dHealth 2022
G. Schreier et al. (Eds.)

doi:10.3233/SHTI220377

Digital Responsibility Goals – A Framework for a Human-Centered Sustainable Digital Economy with a Focus on Trusted Digital Solutions

Jutta Juliane MEIER[a,1], Kai HERMSEN [a], Jochen BAUER[b] and Björn M. ESKOFIER[c]
[a] *Identity Valley Research gUG, Unkel, Germany*
[b] *Lehrstuhl für Fertigungsautomatisierung und Produktionssystematik, Friedrich-Alexander Universität Erlangen-Nürnberg, Erlangen, Germany*
[c] *Machine Learning and Data Analytics (MaD) Lab Friedrich-Alexander Universität Erlangen-Nürnberg, Erlangen, Germany*

Abstract. This paper describes the Digital Responsibility Goals, their purpose, and the associated guiding criteria and their relevance particularly for health. In addition, the document makes a first proposal for measuring digital responsibility.

Keywords: Framework, Healthcare, Patient Participation, Responsibility, Trust

1. Introduction

Digital technologies have the potential to improve people's lives, but technological innovations and the use of innovative technologies must be geared more to taking responsibility for the well-being of people and society, especially in the sector of healthcare provision.

Leading organizations and companies are committed to the UN's 17 Sustainable Development Goals (SDGs) [1]. Similarly, the 7 Digital Responsibility Goals (DRG) [2] aim to guide companies and other stakeholders, such as researchers and users, to develop and demand for trustworthy technology products and services.

2. Challenges

Guidelines and laws are indispensable in this regard [3], but the dynamics of technological development in health also challenge social developments and the ethical dimension in dealing with digital technologies[1].

Likewise, the internet and digital technologies bring negative side effects: for example, in many places in the world, especially in totalitarian states, the internet is

Corresponding Author: J.J. Meier, Identity Valley, Unkel, Germany, E-Mail: jj.meier@identityvalley.org

restricted, regulated, monitored, and used for their propaganda; also, fake news and hate speech poison [4] the atmosphere and make social discourse more difficult.

For the health vertical, there is a lack of access, integration and use as well as education and, above all, a lack of trust in digital solutions. This is explained by the fact that medical data are among the most critical data of all, as they are always personal and usually highly sensitive [5]. Significant ethical questions also arise in the medical field. How can one ensure that my right to informational self-determination is protected in accordance with the basic data protection regulation in force in Europe and still make data available for research purposes - keyword data donation [6]?

3. Concept

Going beyond a purely "corporate perspective" as proposed by the Corporate Digital Responsibility approach [7], the DRGs provide an opportunity for various stakeholders and decision-makers from businesses, regulators, academia and civil society to form a common agenda and plan a common course of action to deal with a human-centered digital transformation. Similar to how the UN Sustainable Development Goals galvanized the international community into action and enabled an agenda for a more sustainable planet, the DRGs seek to promote digital technologies based on democratic rights and values. Developing the DRGs was started by a consortium - consisting of academics, NGOs, and industry experts – and will be further refined continuously in a multi-stakeholder approach [8]. The DRGs propose concrete measures for seven focus areas (see Fig. 1) to shape the digital economy in a way that conforms to values and is ethically sensitive [9].

Figure 1: The seven Digital Responsibility Goals for a Sustainable Digital Economy with a focus on trusted digital solutions

In the following, we describe the DRGs more precisely. Furthermore, we list so-called guiding criteria (GC) of each DRG and give an example for an effective implementation.

3.1. DRG#1 Digital Literacy

Digital Literacy and free and competent access to digital services and infrastructure are prerequisites for the sovereign and self-determined use of digital technologies. They are the basis for all other goals of the DRGs.

- DRG_GC#1.1: The information offered for digital products, services, and processes must be designed individually and in a way that is suitable for the target group.
- DRG_GC#1.2: Access to digital products, services, and processes must be reliable and barrier-free.
- DRG_GC#1.3: The acceptance of digital products, services, and processes must be proactively considered in design and operation.
- DRG_GC#1.4: Education on the opportunities and risks of digitization is essential, so everyone has a right to education on digital matters.
- DRG_GC#1.5: The education and information offered should be designed to create awareness of related topics such as sustainability, climate protection, and diversity/inclusion (for example along the UN SDGs) where applicable.

Example (DRG4GovTech): In the design and operation of an authority website for the electronic application of a car license plate, principles of accessibility were implemented in accordance with DRG GC#1.2, for example in accordance with BITV 2.0 (Barrier-free Information Technology Ordinance). This includes perceptibility, usability, comprehensibility, and robustness for the relevant target groups.

