DR toward an educational framework. Given the extensive scope of the ESCO taxonomy, which comprises more than 14,000 skills and competences, a multi-stage selection procedure was employed. In the first stage, we screened the ESCO database for skills potentially related to the 8 principles from Trier et al. (2023). This process was kept intentionally broad in order to ensure that all potentially relevant skills were captured (see the following example). After several iterations using automated text-matching, we converged on 1,000 skill and competence labels that were subsequently subjected to manual screening. Each skill was assessed in terms of its conceptual fit with the the 8 DR principles (Trier et al., 2023) and its relevance for either PDR or CDR level. Skills that were too generic, only loosely related, or redundant, were removed, while others were reclassified to ensure coherence across principles and levels.

5.1.4 Demonstration

According to Peffers et al. (2007), demonstration refers to showing how the artefact can be used to address the identified problem. In this project, the preliminary DR Competence Framework was demonstrated in a project consortium meeting held in Athens, Figure 3. During this session, consortium partners worked with a pre-filtered set of ESCO skills and attempted to match these skills to the preliminary framework dimensions derived from Trier et al. (2023). Where necessary, participants were also invited to add further skill descriptions that they considered relevant to the respective DR principles.

This demonstration served two purposes. First, it enabled the project team to assess whether the preliminary framework could be meaningfully applied by stakeholders outside the immediate research team. Second, it provided a realistic application setting in which the usability, interpretability, and completeness of the framework could be explored through collaborative use. In this sense, the consortium meeting functioned as a practical instantiation of the artefact in a setting closely aligned with its intended use.

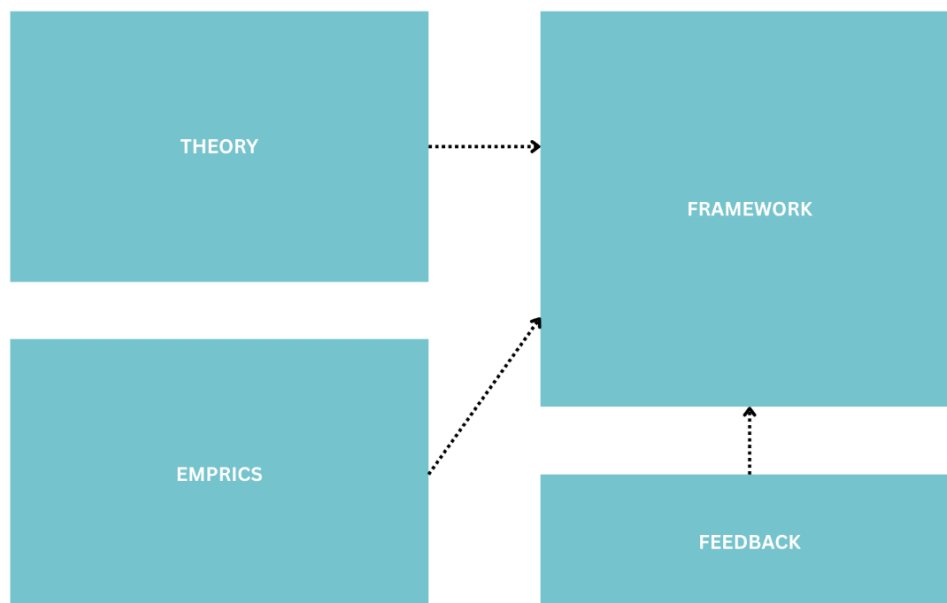


Figure 3: Demonstration of interim DR framework artefact

5.1.5 Evaluation

The fifth step in the DSR process is evaluation, that is, assessing how well the artefact meets the defined objectives and addresses the identified problem (Peffers et al., 2007). In the present study, evaluation was conducted through the structured discussions and reflections that emerged from the consortium workshop in Athens. The workshop generated



substantive feedback on the applicability and comprehensibility of the preliminary framework dimensions, particularly with regard to their suitability for a competence-oriented educational artefact.

The evaluation showed that several of the principles proposed by Trier et al. (2023) were perceived by participants as too abstract to be translated into a DR competence framework. For example, the principle of *Functionality* proved difficult for participants to interpret consistently and was therefore considered insufficiently suited to the project's design objective of creating a practically usable educational framework. More broadly, the evaluation indicated that some principles were conceptually valuable at a normative level, but lacked the specificity required for competence identification, curriculum design, and training-oriented application.

