Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

COEUS TRAINING PRESENTATIONS

Additional material for the trainers



UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

CDR train the trainers programes

VŽ KC

MMI



First Day Online
05.05.2025.

Martina Mak
University North
Varaždin, Croatia

Basic understand of the Course CDR for the trainee

COEUS

What is the concept of CDR?

Based on a substantial body of scientific and professional work, as well as practical application, Corporate Digital Responsibility (CDR) can be defined as a set of practices, norms, and values through which organizations manage digital technologies and data in a socially, economically, and environmentally responsible manner. There is no universally accepted definition of CDR. Various interpretations exist, largely aligned on fundamental principles but incorporating additional factors depending on industry and context.CDR is still in a developmental phase, with its application in the economy, particularly among small and medium-sized enterprises (SMEs), being relatively new.

We propose that digital technologies and related data become increasingly prevalent and that, consequently, ethical concerns arise. Looking at four principal stakeholders, we propose corporate digital responsibility (CDR) as a novel concept. We define CDR as the set of shared values and norms guiding an organization's operations with respect to four main processes related to digital technology and data. These processes are the creation of technology and data capture, operation and decision making, inspection and impact assessment, and refinement of technology and data.

Basic understand of the

Course CDR



For the last couple of decades, digital advances have enabled a wide variety of systems with vast capabilities. Specifically, the benefits of automation, data analytics, artificial intelligence (AI), and machine learning to society are increasingly evident in daily life (Brynjolfsson & McAfee, 2017), and applications range from fulfilling consumer requests, making lending decisions, providing health advice, taking on high-risk jobs, protecting endangered species, to transporting people and goods (Wirtz et al., 2018). Yet along with this unprecedented power comes ethical dilemmas, in both consumer and business contexts, such as those associated with smart devices that constantly record data, the actions of autonomous vehicles in dangerous situations, and algorithms making recruitment decisions. Even if introduced with the best of intentions, malleable AI systems can be at risk of exploitation for unintended purposes (e.g., Nambisan et al., 2017, Richter and Riemer, 2013). It is the responsibility of system designers and the organizations that use these systems to recognize that their technologies may be used in ways other than they had anticipated with unwanted consequences for different stakeholders and society at large. However, existing research providing guidance for organizations in the face of ethical dilemmas related to the digital is scant.

Background history

In this sense, digital technologies that assist in human decision making or make decisions autonomously need to be subject to moral norms and ethical considerations similar to those that apply to humans. If we accept the premise that human behavior (individual and collective) should be governed by moral norms and ethical considerations, then any creation, operation, impact assessment, and refinement of digital technology and data should be assessed according to such rules.

This argument presupposes that ensuring the ethical design and uses of digital technologies and related data is not solely a technological challenge (e.g., developing algorithms for ethical reasoning). Rather, it requires organizations to develop a comprehensive, coherent set of norms, embedded in their organizational culture, to govern the development and deployment of digital technology and data. We refer to this idea as corporate digital responsibility (CDR), defined as the set of shared values and norms guiding an organization's operations with respect to the creation and operation of digital technology and data. It requires tech companies, individual developers and designers, and any corporate actor employing digital technologies or data processing to be aware that the code they produce or deploy, as well as data they collect and process, inherently create an ethical responsibility for them. Consequently, organizations must determine how to operate responsibly in the digital age, while also complying with legal requirements and considering economic impacts on the organization (Schwartz & Carroll, 2003).

CDR vs CSR

Corporate Digital Responsibility (CDR) and Corporate Social Responsibility (CSR) are both frameworks guiding organizations to act responsibly, but they differ in scope and focus.

Key Differences

Aspect	Corporate Social Responsibility (CSR)	Corporate Digital Responsibility (CDR)
Scope	Broad: social, environmental, ethical, and economic	Focused: digital technologies, data, and digital impact
Focus Areas	Environment, ethics, philanthropy, community, governance	Data privacy, cybersecurity, AI ethics, digital inclusion, digital environmental impact
Purpose	Ensure positive impact on society and the environment	Ensure responsible use and impact of digital tech
Drivers	Societal expectations, regulations, stakeholder pressure	Digital transformation, data proliferation, tech risks
Examples	Reducing emissions, fair labor, charitable giving	Data protection, algorithmic fairness, digital accessibility, managing e-waste
Relationship	Foundational framework	Extension or complement to CSR, addressing digital-specific challenges

How They Relate and Differ

CSR is the overarching concept that companies should operate in ways that benefit society and minimize harm, traditionally covering environmental stewardship, ethical conduct, philanthropy, and economic responsibility.

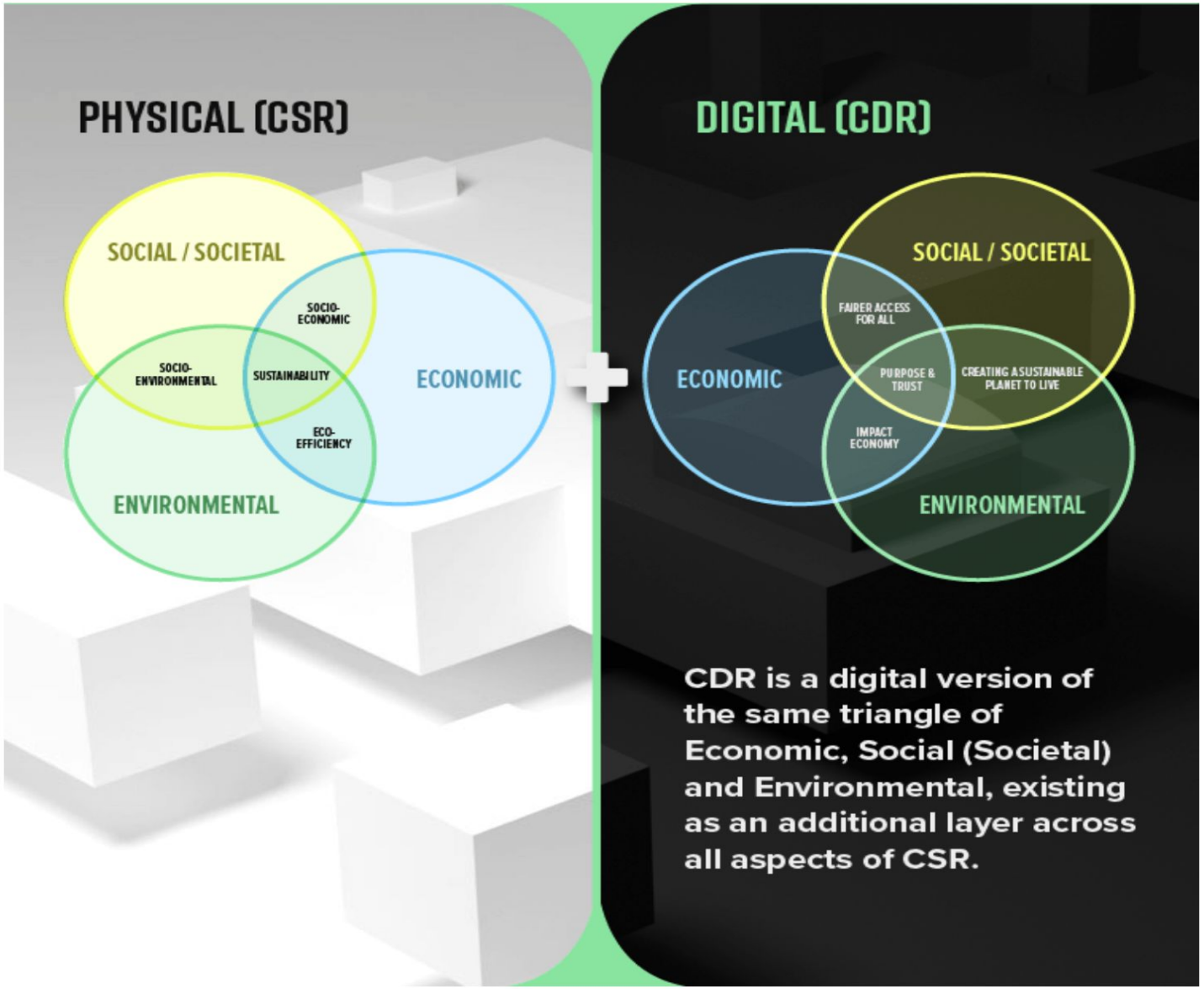
CDR is an emerging extension of CSR that specifically addresses the ethical, social, and environmental responsibilities related to digital technologies and data. It covers issues like data privacy, AI bias, digital accessibility, and the carbon footprint of IT infrastructure.

While CDR builds on CSR's principles of trust, accountability, and stakeholder engagement, it introduces new challenges unique to the digital age-such as managing data responsibly, ensuring digital inclusion, and mitigating the environmental impact of digital operations



CDR is a new and unavoidable extension of CSR, which is based on the same principles of trust, accountability, ethics and exchanges with companies stakeholders. The cross-cutting nature of digital technology and its omnipresence mean that the value creation it generates must be understood and shared by all, with regard to democratic, social and societal issues."

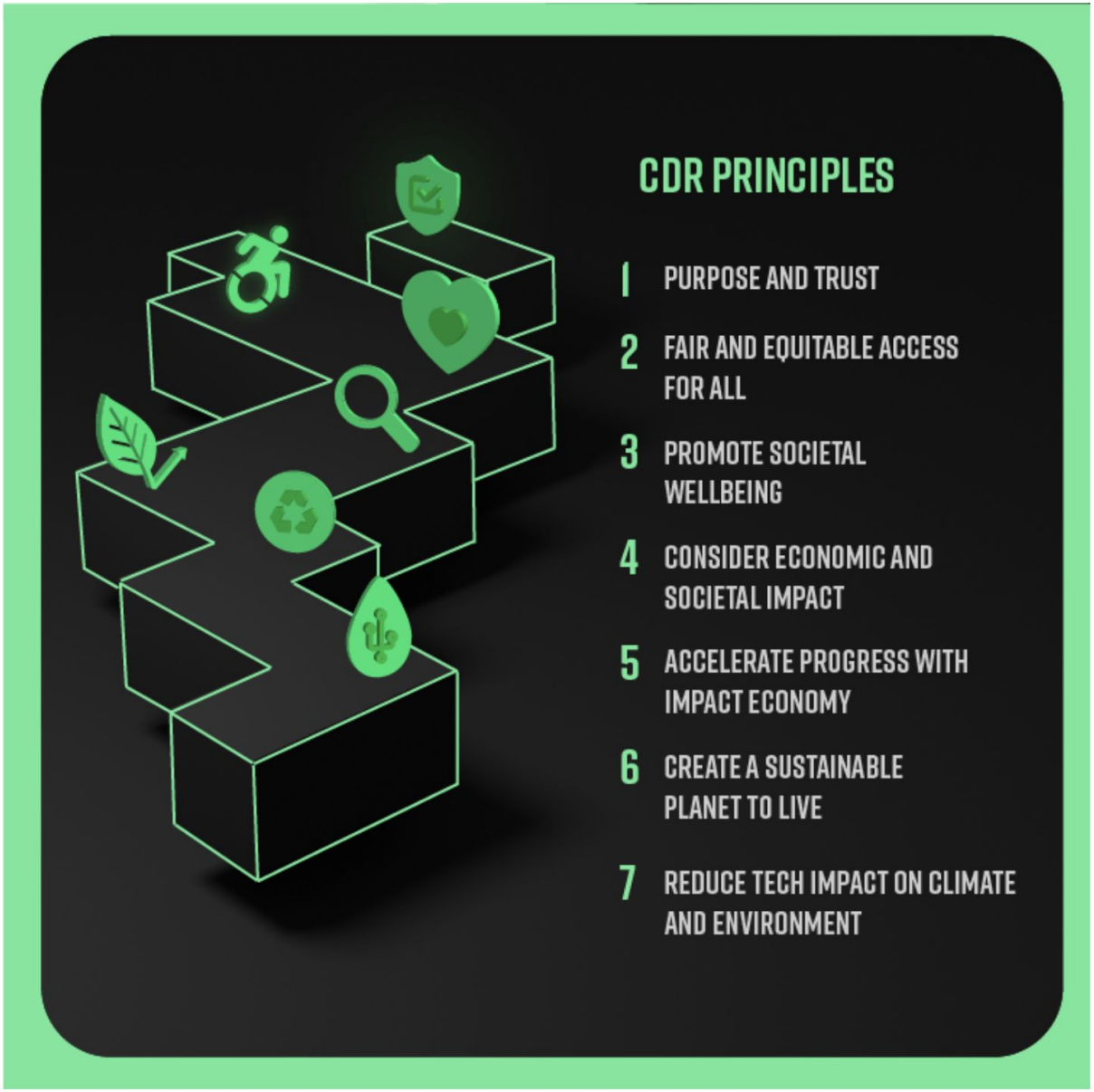
CSR is about a company's overall responsibility to society, covering a wide range of issues. CDR zooms in on the digital dimension-how companies create, use, and manage technology and data responsibly. Both frameworks are complementary; CDR does not replace CSR but addresses gaps in traditional CSR related to digital transformation. In today's digital-first world, organizations are increasingly expected to embrace both CSR and CDR to build trust, drive innovation, and meet evolving stakeholder expectations.



ID: Side-by-side three-ring Venn diagrams showing the similarities between Corporate Social Responsibility (CSR) and Corporate Digital Responsibility (CDR). Bottom right text reads "CDR is the digital realization of the same triangle of Economic, Social (Societal), and Environmental, existing as an additional layer across all aspects of CSR."

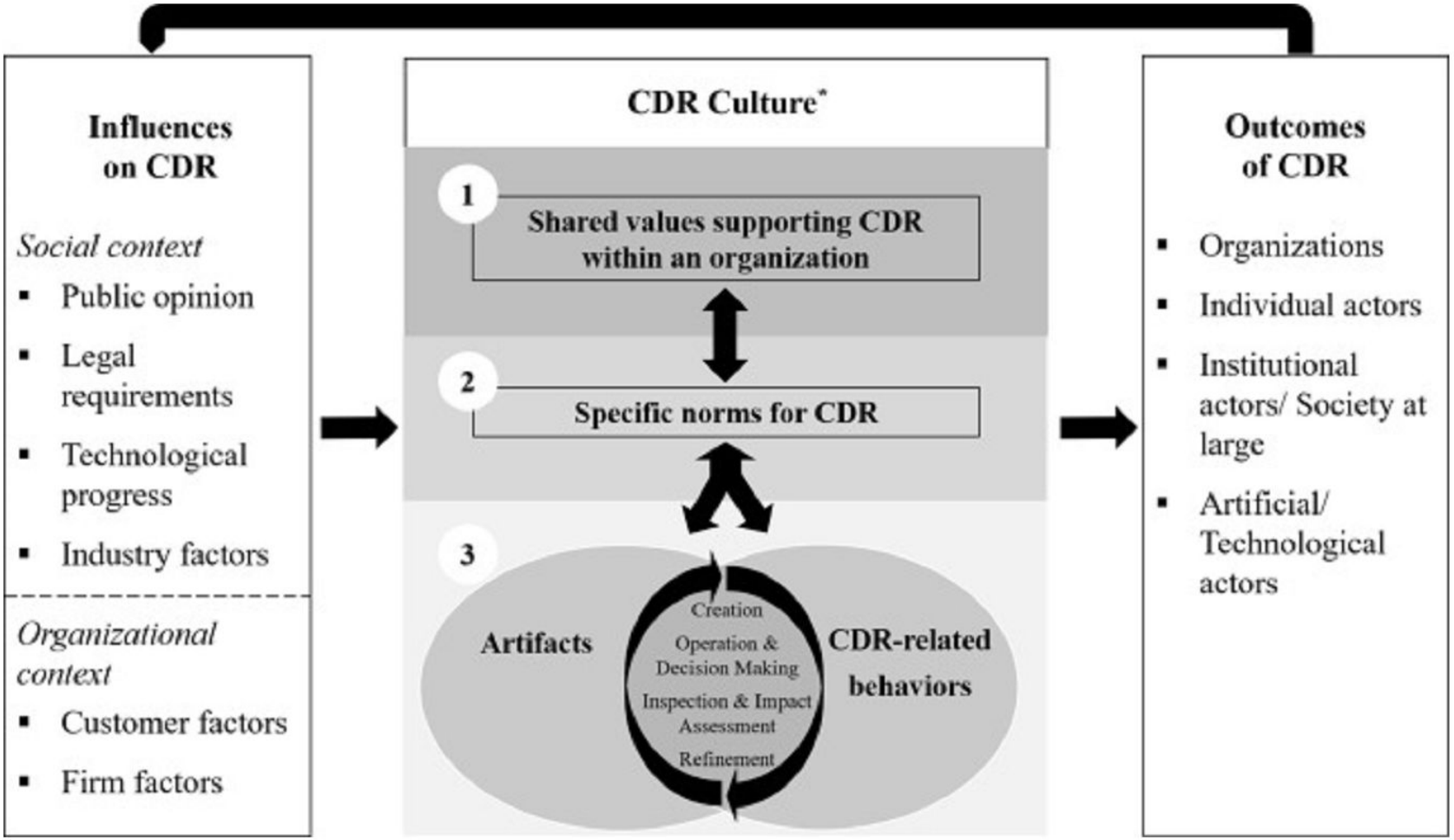
CDR MANIFESTO

The CDR -is an internationally developed set of principles designed to guide organizations in acting responsibly with digital technologies and data.



ID: An image with icons and topics under the banner of Corporate Digital Responsibility (CDR). Details for each principle are outlined below.

UNIVERSITY NORTH



SVEUČILIŠTE SJEVER

Core dimensions of the CDR construct

1. Understanding of Corporate Digital Responsibility (CDR) Principles
2. Adaptation of the training program for the particular type of SME
3. Data Privacy and Protection Compliance/Strategies
4. Cybersecurity Fundamentals and Best Practices
5. Ethical Use of Data, AI, and Digital Technologies
6. Promoting Digital Inclusion and Accessibility
7. Sustainable Digital Practices
8. Developing Governance and Accountability Structures
9. Effective Stakeholder Engagement and Communication
10. Continuous Improvement and Innovation in Digital Responsibility

Modified core dimensions of the CDR construct

MODULE 1: Fundamental Principles of Corporate Digital Responsibility

1. Understanding the basic principles of Corporate Digital Responsibility (CDR) and its integration into the business strategies of small and medium-sized enterprises (SMEs).
2. Compliance with data privacy regulations / Data protection strategies.