3.2. DRG#2 Cybersecurity

Cybersecurity protects systems against compromise and manipulation by unauthorized persons and ensures the protection of users and their data: the basis for a trustworthy and secure digital cooperation.

- DRG_GC#2.1: Developers, providers, and operators of digital products, services, and processes assume responsibility for cybersecurity. Users also bear some of the shared responsibility - awareness (see DRG #1) is essential here.
- DRG_GC#2.2: Developers, providers, and operators of digital solutions are responsible for appropriate security measures and are constantly developing them further. Products, services, and processes are designed from the outset to be resistant to compromise by unauthorized persons (security by design).
- DRG_GC#2.3: A holistic view and appropriate implementation are considered along the lifecycle, the value chain, and across the entire service or solution.
- DRG_GC#2.4: Developers, providers, and operators of digital products, services, and processes must account for how they provide security for users and their data - while maintaining necessary trade secrets and information security.
- DRG_GC#2.5: Business, politics, authorities, and science must jointly and collaboratively shape the framework for cybersecurity with appropriate objectives, measures, and targets. This requires open and transparent cooperation (for example according to principles of “responsible disclosure”).

Example (DRG4Finance): A bank offering online services has been certified ISO 27000 to - in accordance with DRG GC#2.2 - demonstrates it possesses a robust security system based on appropriate measures to prevent unauthorized access to private

information, internal systems, and networks. Ultimately, this helps minimize the risk of security breaches, making the company more reliable and reputable in the eyes of potential customers.

3.3. DRG#3 Privacy

Privacy is a key part of protecting human dignity. Privacy protection - with a consistent purpose limitation and data minimization beyond current regulation - allows users to act with confidence in the digital world.

- DRG_GC#3.1: Operators and providers of all digital products, services, and processes must take responsibility for protecting the privacy of their users.
- DRG_GC#3.2: When dealing with personal data, strict purpose limitations and data economy are observed.
- DRG_GC#3.3: Privacy protection is considered throughout the entire lifecycle. Privacy protection is the default setting.
- DRG_GC#3.4: Users have control over their personal data and its use – this includes the rights to access, rectify, erase, restrict processing, object, avoid automated decision-making and ensure data portability.
- DRG_GC#3.5: Providers must account for how they protect users' privacy and personal data - while maintaining necessary trade secrets and information security.

Example (DRG4ResponsibleTech): An online search engine assumes responsibility for protecting the privacy of its users in accordance with DRG GC#3.1. Privacy protection is clearly anchored in the organization, and sufficient financial resources are available for additional expenses incurred as a result. Responsibilities for privacy protection in the organization are clearly defined, with a clear mandate at the highest organizational level.

3.4. DRG#4 Data Fairness

Data Fairness means that even non-personal data must be protected and treated carefully and transparently according to its value, to ensure balanced and fair collaboration between all actors in the data ecosystem: a new understanding of data.

- DRG_GC#4.1: When collecting data, proactive care is taken to ensure that it fairly reflects and represents the context in which it is collected.
- DRG_GC#4.2: In digital ecosystem structures, the mutual exchange of data between all parties involved must be clearly described and regulated (data governance). The goal must be fair participation in the benefits achieved through the exchange of data.
- DRG_GC#4.3: Developers, providers, and operators of digital solutions must clearly define and communicate the purpose (wherever possible) with which they use and process data (including non-personal data). Exceptions are approaches like “open data”.

- DRG_GC#4.4: Data is designed "FAIR", especially for use cases relevant to society as a whole - "FAIR" stands for Findable, Accessible, Interoperable, Reusable.
- DRG_GC#4.5: Data providers must be equipped with mechanisms to control and withdraw their data – they shall be able to have a say regarding the usage policies.

Example (DRG4GovTech): In line with DRG GC#4.4 a municipal government has a dedicated strategy to ensure the use of data based on the „FAIR“ principles. It takes a number of dedicated measures with the aim of bringing data including traffic information, environmental data, and economic indicators to the public and promoting its use.

3.5. DRG#5 Trustworthy Algorithms

Trustworthy Algorithms ensure that even after data collection the data will be processed based on fundamental principles such as explainability, verifiability, and fairness: The pre-condition for trustworthy artificial intelligence (AI).