Based on this evaluative feedback, the framework was revised once more. The additional input provided by consortium members informed a further iteration of the design, ultimately leading to the final version of the framework presented in this report. The evaluation should thus be understood as formative and iterative: rather than serving as a summative end-point, it directly informed the refinement of the artefact and improved its practical usability and conceptual fit.

5.1.6 Communication

The final step of the DSR process is communication. In accordance with Peffers et al. (2007), the resulting artefact and the knowledge generated through its development are communicated to relevant audiences in forms appropriate to both research and practice. In the present project, the primary vehicle of communication is this deliverable, which documents the problem context, design process, evaluation, and final artefact. Beyond the report itself, the framework is intended to be disseminated further through practitioner-oriented and scientific publications, as envisaged in the DIRECT project plan.

Through this communication, the project seeks not only to document the developed artefact, but also to contribute to ongoing scholarly and practical discussions on how DR can be translated into actionable educational and organizational capabilities.

6 Next steps

The next phase of the project entails a transition from WP2 to WP3. This transition also requires close alignment of the work across both work packages, ensuring that the conceptual outputs of WP2 are consistently reflected in the design and content of WP3. Further, this involves developing specific case-based scenarios based on real-world sources, selecting and refining situations that illustrate key dilemmas related to DR. These



cases will be designed to align with the identified principles and ESCO-linked competences and will include guiding questions and learning activities to support reflection, discussion, and decision-making. In this way, the transition from WP2 to WP3 marks the shift from framework-building to the practical creation of teaching and learning resources.





References

- Aragón, P., Kaltenbrunner, A., Calleja-López, A., Pereira, A., Monterde, A., Barandiaran, X. E., & Gómez, V. (2017). Deliberative platform design: The case study of the online discussions in Decidim Barcelona. In *Lecture Notes in Computer Science* (pp. 277–287). Springer. https://doi.org/10.1007/978-3-319-67256-4_22
- Arcep, Arcom, ADEME, DINUM, & Institut du Numérique Responsable. (2024). *Référentiel général d'écoconception de services numériques (RGESN), version mai 2024*. République Française. <https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/>
- Bertino, E., & Sandhu, R. (2005). Database security: Concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing*, 2(1), 2–19. <https://doi.org/10.1109/TDSC.2005.9>
- Bhatt, U., Antorán, J., Zhang, Y., Liao, Q. V., Sattigeri, P., Fogliato, R., Gauthier Melançon, G., Krishnan, R., Stanley, J., Tickoo, O., Nachman, L., Chunara, R., Srikumar, M., Weller, A., & Xiang, A. (2021). Uncertainty as a form of transparency: Measuring, communicating, and using uncertainty. *Proceedings of the AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society*, 401–413. <https://doi.org/10.1145/3461702.3462571>
- Biega, A. J., Potash, P., Daumé, H., Diaz, F., & Finck, M. (2020). Operationalizing the legal principle of data minimization for personalization. In *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 399–408). ACM. <https://doi.org/10.1145/3397271.3401034>
- Black Duck Software. (2025). *2025 open source security and risk analysis (OSSRA) report* (10th ed.). <https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html>
- Blancco Technology Group & Kroll Ontrack. (2016). *The leftovers: A data recovery study* [Industry report]. Blancco Technology Group.
- Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., & Krathwohl, D. R. (1956). *Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain*. Longman.
- Bourdoucen, A., & Lindqvist, J. (2024). Privacy of default apps in Apple's mobile ecosystem. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Article 786). Association for Computing Machinery. <https://doi.org/10.1145/3613904.3642831>
- Brinker, J. (2024). Design Science Research: Ein problemfokussierter Forschungsansatz. In *Macht und Digitalisierung innerhalb der Supply Chain: Eine Betrachtung von Machtstrukturen unter Einfluss der Digitalisierung und der digitalen Transformation* (pp. 81–121). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-43866-1_3



- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In S. A. Friedler & C. Wilson (Eds.), *Proceedings of Machine Learning Research* (Vol. 81, pp. 1–15). PMLR.
- Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
- Center for Internet Security. (2024). *CIS critical security controls version 8.1*. <https://www.cisecurity.org/controls>
- Cox, L. A., Jr. (2008). What's wrong with risk matrices? *Risk Analysis*, 28(2), 497–512. <https://doi.org/10.1111/j.1539-6924.2008.01030.x>
- Danish Institute for Human Rights. (2020). *Guidance on human rights impact assessment of digital activities*. Danish Institute for Human Rights.
- Dansk Design Center. (n.d.). *Toolkit: The Digital Ethics Compass*. <https://ddc.dk/vaerktoejer/toolkit-the-digital-ethics-compass/>
- European Commission. (2019). *Ethics guidelines for trustworthy AI*. High-Level Expert Group on Artificial Intelligence. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- European Commission. (2020). *A new circular economy action plan for a cleaner and more competitive Europe*(COM/2020/98 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0098>
- European Commission. (n.d.). *ESCO: European Skills, Competences, Qualifications and Occupations*. <https://esco.ec.europa.eu/en>
- European Data Protection Board. (2023). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: How to recognise and avoid them* (Version 2.0). https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf



- Faria, P. C. S., & Labutong, N. (2020). A description of four science-based corporate GHG target-setting methods. *Sustainability Accounting, Management and Policy Journal*, 11(3), 591–612. <https://doi.org/10.1108/SAMPJ-03-2017-0031>
- Freitag, C., Berners-Lee, M., Widdicks, K., Knowles, B., Blair, G. S., & Friday, A. (2021). The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations. *Patterns*, 2(9), Article 100340. <https://doi.org/10.1016/j.patter.2021.100340>
- Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems*, 14(3), 330–347. <https://doi.org/10.1145/230538.230561>
- Gallego-Arrufat, M.-J., García-Martínez, I., Romero-López, M.-A., & Torres-Hernández, N. (2024). Digital rights and responsibility in education: A scoping review. *Education Policy Analysis Archives*, 32(3). <https://doi.org/10.14507/epaa.32.7899>
- Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé, H., III, & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, 64(12), 86–92. <https://doi.org/10.1145/3458723>
- Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. In *Proceedings of the 4th International Conference on Computers, Privacy & Data Protection (CPDP 2011)*. KU Leuven.
- Halskov, K., & Hansen, N. B. (2014). The diversity of participatory design research practice at PDC 2002–2012. *International Journal of Human-Computer Studies*, 74, 81–92. <https://doi.org/10.1016/j.ijhcs.2014.09.003>
- Hardebolle, C., Macko, V., Ramachandran, V., Holzer, A., & Jermann, P. (2023). Digital ethics canvas: A guide for ethical risk assessment and mitigation in the digital domain. In *Proceedings of the 51st SEFI Annual Conference 2023*. European Society for Engineering Education. <https://doi.org/10.21427/9WA5-ZY95>
- Harrington, C., Erete, S., & Piper, A. M. (2019). Deconstructing community-based collaborative design. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), Article 229. <https://doi.org/10.1145/3359318>
- Hollimon, L. A., Taylor, K. V., Fiegenbaum, R., Carrasco, M., Garchitorena Gomez, L., Chung, D., & Seixas, A. A. (2025). Redefining and solving the digital divide and exclusion to improve healthcare: Going beyond access to include availability, adequacy, acceptability, and affordability. *Frontiers in Digital Health*, 7, Article 1508686. <https://doi.org/10.3389/fdgth.2025.1508686>
- Huang, C., Zhang, Z., Mao, B., & Yao, X. (2022). An overview of artificial intelligence ethics. *IEEE Transactions on Artificial Intelligence*, 4(4), 799–819. <https://doi.org/10.1109/TAI.2022.3194503>
- Hubbard, D. W., & Seiersen, R. (2023). *How to measure anything in cybersecurity risk* (2nd ed.). Wiley.



