VALUE DESIGN
PRIVACY | RISK AND ETHIC MANAGEMENT

CORPORATE DIGITAL RESPONSIBILITY

Ethik, Frameworks und Governance

Online | 04.11.2026 | AI:AT Webinar

MAG.A KARIN DIETL

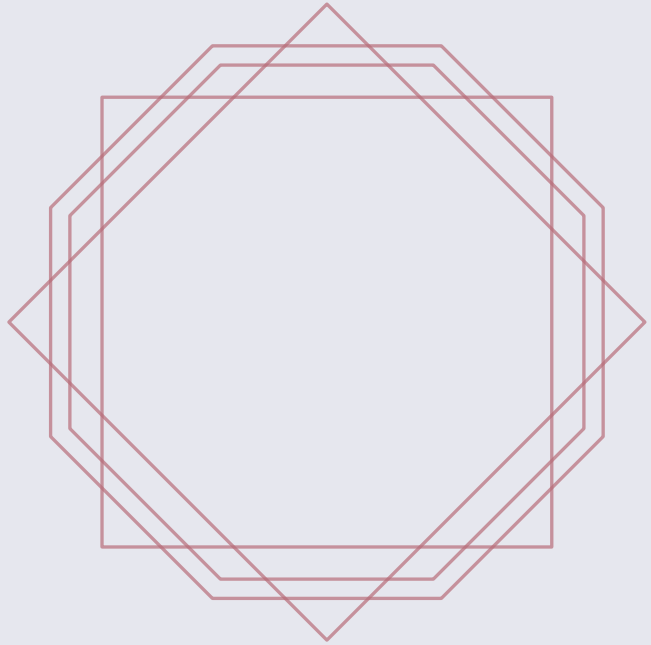
Gründerin Beratungsagentur Value Design

- **2026** FH Burgenland, Jurymitglied Digital Responsibility Award
- **seit 2025** WIFI-Trainerin für Chief AI Officer, KI-Beauftragte
- **2024** Digital Trust Ecosystem Framework Certificate
- **2021** Plattform CDR Austria
- **2019** Anwaltsprüfung, Gründung Value Design
- **2008** HTL Dornbirn, Chemieingenieurwesen



AGENDA

1. ETHIK IM DIGITALEN KONTEXT
2. CORPORATE DIGITAL RESPONSIBILITY: DEFINITION UND GRUNDLAGEN
3. VON DER ETHIK ZUR GOVERNANCE
4. FALLBEISPIELE UND DISKUSSION



01

ETHIK IM DIGITALEN KONTEXT

Philosophische Impulse als Denkwerkzeug

IHR ERSTER GEDANKE

Was bedeutet „digital verantwortungsvoll“ für Sie? Schreiben Sie ein Stichwort in den Chat.



DIGITALE ETHIK

Was bedeutet „Gut“ oder „Böse“ im Kontext der Digitalisierung? Und warum?

- **Bereichsethik** innerhalb der angewandten Ethik
- **Drei Ebenen:** Individuum, Organisation, Staat und Gesellschaft
- **Gestaltbarkeit ist Voraussetzung von Verantwortung**
  - „Die Digitalisierung kommt sowieso“ greift zu kurz
  - Jede Systemarchitektur, jedes Datenmodell, jede Plattformregel ist eine menschliche Entscheidung – und damit verantwortbar und gestaltbar

Definitionen

- **Moral:** „befasst sich mit den Normen, Werten und Überzeugungen (…), die für eine Person oder eine Gemeinschaft festlegen, was richtig und was falsch ist“ (Crane et al. 2019: 8)
- **Ethik:** „ein rationaler und systematischer Zugang zur Moral, der es ermöglicht, persönliche Ansichten zu überprüfen und die Moralität menschlichen Handelns und Verhaltens zu bewerten“ (Melé 2020: 7)

DIGITALE ETHIK

Das gute Leben im Kontext der Digitalität

Was ist Wirtschaftsethik?

- **Ethik**
  - akademische Disziplin und Teil der Philosophie
  - die wissenschaftliche Reflexion moralischer Fragen
  - liefert Gründe, wie Menschen handeln sollen, und Kriterien für die ethische Qualität von Verhalten: richtig/falsch, gut/schlecht, gerecht/ungerecht
- **Wirtschaftsethik**
  - „die Untersuchung wirtschaftlicher Situationen, Aktivitäten und Entscheidungen, in denen Fragen von Richtig und Falsch behandelt werden“ (Crane et al. 2019: 45)
  - befasst sich mit den „Grauzonen der Wirtschaft“ ohne rechtliche Vorgaben (Crane et al. 2019: 6) und mit Situationen, in denen „Werte im Konflikt stehen“ (Treviño & Nelson 2021: 26)

Warum ist Wirtschaftsethik wichtig?

- **Macht:** Unternehmen prägen den Alltag der Menschen und die Politik
- **Positive Wirkung:** Produkte, Arbeitsplätze, Steuern, wirtschaftliche Entwicklung, Lösung sozialer Probleme
- **Negative Wirkung:** großer Schaden für Einzelne, Gemeinschaften und Umwelt möglich
- **Erwartungen der Stakeholder:** komplexe, teils widersprüchliche Ansprüche
- **Gesellschaftliche Akzeptanz:** Reputation und Vertrauen

DIGITALE VERANTWORTUNG

Digitale Ethik

Datenethik

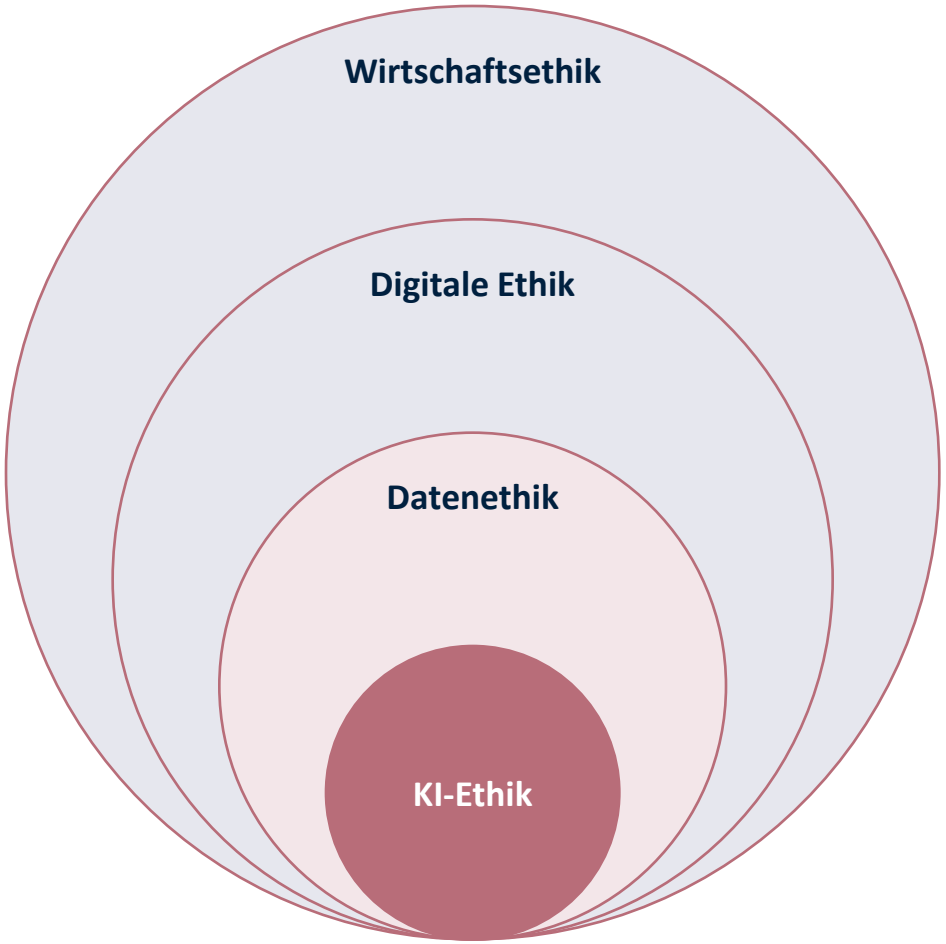
- Ethischer Umgang mit Daten, insbesondere mit persönlichen und sensiblen Informationen
- Wichtige Aspekte: Datenschutz, Einwilligung, Datenhoheit und Transparenz bei Erhebung und Nutzung von Daten

Digitale Ethik

- Umfasst einen breiteren Bereich: die ethischen Implikationen aller digitalen Technologien
- Thematisiert soziale Medien, digitale Plattformen, Cybersicherheit und die digitale Kluft
- Schließt Datenethik und KI-Ethik häufig ein, da Daten- und KI-Technologien integrale Bestandteile der digitalen Landschaft sind

KI-Ethik

- Befasst sich speziell mit den ethischen Herausforderungen durch Künstliche Intelligenz
- Wichtige Themen: algorithmische Verzerrungen (Bias), Autonomie, Verantwortlichkeit, Transparenz und gesellschaftliche Auswirkungen von KI-Systemen



European Declaration on Digital Rights and Principles for the Digital Decade

The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade

Preamble

Whereas:

1. The European Union (EU) is a 'union of values', as enshrined in Article 2 of the Treaty on European Union, founded on respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. Moreover according to the Charter of fundamental rights of the European Union, the EU is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity. The Charter also reaffirms the rights as they result, in particular, from international obligations common to the Member States.
2. The digital transformation affects every aspect of people's lives. It offers significant opportunities for a better quality of life, economic growth and sustainability.
3. The digital transformation also presents challenges for our democratic societies, our economies and for individuals. With the acceleration of the digital transformation, the time has come for the EU to spell out how its values and fundamental rights applicable offline should be applied in the digital environment. The digital transformation should not entail the regression of rights. What is illegal offline, is illegal online. This Declaration is without prejudice to "offline policies", such as having access to key public services offline.
4. The Parliament has made several calls for the establishment of ethical principles guiding the EU's approach to the digital transformation, as well as ensuring the full compliance with fundamental rights such as data protection, the right to privacy, non-discrimination and gender equality, and with principles such as consumer protection, technological and net neutrality, trustworthiness and inclusiveness. It has also called for a strengthened protection of users' rights in the digital environment, as well as workers' rights and the right to disconnect[1].
5. Building on previous initiatives such as the "Tallinn Declaration on eGovernment" and the "Berlin Declaration on Digital Society and Value-based Digital Government", the Member States have called, through the "Lisbon Declaration – Digital Democracy with a Purpose", for a model of digital transformation that strengthens the human dimension of the digital ecosystem with the Digital Single Market at its core. Member States have called for a model of digital transformation that ensures that technology assists in addressing the need to take climate action and protect the environment.
6. The EU vision for digital transformation puts people at the centre, empowers individuals and fosters innovative businesses. The Decision on the "Digital Decade Policy Programme 2030" sets out the concrete digital targets based on four cardinal points (digital skills, digital infrastructures, digitalisation of businesses and of public services). The EU way for the digital transformation of our societies and economy encompasses in particular digital sovereignty in an open manner, respect for fundamental rights, rule of law and democracy, inclusion, accessibility, equality, sustainability, resilience, security, improving quality of life, the availability of services and respect of everyone's rights and aspirations. It should contribute to a dynamic, resource efficient, and fair economy and society in the EU.
7. This Declaration spells out shared political intentions and commitments, and recalls the most relevant rights in the context of the digital transformation. The Declaration should also guide policy makers when reflecting on their vision of the digital transformation: putting people at the centre of the digital transformation; supporting solidarity and inclusion, through connectivity, digital education, training and skills, fair and just working conditions as well as access to digital public services online; restating the importance of freedom of choice in interactions with algorithms and artificial intelligence systems and in a fair digital environment; fostering participation in the digital public space; increasing safety, security and empowerment in the digital environment, in particular for children and young people; while ensuring privacy and individual control over data; promoting sustainability. The various chapters of this Declaration should form a holistic reference framework and should not be read in isolation.
8. This Declaration should also serve as a reference point for businesses and other relevant actors when developing and deploying new technologies. Promoting research and innovation is important in this respect. Special attention should also be given to SMEs and start-ups.
9. The democratic functioning of the digital society and economy should be further strengthened, in full respect of the rule of law, effective remedies and law enforcement. This Declaration does not affect lawful limits on the exercise of rights, in order to reconcile them with the exercise of other rights, or necessary and proportionate restrictions in the public interest.
10. This Declaration notably builds on primary EU law, in particular the Treaty on European Union, the Treaty on the Functioning of the European Union, the Charter of Fundamental Rights of the European Union, as well as on secondary law and the caselaw of the Court of Justice of the European Union. It also builds on and complements the European Pillar of Social Rights. It has a declaratory nature and, as such, does not affect the content of legal rules or their application.
11. The EU should promote the Declaration in its relations with other international organisations and third countries, including by reflecting these rights and principles in its trade relations, with the ambition that the principles guide international partners towards a digital transformation that puts people and their universal human rights at the centre throughout the world. The Declaration should notably serve as a reference for activities in the context of international organisations, such as the realisation of the Agenda 2030 for Sustainable Development, as well as the multistakeholder approach to Internet governance.
12. The promotion and implementation of the Declaration is a shared political commitment and responsibility of the EU and its Member States within their respective competences and in full compliance with EU law. The Commission will regularly report to the Parliament and the Council on the progress made. The Member States and Commission should take into account the digital principles and rights as laid down in this Declaration when cooperating in view of achieving the general objectives as set out in the Decision on the "Digital Decade Policy Programme 2030".

