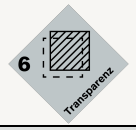
Identity Valley

Digital Responsibility Goals – Leitkriterien

DRG#1 	DRG#2 	DRG#3 	DRG#4 
1.1 Das Informationsangebot für digitale Produkte, Dienstleistungen und Prozesse ist individuell und zielgruppengerecht zu gestalten.	2.1 Entwicklerinnen, Anbieterinnen und Betreiber von digitalen Produkten, Dienstleistungen und Prozessen übernehmen Verantwortung für Cybersicherheit. Nutzer tragen auch einen Teil der geteilten Verantwortung – hier ist Aufklärung (siehe DRG#1) unerlässlich.	3.1 Betreiberinnen und Anbieterinnen jeglicher digitaler Produkte, Dienstleistungen und Prozesse müssen Verantwortung für den Schutz der Privatsphäre der Nutzer übernehmen.	4.1 Bei der Erhebung von Daten wird proaktiv darauf geachtet, dass sie den Kontext, in dem sie erhoben werden, fair wiedergeben und repräsentieren.
1.2 Der Zugang zu digitalen Produkten, Dienstleistungen und Prozessen ist verlässlich und barrierefrei zu gestalten.	2.2 Entwicklerinnen, Anbieterinnen und Betreiber von digitalen Lösungen sind verantwortlich für angemessene Sicherheitsmaßnahmen gemäß dem Stand der Technik und entwickeln diese stets weiter. Produkte, Dienstleistungen und Prozesse sind von Anfang an widerstandsfähig gegen Kompromittierung oder Missbrauch durch Unbefugte gestaltet (security by design).	3.2 Beim Umgang mit personenbezogenen Daten wird auf die Datenschutzgrundsätze, insbesondere auf strenge Zweckbindung und Datensparsamkeit geachtet.	4.2 In digitalen Ökosystemstrukturen ist der gegenseitige Austausch von Daten zwischen allen beteiligten Parteien klar zu beschreiben und zu regeln (Data Governance). Ziel muss eine faire Beteiligung am erzielten Nutzen durch den Datenaustausch sein.
1.3 Die Akzeptanz von digitalen Produkten, Dienstleistungen und Prozessen ist proaktiv im Design und im Betrieb zu berücksichtigen. Das sollte Maßnahmen zur Steigerung der Chancengleichheit, Vielfalt und Integration beinhalten.	2.3 Es wird eine gesamtheitliche Betrachtung und angemessene Implementierung entlang des Lebenszyklus, der Wertschöpfungskette und über die gesamte Lösung oder den gesamten Service vorgenommen.	3.3 Der Schutz der Privatsphäre wird durchgängig entlang des gesamten Lebenszyklus berücksichtigt.	4.3 Entwicklerinnen, Anbieterinnen und Betreiber digitaler Lösungen müssen den Zweck (wo immer möglich), mit dem sie (auch nicht personengebundene) Daten nutzen und verarbeiten, klar definieren und kommunizieren. Ausnahmen bilden beispielsweise „Open Data“-Ansätze.
1.4 Die Aufklärung über Chancen und Risiken der Digitalisierung ist unerlässlich, daher haben alle Menschen einen Anspruch auf Bildung zu digitalen Fragestellungen.	2.4 Entwicklerinnen, Anbieterinnen und Betreiber von digitalen Produkten, Dienstleistungen und Prozessen müssen Rechenschaft ablegen, wie sie für die Sicherheit der Benutzer und deren Daten sorgen – unter Wahrung der notwendigen Geschäftsgeheimnisse und Informationssicherheit.	3.4 Nutzerinnen haben die Kontrolle über ihre personenbezogenen Daten und deren Verwendung – dies umfasst das Recht auf Zugang, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch, Vermeidung automatisierter Entscheidungsfindung und Gewährleistung der Datenübertragbarkeit.	4.4 Daten werden „FAIR“ gestaltet, insbesondere für gesamtgesellschaftlich relevante Anwendungsfälle. FAIR steht dabei für Findable (Auffindbar), Accessible (Zugänglich), Interoperable (Interoperabel), Reusable (Wiederverwendbar).
1.5 Das Bildungs- und Informationsangebot ist so zu gestalten, dass es Bewusstsein für angrenzende Themenbereiche wie Nachhaltigkeit, Klimaschutz und Diversität/Inklusion (zum Beispiel entlang der UN SDGs) schafft – wo immer zutreffend.	2.5 Wirtschaft, Politik, Behörden, Zivilgesellschaft und Wissenschaft müssen gemeinsam und kollaborativ mit geeigneten Richtlinien, Maßnahmen und Zielen den Rahmen für Cybersicherheit gestalten. Dies erfordert offene und transparente Zusammenarbeit (zum Beispiel im Rahmen von „responsible disclosure“ = verantwortungsvolle Offenlegung).	3.5 Anbieterinnen müssen Rechenschaft ablegen, wie sie die Privatsphäre der Nutzer und ihre personenbezogenen Daten schützen – unter Wahrung der notwendigen Geschäftsgeheimnisse und Informationssicherheit.	4.5 Den Datengebenden müssen Mechanismen zur Kontrolle und zum Rückzug ihrer Daten zur Verfügung gestellt werden – sie sollten über die Datennutzungsbedingungen mitbestimmen können.