- DRG_GC#5.1: Algorithms, their application, and the datasets on which they are based are designed to provide the highest level of fairness and inclusion.
- DRG_GC#5.2: The individual and overall societal impact of algorithms is regularly reviewed and the review documented. Depending on the results, proportional measures must be taken.
- DRG_GC#5.3: The results of algorithmic processing and their occurrence are comprehensible.
- DRG_GC#5.4: AI systems must be designed to be reliable and precise to be able to withstand subtle attempts to manipulate data or algorithms. It must be possible to reproduce results where possible.
- DRG_GC#5.5: AI systems must be designed and implemented in such a way that independent control of their mode of action is possible.

Example (DRG4Industry): A startup that develops and markets AI tools for industrial applications implements measures to maintain fairness and inclusion in accordance with DRG GC#5.1. These include active measures to increase diversity in developer teams and the establishment of an AI Ethics Board.

3.6. DRG#6 Transparency

Transparency is an important building block for building trust. In the digital space, it is important to proactively create transparency for users and all other stakeholders as to which principles digital offerings underlie as well as transparency on the digital solution and its components itself.

- DRG_GC#6.1: To gain the trust of users, organizations establish transparency about their digital ventures and solutions - for the final digital products, services,

and processes as well as the organization, business models, data flows, and technology behind them.

- DRG_GC#6.2: Transparency is implemented in interactive communication (for example, between providers and users), and mechanisms for interaction are actively offered.
- DRG_GC#6.3: Organizations set out which (further) principles they follow, for example along the UN SDGs.
- DRG_GC#6.4: In addition to transparency for users, transparency should also be provided for professionals - while maintaining the necessary business secrets and information security.
- DRG_GC#6.5: Organizations must outline how they will make transparency verifiable and thus hold themselves accountable for their actions in the digital space.

Example (DRG4Health): In a tool for diagnostic imaging in line with DRG GC#6.1 it is made transparent to physicians upon use that image recognition and analysis is used for diagnostic purposes in healthcare. Furthermore, this is also clearly communicated to relevant patients in the physician-patient conversation.

3.7. DRG#7 Human Agency and Identity

Human Agency and Identity are crucial signposts and prerequisites for the development of digital products, services, and processes. These are to be developed and deployed in a human-centric, sustainable, integrative manner and under human supervision: Our future is at stake. Now.

- DRG_GC#7.1: The preservation of the multifaceted human identity is a basic requirement and must be the basis for any digital development. The resulting digital approaches are always user-centric – they respect personal autonomy and dignity, limit commoditization, and open up new perspectives.
- DRG_GC#7.2: Sustainability and climate protection must be part of digital business models and implemented in practice (especially in accordance with the SDGs).
- DRG_GC#7.3: Digital products, services, and processes promote responsible, nonmanipulative communication. Where possible, communication takes place unfiltered.
- DRG_GC#7.4: Digital technology always remains under human authorship and control - it can be shaped throughout its deployment.
- DRG_GC#7.5: Technology may only be applied if it is of use to individuals and mankind, and promotes welfare.

Example (DRG4ResponsibleTech): In line with DRG GC#7.5 a technology company conducts an impact assessment on the effects of the technology of facial recognition. Discovering the risk of malicious and unfair use, it decides to clearly limit the use of that technology to dedicates, risk-mitigated use cases and transparently communicates that decision.

The DRGs are intended as a benchmark for all players in the digital space. The DRGs take an inclusive and collaborative approach for all relevant actors to promote trust in digital technologies and business models. The DRGs present a framework to measure the degree of successful value-based digitization, strengthen the responsibility of digital actors, and provide participants with clear guidance for their digital strategies. In addition, a code of conduct accepted and shared in this way can help engage like-minded companies while providing guidance on implementation, transparency and accountability.

4. Implementation and Evaluation

4.1. Measurability

Each of the seven goals for responsible digital transformation represents an urgent need for action in the digital space. Comprehensible, innovative, and applicable measures are needed. Such measures require appropriate measurement and reporting of progress achieved. Measurability happens in stages and in the end, a DRG Index will be created. The guiding criteria define the desired actions to enable a responsible digital space. These actions are each backed by concrete maturity levels that allow an assessment of whether the criteria are met. In addition, specific evidence is requested to support the respective assessment (see Fig. 2).