[1] 2020/2012(INL); 2020/2009(INL); 2020/2018(INL); 2020/2019(INL); 2020/2014(INL); 2020/2015 (INI); 2020/2017 (INI); 2019/2186(INI); 2019/2181(INL); 2020/2266 (INI).

Declaration on Digital Rights and Principles for the Digital Decade

We aim to promote a European way for the digital transformation, putting people at the centre, built on European values and EU fundamental rights, reaffirming universal human rights, and benefiting all individuals, businesses, and society as a whole.

We therefore declare:

Chapter I: Putting people at the centre of the digital transformation

1. People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights.

We commit to:

a. strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all people living in the EU;
b. taking necessary measures to ensure that the values of the EU and the rights of individuals as recognised by EU law are respected online as well as offline;
c. fostering and ensuring responsible and diligent action by all actors, public and private, in the digital environment;
d. actively promoting this vision of the digital transformation, also in our international relations.

Chapter II: Solidarity and inclusion

2. Technology should be used to unite, and not divide, people. The digital transformation should contribute to a fair and inclusive society and economy in the EU.

We commit to:

a. making sure that the design, development, deployment and use of technological solutions respect fundamental rights, enable their exercise and promote solidarity and inclusion;
b. a digital transformation that leaves nobody behind. It should benefit everyone, achieve gender balance, and include notably elderly people; people living in rural areas; persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf. It should also promote cultural and linguistic diversity;
c. developing adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all people living in the EU.

Connectivity

3. Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity.

We commit to:

a. ensuring access to high-quality connectivity, with available Internet access, for everyone wherever in the EU, including for those with low income;
b. protecting and promoting a neutral and open Internet where content, services, and applications are not unjustifiably blocked or degraded.

Digital education, training and skills

4. Everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills.

We commit to:

a. promoting high-quality digital education and training, including with a view to bridging the digital gender divide;
b. supporting efforts that allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes;
c. promoting and supporting efforts to equip all education and training institutions with digital connectivity, infrastructure and tools;
d. giving everyone the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling.

Fair and just working conditions

5. Everyone has the right to fair, just, healthy and safe working conditions and appropriate protection in the digital environment as in the physical work place, regardless of their employment status, modality or duration.
6. Trade unions and employers' organisations play an important role in the digital transformation, particularly in relation to the definition of fair and just working conditions, including with regard to the use of digital tools at work.

We commit to:

a. ensuring that everyone is able to disconnect and benefit from safeguards for work-life balance in a digital environment;
b. ensuring that, in the working environment, digital tools do not put workers' physical and mental health at risk in any way;
c. ensuring respect for workers' fundamental rights in the digital environment, including their right to privacy and the right to associate, right of collective bargaining and action, as well as protection against unlawful and unjustified surveillance;
d. ensuring that the use of artificial intelligence in the workplace is transparent and follows a risk-based approach and that corresponding prevention measures are taken to maintain a safe and healthy working environment;
e. ensuring in particular that human oversight is guaranteed in important decisions affecting workers, and that workers are generally informed that they are interacting with artificial intelligence systems.

Digital public services online

7. Everyone should have online access to key public services in the EU. Nobody is to be asked to provide data more often than necessary when accessing and using digital public services.

We commit to:

a. ensuring that people living in the EU are offered the possibility to use an accessible, voluntary, secure and trusted digital identity that gives access to a broad range of online services;
b. ensuring wide accessibility and re-use of public sector information;
c. facilitating and supporting seamless, secure and interoperable access across the EU to digital public services designed to meet people's needs in an effective manner, including and in particular digital health and care services, notably access to electronic health records.

Chapter III: Freedom of choice

Interactions with algorithms and artificial intelligence systems

8. Artificial intelligence should serve as a tool for people, with the ultimate aim of increasing human well-being.
9. Everyone should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems including by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights.

We commit to:

a. promoting human-centric, trustworthy and ethical artificial intelligence systems throughout their development, deployment and use, in line with EU values;
b. ensuring an adequate level of transparency about the use of algorithms and artificial intelligence, and that people are empowered to use them and are informed when interacting with them;
c. ensuring that algorithmic systems are based on adequate datasets to avoid discrimination and enable human supervision of all outcomes affecting people's safety and fundamental rights;
d. ensuring that technologies such as artificial intelligence are not used to pre-empt people's choices, for example regarding health, education, employment, and their private life;
e. providing for safeguards and taking appropriate action, including by promoting trustworthy standards, to ensure that artificial intelligence and digital systems are, at all times, safe and used in full respect for fundamental rights;
f. taking measures to ensure that research in artificial intelligence respects the highest ethical standards and relevant EU law.

A fair digital environment

10. Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible and reliable information.
11. Everyone should have the possibility to compete fairly and innovate in the digital environment. This should also benefit businesses, including SMEs.

We commit to:

a. ensuring a safe and secure digital environment based on fair competition, where fundamental rights are protected, users rights and consumer protection in the Digital Single Market are ensured, and responsibilities of platforms, especially large players and gatekeepers, are well defined;
b. promoting interoperability, transparency, open technologies and standards as a way to further strengthen trust in technology as well as consumers' ability to make autonomous and informed choices.

Chapter IV: Participation in the digital public space

12. Everyone should have access to a trustworthy, diverse and multilingual digital environment. Access to diverse content contributes to a pluralistic public debate and effective participation in democracy in a non-discriminatory manner.
13. Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment.
14. Everyone should be able to access information on who owns or controls the media services they are using.
15. Online platforms, particularly very large online platforms, should support free democratic debate online. Given the role of their services in shaping public opinion and discourse, very large online platforms should mitigate the risks stemming from the functioning and use of their services, including in relation to misinformation and disinformation campaigns, and protect freedom of expression.

We commit to:

a. continuing safeguarding all fundamental rights online, notably the freedom of expression and information, including media freedom and pluralism;
b. supporting the development and best use of digital technologies to stimulate people's engagement and democratic participation;
c. taking proportionate measures to tackle all forms of illegal content, in full respect for fundamental rights, including the right to freedom of expression and information, and without establishing any general monitoring obligations or censorship;
d. creating a digital environment where people are protected against disinformation and information manipulation and other forms of harmful content, including harassment and gender-based violence;
e. supporting effective access to digital content reflecting the cultural and linguistic diversity in the EU;
f. empowering individuals to make freely given, specific choices and limiting the exploitation of vulnerabilities and biases, namely through targeted advertising.

Chapter V: Safety, security and empowerment

A protected, safe and secure digital environment

16. Everyone should have access to digital technologies, products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability and authenticity of the information processed.

We commit to:

a. taking further measures to promote the traceability of products [illegible] make sure they put on the [illegible] safe and compliant with EU legislation are offered on the Digital [illegible] Market;
b. protecting the interests of people, businesses and public institutions [illegible] cybersecurity including data breaches and identity theft or manipulation. This includes cybersecurity requirements for connected products placed on the single market;
c. countering and holding accountable those that seek to undermine, within the EU, security online and the integrity of the digital environment or that promote violence [illegible] digital space.

Privacy and individual control over d[illegible]

17. Everyone has the right to privacy and to the protection of their personal data. [illegible] control by individuals on how their personal data are used and with [illegible] have.
18. Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and not to be subjected to unlawful online surveillance, unlawful pervasive tracking or interception measures.
19. Everyone should be able to determine their digital legacy, and decide what happens with [illegible] accounts and information that concerns them after their death.

We commit to:

a. ensuring that everyone has effective control of their personal [illegible] data protection rules and relevant EU law;
b. ensuring effectively the possibility for individuals to easily move their personal and non-personal data between different digital services in line with portability rights;
c. effectively protecting communications from unauthorised third [illegible];
d. prohibiting unlawful identification as well as unlawful retention [illegible].

Protection and empowerment of children and young people [illegible] digital environment

20. Children and young people should be empowered to make safe and informed choices and express their creativity in the digital environment.
21. Age-appropriate materials and services should improve experiences, well-being and participation of children and young people in the digital environment.
22. Specific attention should be paid to the right of children and young [illegible] to be protected from all crimes committed via or facilitated through digital technologies.

We commit to:

a. providing opportunities to all children and young people to acquire the necessary skills and competences, including media literacy and critical thinking, in order to navigate and engage in the digital environment actively, safely and to make informed choices;
b. promoting positive experiences for children and young people in an age-appropriate and safe digital environment;
c. protecting all children and young people against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes;
d. protecting all children and young people against illegal tracking, profiling and targeting, in particular for commercial purposes;
e. involving children and young people in the development of digital policies that concern them.

Chapter VI: Sustainabil[illegible]

23. To avoid significant harm to the environment and to promote a [illegible] economy, digital products, services and services should be designed, produced, used, repaired, recycled and disposed of in a way that mitigates their negative impact on the environment and on society and avoids premature obsolescence.
24. Everyone should have access to accurate, easy-to-understand information on the environmental impact and energy consumption of digital products and services, their repairability and lifetime, allowing them to make responsible choices.

We commit to:

a. supporting the development and use of sustainable digital technologies that have minimal negative environmental and social impact;
b. incentivising sustainable consumer choices and business models, and fostering sustainable and responsible corporate behaviour throughout global value chains of digital products and services, including with a view to combating forced labour;
c. promoting the development, deployment and active use of innovative digital technologies with a positive impact on the environment and climate, in order to accelerate the green transition;
d. promoting sustainability standards and labels for digital products and services.