MODULE 2: Cybersecurity Fundamentals and Best Practices

3. Cybersecurity fundamentals and best practices.

MODULE 3: Ethical Use of Data, Artificial Intelligence, and Digital Technologies

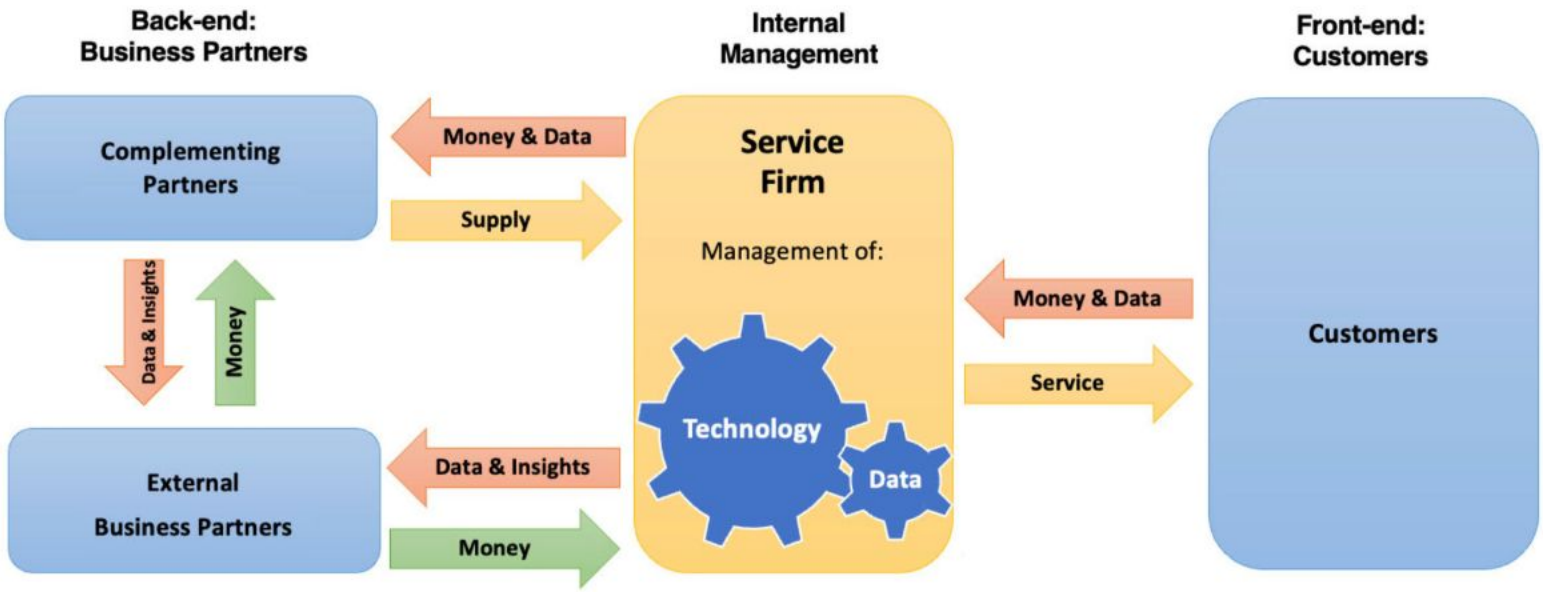
4. Ethical use of data, artificial intelligence, and digital technologies.
5. Promoting digital inclusion and accessibility.
6. Sustainable digital practices.

UNIVERSITY
NORTH

VŽ KC

MMI

SVEUČILIŠTE
SJEVER



CDR Tools

- Ethical Value Alignment
- CDR Advocacy and Shared Norms
- Shared Governance Models

- CDR Culture
- CDR Management Structure
- Digital Governance

- Ethical and Fair Treatment
- Focus on Customer Wellbeing
- Protect Customer Privacy

CDR Calculus

Value of Good CDR = **Benefits** - **Opportunity Costs / Costs of Good CDR**

Benefits

- Mitigation of CDR Risks
- Brand Equity and Trust

Opportunity Costs / Costs of Good CDR

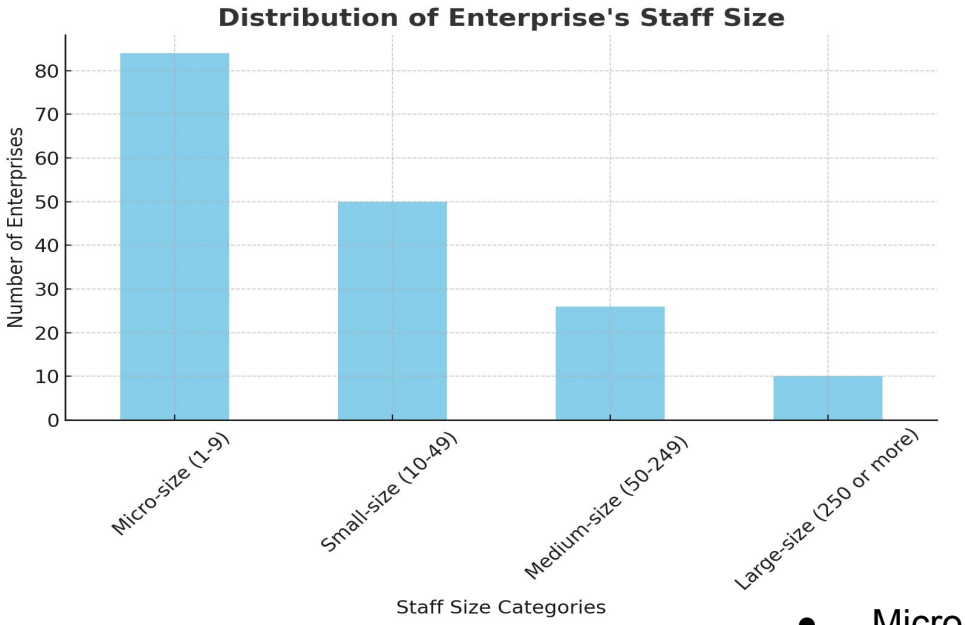
- Lost Incremental Revenues
- Reduced CX
- Missed Cost Savings
- Cost of Robust CDR

Survey results of digital readines of SME

Digital Corporate Responsibility Assessment (DCRA) Tool

We had a total of 170 respondents:

- Italy: 56 respondents
- Austria: 32 respondents
- Czech Republic: 31 respondents
- Slovenia: 30 respondents
- Poland: 16 respondents
- Croatia: 5 respondents



- Micro-size (1-9 employees): 84
- Small-size (10-49 employees): 50
- Medium-size (50-249 employees): 26
- Large-size (250 or more employees): 10

Education Need Score (ENS)

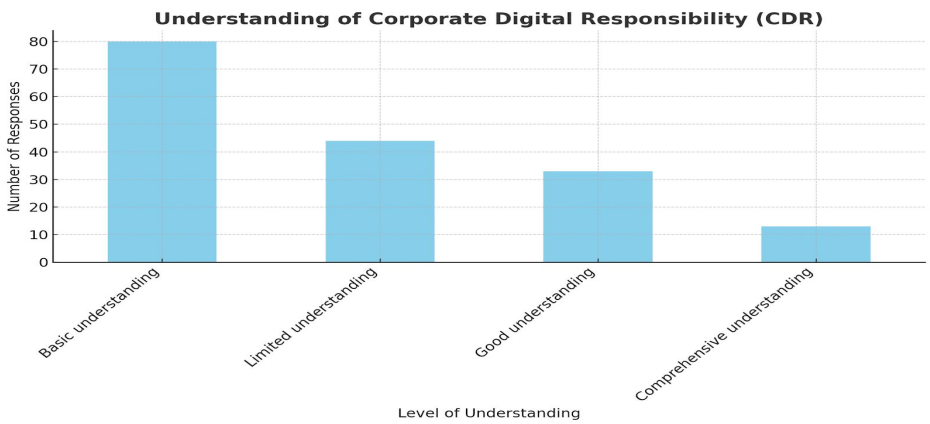
- **Comprehensive**: 1 (lowest need for education)
- **Good**: 2
- **Limited**: 3
- **Basic**: 4 (highest need for education)

Example

For the variable "How well can you define Corporate Digital Responsibility (CDR) and explain its importance for SMEs?" the ENS is 3.12.

The distribution of responses was as follows:

- Basic understanding of CDR, with some ability to explain its importance: 80 responses
- Limited understanding of CDR, unable to explain its importance: 44 responses
- Good understanding of CDR, able to explain its importance clearly: 33 responses
- Comprehensive understanding of CDR, with a detailed explanation of its importance and benefits for SMEs: 13 responses



We multiply 80 by 4,
44 by 3,
33 by 2,
and 13 by 1.

We summ up 320 + 132 + 66 + 13 = 531

And devide with 170

ENS = 3.12

Items ranked by ENS values

Description	ENS
Effectivness of network security measures	2.23
GDPR complience	2.24
Effectivness of access controls to prevent unauthorized access	2.26
Understanding of the risks associated with ransomware attacks	2.32
Understanding of the various types of cybersecurity threats	2.33
Phising protection measures implemented	2.34
Extent of compliance with legal and regulatory accessibility standards	2.37
Consideration of the needs of diverse user groups	2.47
Effectivness of iinclusive language and imagery	2.47
General Data Protection Regulation (GDPR) understanding	2.55
Identifying and responding to malware infections	2.55
Effectivness in reducing carbon footprint	2.56
Ethical considerations integrated into digital governance	2.58
Energy efficiency measures and environmental footprint reduction	2.61
Promotion of the digital literacy and skills	2.65
Employees trained to recognize and respond to cybersecurity threats	2.68
Incident response plan for cybersecurity breaches	2.69
Implementation of sustainable procurement policies	2.73
Benchmarking against industry best practices in digital responsibility	2.74
Stakeholders engagement in promoting socially and environmentally responsible digital practices	2.84
Extent of renewable energy use	2.92
Digital Services Act (DSA) and the Digital Markets Act (DMA) compience	2.98
Corporate Digital Responsibility (CDR) understanding	3.12

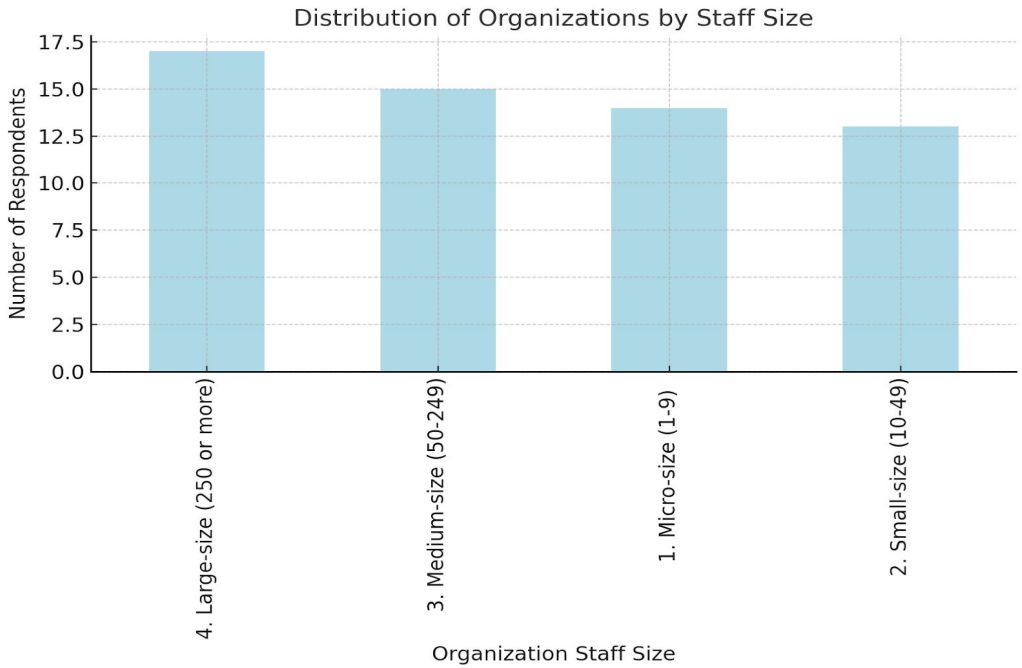
Stakeholder Corporate Digital Responsibility (CDR) Assessment Tool

Two key groups of questions:

1. The motivation of stakeholders to participate.
2. Competencies across different dimensions of CDR.

We had a total of 59 respondents:

- Italy: 9 respondents
- Austria: 11 respondents
- Czech Republic: 12 respondents
- Slovenia: 10 respondents
- Poland: 11 respondents
- Croatia: 6 respondents



- Micro-size (1-9 employees): 14
- Small-size (10-49 employees): 13
- Medium-size (50-249 employees): 15
- Large-size (250 or more employees): 17

UNIVERSITY NORTH
Interreg CENTRAL EUROPE
Co-funded by the European Union

- The general conclusion: the project has stakeholders who are highly motivated and possess a solid understanding of digital responsibility.

- A large number of stakeholders express strong motivation to participate in the project.

- Many stakeholders view their involvement in the project as an opportunity for personal development, improving their reputation within their networks, and gaining recognition for their importance.

- Stakeholders already possess solid knowledge of key aspects of corporate digital responsibility

- Most stakeholders have a good or very good understanding of digital responsibility, including areas such as data protection (GDPR), cybersecurity, and digital ethics. This knowledge can assist in shaping specific training modules.
  A significant number of stakeholders understand key legal regulations such as the Digital Services Act (DSA) and the Digital Markets Act (DMA), which can help ensure the training aligns with the latest European regulations.
  Most stakeholders are willing to actively contribute to content creation, provide feedback, and share best practices.

VŽ KC
IMM
SVEUČILIŠTE SJEVER

UNIVERSITY NORTH

VŽ KC

Challenges of CDR set-up for SME

MMI

SVEUČILIŠTE SJEVER

Handbook

The Handbook itself is structured into three modules and complements the three sets of learning outcomes. It is the primary learning material and is recommended for future trainers to guide the course.

The Handbook is a resource that trainers will adapt to the specific needs of different SME groups, based on the need to enhance skills in particular topics. In cases where the questionnaire indicates a lower need for one module and a higher need for another, the trainer will focus more on the module that is more needed in presentations, exercises, and lectures, while giving less attention to the module that is less needed.

- The learning material is general and covers all dimensions of the CDR construct.
- At the first level of education (trainer education), the material serves to educate future trainers.
- At the second level of education (SME employee training), trainers administer the questionnaire to each participant group (either the same or a similar version of the existing one).
- Based on the results, the trainer adjusts the training structure and learning material to the specific needs of the group.

Additional learning outcome in trainer training

Trainers will be able to identify the specific training needs of the organization and its employees, taking into account the specific type of SME and the digital literacy level of its employees, and will be able to tailor the basic training program to meet the specific needs of the SME type.

How you will do that

Define the SME digitalization needs and capabilities / maturity - QUESTIONNAIRE / TOOL

Strategic steps for implementing CDR in SMEs

the focus shifts to nurturing a culture of CDR awareness among employees. The depth of employee training—encompassing both technical understanding and the ethical implications of digital practices—directly correlates with how deeply CDR principles are embedded into the organizational culture. In other words, the more employees comprehend why and how to integrate responsible digital principles in their day-to-day operations, the stronger the culture of CDR becomes within the SME.

Identify the Digital Business Aspects Under CDR Principles:

Begin by mapping out all areas of your digital operations that may be influenced by Corporate Digital Responsibility. This includes data collection and storage, online transaction systems, digital marketing activities, and customer relationship management tools. Determine which processes involve personal data, environmental considerations (like energy consumption of servers), or potential social impacts (such as inclusive website design).

Determine Which CDR Measures Can Be Implemented at No Additional Cost

Explore CDR Aspects that Can Be Supported by Public Entities and BSOs:

UNIVERSITY
NORTH

Handbook

VŽ KC

MMI

SVEUČILIŠTE
SJEVER

Barriers to Implementing CDR in European SMEs

The implementation of Corporate Digital Responsibility (CDR) faces numerous challenges, particularly for SMEs, due to their limited resources and structural specificities. One of the most significant barriers for SMEs is their resource constraints. Financial resources and human capacities are often allocated to core operational activities, leaving little room for the implementation of new digital and ethical initiatives. SMEs struggle to finance essential CDR activities, such as ensuring data privacy, complying with regulatory requirements like GDPR, and investing in employee training.

Adopting regulatory requirements, such as the General Data Protection Regulation (GDPR), and aligning with global CDR standards is often challenging for SMEs. Adapting to these norms demands technical expertise and resources that smaller organizations often lack. Additionally, the absence of standardized tools for measuring and implementing CDR further complicates their approach to digital responsibility.

The technological infrastructure required for implementing CDR, such as systems for data protection, transparent algorithm management, and resource optimization, frequently exceeds the capabilities of SMEs. Tools like artificial intelligence (AI) and automation, while promising productivity gains, also introduce ethical challenges such as algorithmic bias, necessitating sophisticated methods for oversight and evaluation.

Awareness of the importance of CDR within SMEs is often low. Managers and employees do not fully understand the societal and environmental impacts of digital technologies, making it difficult to embrace new practices. The lack of internal educational programs on key CDR principles, such as ethical data use and responsible digitalization, exacerbates this issue.

While large corporations possess the resources to meet high consumer expectations regarding digital responsibility, SMEs often face pressure to remain competitive, even if this means neglecting CDR practices. Market segmentation reveals that different consumer groups have varying priorities, but SMEs frequently lack the capacity to tailor their offerings to these specific needs.

Unlike large organizations, SMEs do not have access to specialized teams for data management and digital solution implementation. The assistance of external consultants or partnerships often exceeds their financial capabilities, and local incentives or grants are not always accessible or tailored to the unique needs of the SME sector.

UNIVERSITY
NORTH

SVEUČILIŠTE
SJEVER

UNIVERSITY NORTH

Why SME would like to concerned about CDR implementation

Is CDR bring them economic benefit or advantage ?

Is CDR new obligation which ask more time and finance effort ?

VŽ KC
MMI
SVEUČILIŠTE SJEVER

UNIVERSITY NORTH



CDR is bringing the status and reputation of responsible company – its BREND and trustfully business

VŽ KC
MMI
SVEUČILIŠTE SJEVER

UNIVERSITY NORTH

There are numerous research papers, reports, and studies that confirm the significant impact sustainable practices can have on a company's reputation and its ability to attract eco-conscious consumers.

Market studies show that consumers increasingly prefer products and services from companies known for their sustainable practices.
Research has also shown that companies that actively communicate their sustainability initiatives are more likely to build stronger trust and loyalty among consumers.