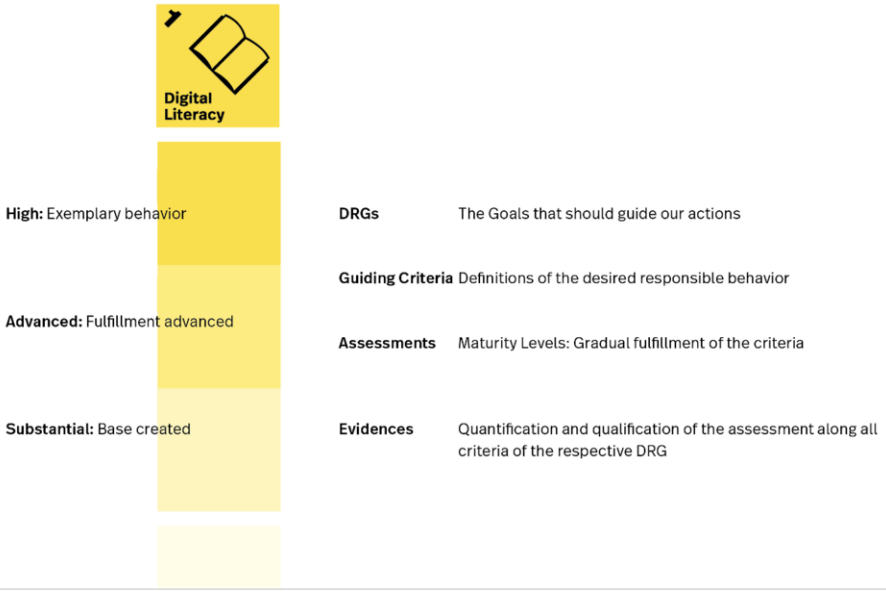

Figure 2: The Digital Responsibility Goals, their criteria, evaluation and evidence aggregated in the Digital Responsibility Goal Index, exemplary for DRG#1

4.2. System and Process Perspective combined with Human Centricity

The trustworthiness of digital products, services, and processes is not just a question of technology, but one in which human behavior and procedures within and between organizations are equally important.

In the definition of the Digital Responsibility Goals, a system perspective is therefore combined with a process perspective: The system perspective refers to the requirements for an artifact, the digital solutions themselves. The process perspective specifies the requirements for the design, implementation, and operational processes of the organizations, manufacturers, or service providers behind them. Both perspectives are independent, have their strengths and weaknesses, but are groundbreaking when combined. The way a digital solution is set up should be given equal weight to how it was conceived, created, implemented, and how it is operated. Overall, the method for dealing with responsible digitization in practice requires a "best of both worlds" approach that incorporates both the system and process perspectives and is human-centric. Our holistic approach, that adds another perspective in order to guarantee all assessments and developments are verifiably human-centered, is depicted below (see Fig. 3).

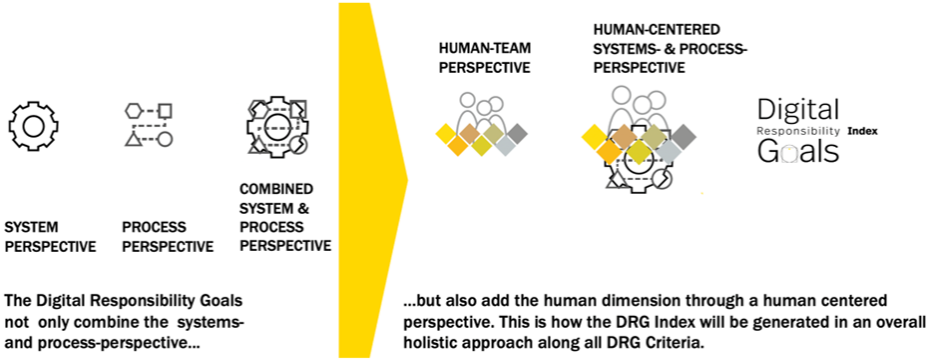

Figure 3: Human-centered approach to consider systems, processes, and teams.

4.3. Dashboard

To assess trustworthiness, it is crucial to communicate and convey the responsibility-enhancing characteristics of that digital solution in a way that citizens, users, and consumers, as well as policymakers, business leaders, regulators, and/or standard-setting bodies can easily understand and comprehend [10]. This importance of clear communication is especially true in the doctor patient relationship [11].

We propose to represent the complexity of these demonstrated behaviors in an overarching index -– the Digital Responsibility Index. This relative score will be created for each of the seven Digital Responsibility Goals and will include multiple levels. Sufficient differentiation between different levels of maturity in value fulfillment thus becomes visible according to the granularity of the observation data (see Fig. 4).

Figure 4: Symbolic Presentation of the DRI Digital Responsibility Index maturity levels (under development)

5. Discussion and Conclusion

Changes can best be shaped along with clear criteria and target images. As a target picture to shape sustainable human-centered digital transformation, the DRGs offer an opportunity to promote greater responsibility in the digital space across sectors. Responsible behavior all along the data life cycle is at the core of establishing trust. By adhering to the framework of the DRGs, building trust will no longer be a random by-product, but a pro-active and targeted achievement.