For the European Parliament — **Roberta Metsola**, *The President*

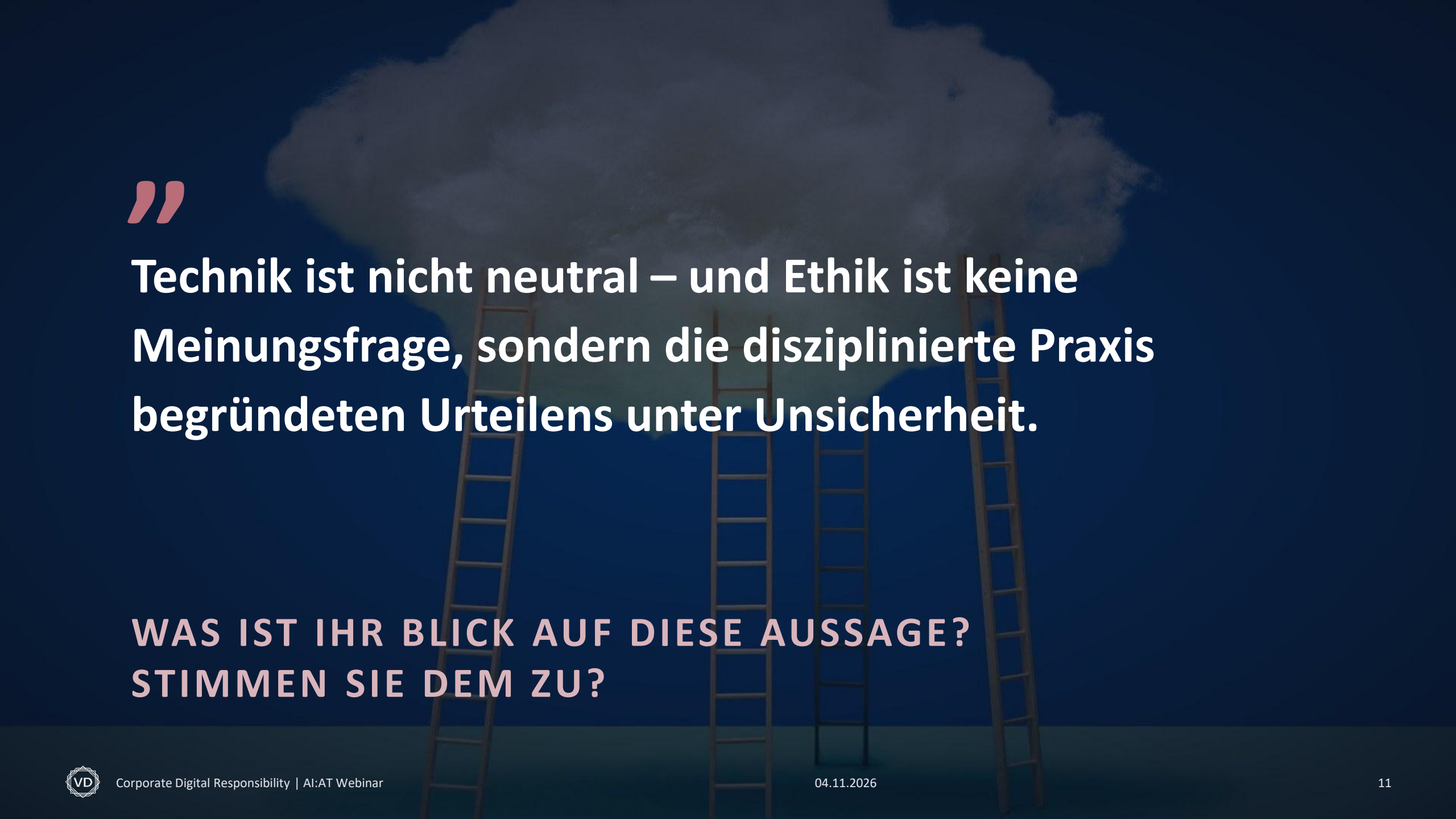
For the Council of the European Union — **Petr Fiala**, *The President*

For the European Commission — **Ursula von der Leyen**, *The President*

EUROPÄISCHE ERKLÄRUNG ZU DIGITALEN RECHTEN UND GRUNDSÄTZEN SINCE 2022

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition & Single Market	Media	Finance
Digital Europe Programme Regulation (EU) 2021/694	Recovery and Resilience Facility Regulation (EU) 2021/241	Frequency Bands Directive (EEC) 1987/372	ePrivacy Directive (EC) 2002/58	Database Directive (EC) 1996/9	Regulation for a Cybersecurity Act (EU) 2019/881	Law Enforcement Directive (EU) 2016/680	Toys Regulation (EC) 2009/48, 2023/0290(COD)	Unfair Contract Terms Directive (UCTD) (EEC) 1993/13	EC Merger regulation (EC) 2004/139	Satellite and Cable Directive (EEC) 1993/83	Common VAT system (EC) 2006/112, 2022/0407(CNS), 2022/0409(CNS)
Horizon Europe Regulation (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation (EU) 2021/523	Radio Spectrum Decision (EC) 2002/676	European Statistics (EC) 2009/223	Community Design Directive (EC) 2002/6	Regulation to establish a European Cybersecurity Competence Centre (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment (EU) 2019/713	European Standardization Regulation (EU) 2012/1025	Price Indication Directive (EC) 1998/6	Technology Transfer Block Exemption (EC) 2014/316	Information Society Directive (EC) 2001/29	Administrative cooperation in the field of taxation (EU) 2011/16
Regulation on a pilot regime distributed ledger technology (EU) 2022/858	Connecting Europe Facility Regulation (EU) 2021/1153	Electromagnetic compatibility Directive (EMC) (EU) 2014/30	General Data Protection Regulation (GDPR) (EU) 2016/679	Enforcement Directive (IPR) (EC) 2004/48	NIS 2 Directive (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa (EU) 2019/817	Radio Equipment Directive (RED) (EU) 2014/53	E-commerce Directive (EC) 2000/31	Company Law Directive (EU) 2017/1132	Audio-visual Media Services Directive (AVMSD) (EU) 2010/13	Payment Service Directive 2 (PSD2) (EU) 2015/2366, 2023/0209(COD)
European Innovation Act	Regulation on High Performance Computing Joint Undertaking (EU) 2021/1173	Open Internet Access Regulation (EU) 2015/2120	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies (EU) 2018/1725	Protection of trade secrets (Directive) (EU) 2016/943	Cybersecurity Regulation (EU) 2023/2841	Regulation on terrorist content online (EU) 2021/784	eIDAS Regulation (European Digital Identity Framework) (EU) 2014/910	Unfair Commercial Practices Directive (UCPD) (EC) 2005/29	Screening of foreign direct investments Regulation (EU) 2019/452	Portability Regulation (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation) (EU) 2022/2554
European Research Area Act	Regulation on Joint Undertakings under Horizon Europe (EU) 2021/2085	European Electronic Communications Code Directive (EECC) (EU) 2018/1972	Free flow of non-personal data (Regulation) (EU) 2018/1807	Design Directive (EU) 2024/2823	Cyber Resilience Act (EU) 2024/2847	Temporary CSAM Regulation (EU) 2021/1232, 2022/0155(COD)	Regulation for a Single Digital Gateway (EU) 2018/1724	Directive on Consumer Rights (CRD) (EU) 2011/83	Market Surveillance Regulation (EU) 2019/1020	Satellite and Cable II Directive (EU) 2019/789	Crypto-assets Regulation (MiCA) (EU) 2023/1114
	Decision on a path to the Digital Decade (EU) 2022/2481	.eu top-level domain Regulation (EU) 2019/517	Open Data Directive (PSI) (EU) 2019/1024	Compulsory licensing of patents 2023/0129(COD)	Cyber Solidarity Act (Regulation) (EU) 2025/38	E-evidence Regulation (EU) 2023/1543	General Product Safety Regulation (EU) 2023/988	e-invoicing Directive (EU) 2014/55	P2B Regulation (EU) 2019/1150	Copyright Directive (EU) 2019/790	Anti-money laundering Regulation (AML) (EU) 2024/1624
	European Chips Act (Regulation) (EU) 2023/1781	Roaming Regulation (EU) 2022/612	Data Governance Act (Regulation) (EU) 2022/868		Information Security Regulation 2022/0084(COD)	Digitalisation of cross-border judicial cooperation (EU) 2023/2844	Machinery Regulation (EU) 2023/1230	Consumer Protection Cooperation Regulation (EU) 2017/2394	Single Market Programme (EU) 2021/690	European Media Freedom Act (EU) 2024/1083	Financial Data Access Regulation 2023/0205(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP) (EU) 2024/795	Union Secure Connectivity Programme (EU) 2023/588	Data Act (Regulation) (EU) 2023/2854		Digital package	Directive on combating violence against women (EU) 2024/1385	AI Act (Regulation) (EU) 2024/1689	Geo-Blocking Regulation (EU) 2018/302	Vertical Block Exemption Regulation (VBER) (EU) 2022/720		Payment Services Regulation 2023/0210(COD)
	European Critical Raw Materials Act (Regulation) (EU) 2024/1252	Gigabit Infrastructure Act (EU) 2024/1309	Interoperable Europe Act (EU) 2024/903			Directive for combating sexual abuse and child sexual abuse material 2024/0035(COD)	Eco-design Regulation (EU) 2024/1781	Digital content Directive (EU) 2019/770	Digital Market Act (DMA Regulation) (EU) 2022/1925		Digital Euro 2023/0212(COD)
	Net Zero Industry Act (EU) 2024/1735	Digital Networks Act	Regulation on data collection for short-term rental (EU) 2024/1028			EU Digital Travel application, 2024/0670(COD)	Product Liability Directive (PLD) (EU) 2024/2853	Digital Contracts for Goods Directive (EU) 2019/771	Regulation on distortive foreign subsidies (EU) 2022/2560		Regulation on combating late payment 2023/0323(COD)
	EU Space Act	EU Cloud and AI Development Act	European Health Data Space (Regulation) (EU) 2025/327					Digital Services Act (DSA Regulation) (EU) 2022/2065	Horizontal Block Exemption Regulations (HBER) (EU) 2023/1066, (EU) 2023/1067		
	Quantum Act		Harmonization of GDPR enforcement procedures 2023/0202(COD)					Political Advertising Regulation (EU) 2024/900	Internal Market Emergency and Resilience Act (EU) 2024/2747		

Quelle: Zenner, K., Marcus, J.S., and Sekut, K. (2025), "A dataset of international legal and policy instruments for the digital world", CEPS.



”

Technik ist nicht neutral – und Ethik ist keine Meinungsfrage, sondern die disziplinierte Praxis begründeten Urteilens unter Unsicherheit.

WAS IST IHR BLICK AUF DIESE AUSSAGE? STIMMEN SIE DEM ZU?

DIGITALE VERANTWORTUNG

Wortwolke: Schlagworte der aktuellen Debatte

Anthropomorphisierung
Token
Habsburger KI
„Hat Schreiben, hat Denken eine Zukunft?“
Echokammer
Kognitives Auslagern
Bossware
Cyborg
Prompts
Einsamkeitsepidemie
Überwachungskapitalismus
Technostress
Desinformation
Digitale Souveränität
Dequalifizierung
Rote Pille, blaue Pille
Deepfake
KI-Kompetenz
Bias
Transhumanismus
Identitätsverlust
AGI / Super-KI
Diskriminierung
Effizienz vs. Eigenleistung
Digitale Kolonie
Technofaschismus
KI-Avatar
Social Engineering 2.0
Posthumanismus
KI-Schrott
Falschmeldungen
Kennzeichnung
„Cybercrime ist okay“
Von woke zu vibe
Auflösung der Grenze zwischen Mensch und Maschine
Mensch-Maschine-Interaktion
Brainrot
„Nicht gut, nicht schlecht, aber auch nicht werteneutral“
Menschliche Selbstoptimierung
Sozial-emotionale Hilfe vs. Selbstbestimmung

WERTE UND ETHISCHE ANSÄTZE

Es gibt nicht „die“ eine ethische Beurteilung

Was sind Werte?

Werte sind **Vorstellungen, Ideen oder Ideale**. Sie bezeichnen, was wünschenswert ist: bewusste oder unbewusste Orientierungsstandards und Leitvorstellungen.

Als ethisches Phänomen bezeichnet ein Wert:

- ein Gut
- einen Maßstab für das Gute
- ein Kriterium für Ziele und Zwecke, die wir anstreben sollten
- einen normativen Standard zur Beurteilung von Phänomenen

Ethische Ansätze

Je nach Perspektive setzen sie andere Schwerpunkte der ethischen Reflexion:

1

Konsequenzialismus / Utilitarismus

Lenkt den Blick auf den ethischen Nutzen und die Folgen von KI-Technologien.

2

Deontologische Perspektive

Griech. deon „Pflicht“: verweist auf moralische Prinzipien, etwa Verantwortung, und auf die Notwendigkeit, Werte abzuwägen.

3

Tugendethische / eudämonistische Perspektive

Griech. eudaimonía „Glück“: fragt, wie mit KI-Technologien ein gutes Leben gelingen kann.

ETHIK IST DAS NAVIGATIONSSYSTEM IN DEN GRAUZONEN

01

Werte

Was ist uns wichtig?
Code of Conduct
Rote Linien

→

02

Moral

Was gilt als richtig oder falsch?
Was könnten wir zwar rechtmäßig, aber moralisch nicht?

→

03

Ethik

Wie begründen wir unser Urteil?
Warum sollten wir danach handeln?

→

04

Verantwortung

Welche Handlung folgt daraus?
“gut sein, auch wenn niemand hinsieht”

Digitale Ethik fragt: Wie wollen wir in einer digitalisierten Welt handeln – und was ändern wir konkret?