VŽ KC
MMI
SVEUČILIŠTE SJEVER

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

INTRODUCTION TO CORPORATE DIGITAL RESPONSIBILITY (CDR) IN SMEs

VŽ KC

MMI

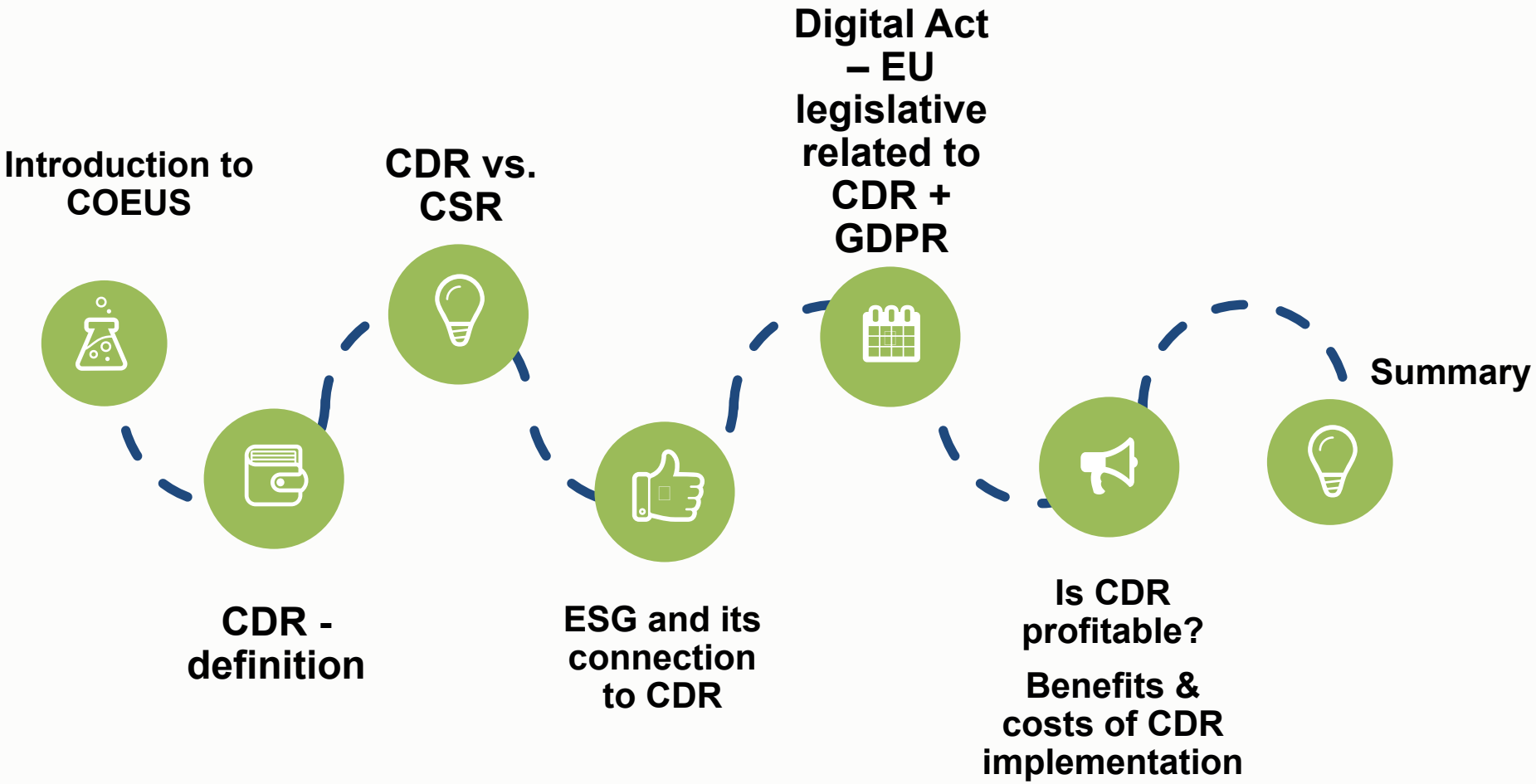


Katerina Fotova Čiković, PhD

Assist. Prof., University North, Croatia

kcikovic@unin.hr

Syllabus – What to expect



Lecture 1: Introduction to COEUS

Interreg Central Europe
Lead Partner Organization: Digital Innovation Hub Slovenia

Programme priority specific objective: SO1.2: Strengthening skills for smart specialisation, industrial transition and entrepreneurship in central Europe

COEUS tackles the challenge not only of ensuring that digitalisation is achieved in Central Europe (CE), but that it is achieved with social, economic, technological and environmental responsibility.
It does so by supporting Corporate Digital Responsibility (CDR) skills for traditional and innovative SMEs, with a focus on smart specialisation priorities for digitalisation.

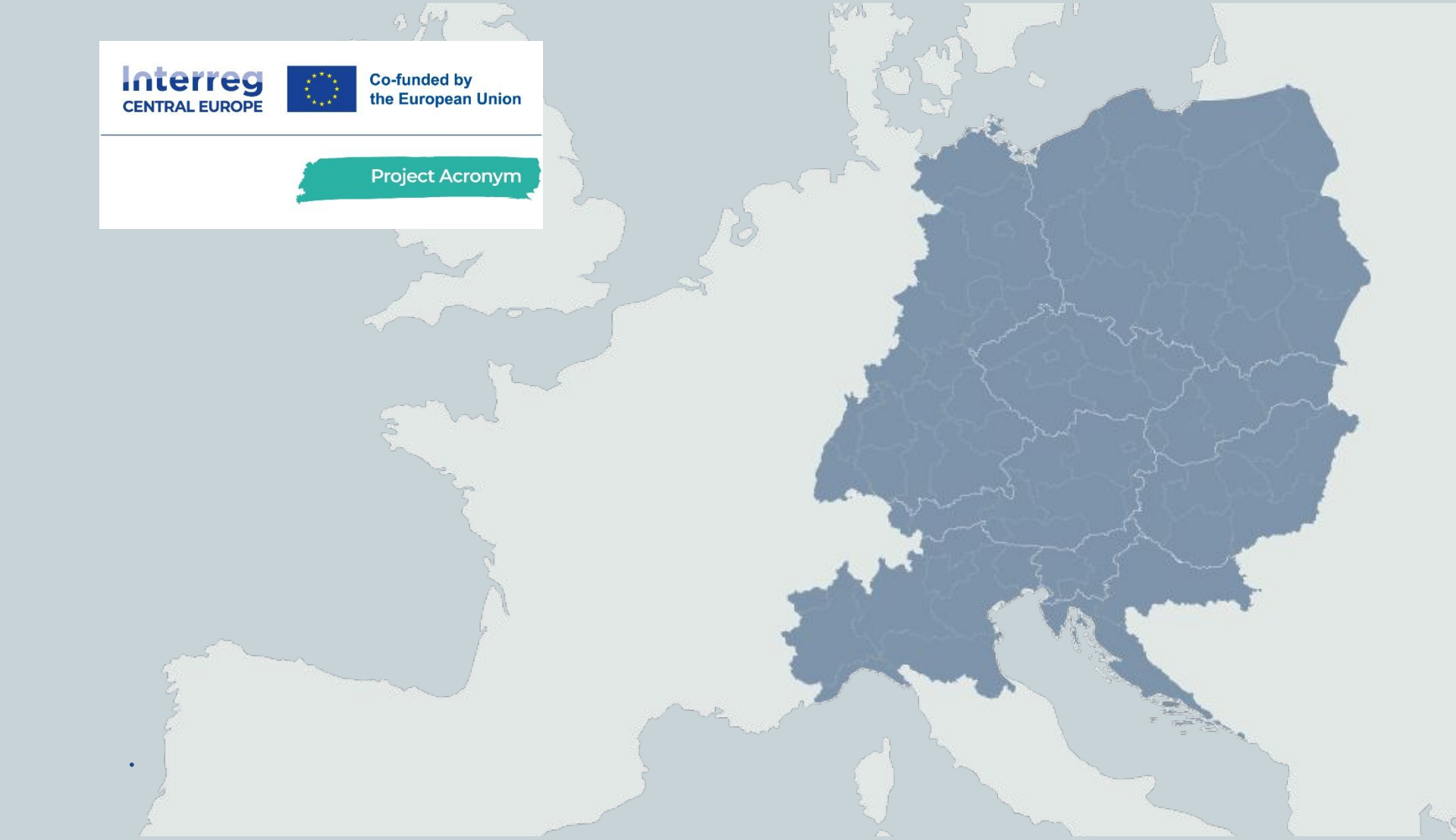
Project partner overview

Partner Number	Status	Name of the organisation in English	Partner role in the project	Country (NUTS 0)
1	Active	Digital Innovation Hub Slovenia	LP	Slovenija (SI)
2	Active	Metropolitan City of Turin	PP	Italia (IT)
3	Active	Styrian Business Promotion Agency	PP	Österreich (AT)
4	Active	Innovation Centre of Usti Region (registered association)	PP	Česko (CZ)
5	Active	Chamber of Commerce and Industry of Slovenia	PP	Slovenija (SI)
6	Active	Lubelskie Voivodeship	PP	Polska (PL)
7	Active	University North	PP	Hrvatska (HR)

Interreg
CENTRAL EUROPE

Co-funded by
the European Union

Project Acronym



Current world challenges

Climate Emergency

One of the largest modern challenges of mankind is undoubtedly the reduction of greenhouse gases and slowing the global warming rate.

Waste of Natural Resources

The earth's surface, its natural resources, and their regeneratio rate, are finite. By 2050 it is estimated that people will consume for three planets



Uncontrolled marine pollution

Marine Litter is one of the most important environmental problems of the seas, coastal areas and inland waters.

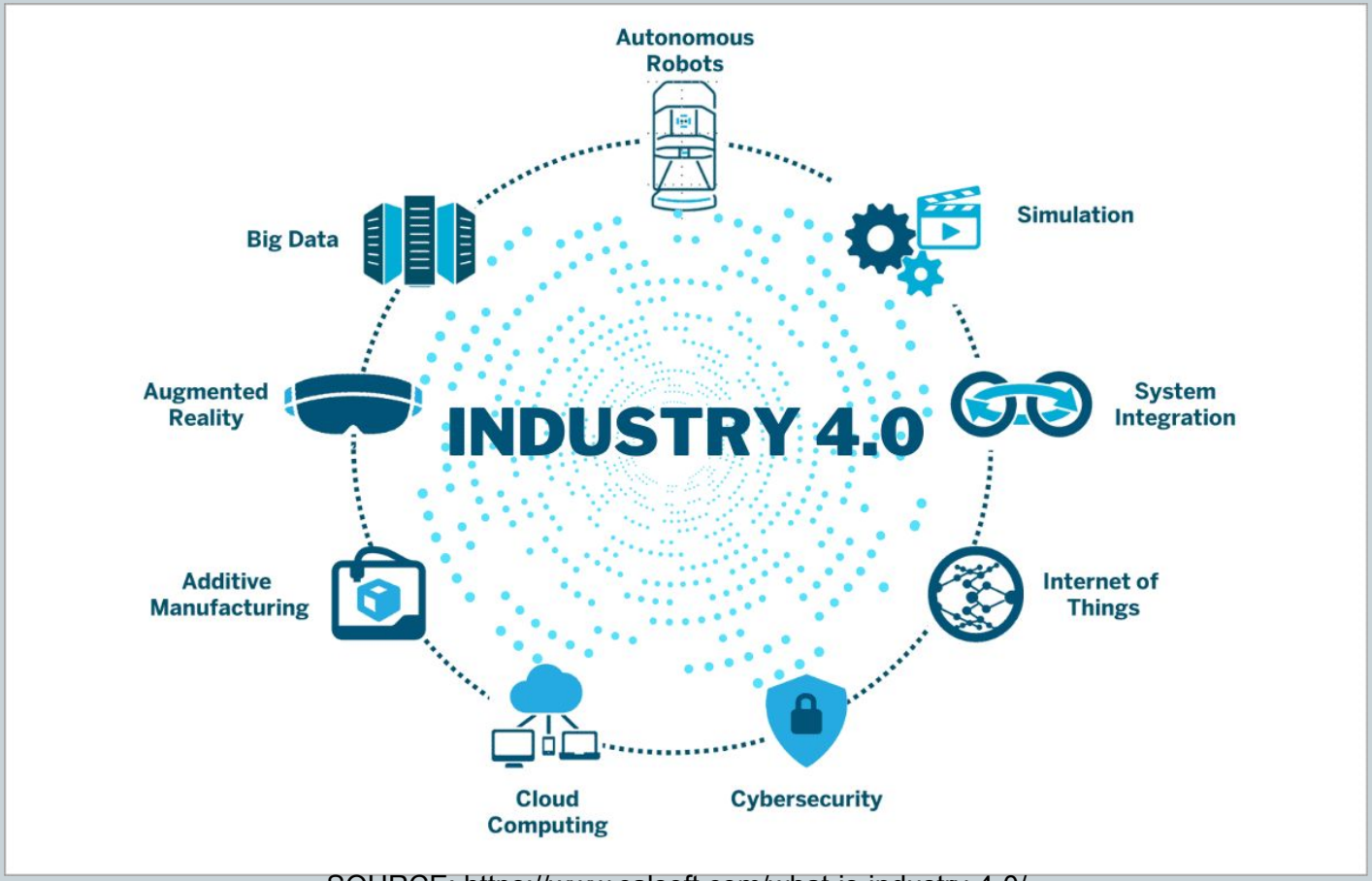
Loss of Biodiversity

Biodiversity is the key to healthy ecosystems and human life. According to a UN report (IPBES, 2019), up to a million species of fauna and flora are expected to be threatened with extinction.

SOURCE: https://iasi-inco.com/sustainable-development-our-priority-for-years-now/

On the other hand…

Digital transformation,
Industry 4.0,
cloud computing,
artificial intelligence,
robotics,
Internet of Things (IoT)
Blockchain technology
…..



SOURCE: https://www.calsoft.com/what-is-industry-4-0/

global buzzwords that are being used more and more frequently, not only in politics, business and society, and are becoming increasingly important these days

All these terms are often summarised under the synonym **digitalisation**.

The digital transition is **one of the great transformative forces** of our time

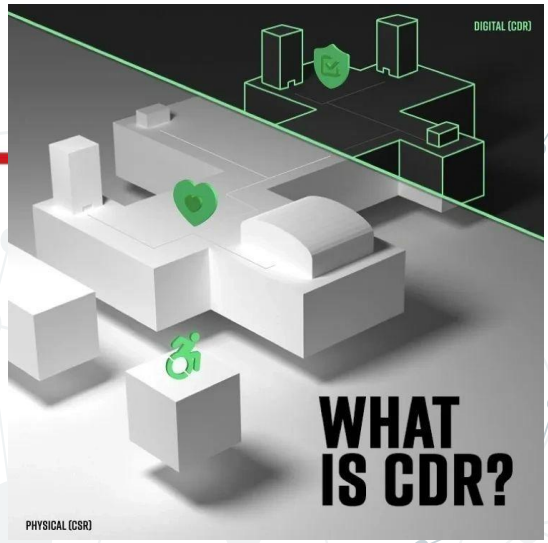
The digital transition brings **new hope**, but also raises **new questions**.

What are its environmental and social consequences?

What are the consequences regarding the work organisation and professional relations?

https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-2021-corporate-digital-responsibility-2._environmental_and_social_issues.pdf

Lecture 2: CDR - definition



Corporate Digital Responsibility (CDR) is a set of practices and behaviour that help an organisation to use data and digital technologies in a way that is **socially, economically, technologically, and environmentally responsible**.
In theory, it sounds obvious.
In practice, it is not so easy to achieve, particularly for SMEs (CDR Europe Interreg)

A <u>digitally responsible company</u> should thus respond to several major challenges - in line with the Sustainable Development Goals:

- **Regulatory responsibility** for data protection and compliance with the GDPR and sectoral regulations;
- the **ethical responsibility** of artificial intelligence software;
- **societal responsibility** in relation to data management, transformation of working patterns, data sharing, inclusion of all;
- **environmental responsibility** for the use of data in considering the environmental impacts of business activities.

CSR Platform (2020), Corporate Digital Responsibility
-1. L'enjeu des données, France Stratégie, July.

Companies nowadays are particularly required to take responsibility for their digital actions and to communicate what place they want to occupy in the digital society.

Under the term Corporate Digital Responsibility, companies worldwide are committing to greater responsibility for sustainability, data protection and consumer protection.

SOURCE: https://ihk-kompetenz.plus/wissenswertes/corporate-digital-responsibility-cdr-definition/

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Lecture 3: CDR vs. CSR



VŠ KC

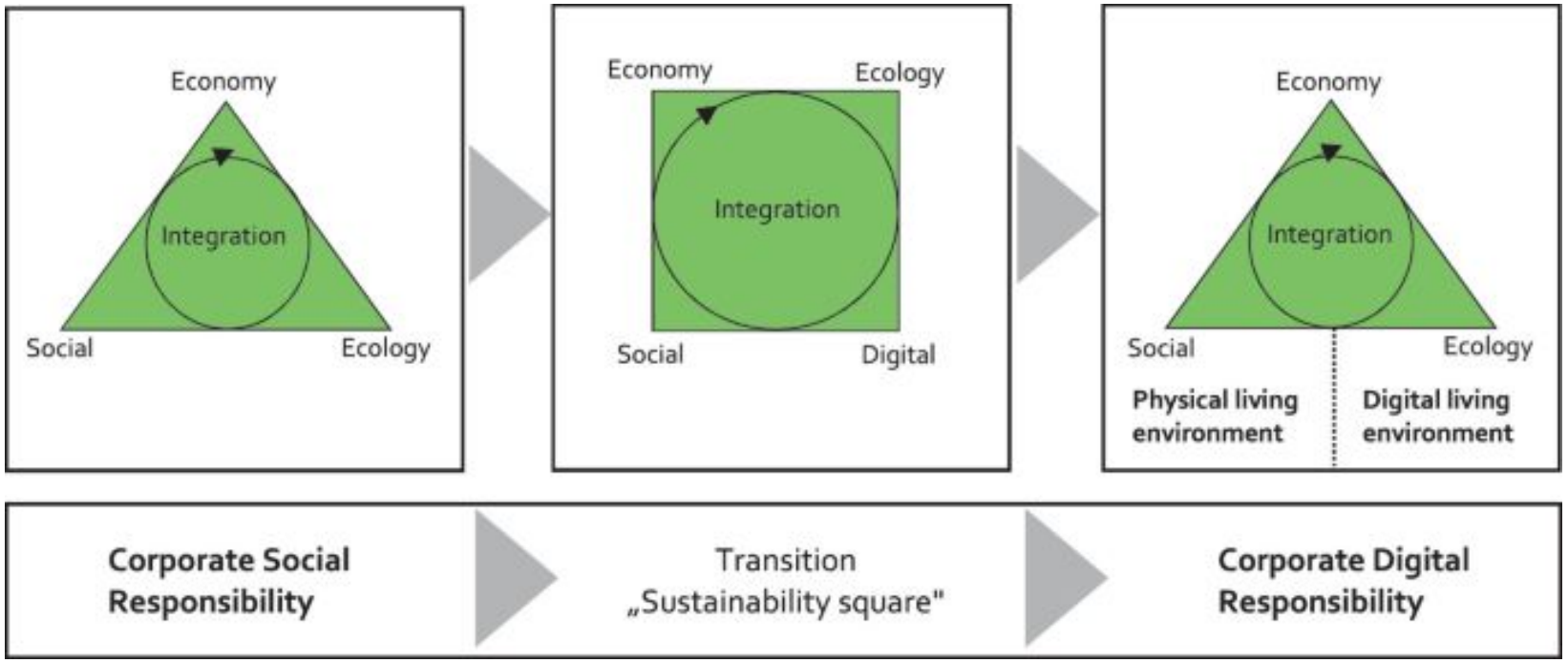
MMI

In essence, the main difference between CDR and CSR is given by the role that **technology** plays in the respective concept. While CSR has a relatively broad goal towards society that affords technology only subordinate importance, CDR revolves around technology and its implications for corporations and society. Besides these main differences between CDR and CSR, there is no clear cut between the two concepts, so that thematic overlaps are possible (Lobschat et al. 2021).