Digital Responsibility Goals – Leitkriterien

DRG#5	DRG#6	DRG#7
		
5.1 Algorithmen, ihre Anwendung und die Datensätze, die ihnen zugrunde liegen, sind so konzipiert, dass sie ein Höchstmaß an Fairness und Inklusion bieten.	6.1 Um das Vertrauen der Nutzerinnen zu gewinnen, stellen Organisationen Transparenz hinsichtlich ihrer digitalen Unternehmungen und ihrer digitalen Lösungen her – einschließlich der finalen digitalen Produkte, Dienstleistungen und Prozesse sowie die Organisation, Geschäftsmodelle, Datenflüsse und Technik.	7.1 Die Wahrung der vielschichtigen menschlichen Identität ist eine Grundvoraussetzung und muss Basis für jede digitale Entwicklung sein – daraus resultierende Ansätze sind stets nutzerzentriert – sie respektieren die persönliche Autonomie und Würde, begrenzen die Kommodifizierung und öffnen neue Perspektiven.
5.2 Die individuellen und gesamtgesellschaftlichen Auswirkungen von Algorithmen werden regelmäßig überprüft und die Überprüfung wird dokumentiert. Abhängig von den Ergebnissen werden angemessene Maßnahmen ergriffen.	6.2 Transparenz wird in interaktiver Kommunikation (beispielsweise zwischen Anbieterinnen und Nutzern) realisiert und es werden aktiv Mechanismen zur Interaktion angeboten.	7.2 Nachhaltigkeit und Klimaschutz müssen Bestandteil digitaler Geschäftsmodelle sein und praktisch umgesetzt werden (insbesondere gemäß der Nachhaltigkeitsziele der UN).
5.3 Die Ergebnisse von algorithmischer Verarbeitung und deren Zustandekommen sind nachvollziehbar.	6.3 Der Einsatz digitaler Lösungen wird transparent gestaltet, wo auch immer eine digitale Interaktion zwischen Menschen und digitaler Lösung stattfindet (beispielsweise beim Einsatz von Chatbots).	7.3 Digitale Produkte, Dienstleistungen und Prozesse fördern verantwortungsvolle, nicht manipulative Kommunikation. Wo möglich, findet Kommunikation ungefiltert statt.
5.4 KI-Systeme müssen zuverlässig und präzise gestaltet werden, um auch gegen subtile Versuche, Daten oder Algorithmen zu manipulieren, gewappnet zu sein. Ergebnisse müssen sich – wo möglich – reproduzieren lassen können.	6.4 Neben der Transparenz für Nutzerinnen sollte auch Transparenz für das Fachpublikum hergestellt werden – unter Wahrung der notwendigen Geschäftsgeheimnisse und Informationssicherheit.	7.4 Digitale Technologie bleibt zu jeder Zeit unter menschlicher Autorenschaft und Kontrolle – sie ist während des gesamten Einsatzes gestaltbar.
5.5 KI-Systeme sind so zu konzipieren und zu implementieren, dass eine unabhängige Kontrolle ihrer Wirkweise möglich ist.	6.5 Die Organisationen müssen darlegen, wie sie die Transparenz überprüfbar machen und somit über ihr Handeln im digitalen Raum Rechenschaft ablegen.	7.5 Technologie darf nur dann angewendet werden, wenn ein klarer Nutzen sowohl für den einzelnen Menschen als auch für die Menschheit besteht und Wohlergehen gefördert wird.

Identity Valley

It's all about trust.