COLLINGRIDGE-DILEMMA

FRÜH

Wirkung noch unsicher

Gestaltungsspielraum groß

Noch ist die Richtung formbar – aber die Folgen sind schwer vorherzusagen.

SPÄT

Folgen sichtbar

Korrektur wird teuer

Technologie und Gewohnheiten sind bereits eingebettet – der Kurswechsel wird schwieriger.

CDR-Frage: Welche Leitplanke müssen wir einbauen, solange wir noch gestalten können?

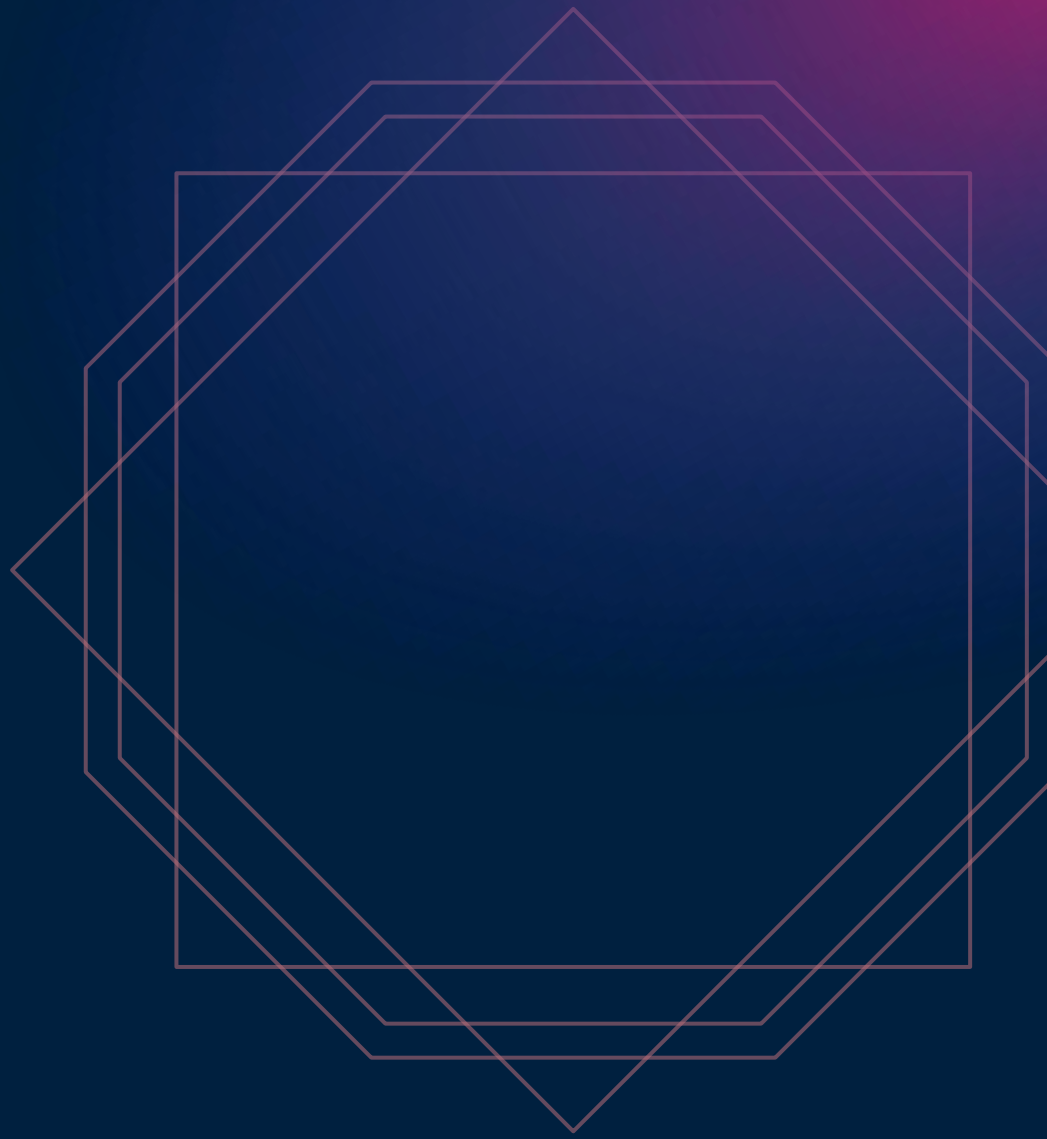


ZEIT / VERBREITUNG

02

CORPORATE DIGITAL RESPONSIBILITY

Begriff, Rahmen, Abgrenzung



WAS IST CORPORATE DIGITAL RESPONSIBILITY?

Definition der Initiative D21 (2025)

„Ganzheitliches verantwortungsbewusstes Handeln von Unternehmen in Bezug auf die Auswirkungen digitaler Technologien und Daten.“

- Einhaltung der für die Digitalisierung relevanten Gesetze und Normen
  - plus freiwillige Selbstverpflichtung darüber hinaus
- **Vom Sollen zum Machen:** CDR schafft Prozesse, Rollen und Frameworks
- Ziel: Digital Trust – die Währung der Digitalwirtschaft

CDR ERGÄNZT CSR – UND GEHT ÜBER COMPLIANCE HINAUS

COMPLIANCE	CSR	CDR
Was müssen wir von Gestzes wegen einhalten?	**Wie wirkt unser Unternehmen auf Gesellschaft und Umwelt?**	**Wie handeln wir verantwortlich im Digitalen?**
Rechtliche Mindestanforderungen, Rollen und Kontrollen.	Unternehmensverantwortung über verschiedene Wirkungsfelder hinweg.	Daten, Algorithmen, digitale Produkte und digitale Geschäftsmodelle.

Keine Entweder-oder-Entscheidung: CDR macht digitale Verantwortung im bestehenden Management konkret.

CDR IST UMFASSENDER ALS KI-ETHIK

01 **Daten**

Zweck, Fairness, Kontrolle

02 **KI**

Bias, Aufsicht, Erklärbarkeit

03 **Plattformen**

Macht, Sichtbarkeit, Zugang

04 **IoT & Räume**

Sicherheit, Vernetzung, Autonomie

05 **Inklusion, Arbeitswelt**

Barrierefreiheit, Teilhabe, Skills

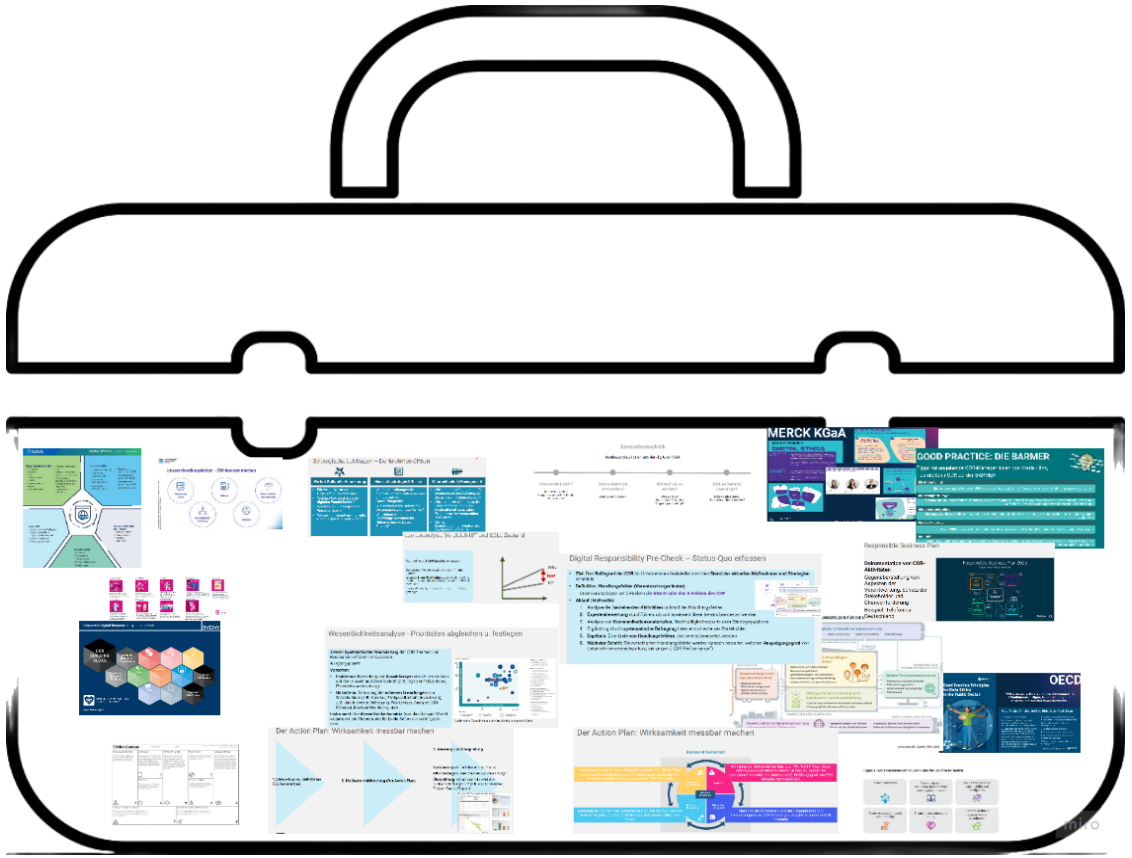
06 **Green Digital**

Energie, Ressourcen, Lebenszyklus

CDR NETZWERK UND FRAMEWORKS

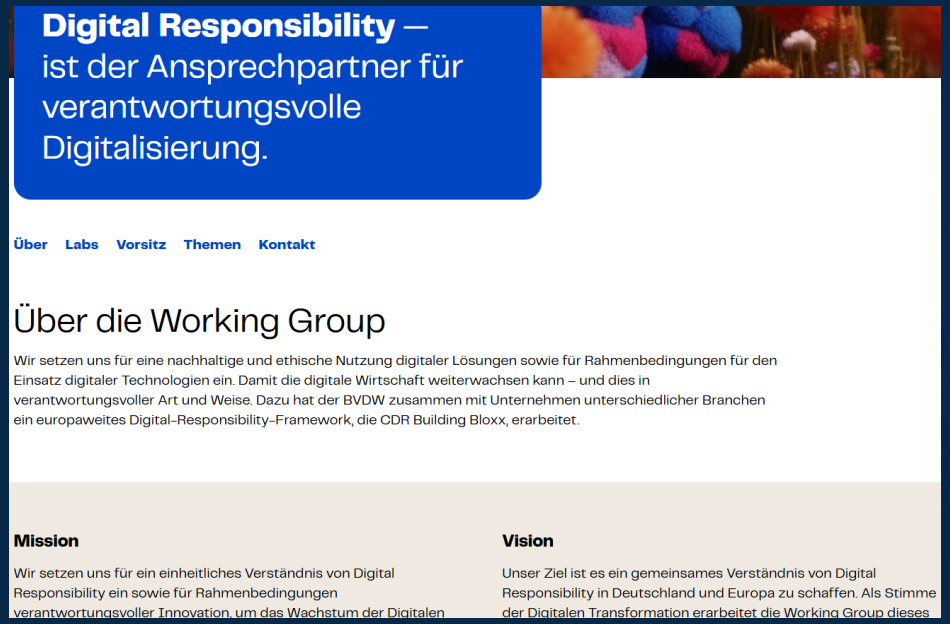
Akteure und die CDR-Toolbox

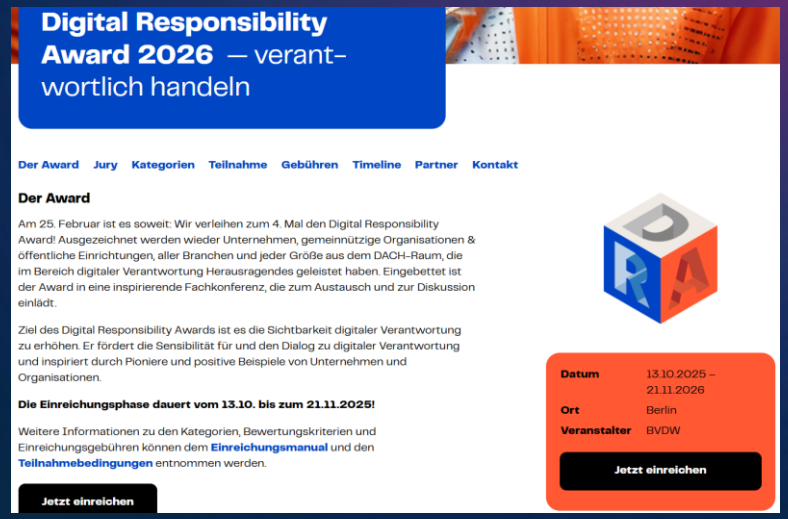




BVDW

Fördert die Selbstregulierung durch praktische Leitfäden wie die "Building Bloxx" und zeichnet Best Practices mit dem Corporate Digital Responsibility Preis aus