- CDR is increasingly seen as a subset of Corporate Social Responsibility (CSR).

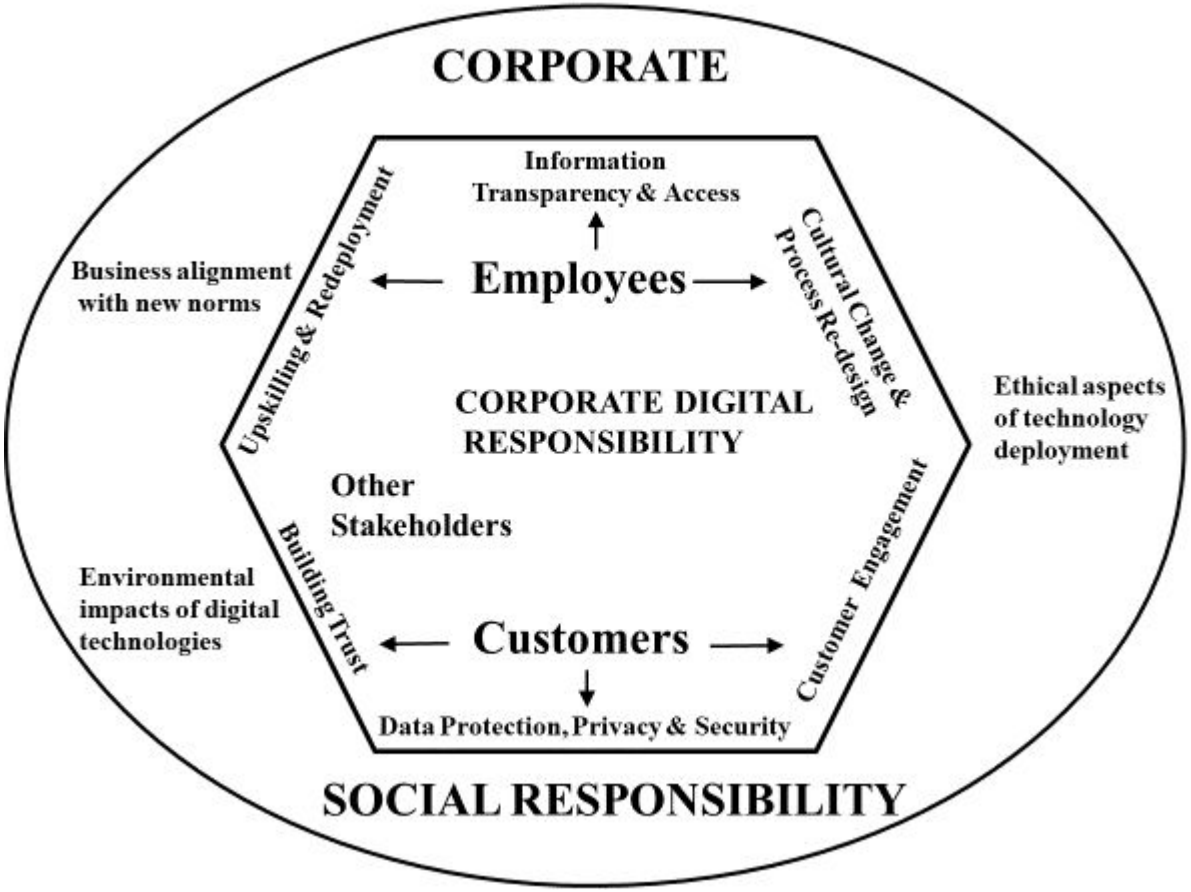
Lobschat L, Mueller B, Eggers F et al (2021) Corporate digital responsibility. J Bus Res 122:875–888

CSR vs. CDR



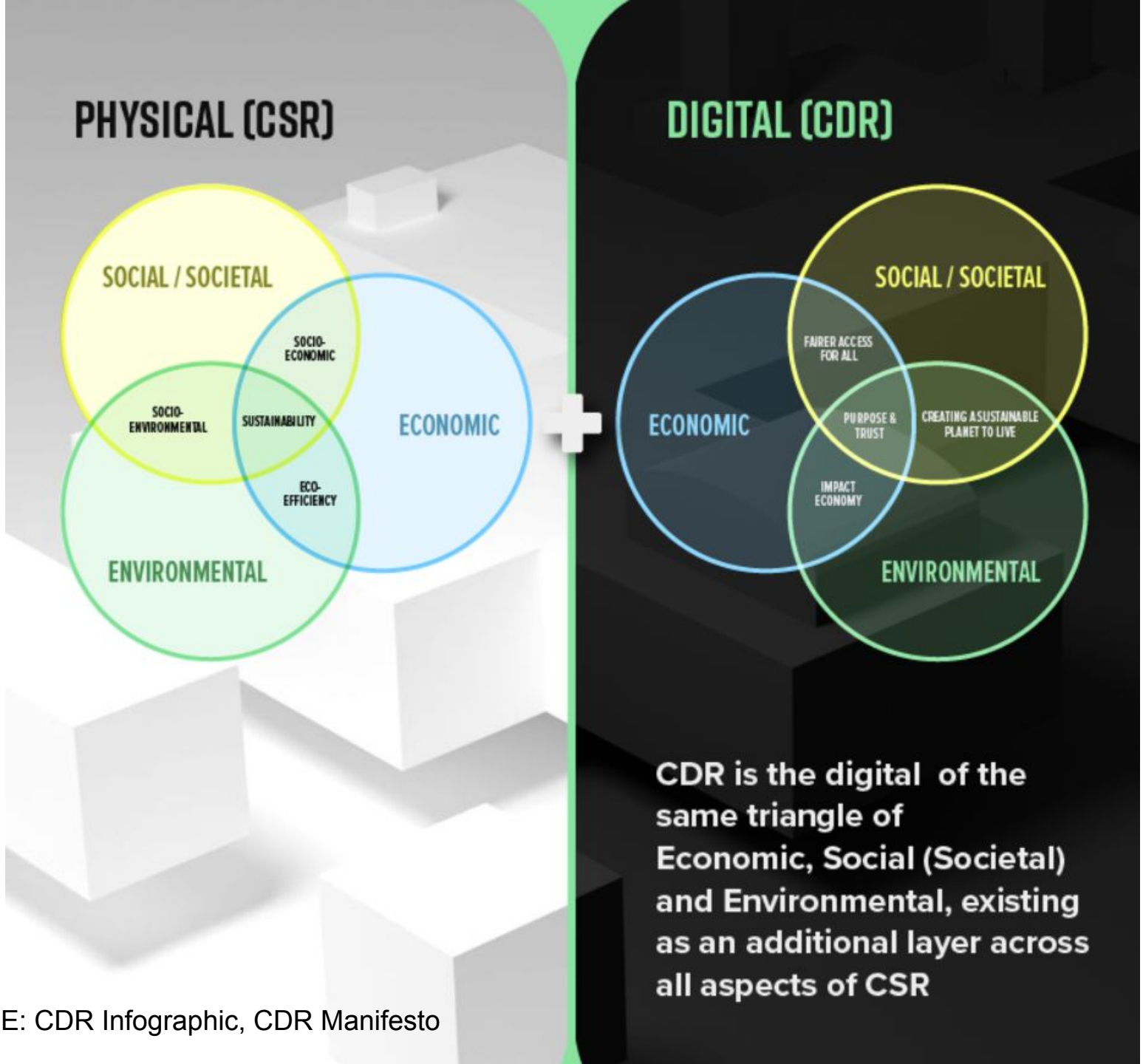
Pelters, E. (2021). Corporate Digital Responsibility—Understanding and Applying. In: Herberger, T.A., Dötsch, J.J. (eds) Digitalization, Digital Transformation and Sustainability in the Global Economy. Springer Proceedings in Business and Economics. Springer, Cham. https://doi.org/10.1007/978-3-030-77340-3_6

UNIVERSITY NORTH



SOURCE: Wynn, M., & Jones, P. (2023). Corporate responsibility in the digital era. *Information*, *14*(6), 324.

VŽ KC
MMI
SVEUČILIŠTE SJEVER



SOURCE: CDR Infographic, CDR Manifesto

Corporate Digital Responsibility Examples

Implementation
The CDR manager is responsible for creating and implementing a CDR policy (a company guideline to promote corporate digital responsibility). Do you want to make digitalization in your company sustainable and responsible?

Data protection
"What happens to my data?" This question is becoming increasingly important for customers. Not only do applicable regulations such as the General Data Protection Regulation require companies to protect data, but trusting data handling is also important for their customer relationships. The most important procedures are the ones covering how you can collect and evaluate data securely.

Artificial intelligence
A relatively new development that has been gaining momentum since the appearance of Chat GPT and Co.: Artificial intelligence (AI). AI is changing companies. Accompanying this transformation safely and responsibly in the spirit of corporate digital responsibility is the job of an AI manager.

https://ihk-kompetenz.plus/wissenswertes/corporate-digital-responsibility-cdr-definition/

Real-life CDR implementation examples

Zalando publishes first Corporate Digital Responsibility Report in partnership with the German government



The CDR code has a section that focuses on making sure data is used in a way that customers expect and are aware of, how is Zalando doing this?

Internet users sometimes fear that they are being tracked and their data is being used, but they don't know how and what for exactly. For Zalando it is very important to offer an experience of trust. We process customer data in accordance with all applicable data protection laws on national and EU level.

https://corporate.zalando.com/en/company/zalando-publishes-first-corporate-digital-responsibility-report-partnership-german

Real-life examples

It is essential for organizations to be aware that **digitalization can lead to negative impacts if misused**, including harm to customers and unwanted societal consequences.

For example, **Goldman Sachs** faced public backlash after being investigated for discrimination arising from their algorithm which was providing women with lower lines of credit than men.

Further, incidences such as the 'Robot debt' debacle by the **Australian government** resulted in lower socio-economic residents being forced to repay erroneous welfare repayments, causing bankruptcy, psychological stress and even reports of suicide as a result of the algorithmic anomalies that underpinned the repayment demands.

Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*, *53*(2), 101056.



UNIVERSITY NORTH

Real-life CDR implementation examples

Social This involves an organization's relationship with people and society. Topics include data privacy protection and aspects related to digital diversity and inclusion, such as bridging the digital divide between geographies, social classes, and age demographics.

Example: When online insurance applications are denied with Swiss insurance company **Die Mobiliar**, the affected individual has the right to speak to an employee to understand the reasoning behind the decision.

Economic This concerns the responsible management of the economic impacts of digital technologies. Topics include replacement of existing jobs by robots and the creation of the new digital-era jobs that are enriching and fulfilling. Questions include how firms share the economic benefits of digitalization with society at large.

Example: **Weleda, a Swiss holistic natural cosmetics** and anthroposophical medicines company, has said that any use of robotic process automation will not result in staff reductions or job losses. Affected employees would be upskilled and transferred into other functions.

VŽ KC
MMI
SVEUČILIŠTE SJEVER

Real-life CDR implementation examples

Technological This is linked to the responsible creation of the technologies themselves. For example, biased or inaccurate AI decision-making algorithms can lead to unfair or discriminatory practices. Other technologies such as so-called deepfake videos can also have harmful effects on society.
Example: Employees of German telecommunications company **Deutsche Telekom** are encouraged to follow corporate ethical guidelines related to AI engineering and usage.

Environmental This concerns the link between digital technologies and the physical environment, including issues of responsible recycling or the disposal of old computer equipment. Another consideration is limiting power consumption for firm activities.

Example: By committing to net zero Scope 1 and 2 emissions by 2025, financial services group UBS leverages connected sensors in its physical infrastructure to reduce their energy consumption and measure carbon emissions more effectively.

https://swiss-digital-initiative.org/wp-content/uploa
22/11/SDI_IMD-CDR-Report_2022.pdf

UNIVERSITY NORTH

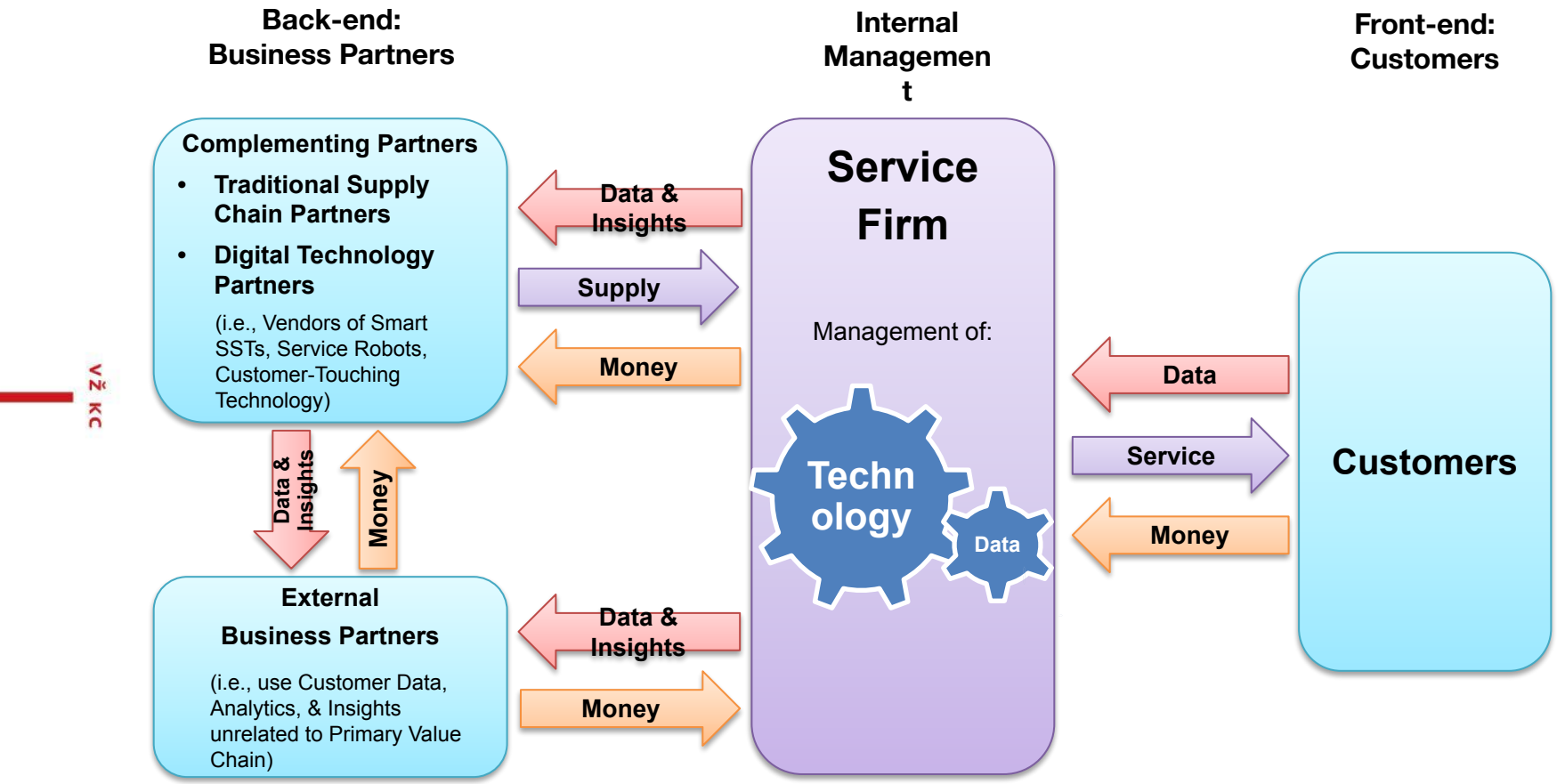
Table 2. Activities and Potential Concerns in the Example of Wearable Personal Health Devices

	Creation	Operation and Decision-making	Inspection and Impact Assessment	Refinement
Activities	• Designing the wearable device (e.g., wristband) and deciding which sensors to use • Building software and deciding which sensors of the host device (e.g., smartphone) to use • Deciding which existing personal health data on the host device to use • Building a data and prediction model for data analysis • Capturing of data from the user • Inferring health data from other sources (e.g., social media) • Deciding on storage location of data and data ownership	• Ongoing and continued collection of user data • Analyzing user preferences and routines (e.g., exercise regime) • Compiling data into comprehensive user profile • Matching of user characteristics to other users based on selected variables • Probabilistically extrapolating unobservable data (e.g., future development of health) and future events (e.g., health incidents) • Making recommendations to the user on health-related issues	• Analyzing users' progress vis-à-vis their goals / intentions • Assessing health advice • Analyzing customer complaints (e.g., on social media) • Inspecting algorithms and analytics to understand decision models • Benchmarking with technological progress and legislation • Assessing wider network of stakeholders (e.g., third-parties interested in data) • Analyzing of unintended effects (and ability to discover these)	• Refining analytics / algorithms (even re-training if need be) • Refining decision rules; deciding when what recommendation is given to users • Implementing additional safety / security measures for users' data • Deciding which new data need to be collected and which data need to be discontinued / deleted • Improving algorithms and predictive models
Potential Concerns	• Users are not given fair chance at informed consent to collect data • Privacy concerns not considered • Data accuracy not considered • Over-collection of unrelated data (e.g., by using additional sensors in host device) • "Coerced" data provision by customer to gain customization, convenience, promotions • Safekeeping of data (data breach; hacking; identity theft)	• Lack of transparency of data collection (e.g., which sensors) and analytics (e.g., why specific recommendations were made) • Lack of transparency and control to potential and current users about how data are used • Algorithmic decisions / recommendation lack validity (accurately reflecting underlying truth) • "Hidden agenda" / unrelated variables infused into analytics	• Lack of transparency in algorithms leaves systemic biases undetected • Security concerns due to outdated technology or algorithms (e.g., data not stored securely) • Lack of contingency governance (e.g., who owns data in case company is being bought) • Decisions / recommendations based on outdated medical advice • Unintended discrimination, biases (e.g., gender, ethnicity)	• Right to "forget" not followed; data are kept without clear retirement dates • Technology embodies sustained biases, discrimination, etc. • Technology cannot be retired because data has become systemic (e.g., health devices required for insurance coverage) • Data ownership changes without clear information to users (e.g., data acquisition)

VŽ KC
MMI
SVEUČILIŠTE SJEVER

Lobschat, Lara & Mueller, Benjamin & Eggers, Felix & Brandimarte, Laura & Diefenbach, Sarah & Kroschke, Mirja & Wirtz, Jochen. (2021). Corporate Digital Responsibility. Journal of Business Research. 122. 875-888. 10.1016/j.jbusres.2019.10.006.