- International Organization for Standardization & International Electrotechnical Commission. (2020). *Information technology — OpenChain specification* (ISO/IEC 5230:2020). <https://www.iso.org/standard/81039.html>
- International Organization for Standardization & International Electrotechnical Commission. (2021). *Information technology — SPDX specification V2.2.1* (ISO/IEC 5962:2021). <https://www.iso.org/standard/81870.html>
- International Organization for Standardization & International Electrotechnical Commission. (2024). *Information technology — Software carbon intensity (SCI) specification* (ISO/IEC 21031:2024). <https://www.iso.org/standard/86612.html>
- International Organization for Standardization. (2015). *Quality management systems: Requirements* (ISO 9001:2015).
- International Organization for Standardization. (2018a). *Guidelines for auditing management systems* (ISO 19011:2018).
- International Organization for Standardization. (2018b). *Risk management: Guidelines* (ISO 31000:2018).
- International Organization for Standardization. (2022a). *Information security, cybersecurity and privacy protection: Information security management systems: Requirements* (ISO/IEC 27001:2022).
- International Organization for Standardization. (2022b). *Information security, cybersecurity and privacy protection: Information security controls* (ISO/IEC 27002:2022).
- International Organization for Standardization. (2022c). *Information security, cybersecurity and privacy protection: Guidance on managing information security risks* (ISO/IEC 27005:2022).
- International Organization for Standardization. (2025). *The ISO survey of management system standard certifications 2024*. <https://www.iso.org/the-iso-survey.html>
- Irish Data Protection Commission. (2023). *Guidance note: Records of processing activities (RoPA) under Article 30 GDPR*. <https://www.dataprotection.ie>
- Joint Research Centre, European Commission. (2022). *Towards an effective right to repair for electronics: Overcoming legal, political and supply barriers to contribute to circular electronics in the EU*. Publications Office of the European Union. <https://op.europa.eu/en/publication-detail/-/publication/10373afc-1f6b-11ed-8fa0-01aa75ed71a1/language-en>
- Kaminski, M. E., & Urban, J. M. (2021). The right to contest AI. *Columbia Law Review*, 121(7), 1957–2048. https://columbialawreview.org/wp-content/uploads/2021/11/Kaminski-Urban-The_Right_to_Contest_AI.pdf
- KPMG International. (2024). *Survey of sustainability reporting 2024: The move to mandatory reporting*. <https://kpmg.com/xx/en/our-insights/esg/the-move-to-mandatory-reporting.html>
- Liu, B., Andersen, M. S., Schaub, F., Almuhiemedi, H., Zhang, S. A., Sadeh, N., Agarwal, Y., & Acquisti, A. (2016). Follow my recommendations: A personalized privacy assistant



- for mobile app permissions. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 27–41). USENIX Association.
- López, A. E. A., Cajiao, M. C. R., Mejia, M. P., Durán, L. F. P., & Díaz, E. E. E. (2018). Participatory design and technologies for sustainable development: An approach from action research. *Systemic Practice and Action Research*, 32(2), 167–191. <https://doi.org/10.1007/s11213-018-9459-6>
- Microsoft. (n.d.). *Security development lifecycle (SDL)*. Retrieved June 1, 2026, from <https://www.microsoft.com/en-us/securityengineering/sdl>
- Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT'19)** (pp. 220–229). Association for Computing Machinery. <https://doi.org/10.1145/3287560.3287596>
- National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30, Rev. 1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-30r1>
- National Institute of Standards and Technology. (2014). *Guidelines for media sanitization* (NIST Special Publication 800-88, Rev. 1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-88r1>
- National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Nemat, A. T., Becker, S. J., Lucas, S., Thomas, S., Gadea, I., & Charton, J. E. (2023). The principle-at-risk analysis (PaRA): Operationalising digital ethics by bridging principles and operations of a digital ethics advisory panel. *Minds and Machines*, 33(5), 737–760. <https://doi.org/10.1007/s11023-023-09654-w>
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Paper 194, pp. 1–13). Association for Computing Machinery. <https://doi.org/10.1145/3313831.3376321>
- Obwegeser, N., Peškova, M., Hall, M., & Grispos, G. (2026). Digital responsibility as responsible organizing. *Journal of Information Technology Case and Application Research*, 1-7.
- OECD. (2020). *Innovative citizen participation and new democratic institutions: Catching the deliberative wave*. OECD Publishing. <https://doi.org/10.1787/339306da-en>
- Open Source Security Foundation. (2023). *Supply-chain levels for software artifacts (SLSA) specification v1.0*. The Linux Foundation. <https://slsa.dev/spec/v1.0/>
- Organisation for Economic Co-operation and Development. (n.d.). *AI principles*. <https://www.oecd.org/en/topics/ai-principles.html>



