

Identity Valley®: It's all about trust.
Für eine vertrauenswürdige digitale Zukunft.

Die gemeinnützige Organisation **IDENTITY VALLEY** setzt sich für eine Gestaltung digitaler Technologien ein, bei der vertrauenswürdige und ethische Grundsätze im Vordergrund stehen.



Digital
Responsibility
Goals®

Digital Responsibility Goals® (DRGs): Im Fokus steht dabei eine grundlegende Neuausrichtung der gesellschaftlichen Beziehung zu Technologien, bei der nicht nur deren Möglichkeiten hinterfragt, sondern auch ihre Auswirkungen auf die Gesellschaft beleuchtet werden. Diese Vision hat die **Digital Responsibility Goals®** hervorgebracht: ein Wertethemen, der klare und messbare Leitkriterien für die Gestaltung der digitalen Landschaft bietet und bei dem Vertrauen und Menschen im Mittelpunkt stehen.

Wie die **Sustainable Development Goals (SDGs)** der Vereinten Nationen die Weltgemeinschaft hinter eine gemeinsame Agenda für Nachhaltigkeit, Frieden und Wohlstand gebracht haben, so geben auch die DRGs einen vergleichbaren Rahmen für die digitale Welt vor. Denn wie bei der nachhaltigen Entwicklung erfordern auch die Herausforderungen des digitalen Wandels (z. B. Schutz der Privatsphäre, vertrauenswürdige KI) ein **gesamtgesellschaftliches Engagement**. Hierfür bieten die DRGs einen konkreten Werterahmen, dessen Leitkriterien (siehe ANHANG) Handlungsanweisungen für eine vertrauenswürdige Digitalisierung geben. So kann mit dem DRG-Werterahmen die Komplexität bestehender Zertifikate, Standards und Gesetze auf ein für Nutzer/innen und Entscheidungsträger/innen **verständliches Maß** heruntergebrochen werden.

Die DRGs tragen dazu bei, aus einer immer komplexer werdenden virtuellen Welt, ein vertrauenswürdige digitales Ökosystem zu entwickeln, in dem soziale und wirtschaftliche Beziehungen möglich sind: **Regierungen** können die DRG als Kompass für digitale Strategien nutzen, **Unternehmen** können digitale Lösungen auf vertrauenswürdiger Basis entwickeln und **Individuen** können in ihrem zunehmend digitalen Leben selbstbestimmt nach vertrauenswürdigen Produkten greifen.

Immer mehr Regierungen und Branchen erkennen die Bedeutung von Vertrauenswürdigkeit und Verantwortung in der Digitalisierung. Daher sind die **Digital Responsibility Goals** richtungweisend für eine gemeinsame Mensch-zentrierte digitale Transformation.

Als gemeinnützige Organisation bringt Identity Valley Vordenker/innen, politische Entscheidungsträger/innen, Bürger/innen und Branchenexpert/innen zusammen, um sich durch Vernetzung, Forschung und Kommunikation für eine wertebasierte digitale Welt einzusetzen:

- Mensch-zentrierte Interessenvertretung:** Wir setzen uns für ein Technoligiedesign ein, das sich an den Bedürfnissen, Werten und Erfahrungen der Menschen orientiert und nicht nur an Profit oder Datengewinnung.
- Sicherstellung von Vertrauenswürdigkeit:** Durch die Zusammenarbeit mit Technologieunternehmen stellen wir sicher, dass bei der Entwicklung digitaler Lösungen Transparenz, Sicherheit und ethische Standards im Mittelpunkt stehen.
- Bildung und Befähigung:** Mit Handlungshinweisen und Informationen helfen wir der Gesellschaft, die sich entwickelnde digitale Landschaft besser zu verstehen und ihr mit Zuversicht zu begegnen.

Gestalten Sie mit Identity Valley eine digitale Zukunft, bei der Innovation und Verantwortung miteinander harmonieren. Helfen Sie uns, die Rolle der Technologie in der Gesellschaft neu zu definieren, angetrieben von menschlichen Werten und gemeinsamen Zielen.