Figure 2. The digital service ecosystem model.



Source: Wirtz, Jochen, Werner Kunz, Nicole Hartley, and James Tarbit (2022), "Corporate Digital Responsibility in Service Firms and their Ecosystems", *Journal of Service Research*, published online first, https://doi.org/10.1177/10946705221130467.

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

CDR vs. CSR: the scholarly literature i.e. what is thus far found

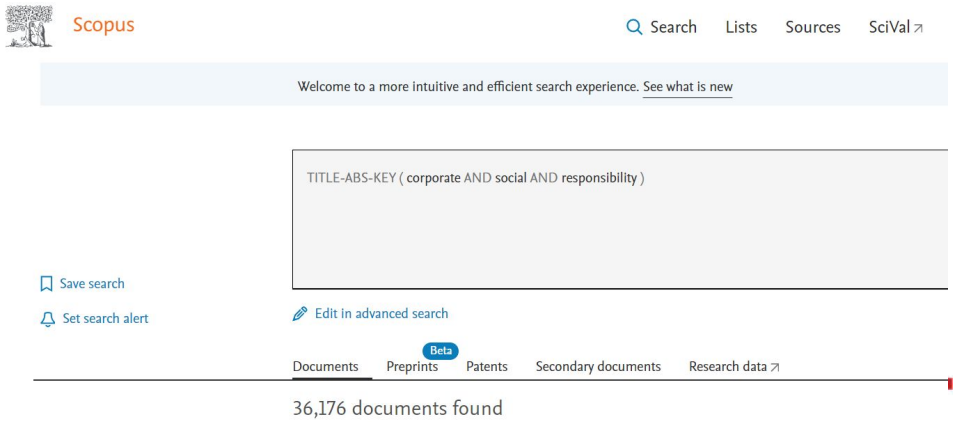


VŠ KC

MMI

CSR (Corporate Social Responsibility)

Scopus



36.176 papers

Clarivate Web of Science™



43.288 papers

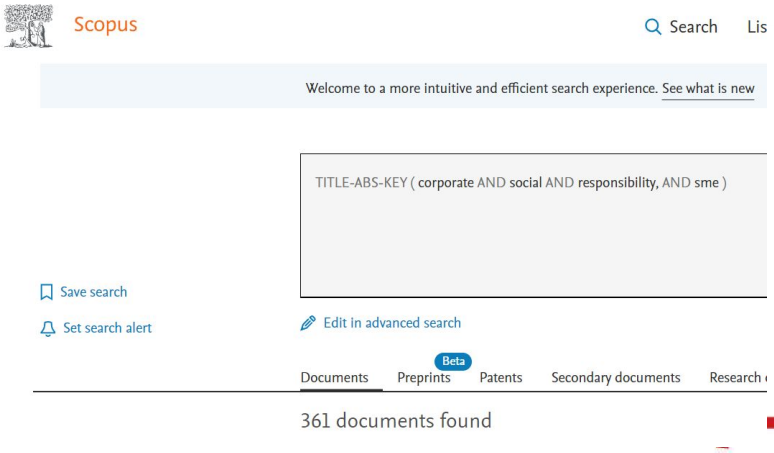
CSR in SMEs

Interreg CENTRAL EUROPE

Co-funded by the European Union

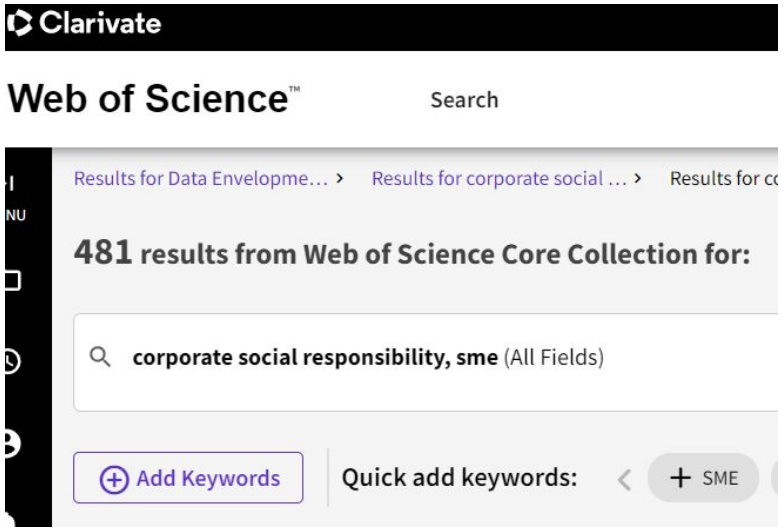
COEUS

Scopus



361 papers

Clarivate Web of Science™



481 papers

CSR in SMEs

Scholarly discourses on CSR in SMEs are rapidly growing in volume in recent years; yet knowledge in this field of inquiry **is fragmented** across scientific journals, sectors, disciplines, and cultural and geographical contexts.

Oduro, S., Bruno, L., & Maccario, G. (2021). Corporate social responsibility (CSR) in SMEs: what we know, what we don't know, and what we should know. *Journal of Small Business & Entrepreneurship*, *36*(2), 207–238. https://doi.org/10.1080/08276331.2021.1951064

UNIVERSITY NORTH

Findings show that:

1) CSR research in SMEs is rapidly growing with over 136 peer-reviewed articles published in the last decade, appears significantly in top tier journals, and empirically based;

2) **quantitative surveys and panel study designs** dominate the field over other methodological designs such as qualitative case studies and conceptual models;

3) **firm performance** (financial, non-financial, and both) is the topic/theme frequently investigated, followed by drivers/antecedents, perception/knowledge awareness, and CSR green practice and ethics, in that order

4) studies are preponderately **Europe-centric, multi-sectoral, and atheoretical;**

5) there is a limited adoption and development of novel theories and linkage between the conceptual and empirical studies.

VŽ KC
MMI
SVEUČILIŠTE SJEVER

CSR in SMEs - wordcloud

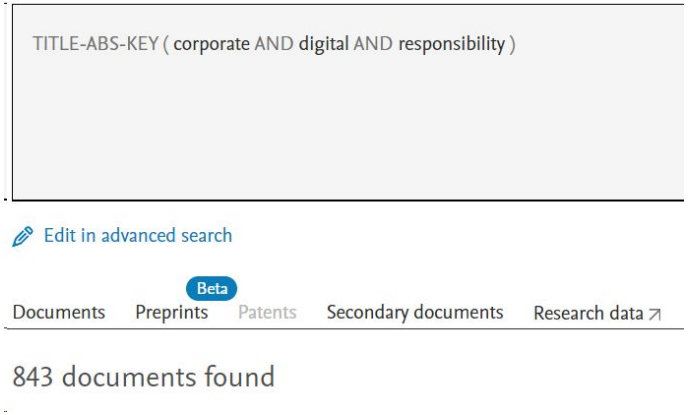


CDR



Scopus

843 papers



Clarivate
Web of Science™

1042 papers



UNIVERSITY NORTH

Scopus

TITLE-ABS-KEY (corporate AND digital AND responsibility)

Edit in advanced search

Beta

Documents | Preprints | Patents | Secondary documents | Research data

843 documents found

Country/territory

- United States 114
- China 110
- United Kingdom 95
- Germany 72
- Italy 48

Show all

SVEUČILIŠTE SJEVER

Scopus

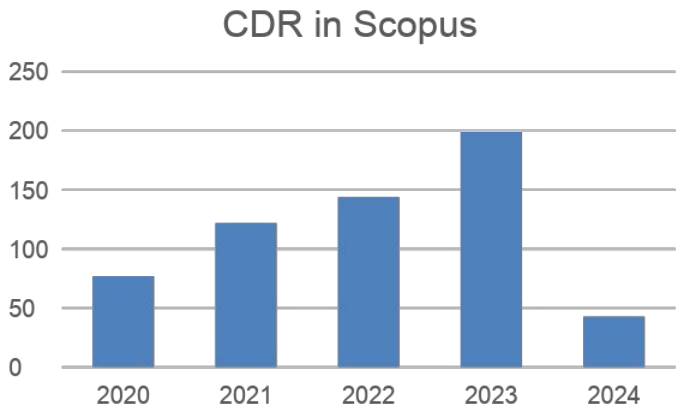
UNIVERSITY NORTH

TITLE-ABS-KEY (corporate AND digital AND responsibility)

Edit in advanced search

Documents | Preprints (Beta) | Patents | Secondary documents | Research data

843 documents found



MMI

SVEUČILIŠTE SJEVER

UNIVERSITY NORTH



Scopus

TITLE-ABS-KEY (corporate AND digital AND responsibility, AND entrepreneurship)

Edit in advanced search

Beta

Documents | Preprints | Patents | Secondary documents | Research data

30 documents found

Subject area

☐	Business, Management and Accounting	18
☐	Economics, Econometrics and Finance	10
☐	Computer Science	7
☐	Engineering	7
☐	Social Sciences	7

SVEUČILIŠTE SJEVER

UNIVERSITY NORTH

Clarivate
Web of Science™

1,042 results from Web of Science Core Collection fo

corporate digital responsibility (All Fields)

Research Areas

Business Economics	464
Environmental Sciences Ecology	187
Science Technology Other Topics	156
Engineering	97
Communication	95

VŽ KC

MMI

2024	31	2016	35	2007	3
2023	222	2015	32	2005	2
2022	183	2014	20	2001	1
2021	133	2013	18	2000	1
2020	132	2012	8	1999	1
2019	76	2011	4	1998	2
2018	87	2010	4	1996	1
2017	42	2009	3	1991	1

SVEUČILIŠTE SJEVER

Clarivate
Web of Science™

72 results from Web of Science Core Collection for:

corporate digital responsibility, entrepreneurship (All Fields)

Research Areas

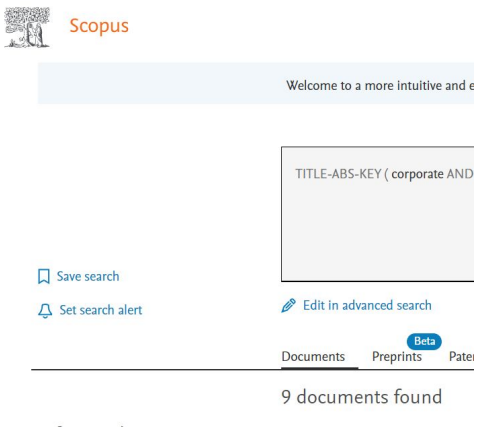
Business Economics	48
Environmental Sciences Ecology	15
Science Technology Other Topics	12
Development Studies	4
Public Administration	3

2024	3	2021	11	2018	8
2023	16	2020	7	2016	8
2022	14	2019	5		

CDR + SMEs

Scopus

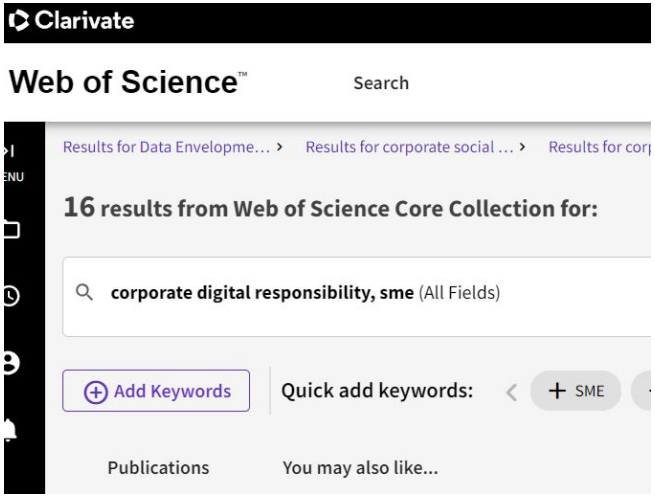
9 papers



Clarivate Web of Science™

16 papers

25 papers



UNIVERSITY
NORTH



VŽ KC
MMI
SVEUČILIŠTE
SJEVER

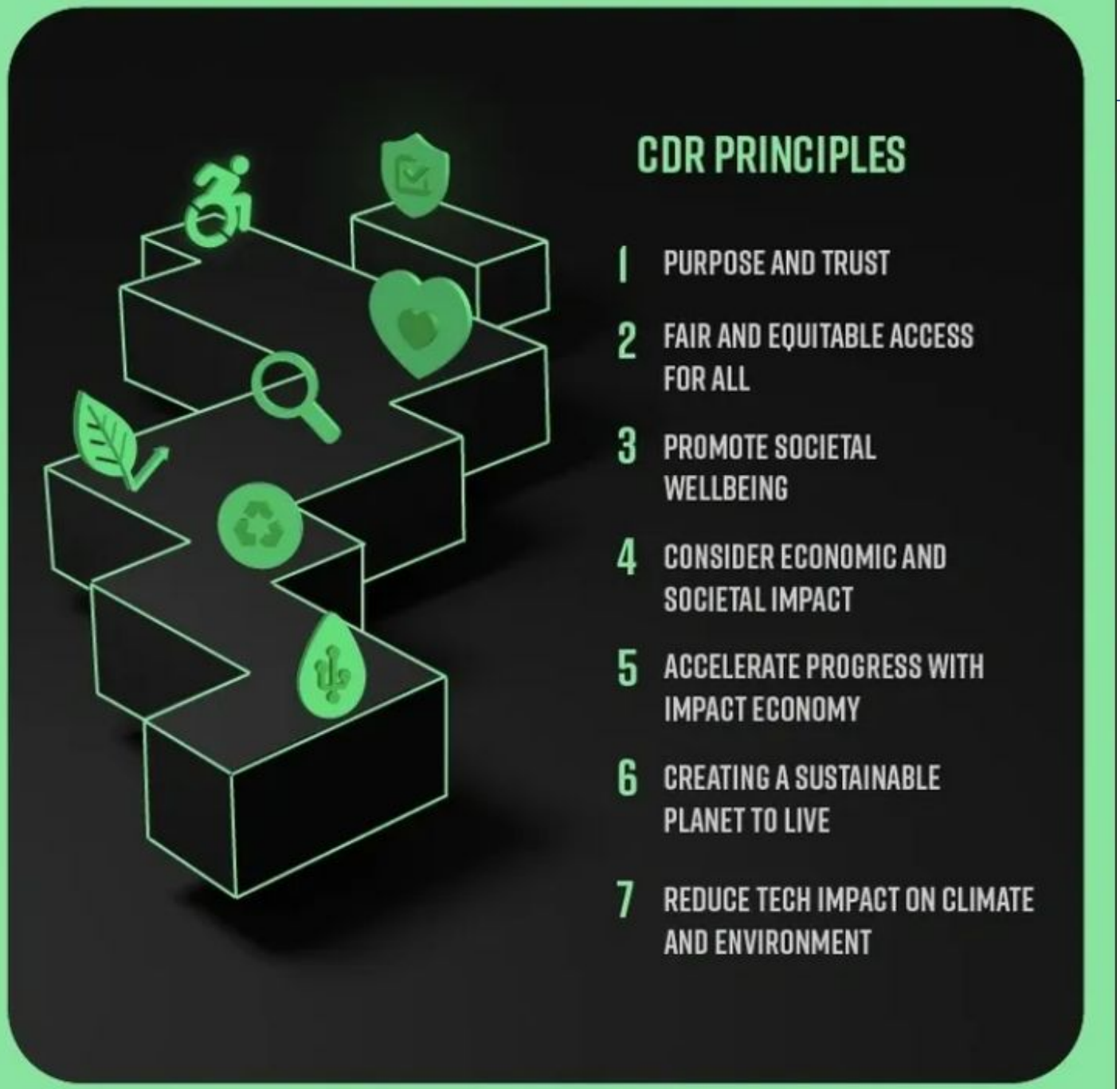
The International CDR Manifesto



The Seven Core Principles of the International definition of Corporate Digital Responsibility

The CDR Manifesto

During 2021, an international group of academics, corporate practitioners and published authors collaborated to aggregate their existing work into a single, international definition that pulls the best from each to build a set of principles to guide you on your Digital Responsibility journey.