- Pappas, I. O., Mikalef, P., Dwivedi, Y. K., Jaccheri, L., & Krogstie, J. (2023). Responsible digital transformation for a sustainable society. *Information Systems Frontiers*, 25(3), 945–953. <https://doi.org/10.1007/s10796-023-10406-5>
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Power, C., Freire, A., Petrie, H., & Swallow, D. (2012). Guidelines are only half of the story: Accessibility problems encountered by blind users on the web. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)* (pp. 433–442). ACM. <https://doi.org/10.1145/2207676.2207736>
- PwC. (2024). *From principles to practice: Responsible AI in action*. <https://www.strategy-business.com/article/From-principles-to-practice-Responsible-AI-in-action>
- Recker, J., Chatterjee, S., Sundermeier, J., & Tarafdar, M. (2025). Digital responsibility: Current perspectives and future directions. *Journal of the Association for Information Systems*, 26(5), 1222–1238. <https://doi.org/10.17705/1jais.00966>
- Rømen, D., & Svanæs, D. (2012). Validating WCAG versions 1.0 and 2.0 through usability testing with disabled users. *Universal Access in the Information Society*, 11(4), 375–385. <https://doi.org/10.1007/s10209-011-0259-3>
- Roozenbeek, J., van der Linden, S., & Nygren, T. (2020). Prebunking interventions based on the psychological theory of "inoculation" can reduce susceptibility to misinformation across cultures. *Harvard Kennedy School Misinformation Review*, 1(2). <https://misinforeview.hks.harvard.edu/article/global-vaccination-badnews/>
- Santa Clara Principles. (2021). *The Santa Clara Principles on transparency and accountability in content moderation* (2nd ed.). <https://santaclaraprinciples.org/>
- Scheerder, A., Van Deursen, A., & Van Dijk, J. (2017). Determinants of internet skills, uses and outcomes: A systematic review of the second- and third-level digital divide. *Telematics and Informatics*, 34(8), 1607–1624. <https://doi.org/10.1016/j.tele.2017.07.007>
- Science Based Targets initiative. (2026). *SBTi trend tracker 2025*. <https://files.sciencebasedtargets.org/production/files/SBTi-TrendTracker-Apr-2026.pdf>
- Siegman, T. (2023). *Introducing Web Sustainability Guidelines*. World Wide Web Consortium. <https://www.w3.org/blog/2023/introducing-web-sustainability-guidelines/>
- Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-218>



- Suzor, N. P., West, S. M., Quodling, A., & York, J. (2019). What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. *International Journal of Communication*, 13, 1526–1543.
- Swiss Post. (2024). *Digital ethics guidelines: Ambitions and support with developing trustworthy digital services*. https://www.post.ch/-/media/portal-opp/k/dokumente/corporate-responsibility/leitfaden-digitaethik-a4.pdf?sc_lang=en&hash=DFB07A4B27FBDC3ADFE6F103832F12ED
- Thoughtworks. (2023). *Responsible technology playbook: Tools for the United Nations*. Thoughtworks & United Nations.
- Trier, M., Kundisch, D., Beverungen, D., Müller, O., Schryen, G., Mirbabaie, M., & Trang, S. (2023). Digital responsibility: A multilevel framework for responsible digitalization. *Business & Information Systems Engineering*, 65(4), 463–474. <https://doi.org/10.1007/s12599-023-00822-x>
- United Nations. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. United Nations Office of the High Commissioner for Human Rights.
- Verizon. (2025). *2025 data breach investigations report*. <https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf>
- Vigo, M., Brown, J., & Conway, V. (2013). Benchmarking web accessibility evaluation tools. In *Proceedings of the 10th International Cross-Disciplinary Conference on Web Accessibility (W4A '13)* (pp. 1–10). ACM. <https://doi.org/10.1145/2461121.2461124>
- W3C. (2023). *Web Content Accessibility Guidelines (WCAG) 2.2*. World Wide Web Consortium. <https://www.w3.org/TR/WCAG22/>
- WebAIM. (2026). *The WebAIM Million: An annual accessibility analysis of the top 1,000,000 home pages*. <https://webaim.org/projects/million/>
- Whiting, R., & Pritchard, K. (2017). Digital ethics. In R. Mir & J. Jain (Eds.), *The SAGE handbook of qualitative business and management research methods* (Vol. 1, pp. 562–579). Sage.
- World Wide Web Consortium. (2013). *PROV-DM: The PROV data model (W3C Recommendation)*. <https://www.w3.org/TR/prov-dm/>



Co-funded by the
European Union



ARISTOTLE
UNIVERSITY OF
THESSALONIKI



idec

UNIVERSITY
OF TWENTE.



ZDRUŽENJE DELODAJALCEV
OBRTI IN PODJETNIKOV
SLOVENIJE



Berner
Fachhochschule



ESTABLISHED 1890

RUSE CHAMBER OF
COMMERCE AND INDUSTRY

ΔΕΛΤΑ 360

Σχολή Ανώτερης Επαγγελματικής Κατάρτισης



POLITEKNIKA
TXORIERRI

Dive deeper into the DIRECT project at
www.directproject.eu and see how we're
shaping responsible digital future.



@DIRECT Project



@DIRECT Project