Die 7 Digital Responsibility Goals (DRGs)



DRG#1 - DIGITALE KOMPETENZ und freier und kompetenter Zugang zu digitalen Dienstleistungen und Infrastrukturen Voraussetzung für den souveränen und selbstbestimmten Umgang mit digitalen Technologien.



DRG#2 - CYBERSECURITY wappnet Systeme gegen Kompromittierung und Manipulation durch unbefugte und stellt den Schutz der Menschen sowie ihrer Daten sicher. Grundvoraussetzung für verantwortungsvollen Betrieb digitaler Lösungen.



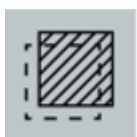
DRG#3 - PRIVATSPÄRE als wichtiger Bestandteil der Menschenwürde. Vertrauensvoller Umgang im digitalen Raum, in dem Daten zweckgebunden und sparsam (so viel wie nötig, so wenig wie möglich) verarbeitet werden.



DRG#4 - DATEN FAIRNESS bedeutet, dass auch nicht personenbezogene Daten geschützt und gemäß ihrer Wertigkeit behandelt werden. Geeignete Mechanismen sollen Austausch und Anwendbarkeit zwischen Akteuren in einem Datenökosystem gewährleisten.



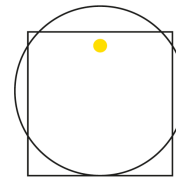
DRG#5 - VERTRAUENSWÜRDIGE ALGORITHMEN stellen sicher, dass die Daten auch nach der Datenerhebung durch Nachvollziehbarkeit, Überprüfbarkeit und Fairness weiterverarbeitet werden. Grundvoraussetzung für vertrauenswürdige KI!








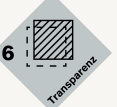

DRG#6 - TRANSPARENZ als Baustein für den Aufbau von Vertrauen. Transparenz hinsichtlich zugrunde liegender Prinzipien von Produkten, Dienstleistungen und Prozessen und Transparenz mit Blick auf die digitale Lösung und deren Komponenten.



DRG#7 - MENSCHLICHES HANDELN UND IDENTITÄT als Voraussetzung für die Entwicklung digitaler Produkte, Dienstleistungen und Prozesse. Diese sind mensch-zentriert, nachhaltig und unter menschlicher Aufsicht zu entwickeln und einzusetzen.