Co-funded by the European Union

COEUS

The Seven Core Principles of the International definition of Corporate Digital Responsibility

The CDR Manifesto

The International CDR Manifesto - the 7 core principles

1. Purpose and Trust

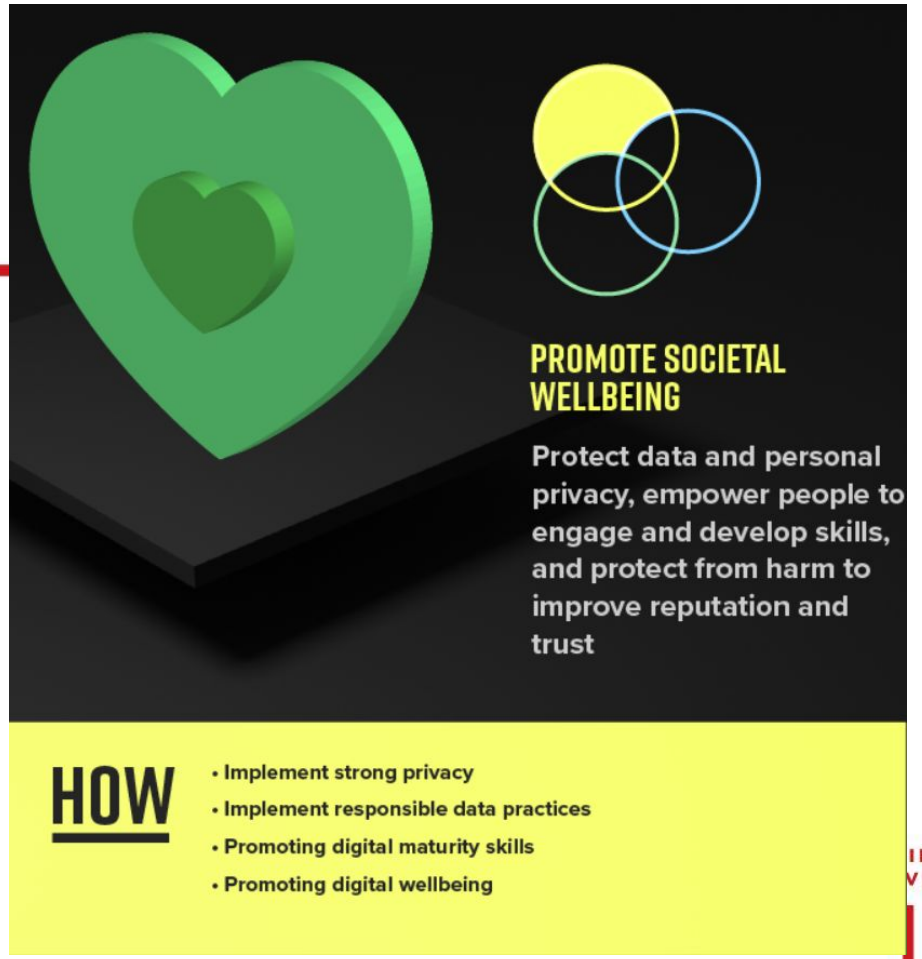


2. Fair and Equitable Access for All

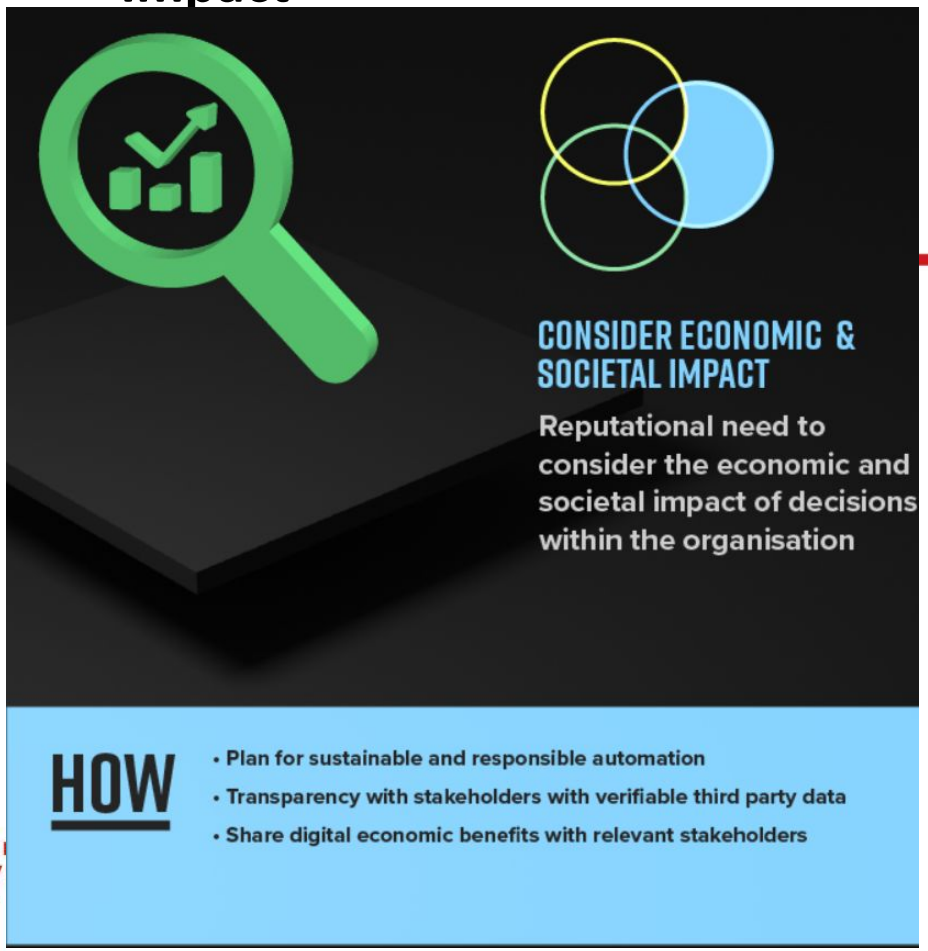


The International CDR Manifesto - the 7 core principles

3. Promote Societal Wellbeing



4. Consider Economic and Societal Impact

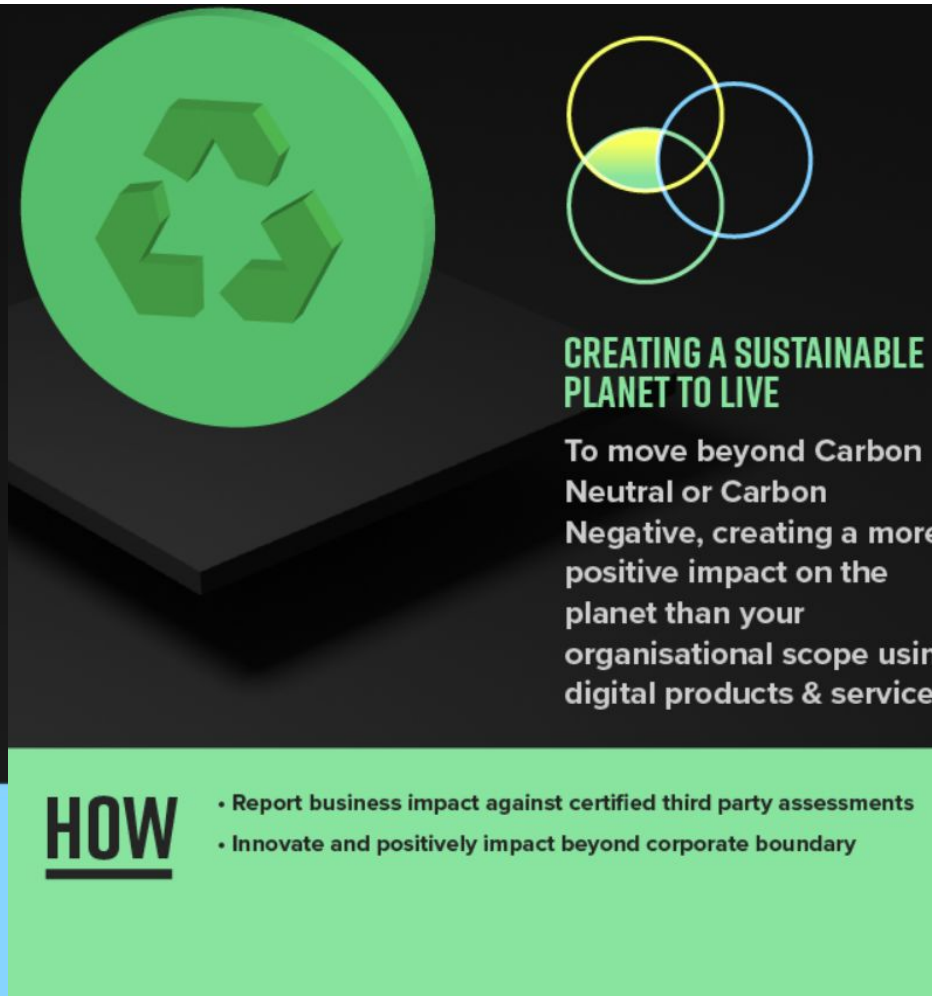


The International CDR Manifesto - the 7 core principles

5. Accelerate Impact Economy Progress

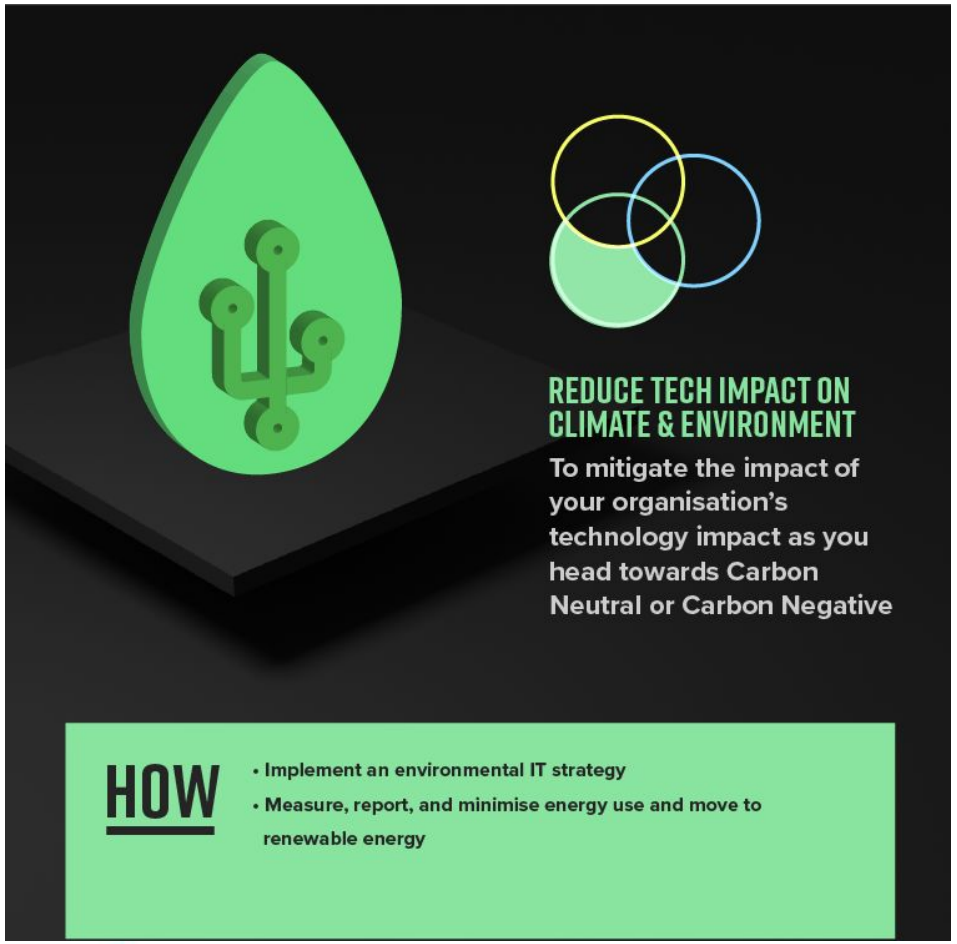


6. Create a Sustainable Planet to Live

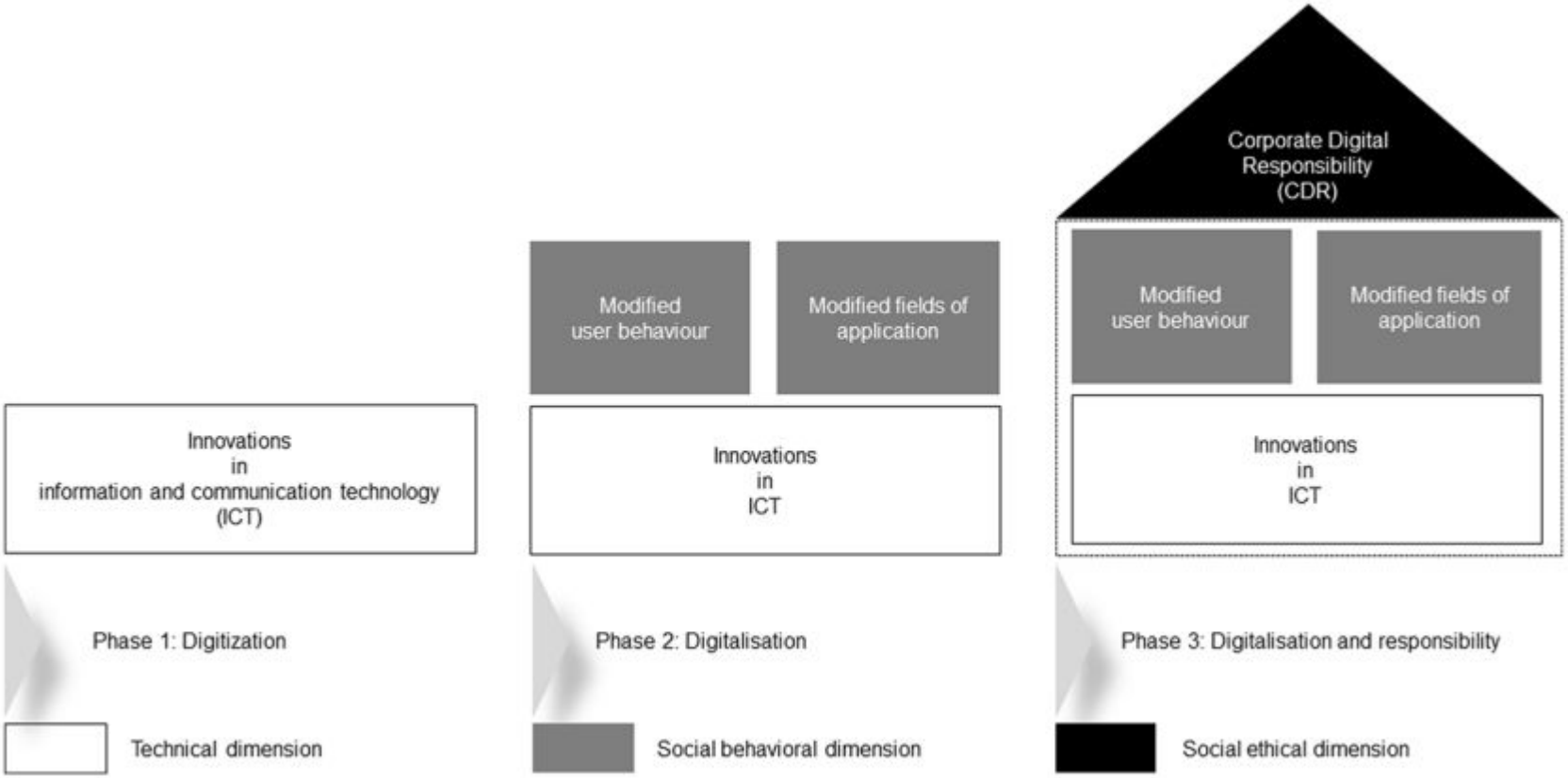


The International CDR Manifesto - the 7 core principles

7. Reduce Tech's Impact on Climate and the Environment



From digitization to corporate digital responsibility



SOURCE: Merbecks, U. Corporate digital responsibility (CDR) in Germany: background and first empirical evidence from DAX 30 companies in 2020. *J Bus Econ* (2023). https://doi.org/10.1007/s11573-023-01148-6

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Lecture 4: ESG and its connection to CDR



VŠ KC

MMI

As part of the initiative for sustainable development of the economy, three basic groups of goals have been determined that are being attempted to be achieved. These are **environmental, social and governance goals abbreviated ESG**.

ESG practice includes and cares about the way companies deal with climate change, the way they take care of their employees and other interested parties, but also about the company's corporate culture and its management. The ever-increasing global attention and focus on environmental, social, and governance (ESG) issues led to the development of the Corporate Sustainability Reporting Directive (CSRD) which will ensure reporting on all sustainability topics (environmental, social and governance factors).

ESG is a new way of thinking and therefore doing business in order to ensure a **green and sustainable future**.

ESG principles were coined back in 2004 at The UN Global Compact summit, as a commitment of twenty major financial companies to start integrating social, environmental and governance problems into investment analysis and decision-making (United Nations Global Compact, 2023).

The ***environmental (E)*** aspect includes environmental matters that may have a positive or negative influence on financial outcomes such as the risks of climate change, the need for waste reduction, and environmentally friendly products.

Social (S) includes social matters that may influence an entity positively or negatively such as the working environment and communication.

Governance (G) includes governance matters in terms of positive or negative impact on all interested parties such as corporate structure, transparency of information and rewarding system (Li et al., 2021).

United Nations Global Compact (2023). The Global Compact Leaders Summit 2004 – Final Report available at https://d306pr3pise04h.cloudfront.net/docs/news_events%2F8.1%2Fsummit_rep_fin.pdf

Li, T. T., Wang, K., Sueyoshi, T., & Wang, D. D. (2021). ESG: Research progress and future prospects. Sustainability, 13(21), 11663.

UNIVERSITY NORTH

Corporate digital responsibility in the age of artificial intelligence

Key question: How effectively are tech companies acknowledging their CDR?

