




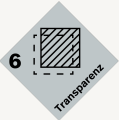



Digital Responsibility Goals – Guiding Criteria

 <p>DRG#1</p>	 <p>DRG#2</p>	 <p>DRG#3</p>	 <p>DRG#4</p>	 <p>DRG#5</p>	 <p>DRG#6</p>	 <p>DRG#7</p>
<p>1.1 Information offered for digital products, services, and processes must be designed individually and in a way that is suitable for the target group.</p>	<p>2.1 Developers and providers of digital products, services and processes assume responsibility for cybersecurity. Users also bear a part of the responsibility.</p>	<p>3.1 Developers and providers of digital products, services, and processes must take responsibility for protecting the privacy of their users.</p>	<p>4.1 When collecting or re-using data, proactive care is taken to ensure the integrity of the data, considering whether any gaps, inaccuracies or bias might exist.</p>	<p>5.1 Algorithms, their application, and the datasets they are trained on are designed to provide a maximum of fairness and inclusion.</p>	<p>6.1 Organizations establish transparency - about digital products, services, and processes as well as the organization, business models, data flows, and technology employed.</p>	<p>7.1 The preservation of the multifaceted human identity must be the basis for any digital development. Resulting digital technologies are user centric, respect personal autonomy, dignity, and limit commoditization.</p>
<p>1.2 Access to digital products, services, and processes must be reliable and barrier-free.</p>	<p>2.2 Developers and providers of digital technology are responsible for appropriate security measures and constantly develop them further. Digital technologies are designed to be resistant to compromise.</p>	<p>3.2 When dealing with personal data basic principles of data protection are respected, in particular strict purpose limitations and data minimisation.</p>	<p>4.2 In digital ecosystems the exchange of data between all parties must be clearly described and regulated. The goal must be fair participation in the benefits achieved through the exchange of data.</p>	<p>5.2 The individual and overall societal impact of algorithms is regularly reviewed and the review documented. Depending on the results, proportional corrective measures must be taken.</p>	<p>6.2 Transparency is implemented through interactive communication (for example, between providers and users), and mechanisms for interaction are actively offered.</p>	<p>7.2 Sustainability and climate protection must be part of design choices of digital technologies and digital business models and implemented in practice (especially in accordance with the UN SDGs).</p>
<p>1.3 Acceptance of digital products, services, and processes must be proactively considered in design and operation. This includes measures on equity, diversity & inclusion.</p>	<p>2.3 A holistic view and appropriate implementation of cybersecurity are considered along the lifecycle, value chain, and the entire service, resp. solution.</p>	<p>3.3 Privacy protection is considered throughout the entire lifecycle and should be considered a default setting.</p>	<p>4.3 Developers and providers of digital technologies must clearly define and communicate the purpose with which they use and process data (including non-personal data).</p>	<p>5.3 Outputs of algorithmic processing are comprehensible and explainable. Where possible outputs should be reproducible.</p>	<p>6.3 The application of digital technology is made transparent wherever there is an interaction between people and the digital technology (for example, the use of chatbots).</p>	<p>7.3 Digital products, services, and processes promote responsible, non-manipulative communication. Where possible, communication takes place unfiltered.</p>
<p>1.4 Education on the opportunities and risks of the digital transformation is essential - everyone is entitled to education on digital matters.</p>	<p>2.4 Developers and providers of digital products, services, and processes must account for how they provide security for users and their data - while maintaining trade secrets.</p>	<p>3.4 Users have control over their personal data and their use - including the rights to access, rectify, erase, data portability, restrict processing and avoid automated decision-making.</p>	<p>4.4 When providing or creating datasets the “FAIR” data principles are satisfied, especially in cases where re-use would benefit society as a whole.</p>	<p>5.4 AI systems must be robust and designed to withstand subtle attempts to manipulate data or algorithms.</p>	<p>6.4 In addition to transparency for users, transparency should also be provided for other stakeholders (e.g., businesses, science, governments) – while maintaining trade secrets.</p>	<p>7.4 Digital technology always remains under human conception and control - it can be reconfigured throughout its deployment.</p>
<p>1.5 Awareness for related topics such as sustainability, climate protection, and diversity/inclusion (e.g., along UN SDGs) should be raised, where applicable.</p>	<p>2.5 Business, politics, authorities, civil society and science must collaboratively shape the objectives and measures of cybersecurity. This requires open and transparent cooperation and disclosure.</p>	<p>3.5 Providers must account for how they protect users’ privacy and personal data - while maintaining necessary trade secrets.</p>	<p>4.5 Users providing or creating data must be equipped with mechanisms to control and withdraw their data - they shall have a say regarding data usage policies.</p>	<p>5.5 AI systems must be designed and implemented in a way that independent control of their mode of action is possible.</p>	<p>6.5 Organizations must outline how they will make transparency verifiable and thus hold themselves accountable for their actions in the digital space.</p>	<p>7.5 Digital technology may only be applied to benefit individuals and humankind and promote the wellbeing of humanity.</p>