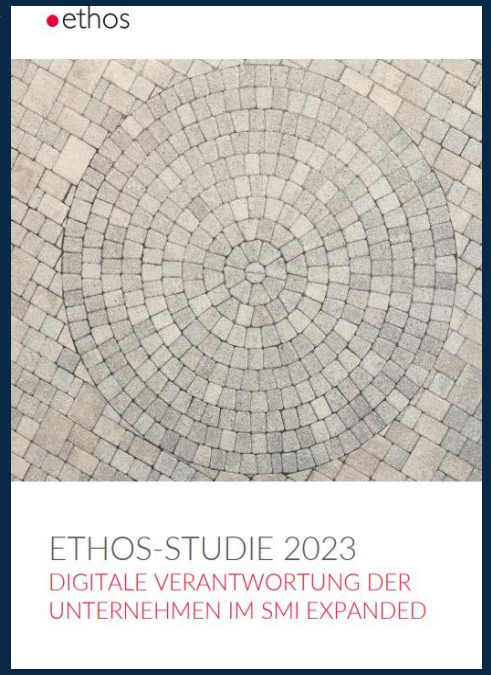








ETHOS STUDIE



DIE 7 GRUNDSÄTZE VON ETHOS IN BEZUG AUF DIGITALE VERANTWORTUNG

Digitale Governance
Einen Kodex für digitale Verantwortung einführen

Digitale Transparenz
Die Transparenz gegenüber den Anspruchsgruppen bezüglich der digitalen Praktiken und des digitalen Fussabdrucks sicherstellen

Datenschutz
Die höchsten Standards bei der Datenverarbeitung und beim Datenschutz einhalten

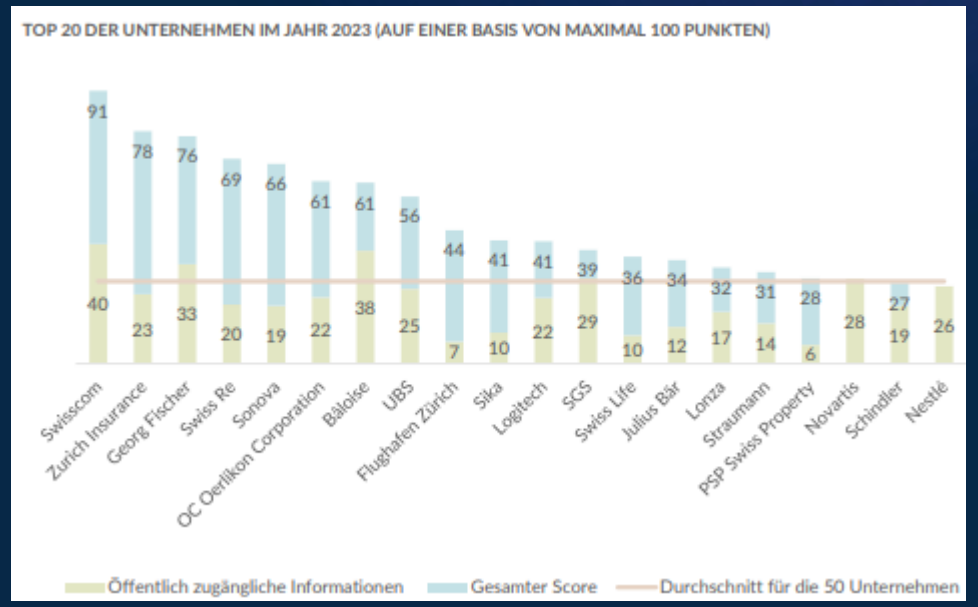
Künstliche Intelligenz
Ethische Grundsätze für die Nutzung von künstlicher Intelligenz (KI) einführen

Sensible Aktivitäten
Sensible Aktivitäten im Zusammenhang mit der Digitalisierung ausschliessen

Soziale Auswirkungen
Einen gerechten und verantwortungsvollen sozialen Übergang sicherstellen

Ökologische Auswirkungen
Zur Verringerung des ökologischen Fussabdrucks der digitalen Technologie beitragen

Führt das CDR-Benchmarking für Schweizer Unternehmen durch und bewertet die Performance aus Investorenperspektive, wodurch Messbarkeit und Wettbewerb gefördert werden

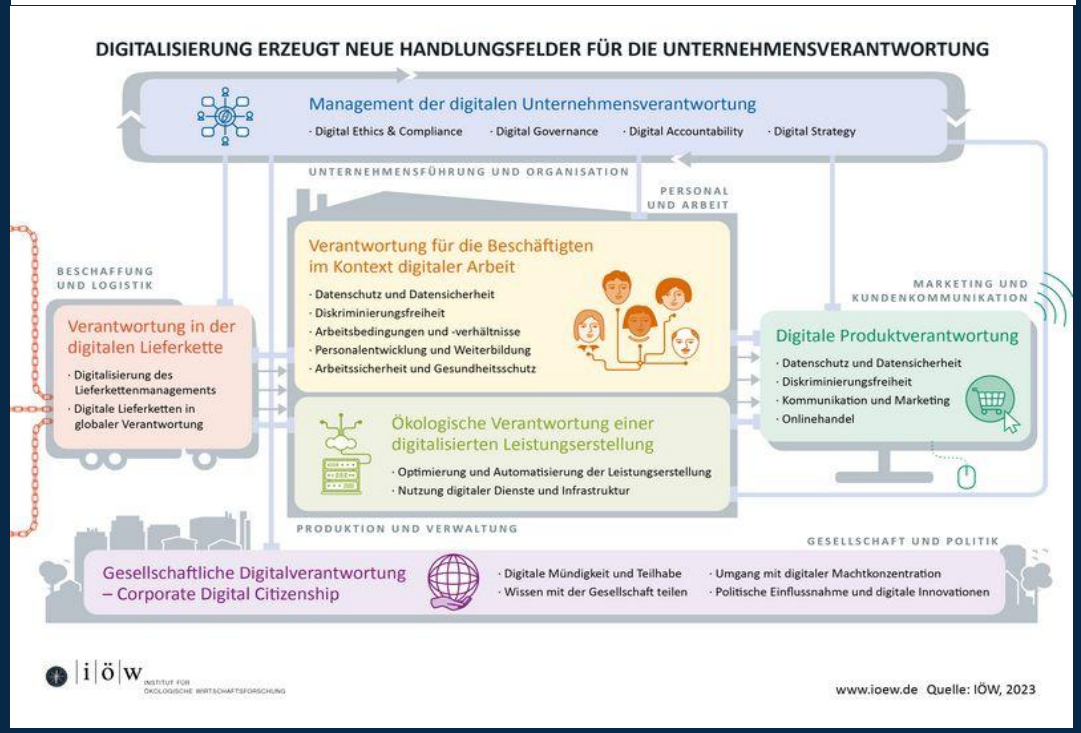


Christian Lautermann, Vivian Frick

Corporate Digital Responsibility

Wie Unternehmen im digitalen Wandel Verantwortung übernehmen

Schriftenreihe des IÖW 227/23



IÖW

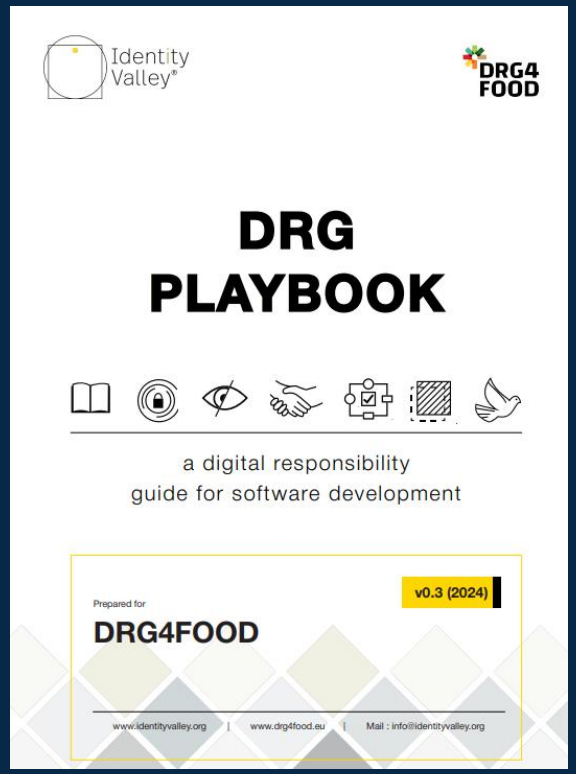
Ganzheitliche Systematik der CDR, indem sechs zentrale Handlungsfelder identifiziert wurden und diese in alle etablierten Verantwortungsbereiche des Unternehmens integriert werden

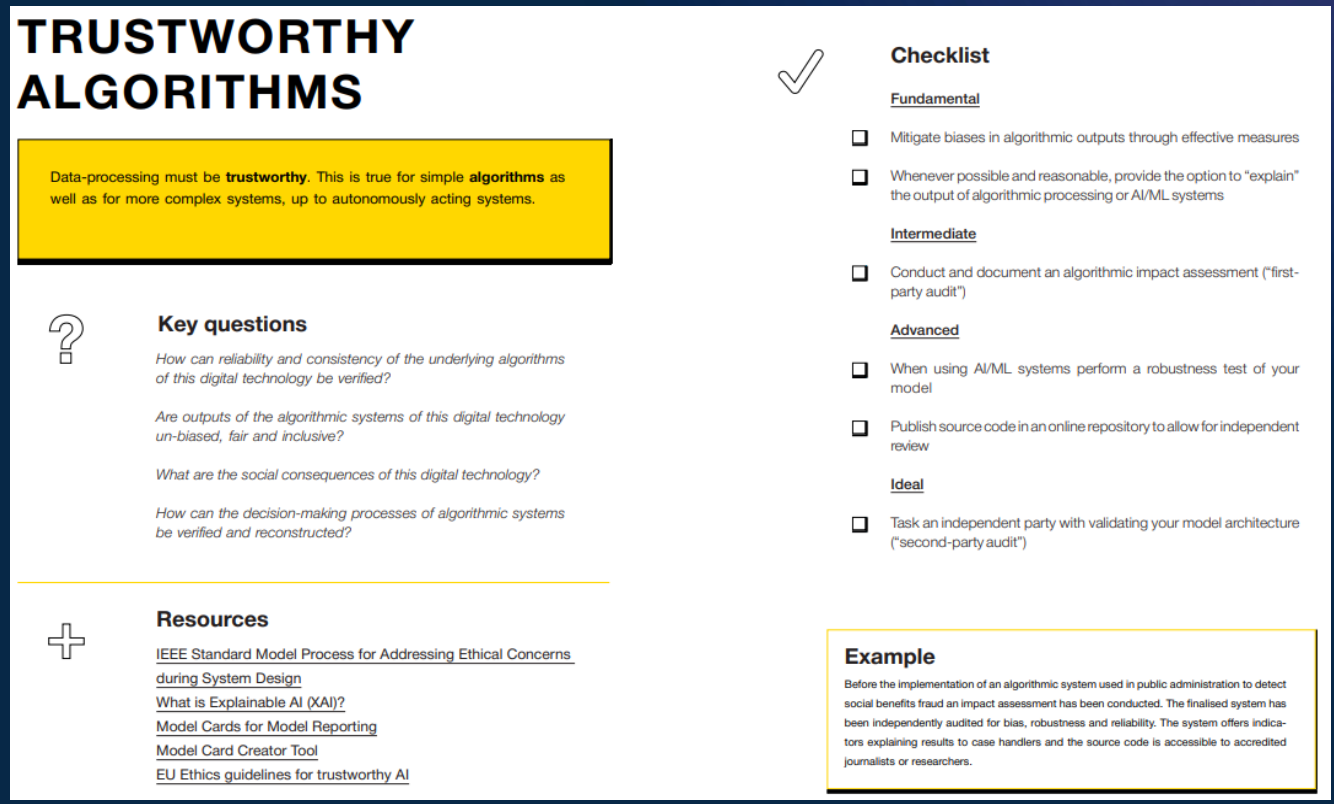
IDENTITY VALLEY

Bietet mit dem DRG (Digital Responsibility Goals) Playbook einen zielorientierten Leitfaden zur praktischen Implementierung und Bewertung von CDR-Maßnahmen



Co-funded by the European Union





TRUSTWORTHY ALGORITHMS

Data-processing must be **trustworthy**. This is true for simple **algorithms** as well as for more complex systems, up to autonomously acting systems.