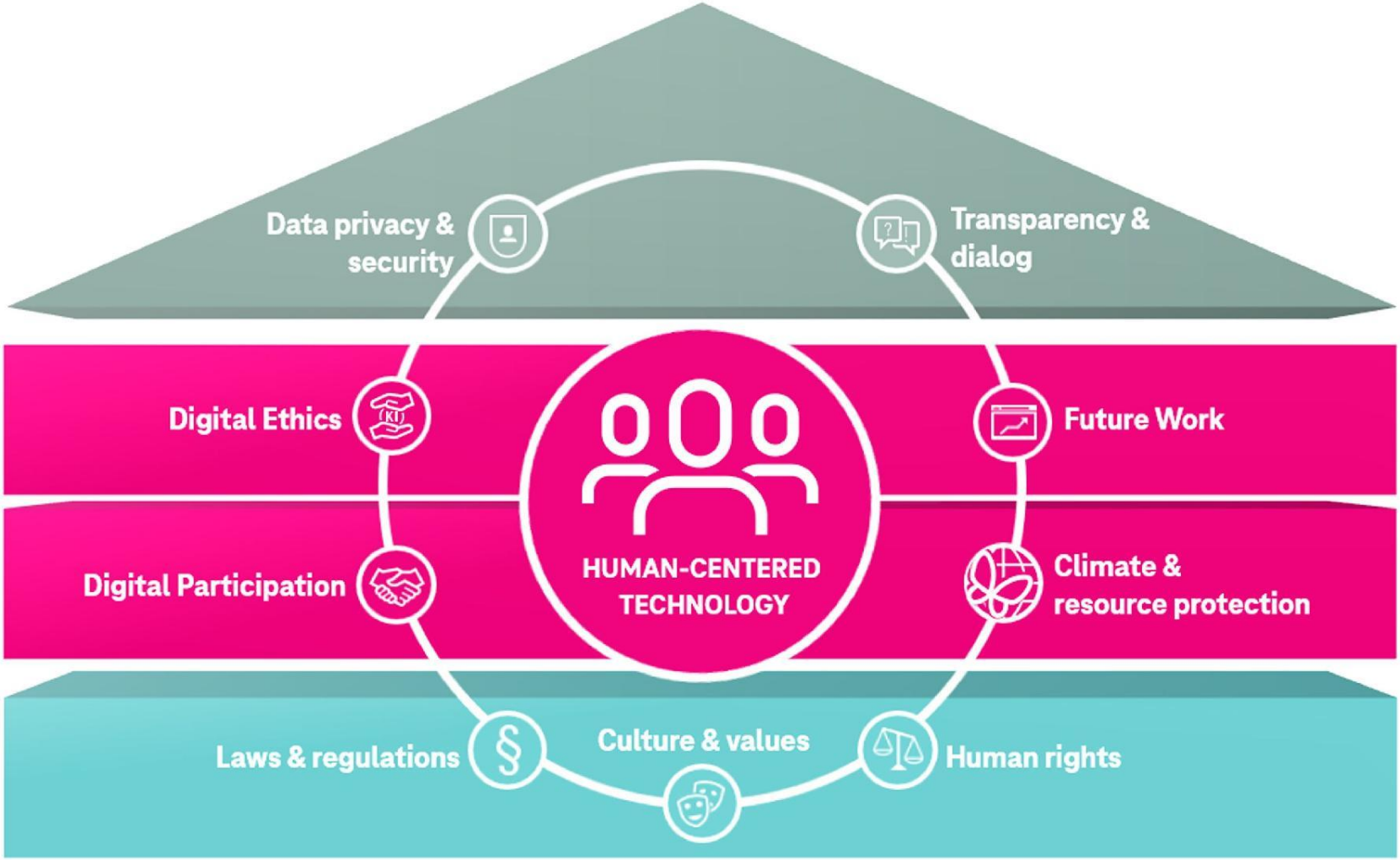
- there are increasing worries regarding AI labs being 'locked in an out-of-control race' to develop and deploy increasingly powerful systems that no one – including their creators – can understand, predict or control

SOURCE: https://theacademic.com/artificial-intelligence-corporate-digital-responsibility/

SVEUČILIŠTE SJEVER

Best practice – real-life examples

Deutsche Telekom - CDR



The House of Digital Responsibility in Deutsche Telekom

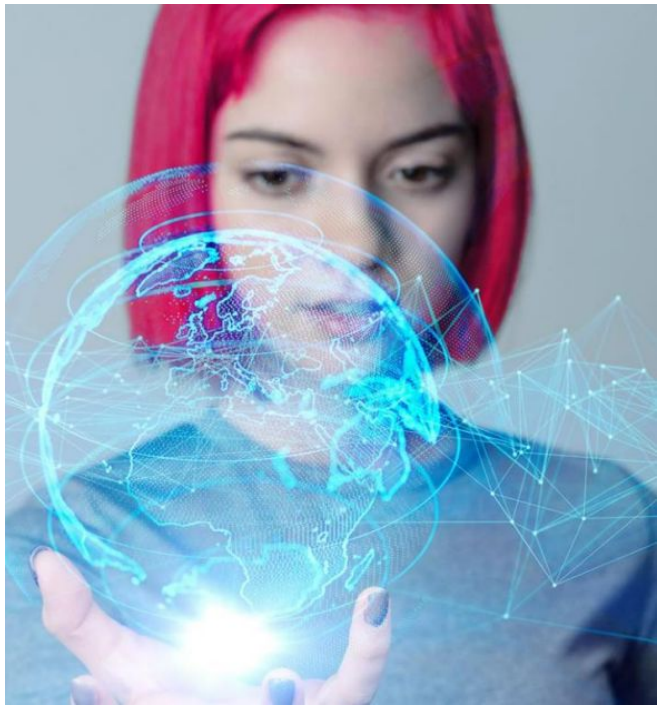
Our actions are based on our firm foundation and our principles. We focus on technologies for people and with people. We currently categorize these actions in four areas:

Digital Ethics – Ensuring sovereignty and supporting people are our focus. We design digital technologies responsibly.

Digital Participation – Deutsche Telekom wants everyone to take part in the digital society. Everyone should have access to the many opportunities afforded by digitalization.

Future Work –Digital responsibility at Deutsche Telekom means thinking about future work as part of its dynamic transformation process and ensuring that despite all the changes, people remain the focus of all decisions.

Climate and resource protection – Protecting the climate together and using resources responsibly – with and through digitalization.



Corporate Digital Responsibility @Deutsche Telekom

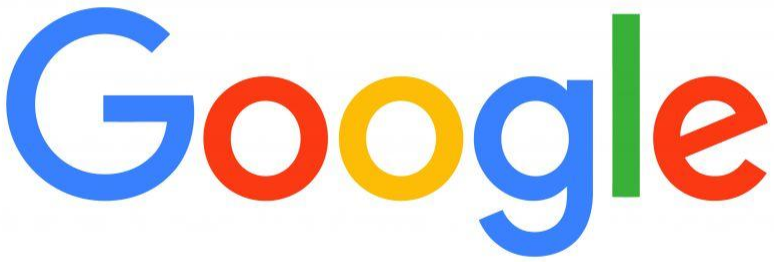
Our definition of digital responsibility



Acting with digital responsibility

Corporate Digital Responsibility @Deutsche Telekom is the result of our CDR community. Contact persons and experts from all Board of Management departments have contributed and continue to contribute to the discussion. Based on our analysis of numerous documents, qualitative surveys, and detailed interviews, we have identified a large number of activities that help foster our digital responsibility. Further activities are already being planned in the various departments.

We see taking digital responsibility as a dynamic process and constant evolution. We will report on new and expanded activities and measures on a regular basis, because meeting our high standards for responsible digitalization is an ongoing challenge and duty – **one that we gladly face**.





AI for intelligent retail service automation

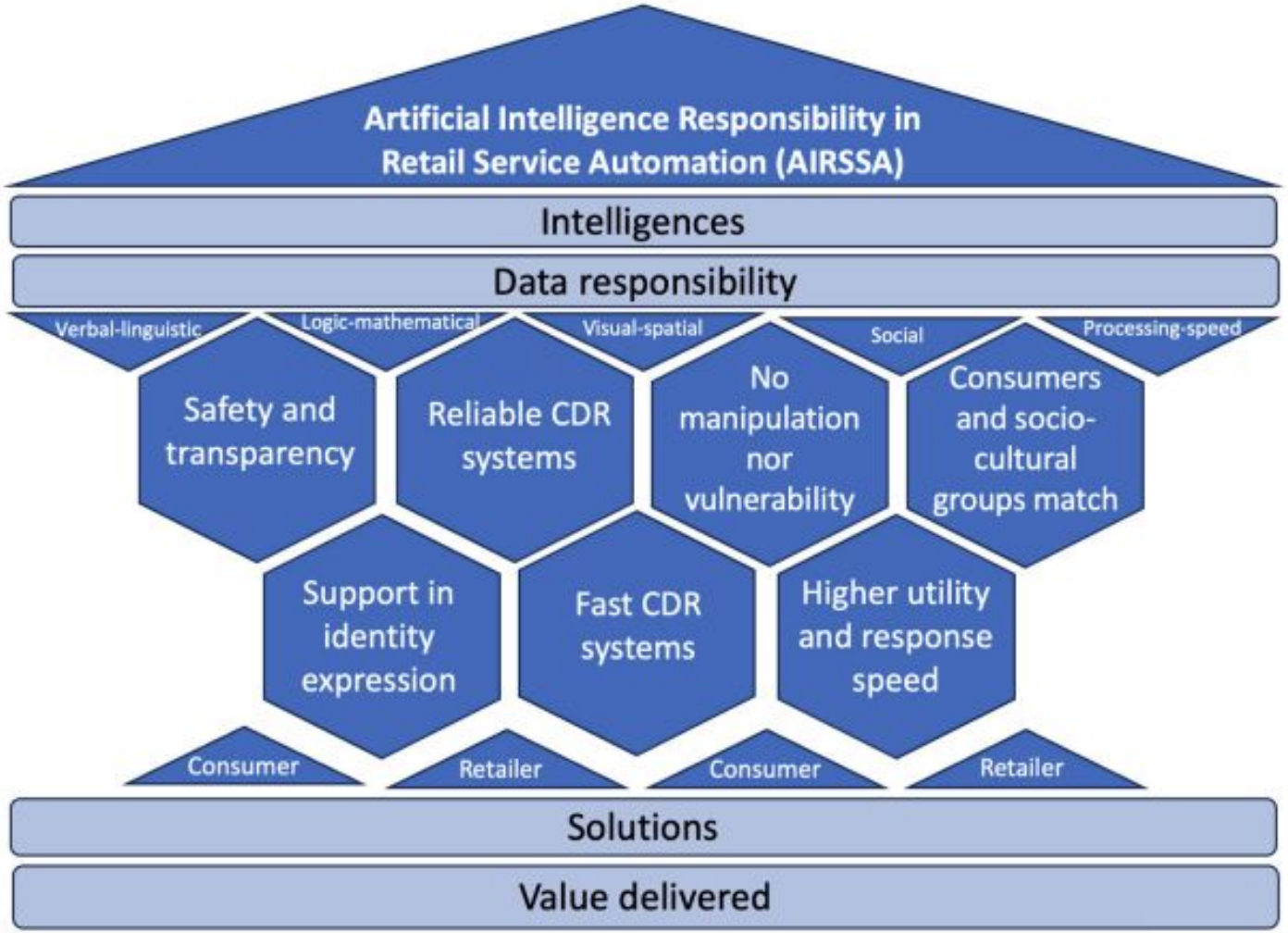
Key elements for AI retail service automation.

Potential advantages for retailers	AI service automation tools	Potential privacy and ethical concerns for consumers
Adopting new ways for replying to consumers' complaints (automatization via social media and online chatbot)	Machine learning algorithms	Potential non-deterministic behavior of the AI (i.e., how will the AI evaluate the importance of the complaint of a certain consumer and consequently accommodate the response if the complaint is slightly different from the one used for training?), which results in a possible lack of validity
Improving personalization (including recommendations, notifications, and products)	Machine learning algorithms	Lack of data transparency in collection, storage, and usage
Capturing and merging data from different sources, including in-store proximity sensors, CCTV, online interactions, mobile apps	Facial recognition systems, iBeacon and RFID	Lack of data transparency in collection, storage, and usage, and a limited possibility to delete or remove past data
Developing new prediction models	Machine learning algorithms and big data analytics	Lack of data accuracy leading to systemic biases undetected

SOURCE: Scarpi, D., & Pantano, E. (2024). "With great power comes great responsibility": Exploring the role of Corporate Digital Responsibility (CDR) for Artificial Intelligence Responsibility in Retail Service Automation (AIRRSA). *Organizational Dynamics*, *53*(2), 101030.

UNIVERSITY NORTH

Artificial Intelligence Responsibility in Retail Service Automation (AIRRSA), from consumers and retailers perspective.



VŽ KC
MMI
SJEVER

Scarpi, D., & Pantano, E. (2024). “With great power comes great responsibility”: Exploring the role of Corporate Digital Responsibility (CDR) for Artificial Intelligence Responsibility in Retail Service Automation (AIRRSA). *Organizational Dynamics*, *53*(2), 101030.

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Lecture 5: Digital Act – EU legislative related to CDR (Regulation (EU) 2022/2065)



VŽ KC

MMI

The Digital Services Act - DSA

The DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.

Its main goal is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment.

As of **17 February 2024**, the DSA rules apply to all platforms. Since the end of August 2023, these rules had already applied to designated platforms with more than 45 million users in the EU (10% of the EU's population), the so-called Very large online platforms (VLOPs) or Very large online search engines (VLOSEs).

What are the key goals of the Digital Services Act?



For citizens

- better protection of fundamental rights
- more control and choice
- stronger protection of children online
- less exposure to illegal content



For providers of digital services

- legal certainty
- a single set of rules across the EU
- easier to start-up and scale-up in Europe



For business users of digital services

- access to EU-wide markets through platforms
- level-playing field against providers of illegal content



For society at large

- greater democratic control and oversight over systemic platforms
- mitigation of systemic risks, such as manipulation or disinformation

SOURCE: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

What the new rules mean for users, businesses and platforms

Europe fit for the Digital Age: New online rules for businesses

- The same rules will apply in the entire Union and will be the basis of a large domestic market for digital services to grow and prosper. Cross-border digital trade in the single market is expected to increase up to 2%
- Small players will have **legal certainty to develop services and protect users from illegal activities** and they will be supported by standards, codes of conduct and guidelines
- **Small and micro-enterprises are exempted from the most costly obligations**, but are free to apply the best practices, for their competitive advantage
- Support to scale-up: **exemptions for small enterprises are extended for 12 months** after they scale past the turnover and personnel thresholds that qualify them as small companies

UNIVERSITY NORTH

What the new Digital Services Act changes (pt. 2):

Removing disincentives for companies to take voluntary measures to protect their users from illegal content, goods or services

Businesses will use new simple and effective mechanisms for flagging illegal content and goods that infringe their rights, including intellectual property rights, or compete on an unfair level

Businesses may also become ‘trusted flaggers’ of illegal content or goods, with special priority procedures and tight cooperation with platforms

Enhanced obligations for marketplaces to apply dissuasive measures, such as "know your business customer" policies, make reasonable efforts to perform random checks on products sold on their service, or adopt new technologies for product traceability

VŽ KC
MMI
SVEUČILIŠTE SJEVER

UNIVERSITY NORTH

DSA: What's in it for SMEs?

- Open up new opportunities for businesses, who will be able to innovate and compete against gatekeepers' own services in equal terms.
- Consumers will be able to see which are the best options available and not just those that the gatekeepers want them to see.
- Business users will know what to expect when dealing with gatekeepers.
- Gatekeepers will know the clear obligations applicable to them.
- Clearly-defined procedural rules will ensure quick decisions that will translate in speedy advantages for both business users and consumers.
- It will allow businesses to have access to more information on how their products or services are performing on third party platforms
- No more unfair ranking of gatekeepers' own services and products compared to those offered by other businesses on the same platform
- Businesses will be able to more easily attract consumers who can no longer be locked in by gatekeeper platforms
- The new rules will make it easier for smaller businesses and new entrants to grow and expand, and compete with gatekeeper platforms.
- Increased competition can be expected to lead to greater innovation potential amongst smaller businesses as well as improved quality of service, with associated increases in consumer welfare.
- Start-up and new businesses will emerge and grow, and will create new jobs, thanks to a level playing field.

VŽ KC
MMI
SVEUČILIŠTE SJEVER

The Digital Services Act package includes:

a. The Digital Services Act,

b. The Digital Markets Act.

The Digital Markets Act (DMA) affects "gatekeeper platforms" like Google, Amazon and Meta, and covers the need for user consent before processing personal data for targeted advertising. It is interesting that most of the companies that are affected by the Digital Markets Act and the Digital Services Act are based in the United States of America.

If you believe that the sanctions for GDPR violations are very strict (up to 4% of global annual turnover), you will be surprised with **the sanctions for Digital Services Act violations (up to 6% of global annual turnover), and the sanctions for Digital Markets Act violations (up to 10% of global annual turnover, or up to 20% in case of repeat offence.)**

The General Data Protection Regulation - GDPR

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. The EU general data protection regulation (GDPR) **governs how the personal data of individuals in the EU may be processed and transferred**.

- entered into application on 25 May 2018

Why is everyone so familiar with the GDPR?

- The **fines for violating the GDPR are very high**. There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages.

The GDPR defines:

- individuals' fundamental rights in the digital age
- the obligations of those processing data
- methods for ensuring compliance
- sanctions for those in breach of the rules

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Lecture 6: Is CDR profitable? Benefits & costs of CDR implementation



VŠ KC

MMI

CDR Calculus

Value of Good CDR = **Benefits** − **Opportunity Costs / Costs of Good CDR**

Benefits

Mitigation of CDR Risks

- Legal risks
- Reputational risks
- Regulatory risks

Brand Equity and Trust

"Warm glow" of being a good organization builds brand equity in:

- Consumer markets
- Labour markets
- Partner and supplier ecosystem

Opportunity Costs / Costs of Good CDR

Lost Incremental Revenues

- Contribution (sales, cross-and up-selling)
- Price discrimination
- Churn prediction and prevention
- Revenues from new services
- Revenues from data, insights, and services sold to 3rd parties

Reduced Customer Experience

- Customization and personalization
- Convenience, accessibility, and speed of service