Die DRG-Leitkriterien

 <p>1 Digitale Kompetenz</p>	 <p>2 Cyber-Sicherheit</p>	 <p>3 Privatsphäre</p>	 <p>4 Daten Fairness</p>	 <p>5 Vertrauenswürdige Algorithmen</p>	 <p>6 Transparenz</p>	 <p>7 Menschliche Würde und Wohlbefinden</p>
<p>1.1 Das Informationsangebot für digitale Produkte, Dienstleistungen und Prozesse ist individuell und zielgruppengerecht zu gestalten.</p>	<p>2.1 Entwickler:innen, Anbieter:innen und Betreiber:innen von digitalen Produkten, Dienstleistungen und Prozessen übernehmen Verantwortung für Cybersicherheit. Nutzer:innen tragen auch einen Teil der geteilten Verantwortung – hier ist Aufklärung (siehe DRG#1) unerlässlich.</p>	<p>3.1 Betreiber:innen und Anbieter:innen jeglicher digitaler Produkte, Dienstleistungen und Prozesse müssen Verantwortung für den Schutz der Privatsphäre der Nutzer:innen übernehmen.</p>	<p>4.1 Bei der Erhebung von Daten wird proaktiv darauf geachtet, dass sie den Kontext, in dem sie erhoben werden, fair wiedergeben und repräsentieren.</p>	<p>5.1 Algorithmen, ihre Anwendung und die Datensätze, die ihnen zugrunde liegen, sind so konzipiert, dass sie ein Höchstmaß an Fairness und Inklusion bieten.</p>	<p>6.1 Um das Vertrauen der Nutzer:innen 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.</p>	<p>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.</p>
<p>1.2 Der Zugang zu digitalen Produkten, Dienstleistungen und Prozessen ist verlässlich und barrierefrei zu gestalten.</p>	<p>2.2 Entwickler:innen, Anbieter:innen und Betreiber:innen 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).</p>	<p>3.2 Beim Umgang mit personenbezogenen Daten wird auf die Datenschutzgrundsätze, insbesondere auf strenge Zweckbindung und Datensparsamkeit geachtet.</p>	<p>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.</p>	<p>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.</p>	<p>6.2 Transparenz wird in interaktiver Kommunikation (beispielsweise zwischen Anbieter:innen und Nutzer:innen) realisiert und es werden aktiv Mechanismen zur Interaktion angeboten.</p>	<p>7.2 Nachhaltigkeit und Klimaschutz müssen Bestandteil digitaler Geschäftsmodelle sein und praktisch umgesetzt werden (insbesondere gemäß der Nachhaltigkeitsziele der UN).</p>
<p>1.3 Die Akzeptanz von digitalen Produkten, Dienstleistungen und Prozessen ist proaktiv im Design und im Betrieb zu berücksichtigen. Das sollten Maßnahmen zur Steigerung der Chancengleichheit, Vielfalt und Integration beinhalten.</p>	<p>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.</p>	<p>3.3 Der Schutz der Privatsphäre wird durchgängig entlang des gesamten Lebenszyklus berücksichtigt.</p>	<p>4.3 Entwickler:innen, Anbieter:innen und Betreiber:innen digitaler Lösungen müssen den Zweck (wo immer möglich), mit dem sie (auch nicht personengebunden) Daten nutzen und verarbeiten, klar definieren und kommunizieren. Ausnahmen bilden beispielsweise „Open Data“ Ansätze.</p>	<p>5.3 Die Ergebnisse von algorithmischer Verarbeitung und deren Zustandekommen sind nachvollziehbar.</p>	<p>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).</p>	<p>7.3 Digitale Produkte, Dienstleistungen und Prozesse fördern verantwortungsvolle, nicht manipulative Kommunikation. Wo möglich, findet Kommunikation ungefiltert statt.</p>
<p>1.4 Die Aufklärung über Chancen und Risiken der Digitalisierung ist unerlässlich, daher haben alle Menschen einen Anspruch auf Bildung zu digitalen Fragestellungen.</p>	<p>2.4 Entwickler:innen, Anbieter:innen und Betreiber:innen von digitalen Produkten, Dienstleistungen und Prozessen müssen Rechenschaft ablegen, wie sie für die Sicherheit der Benutzer:innen und deren Daten sorgen – unter Wahrung der notwendigen Geschäftsgeheimnisse und Informationssicherheit.</p>	<p>3.4 Nutzer:innen 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.</p>	<p>4.4 Daten werden „FAIR“ gestaltet, insbesondere für gesamtgesellschaftlich relevante Anwendungsfälle. „FAIR“ steht dabei für Findable (Auffindbar), Accessible (Zugänglich), Interoperable (Interoperabel), Reusable (Wiederverwendbar).</p>	<p>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.</p>	<p>6.4 Neben der Transparenz für Nutzer:innen sollte auch Transparenz für das Fachpublikum hergestellt werden – unter Wahrung der notwendigen Geschäftsgeheimnisse und Informationssicherheit.</p>	<p>7.4 Digitale Technologie bleibt zu jeder Zeit unter menschlicher Autorenschaft und Kontrolle – sie ist während des gesamten Einsatzes gestaltbar.</p>
<p>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.</p>	<p>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).</p>	<p>3.5 Anbieter:innen müssen Rechenschaft ablegen, wie sie die Privatsphäre der Nutzer:innen und ihre personenbezogenen Daten schützen – unter Wahrung der notwendigen Geschäftsgeheimnisse und Informationssicherheit.</p>	<p>4.5 Den Datengebenden müssen Mechanismen zur Kontrolle und zum Rückzug ihrer Daten zur Verfügung gestellt werden – sie sollten über die Datennutzungsbedingungen mitbestimmen können.</p>	<p>5.5 KI-Systeme sind so zu konzipieren und zu implementieren, dass eine unabhängige Kontrolle ihrer Wirkweise möglich ist.</p>	<p>6.5 Die Organisationen müssen darlegen, wie sie die Transparenz überprüfbar machen und somit über ihr Handeln im digitalen Raum Rechenschaft ablegen.</p>	<p>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.</p>