Key questions

How can reliability and consistency of the underlying algorithms of this digital technology be verified?

Are outputs of the algorithmic systems of this digital technology un-biased, fair and inclusive?

What are the social consequences of this digital technology?

How can the decision-making processes of algorithmic systems be verified and reconstructed?

Resources

IEEE Standard Model Process for Addressing Ethical Concerns during System Design
What is Explainable AI (XAI)?
Model Cards for Model Reporting
Model Card Creator Tool
EU Ethics guidelines for trustworthy AI

Checklist

Fundamental

- ☐ Mitigate biases in algorithmic outputs through effective measures
- ☐ Whenever possible and reasonable, provide the option to "explain" the output of algorithmic processing or AI/ML systems

Intermediate

- ☐ Conduct and document an algorithmic impact assessment ("first-party audit")

Advanced

- ☐ When using AI/ML systems perform a robustness test of your model
- ☐ Publish source code in an online repository to allow for independent review

Ideal

- ☐ Task an independent party with validating your model architecture ("second-party audit")

Example

Before the implementation of an algorithmic system used in public administration to detect social benefits fraud an impact assessment has been conducted. The finalised system has been independently audited for bias, robustness and reliability. The system offers indicators explaining results to case handlers and the source code is accessible to accredited journalists or researchers.

03

VON DER ETHIK ZUR GOVERNANCE

Prinzipien prüfbar machen

FRAMEWORKS UND STANDARDS

Orientierung statt Neuerfindung

Framework	Fokus	Nutzen
CDR-Kodex (BMUV)	Freiwillige Selbstverpflichtung entlang von Handlungsfeldern	Orientierung und Reporting
EU-Ethikleitlinien für vertrauenswürdige KI	Rechtmäßig, ethisch, robust	Strukturierte Selbstbewertung
IÖW-Systematik	Sechs Handlungsfelder der CDR	Ganzheitlicher Überblick
ISACA Digital Trust Ecosystem Framework	Vertrauen als strategischer Vorteil	Vertrauensreife bewerten
ISO/IEC/IEEE 24748-7000	Value-based Engineering	Werte im Systemdesign verankern
DIN (in Arbeit)	CDR als Managementsystemstandard	Prüfbarkeit

MERCK KGaA

SUSTAINABILITY / BUSINESS ETHICS /

DIGITAL ETHICS

WHY DIGITAL ETHICS MATTER

We increasingly use and develop new digital and data-driven technologies, such as artificial intelligence and machine learning. The collection and processing of data by algorithmic systems affects how every single one of us lives and works. In its wake: a whole new set of ethical questions. Regulatory frameworks are expected to be developed in the future. At the moment, however, legislation in this critical area is limited. Digital ethics is still a young field.

At our company, we want to take a pioneering role. We believe that digital technologies require reliable ethical standards and that these standards should guide our daily business in the digital age. That's why we have created a dedicated Digital Ethics Group, our Digital Ethics Advisory Panel and our Code of Digital Ethics.

DIGITAL ETHICS AT OUR COMPANY

In anticipation of the ethical challenges of digitalization, our company has issued
mandate. This mandate is driven by our values and long-established bioethical a
consistently enabled us to develop breakthrough innovations based on sound eth
Since 2020, we have embedded a dedicated digital ethics group within our organ

This group enables our sectors and businesses to operate from a solid ethical po
of the Digital Ethics Advisory Panel (DEAP) and the CoDE, we thus enable respon
digital business models.

our industry leading approach

We deploy a first of its kind framework for Digital Ethics questions

1. Merck Digital Ethics Advisory Panel (DEAP)

- **Independent** advisory panel
- Provides guidance around evolving digital business models and **addresses digital ethics questions** for all three business sectors of Merck
- **Renowned academic and industry experts** in digital ethics, legal and regulatory, big data technology, digital health, etc. from the US and Europe

2. Code of Digital Ethics (CoDE)

- Scientifically sound, principle-based **framework**
  - Enables us to **assess digital products and business models** regarding ethical aspects of data use and algorithms
    - Serves as a **moral compass** to enable responsible decision-making across all matters related to data and digital

THE PANEL MEMBERS ACT AS ADVISORS, PROVIDE ASSESSMENT AND INDEPENDENT GUIDANCE ON COMPLEX ETHICAL QUESTIONS IN THE AREAS OF DATA AND ARTIFICIAL INTELLIGENCE.



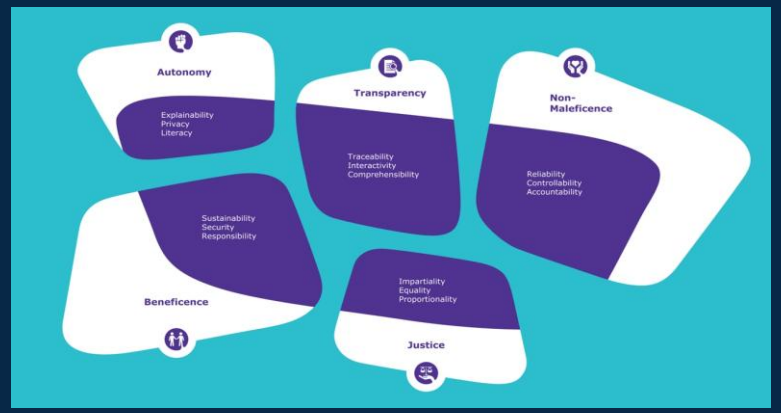
prof. Effy Vayena
ETH Zürich



Esther Bleicher
Hello Heart
Former FDA official



Dr. George Demetri
Dana-Farber Cancer Institute



How we are operationalizing Digital Ethics

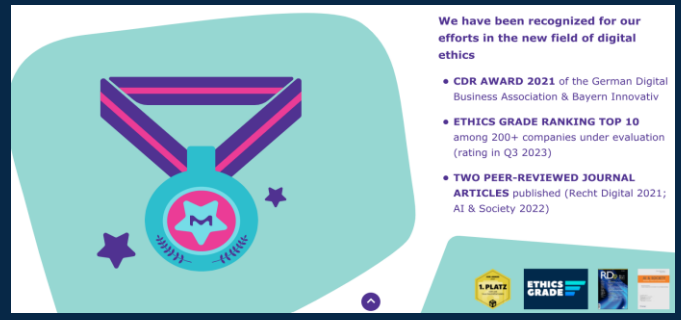
Use case: The Principle-at-Risk-Assessment ("PaRA")

We created a **governance structure and process** to handle questions regarding Digital Ethics:



About the PaRA:

- Helps the Digital Ethics Office **analyze the problem statement**
- Determines **which principles of the CoDE are affected** and at risk for the given problem statement
- Generates a report to **document the ethical assessment process**
- Serves as **guidance** for discussion with DEAP



BEST PRACTICE: MERCK

Code of Digital Ethics – Ethik im Workflow jedes Teams

CoDE

- 5 Kernprinzipien, 20 Leitlinien
- abgeleitet aus 42 Ethik-Dokumenten

PaRA

- Stufe 1: Ist ein Prinzip betroffen?
- Stufe 2: Ist es gefährdet?

MDEC und DEAP

- Halbautomatisches Risiko-Scoring in der Projektplattform
- Digital Ethics Advisory Panel entscheidet

DIGITAL ETHICS CHALLENGE

Principle-at-Risk Analysis (PaRA)

Guideline: Privacy

"We protect the privacy of those who provide data."

We respect and protect the privacy of individuals, both during the collection of data and during interaction with our digital offerings. We therefore ensure that individuals can make sovereign decisions about the use of their data.

Basic Questions for Privacy

	yes	no
Does the problem statement address those who provide data?		
Does the problem statement address the collection of data?		
Does the problem statement address the interaction with digital offerings?		
Principle affected		

The first step of the analysis asks basic questions to find out if a principle is affected, based on the guideline corresponding to the principle

Detailed definition of Privacy

In the context of digital solutions, privacy refers to information about, for example, an individual's family, friends, health and financial circumstances.

Respect for privacy means that each user is able to determine what information is shared with others. This concerns information originally provided by the user as well as information generated about the user in the course of his/her interaction with digital solutions. Otherwise, there is a risk, for example, that users may feel that their privacy is being invaded.

Organisations committed to the principle of privacy respect and guarantee privacy at every stage of the data chain: whether at the beginning when determining the type of processing or at the time of processing within the data chain. This is where measures such as anonymization of personal data, the use of synthetic data or software dashboards to control privacy settings by users come into play.

Since the promotion of the sub-principle of privacy recognises the self-determination of the user, it contributes to preserving the core value of autonomy.

Detail Questions for Privacy

Does the problem statement affect…	yes	no	Explanation (only for "yes") The problem statement affects…
…personalized information about, for example, an individual's family, friends, health or financial circumstances?			
…information originally provided by the user?			
…information generated about the user during his interaction with digital solutions?			
…the need for the protection of personalized user data at any stage of the data chain?			
Principle at risk			

Quelle: https://link.springer.com/article/10.1007/s11023-023-09654-w/figures/1

DER BUSINESS CASE

+3,17 €

pro Monat würden Konsument:innen zusätzlich für verantwortungsvollen Umgang mit ihren Daten zahlen.

CARL ET AL., GOETHE-UNIVERSITÄT FRANKFURT

ROI DER VERANTWORTUNG

- Vertrauen als Differenzierung – Blue Ocean
- Resilienz gegen Ausfälle und Angriffe
- Attraktiv für Talente

KOSTEN DER UNTÄTIGKEIT

- Strafen und Haftung
- Reputationsschaden
- Teurer Umbau statt CDR by Design

WAS DIE FORSCHUNG BELEGT

Zahlungsbereitschaft, Vertrauen und Bindung

3,17–6,52 €

pro Monat latente Zahlungsbereitschaft für ein Bündel freiwilliger Datenschutzmaßnahmen – in drei von vier Kundensegmenten

Carl et al. (2024), Choice-Experiment, Deutschland, n = 663

r = 0,79

Korrelation zwischen Vertrauen und Weiterempfehlung (NPS) bei Schweizer Finanzdienstleistern

Yarza Navarro-Schär et al. (2025), PLOS ONE, Schweiz, n = 1.370

30,5 %

Gewicht von Zugriff und Korrektur eigener Daten in der Kaufentscheidung – gleichauf mit dem Preis (30,2 %)

Carl et al. (2024), relative Wichtigkeit der Attribute



Wirkungskette: Transparenz und Kontrolle im Datenumgang dämpfen Datenrisiken, Vertrauen vermittelt den Effekt auf Kundenverhalten – Martin, Borah und Palmatier (2017), Journal of Marketing

CDR ALS BLUE OCEAN

Beispiel Swisscom: Jugendschutz wird vom Wertethema zum neuen Markt

Blauer Ozean

Jugendmedienschutz als neue Leistung
Beratung und Angebote für Familien
Zielgruppe Eltern statt nur Nutzer:innen
Differenzierung über Verantwortung

Roter Ozean

- Wettbewerb über Preis pro Gigabyte
- Netzabdeckung und Geschwindigkeit
- Gleiche Zielgruppe, gleiche Tarife
- Marge schrumpft mit jedem Anbieter

01
Jugendschutz-beauftragte:r
CDR-Rolle mit Mandat

→ **02**
Neue Zielgruppe Eltern
Bedürfnis: Sicherheit der Kinder

→ **03**
Neue Tarife und Produkte
Familienangebote, Schutzfunktionen

→ **04**
Markt ohne Wettbewerb
Vertrauen statt Preiskampf

Quelle: Blue-Ocean-Logik nach Kim und Mauborgne (2005); Beispiel Swisscom aus der Praxis des Vortragenden

Swisscom

Die Kampagne #MUTE THE HATE ist eine Sensibilisierungskampagne für respektvolles Verhalten im Netz.