Untranslated Potential Cost Savings

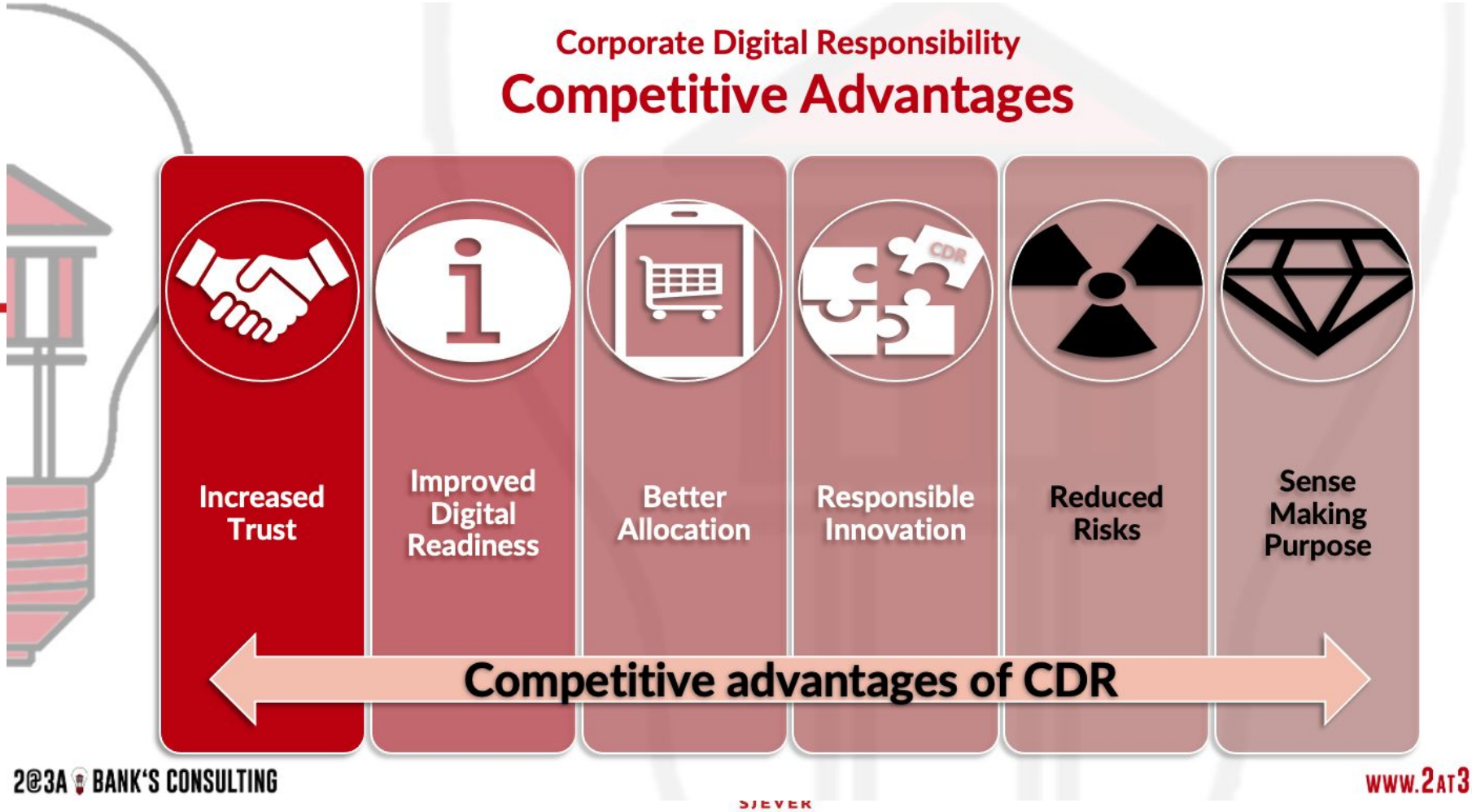
- Optimized and automated service processes
- Compliance to service processes and policies
- Risk assessment, and fraud detection and prevention
- Optimized supply chain

Cost of Robust CDR

- Cost of building a CDR culture and norms
- Cost of a CDR management structure, unit, and team (incl. staffing for CDR activities and CDR training and development)
- Cost of governance (internally and business partner ecosystem)

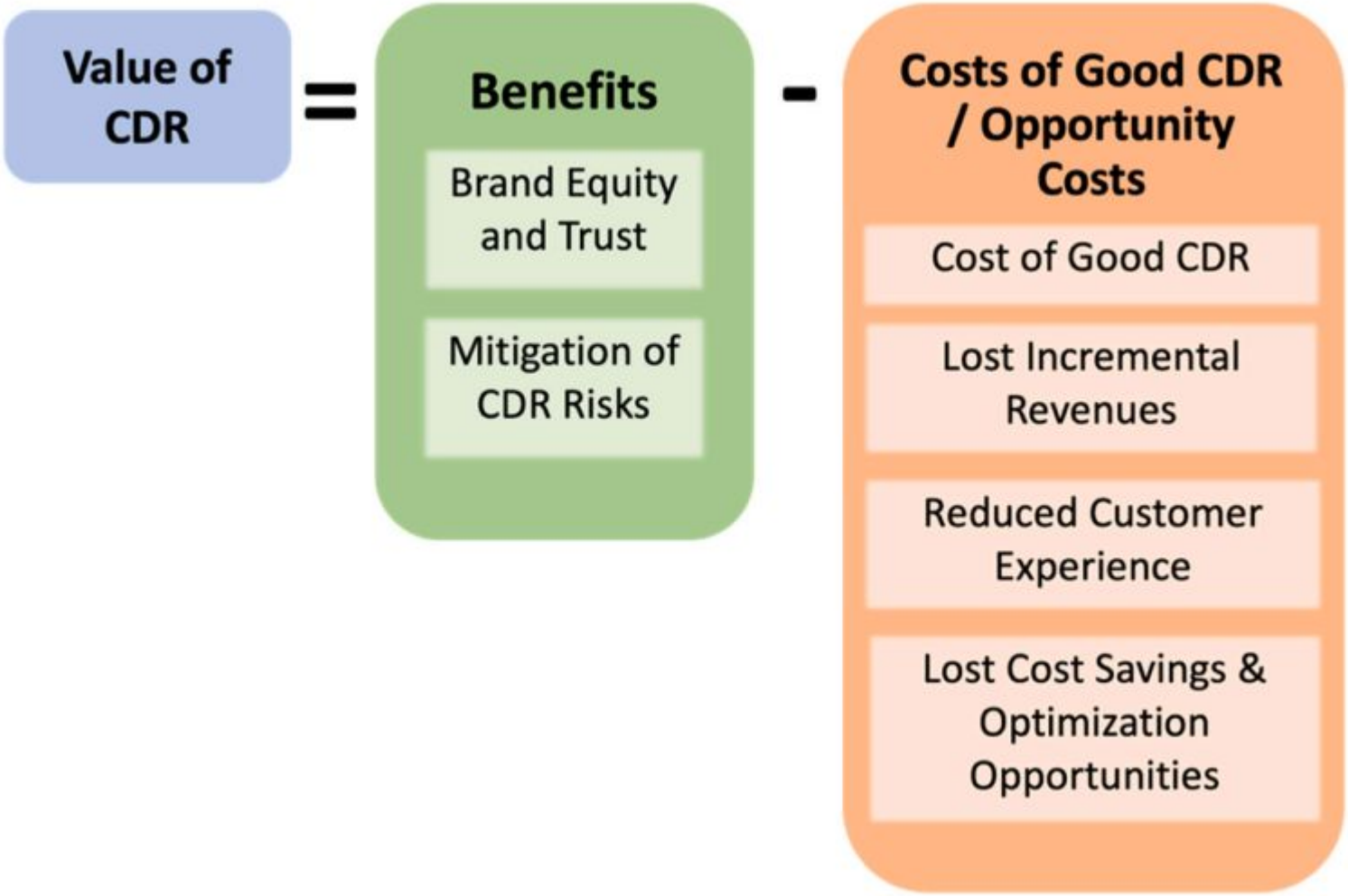
SOURCE: https://www.servsig.org/wordpress/2023/04/corporate-digital-responsibility-cdr-in-the-age-of-ai-why-do-service-firms-engage-in-poor-cdr-practices/

Corporate Digital Responsibility can improve a company's competition for scarce resources along the dimensions of trust, digital readiness, allocation, responsible innovation, risk and sense-making purpose.



Competitive Advantages implementing a Corporate Digital Responsibility Strategy, https://www.linkedin.com/pulse/competitive-advantages-implementing-corporate-digital-marcel-bank/

The CDR calculus



Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*, *53*(2), 101056.

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Lecture 7: Summary



VŽ KC

MMI

Managerial Practices for Sustainable CDR

Interreg CENTRAL EUROPE
Co-funded by the European Union

CDR Culture (shared CDR values, norms, artifacts and behaviors)

Managerial Practices for Sustainable Corporate Digital Responsibility (CDR):

Restructuring Processes and Responsibilities:

- Embed a CDR policy.
- Refine and redesign data management practices.
- Ensure human involvement in the creation, development, and deployment of new technologies and data.
- Restructure roles and responsibilities within different organizational units to cater to CDR requirements.
- Ensure that decisions are justifiable and transparent for CDR robustness.

Strengthen Data Management and Governance Practices:

- Create robust internal governance structures to mediate risks.
- Establish teams, systems, structures, and processes that enhance transparency, increase accountability.
- Ensure governance encompasses the complete data and technology lifecycle and spans across the organization's hierarchy.
- Normalize the reporting of tool utilizations in annual reports to stakeholders.

Invest in Managerial and Employee Competencies:

- Develop dedicated roles like Chief Data or Information Officer and mandated board positions.
- Prioritize upskilling employees in digital competencies to ensure a holistic approach to CDR.
- Embed CDR evaluation metrics in employee performance appraisals to encourage compliance and transparency.

Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*, *53*(2), 101056.

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

Thank you for your time and attention!



VŠ KC

MMI

COEUS | ONLINE TRAINING

Data Security and Cybersecurity for SMEs

Four modules · Concepts, threats, safeguards, and practical cases

Dr. Tomislav Horvat · University North, Croatia

What data security protects

- Business information must remain confidential, accurate, and available when needed.
- Security depends on technology, routines, and the choices people make every day.

Course overview

- Module 1: Data security and cybersecurity fundamentals
- Module 2: Cyber threats and attacks
- Module 3: Security architecture and protective measures
- Module 4: Cybersecurity in SMEs

Everyday choices matter

- A convincing email can lead someone to disclose a password or open a malicious file.
- Clear routines and employee awareness reduce this risk.

Module 1: Cybersecurity fundamentals

- Key concepts and goals
- The people and systems in a cybersecurity ecosystem
- Security measures and incident response

The people behind cyber incidents

- Attackers may use ready-made tools, seek profit, or exploit access they already hold.

- Ethical security specialists find weaknesses with permission and help fix them.

Cybersecurity and its goals

- Cybersecurity protects computers, networks, software, and information from digital harm.

- Confidentiality restricts access. Integrity protects accuracy. Availability keeps services usable.

Why cybersecurity matters to SMEs

- An incident can interrupt orders, service, and communication.

- Lost data and recovery work create costs, while disclosure can damage customer trust.

The cybersecurity ecosystem

- Devices, operating systems, applications, cloud services, networks, and users interact.

- A weakness in one part can expose the rest of the business.

Core security measures

- Firewalls control network traffic; antivirus tools identify malicious software.
- Encryption protects information. Detection systems alert staff to suspicious activity.

Rules and response

- The GDPR governs the handling of personal data in the EU. Relevant standards depend on a business’s activities.

- A response plan covers detection, containment, recovery, and review.

Cyber insurance

- Insurance may help cover recovery and liability costs, depending on the policy.

- Coverage supports a response plan but does not replace prevention, backups, or staff training.

Module 2: Threats and attacks

- A threat is a potential source of harm. An attack is an attempt to exploit it.

- Common forms include malware, phishing, social engineering, DDoS attacks, and insider misuse.

Malware

- Malware can steal information, disrupt operations, or lock files.

- Viruses spread through infected files; worms spread across systems; ransomware encrypts data.

Ransomware example: WannaCry

- The 2017 WannaCry outbreak encrypted files and interrupted organizations worldwide.

- Timely updates, limited access, and tested backups reduce exposure and aid recovery.

Phishing

- Attackers imitate trusted senders and ask recipients to click links, open files, or disclose credentials.

- Verify unusual requests through a separate channel and check the destination before signing in.

Phishing example: a fake PayPal message

- An urgent account warning directs the recipient to an imitation sign-in page.
- The attacker captures credentials entered into the fake page.

Social engineering

- Attackers exploit trust, urgency, or authority to influence employees.

- A caller posing as technical support may ask for passwords or remote access.

DDoS attacks

- Many devices send traffic to a service at once, leaving it unavailable to legitimate users.

- The 2016 attack on DNS provider Dyn disrupted access to several prominent websites.

Insider threats

- Employees, contractors, and former staff may have access to sensitive information.

- Limit privileges to job needs, review access regularly, and remove access when roles change.

Module 3: Protective measures

- Network and device protection
- Backups and recovery
- Staff training, updates, and access controls

Firewalls, antivirus, and detection

- A firewall filters traffic between trusted systems and external networks.

- Antivirus scans for harmful software. IDS and IPS tools monitor and may block suspicious activity.

Backups and recovery

- Keep copies of critical data according to business needs and test that they restore successfully.

- Define who starts recovery, where clean copies are stored, and how services resume.

Prevention as a routine

- Train employees to recognize suspicious requests.

- Keep software current and use unique passwords with multifactor authentication.

Module 4: Cybersecurity in SMEs

- Apply the safeguards to everyday small business situations.

- Choose controls that address actual data, systems, people, and business processes.

Case: SweetBites Bakery

• Online orders and customer information increase the need for secure accounts and reliable backups.

• Use unique passwords, multifactor authentication, role-based access, updates, and a recovery plan.

Case: TechRise Solutions

- A growing software firm needs to protect client systems and its cloud accounts.

- Strengthen access control, secure cloud services, patch systems, and define incident responsibilities.

Practical checklist

- Identify critical information and who can access it.
- Enable multifactor authentication and install updates.
- Test backups and rehearse how to report an incident.

Thank you

- Dr. Tomislav Horvat

- University North, Croatia

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

MODULE 3: Digital Sustainability, Inclusion and Accessibility

VŽ KC

MMI



Online Training
29 May 2025

Josip Hrgović
University North
Varaždin, Croatia

Digital Intensity Index (DII)

- SMEs with 0–49 employees make up **98%** of all businesses in the EU.
- They employ **nearly half of all workers**.
- But in **2022**, only **4%** of SMEs reached a **very high digital intensity**.
- **69%** reached at least a basic level (4 points or more),

And **31%** were still at **very low digital intensity**

- There's a **98% chance** that you'll be training **micro or small businesses**.
- And a **90% chance** that those SMEs will be operating at a **very low or low level** of digital maturity.

Use everyday language. Speak naturally. Avoid academic terms.
Teach through stories, examples, and simple comparisons.
Make it conversational.

Interrupt me anytime. Ask questions. Share experiences. That's how people learn.

Example 1: Client contact and preferences

"You know, when you write down things like your client's name, phone number, or how they like their haircut — that's all personal data.
And just like you keep their hairstyle secrets, you should also keep that information private.
That means not sharing it with others, not leaving it written down in an open notebook, and deleting it if you don't need it anymore.
If you're using a phone or app to store it, make sure it's protected with a password.
That's what we call digital responsibility — **treating other people's data the way you'd want yours to be treated**."

Example 2: Booking apps and online calendars

"Let's say you use an online calendar to schedule appointments.
It might ask for your client's name and number.
Make sure the app is secure and not just something random from the internet.
And don't put too much info in the notes — just enough to remember the appointment, not their full story or details they wouldn't want others to read.
Think of it this way: **if your phone got lost, would you be OK with someone seeing everything you wrote down about your clients?**
If not — keep it simple and safe."

Example 3: Photos and social media

"Sometimes you might want to post a picture of a client's new haircut on Instagram — and that's great for business!
But always ask if they're okay with it, especially if their face is in the photo.
Even better, get their OK in writing or through a message.
And if they ever change their mind, delete it right away.
Respecting their choice is part of being digitally responsible — it builds trust and shows you care about more than just their hair."

You must analyze the digital intensity of each SME you're working with.

"Tell me what you already do… and let's see how we can make it more responsible, more secure, more human, and more sustainable."

CDR training helps improve reputation.

It helps avoid fines and legal issues.

It provides **practical guidance**.

It raises awareness about risks.

"Is there anything in your daily work that you've already digitalized or automated — like appointment scheduling, payment processing, or product inventory?"

"Do you use any system to track customer preferences — like who prefers which hairstyle, color, or product? Would you like to have a tool like that?"

"How do you currently communicate with your clients — through social media, messages, or emails? Do you think you could use those channels more effectively?"

"Do you collect personal information from clients — such as their names, phone numbers, or hair color formulas? Do you know what you should do to protect that data in line with GDPR?"

"Do you have any internal rules or routines about who in the salon can access clients' digital data? What happens if someone accidentally deletes something?"

"Have you ever considered how a person with visual or hearing impairments might access information about your services, prices, or booking options online?"

"Do you have older clients? Do you think it would be easier for them to book an appointment through a simple app or by sending a voice message?"

"When you post information about offers or services on social media or your website, have you ever thought about font size, color contrast, or adding captions to your videos?"

"Do you think your website or online presence could be more useful for people in rural areas, or for those who don't speak the local language very well?"

"Do you think it would be helpful for your clients to book appointments using voice messages or voice commands instead of typing?"

"Have you ever asked your clients how they would like your online presence to look — whether the information is easy to find and clearly presented?"

"Is it important to you that people who aren't very tech-savvy can still book appointments online easily? What might make it harder for them?"

"Do you use a computer, tablet, or smartphone to manage your business? Have you ever checked if those devices are set to energy-saving mode or if they are energy-efficient?"

"What do you do with old electronic devices — like computers, hair dryers, or phones — when you no longer use them? Do you know where you can recycle them responsibly?"

"Do you have a website? Do you know who your hosting provider is, and whether they use renewable energy — what's known as 'green hosting'?"

"When you buy new devices for the salon — like a printer, laptop, or tablet — do you consider how energy-efficient they are, or whether they carry labels like Energy Star?"

"Do you think using more digital tools — like e-invoicing or online bookings — could help reduce the amount of paper and waste in your salon?"

"Do you use your website or social media to share messages about sustainability — for example, why you choose products that aren't tested on animals or that use eco-friendly packaging?"

"Do you think your clients would be interested in a digital loyalty program where they earn points for bringing their own towels or recycling product packaging?"

"Would you be open to adding a simple online calculator to your website that shows clients how much CO2 they save when they use refill products or walk instead of driving?"

"Would you be interested in showing your clients — through digital channels — where your products come from? For example, using a QR code that links to information about the origin and sustainability of the ingredients?"

"Have you ever thought about sharing simple tips on social media for how clients can care for their hair at home — using less water and creating less waste?"

"Do you have any extra products or equipment that you no longer use — like old hair dryers, chairs, or shampoo bottles? Do you think a digital platform for exchanging or selling those items to other salons could be useful?"

"How do you keep track of your inventory — like hair color, shampoo, or other supplies? Do you think a digital tool could help you order more precisely and reduce waste?"

"Do you regularly service your equipment? Did you know that IoT devices can send alerts when maintenance is needed to extend the lifespan and prevent breakdowns?"

"Would you consider offering refillable products — where clients bring back empty containers, and you track their usage digitally and reward them with discounts for sustainable behavior?"

"Do you use a vehicle for business purposes — like picking up products or doing home visits? Have you ever thought about how much CO_2 that creates and whether it could be reduced?"

"Do you know how much electricity your salon uses each month? Would you find it helpful to use a digital tool that shows you how to reduce your energy use — like adjusting lighting, water heaters, or dryers?"

"Do you think about where your products come from — do they travel far, or are they local? And what about the waste, like bottles and packaging — where does it all end up?"

"Would you be interested in using a simple digital calculator that tells you what your carbon footprint is and how you could reduce it?"

"Have you ever considered sharing — on your website or social media — how your salon contributes to sustainability, like using LED lights, recycling, or choosing energy-efficient devices?"

Use AI tools as much as you find helpful!

UNIVERSITY NORTH

Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

THANK YOU

VŽ KC

MMI



Online Training
29 May 2025

Josip Hrgović
University North
Varaždin, Croatia