The DRGs provide a framework to mobilize companies and organizations to invest in digital trust in a continuous and scalable way while pursuing their business interests, sustainably and responsibly. By doing so, they go beyond "traditional" headquarter-centric CSR approaches, that mitigate otherwise unjust business models and are not necessarily addressed within digital strategies, as they are more focused on "corporate social" activities. The aim of the DRG approach is to be ingrained in both business model and organization from end-to-end. They propose clear governance mechanisms to do so (e.g., clear roles, integration in processes, education measures). Finally, they are suitable for deriving metrics that can be used to rank both the status of individual digital projects as well as an overall societal development within the organization.

The goal of a sector-specific application of the DRGs within the Health Industry - „DRG4Health"- is to build protected and trusted digital health data ecosystems, that for example may be based on the Gaia-X infrastructure (still to be researched) for the development of data-driven business models, products, and services.

Within the research project of TEAM-X (Trusted Ecosystem of Applied Medical Data Exchange), funded by the German Federal Ministry for Economic Affairs and Climate Action, two Gaia-X [12] use cases will be developed in the areas of nursing and women's health and in the care sector. As part of this research project, the DRGs will be put into practice through Responsible Leadership training and other methods for the first time.

Based on the DRGs for a more responsible and human-centered digital transformation, more and more actors come together. They jointly shape the living organism of the DRGs, bring them into action, and further develop them towards measurability. For example, in a further publication, it is planned to depict a brief overview of the status quo of existing regulations, standards, and initiatives are planned for each DRG, and to derive the resulting need for action. This will go in line with a discussion, if and how the DRG could be represented through a family of standards. This could help to further depict this view of the DRGs and their concrete application to build trust for example for a European Health Data Space or an extension for existing data spaces like smart living.

Funding: Supported by German Federal Ministry for Economic Affairs and Climate Action.

References

[1] Lim, S. S., Allen, K., Bhutta, Z. A., Dandona, L., Forouzanfar, M. H., Fullman, N., … & Chang, J. C. (2016). Measuring the health-related Sustainable Development Goals in 188 countries: a baseline analysis from the Global Burden of Disease Study 2015. *The Lancet*, **388**(10053), 1813-1850.

[2] Meier, J.J., Hermsen, K., (2022). It'a all about trust. Leitkriterien und Orientierung für digitale Verantwortung. Basierend auf europäischen Werten Identity Valley..https://www.identityvalley.org/assets/download/IDV_DRG_Strategiepapier_Doppelseiten_220212.pdf

[3] Fiedler, B. A. (2017). Managing Smartphone and Tablet Applications. In Managing Medical Devices Within a Regulatory Framework (pp. 331-342). Elsevier.

[4] Paz, María Antonia, Julio Montero-Díaz, and Alicia Moreno-Delgado. "Hate speech: A systematized review." *Sage Open* **10**.4 (2020): 2158244020973022.

[5] Liu, V., Caelli, B., May, L., & Sahama, T. (2009). Privacy and security in open and trusted health information systems. In *Proceeding of the Third Australasian Workshop on Health Informatics and Knowledge Management* (pp. 25-30). Australian Computer Society.

[6] Ahmadpour, N., Ludden, G., Peters, D., & Vold, K. (2022). Responsible Digital Health. *Frontiers in Digital Health*, 213.

[7] Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, 122, 875-888.

[8] Lynn, J., Stachowiak, S., Akey, T., Gase, L., Dane, A., & Roos, J. (2018). When collective impact has an impact: A cross-site study of 25 collective impact initiatives. *Spark Policy Institute,* ORS Impact.

[9] Costa, E., & Pesci, C. (2022). Putting Stakeholders at the Centre: Multi-Stakeholder Approaches to Social Impact Measurement. In *Social Impact Measurement for a Sustainable Future* (pp. 129-144). Palgrave Macmillan, Cham.

[10] Blöbaum, B. (2016). *Trust and communication in a digitized world. Models and Concepts of Trust Research*. Heidelberg et al.: Springer.

[11] Gopichandran, V., & Sakthivel, K. (2021). Doctor-patient communication and trust in doctors during COVID 19 times—A cross sectional study in Chennai, India. *Plos one*, **16**(6), e0253497.

[12] Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Network*, **35**(2), 4-5.

[13] Bauer, J., Konrad, C., Hechtel, M., Wichert, R., Weigand, C., Dengler, S., ... & Franke, J. (2021). ForeSight Approach to improve Privacy and Security in the Smart Living Domain. *Current Directions in Biomedical Engineering*, **7**(2), 903-906.