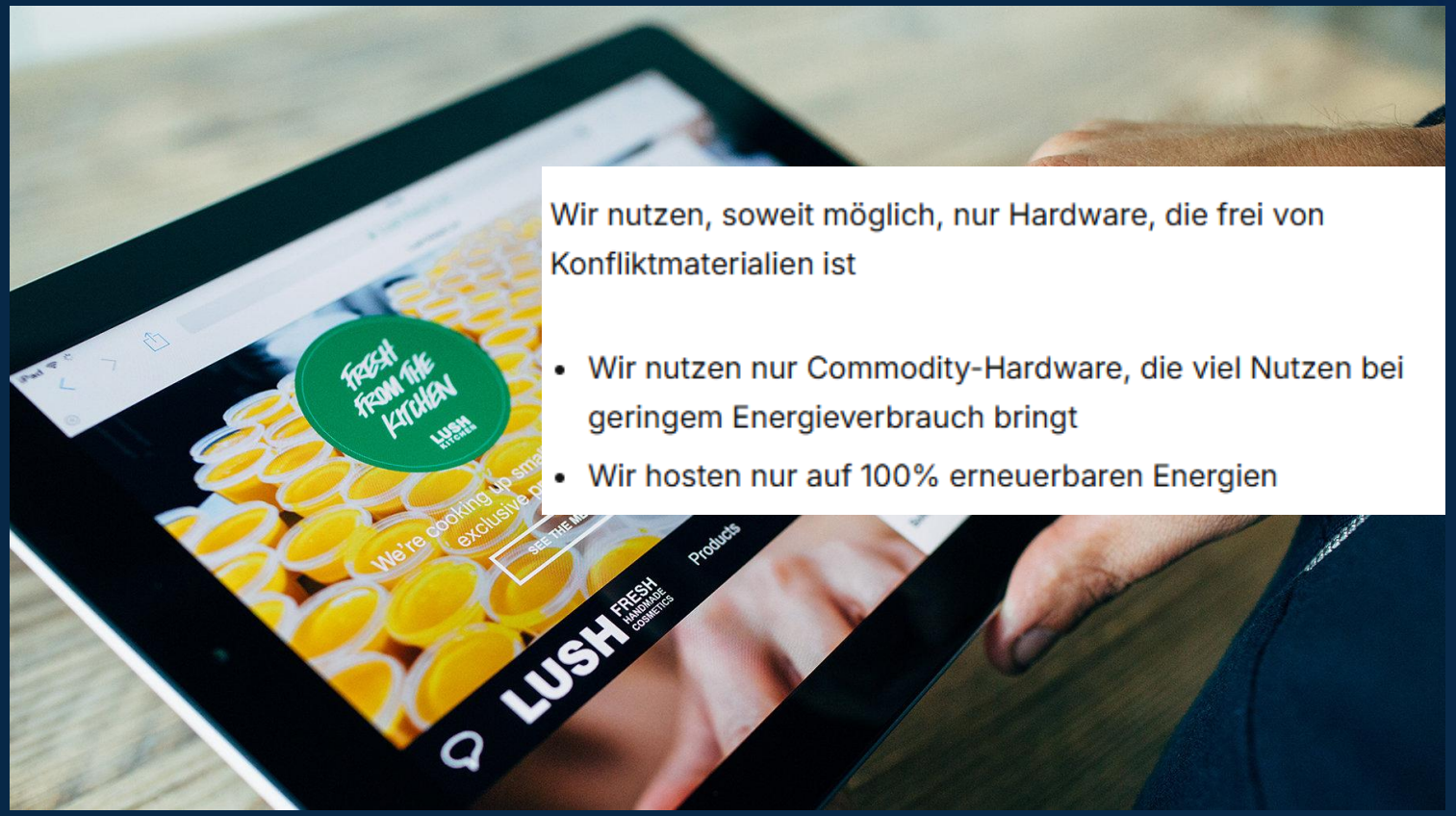
Ziel: nachhaltige Wirkung (Wissen und Verhalten) auf die Mediennutzung der Menschen.





Quelle: https://www.swisscom.ch/de/about/nachhaltigkeit/swisscom-campus/ratgeber-hate-speech.html#acc-3w534g%5Bselected%5D%5B%5D=0

LUSH



> **Zu sagen, dass du dich um Datenschutz nicht scherst, weil du ja nichts zu verbergen hast, ist so egoistisch wie zu sagen, dass du dich nicht um hungernde Menschen kümmerst, weil du ja satt bist.**
>
> — BORIS VAN ZANTEN (CEO @ TNW)

Quelle: https://weare.lush.com/at/lush-life/unsere-werte/digitale-ethik/

LUSH

“

As an inventor of bath bombs, I pour all my efforts into creating products that help people switch off, relax and pay attention to their wellbeing. Social media platforms have become the antithesis of this aim, with algorithms designed to keep people scrolling and stop them from switching off and relaxing.

JACK CONSTANTINE, CDO & PRODUCT INVENTOR

“

I’ve spent all my life avoiding putting harmful ingredients in my products. There is now overwhelming evidence we are being put at risk when using social media. I’m not willing to expose my customers to this harm, so it’s time to take it out of the mix

MARK CONSTANTINE OBE, CO-FOUNDER, CEO & PRODUCT INVENTOR



04

FALLBEISPIELE UND DISKUSSION

Ethische Risiken erkennen

ETHISCHE LEITBILDER DER PAYPAL MAFIA

Vom Zahlungsdienst zum Machtzentrum des Silicon Valley

PayPal entstand 1998 bis 2000 aus Confinity (Thiel, Levchin) und X.com (Musk). 2002 kaufte eBay das Unternehmen um 1,5 Mrd. USD.

Den Begriff prägte das Magazin Fortune 2007 mit einem Gruppenfoto im Stil einer Mafia-Familie. Die frühen Mitarbeiter:innen gründeten oder finanzierten danach einen Großteil der heutigen Tech-Giganten.

Das Originalfoto ist urheberrechtlich geschützt (Fortune, 2007) – daher hier nur zur Erklärung abgebildet.

Person	Danach
Peter Thiel	Palantir, Founders Fund, Clarium
Elon Musk	Tesla, SpaceX, X, xAI
Max Levchin	Slide, Affirm
Reid Hoffman	LinkedIn, Greylock, Inflection AI
David Sacks	Yammer, Craft Ventures, AI- und Krypto-Beauftragter des Weißen Hauses
Keith Rabois	Square, Opendoor, Khosla Ventures
Roelof Botha	Sequoia Capital
Chen, Hurley, Karim	YouTube
Jeremy Stoppelman	Yelp

PLOT TWIST

10,25 %

weniger Geld bekam die weiblich präsentierende KI-Agentin „Johanna“ als ihr männliches Pendant „Jonah“ – bei identischer Technologie und Leistung.

WAS DAS ZEIGT

- Bias reist mit – von Menschen in Maschinen und zurück
- Agentische KI verhandelt, kauft und bezahlt bereits
- Fairness ist eine Designentscheidung, kein Zufall

Quelle: Forbes, 05.10.2026

WELTVORSTELLUNGEN UND WERTE

Wer sind die Personen hinter den Unternehmen?

“

Competition is for losers.

PETER THIEL, WALL STREET JOURNAL, 12.09.2014

Mitgründer PayPal und Palantir, Founders Fund – Monopol statt Wettbewerb

“

The fundamental weakness of Western civilization is empathy.

ELON MUSK, JOE ROGAN EXPERIENCE, 28.02.2025

Mitgründer X.com/PayPal, CEO Tesla und SpaceX – Empathie als Schwäche

WELTVORSTELLUNGEN UND WERTE

Aussagen, die polarisieren

“

They „trust me“ . Dumb f*s.**

MARK ZUCKERBERG, CHAT-NACHRICHT, 2004

Gründer Facebook/Meta, über die ersten Nutzer:innen – 2010 von ihm bestätigt

“

It also takes a lot of energy to train a human. It takes like 20 years of life and all of the food you eat during that time before you get smart.

SAM ALTMAN, THE INDIAN EXPRESS, 02/2026

CEO OpenAI, auf Kritik am Energieverbrauch von KI

WELTVORSTELLUNGEN UND WERTE

Aussagen, die polarisieren

“

If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.

ERIC SCHMIDT, CNBC, 12/2009

CEO Google 2001–2011, auf die Frage nach Privatsphäre bei Google

“

I’m relatively an optimist, so I think there’s a 25% chance that things go really, really badly.

DARIO AMODEI, AXIOS AI+ DC SUMMIT, 09/2025

CEO Anthropic, auf die Frage, wie wahrscheinlich eine KI-Katastrophe ist

DIE NEUE PAYPAL MAFIA

Zehn Praktikant:innen, ein Netzwerk

Winter 2015/16: Der Quant-Händler Hudson River Trading (HRT) nimmt erstmals zehn Praktikant:innen auf. Mindestens vier gründen später Unternehmen im Milliardenwert.

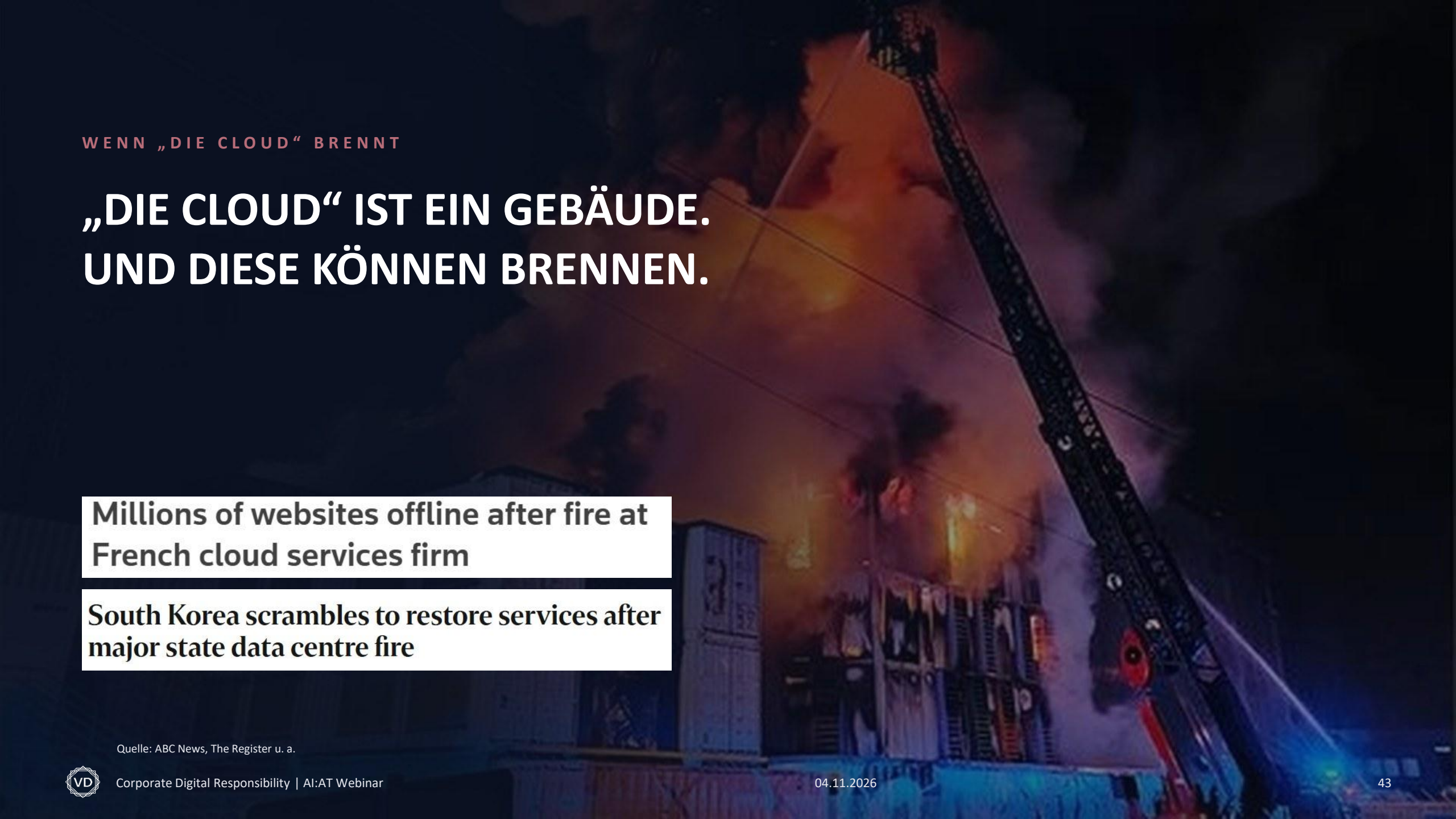
Kennengelernt hatten sich viele schon zuvor bei Informatik- und Physikolympiaden. Gemeinsamer Nenner: Harvard oder MIT, Medaillen, überwiegend asiatisch-amerikanische Herkunft – und ein Wettbewerbsmodus, der in die Produkte eingeht.

Der 19-jährige Alexandr Wang fragte im Freundeskreis, warum die nächste PayPal Mafia nicht sie selbst sein könnten (Colossus, April 2026).

Person	Unternehmen	Weg
Alexandr Wang	Scale AI (Datenlabeling); seit 2025 Leiter der KI-Sparte bei Meta	MIT, abgebrochen
Scott Wu	Cognition – KI-Programmieragent „Devin“	Harvard, abgebrochen; 3 × IOI-Gold
Steven Hao	Cognition, CTO; zuvor Scale AI	Forbes 400 (2026), jüngstes Mitglied
Jesse Zhang	Decagon – KI-Agenten für Kundenservice	Harvard
Johnny Ho	Perplexity – KI-Suche, Mitgründer und CSO	Harvard; 3 × IOI-Gold
Demi Guo	Pika – KI-Videogenerierung	Harvard; Stanford-PhD abgebrochen
Jeff Yan	Hyperliquid – dezentrale Krypto-Börse, Singapur	Harvard; HRT

Quelle: Colossus, „Beyond the Sky“, April 2026; Odaily/KuCoin News, April 2026; TechFlow, Oktober 2026 (Forbes-400-Angabe).

„DIE CLOUD“ IST EIN GEBÄUDE. UND DIESE KÖNNEN BRENNEN.



Millions of websites offline after fire at French cloud services firm

South Korea scrambles to restore services after major state data centre fire

Quelle: ABC News, The Register u. a.

GREEN IT

DER UNSICHTBARE FUßABDRUCK

- Rechenzentren und KI-Training brauchen Strom, Wasser und Fläche
- Tech-Konzerne planen eigene Atomkraftwerke
- Daten und Rechenleistung bewusst einsetzen

Tech-Riesen bauen Atomkraftwerke: So viel Energie braucht KI

Der Stromverbrauch von künstlicher Intelligenz explodiert. Die US-Techriesen bauen sogar Atomkraftwerke, um den wachsenden Energiehunger ihrer KI-Systeme zu stillen. Der neuen Trump-Regierung passt das gut ins Konzept.



A NEW BREED OF DOMINANCE

Gründung: Okt. 2026 von Palmer Luckey (Anduril) und Ben Lamm (Colossal Biosciences), 200 Mio. USD Seed-Kapital, Sitz Texas

Konzept: Die besten US-Diensthunde werden geklont und genetisch optimiert, ausgerüstet mit Andurils kybernetischen „Augments“ und KI-Sicht. Auch sollen ausgestorbene „Schattenwölfe“ als Hybrid-Grauwölfe nachgezüchtet worden sein, die den Wölfen aus Game of Thrones nachgeahmt werden sollen in Größe und Charakter.

Ziel: Unabhängigkeit von Europa, das heute über 80 % der US-Militärhunde liefert

Kritik: Tierwohl und Grenzen militärischer Technologie

Mehr: warhound.com



Quelle: Warhound, warhound.com (Launch 23.10.2026, abgerufen am 03.11.2026)

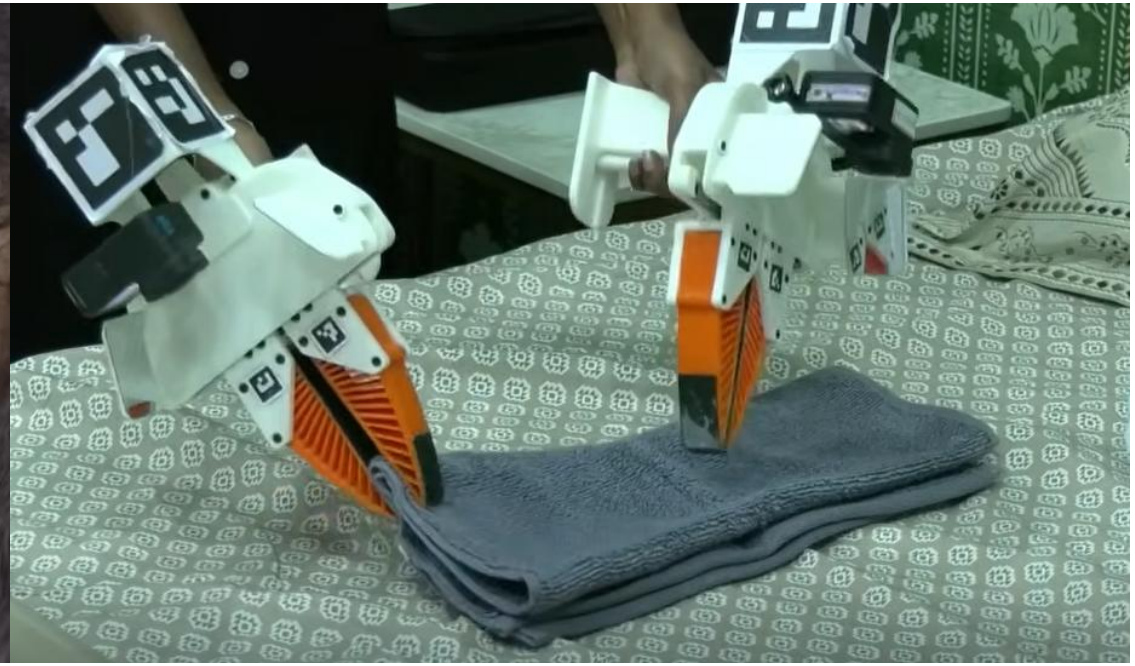
„NUR“ AKADEMISCHE BERUFE IN GEFAHR?

Replacing Workers?





Training of AI Robots



DEAD INTERNET THEORY

POSTEN AUS DEM JENSEITS

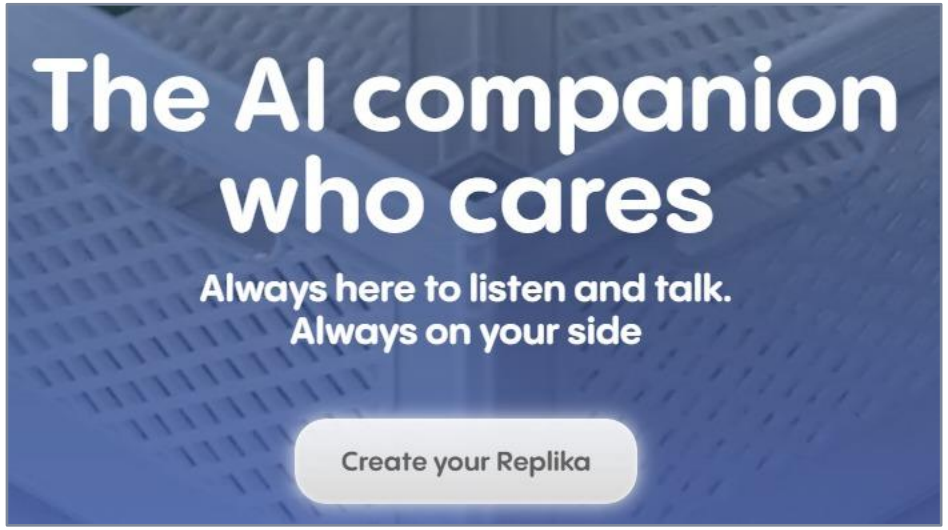
„Das Sprachmodell kann den Nutzer simulieren, wenn er abwesend ist – etwa bei einer langen Pause oder wenn er verstorben ist.“

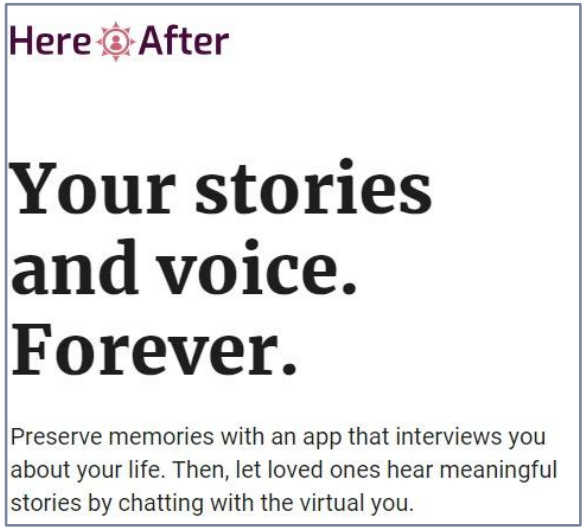
Aus einem Meta-Patent, 2025

Quelle: Meta-Patent 2025

DIGITAL UNSTERBLICH







Kontakt zum Verstorbenen als KI Avatar – Trauerbewältigung oder monatliches Abo, um den letzten Kontakt zum geliebten Menschen nicht zu Verlieren?

ZUM ABSCHLUSS

Sinnieren, Philosophieren, Impulse setzen

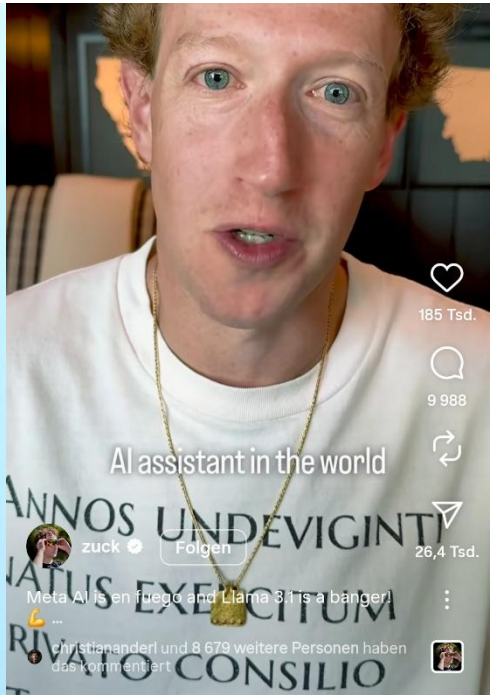
- Fragen, die sich Philosophinnen stellen:
  - Soll eine KI unsterblich sein? Oder müssen wir dafür sorgen, dass sie sterben kann?
  - Posthumanismus: Kostet uns ein Chip im Gehirn die Menschlichkeit? Wären wir nicht erst der KI ebenbürtig, wenn unser Wissenslevel gleich auf ist?
  - Beziehungen mit KI: Lieben wir in Zukunft anders?



Gegen die Apokalypse: Wissenschaftler fordern "Kill-Switch" für KI

Quelle: Kunstprojekt CAN'T HELP MYSELF http://www.sunyuanpengyu.com/works/2016/cant%20help%20myself/cant%20help%20myself9.html







„annos undeviginti natus exercitum privato consilio“

„Neunzehn Jahre alt, führte er das Heer aus eigenem Entschluss.“

beschreibt den jungen Octavian (später Augustus),
der im Alter von 19 Jahren nach der Ermordung Caesars eigenständig ein Heer aufstellte

DANKE FÜR IHRE AUFMERKSAMKEIT

MAG.A KARIN DIETL, CDPSE
+43 660 417 22 78
KARIN.DIETL@VALUEDESIGN.VENTURES
VALUEDESIGN.VENTURES



„DATA ISN'T THE FUEL OF THE DIGITAL ECONOMY – TRUST IS.“

VALUE DESIGN
PRIVACY | RISK AND ETHIC MANAGEMENT