Digital Trust und Corporate Digital Responsibility

Allgemeines

Nicolas Zahn

Haben Sie bei der Nutzung eines digitalen Dienstes schon einmal überlegt, ob Sie dieser Anwendung vertrauen können? Warum fühlen Sie sich sicher, wenn Sie sich bei Ihrem e-Banking anmelden oder mit dem Chatbot Ihrer Krankenkasse über medizinische Vorfälle sprechen? Beunruhigen Sie die ständigen Berichte über Datenlecks und ethisch fragwürdige Geschäftsmodelle in der digitalen Welt? Wollen Sie als Anbieter:in eines digitalen Dienstes bei der Softwareentwicklung sicherstellen, dass Ihre Anwendung vertrauenswürdig ist, und wie wollen Sie das Ihren Kund:innen vermitteln?

Alle diese Fragen stehen im Fokus von **Digital Trust** und **Corporate Digital Responsibility**. Wir befinden uns seit Jahren in der digitalen Welt, in welcher jeder Aspekt unseres Alltags mehr oder weniger von digitalen Anwendungen abhängt. Für Firmen ergeben sich durch die fortschreitende Digitalisierung Möglichkeiten, neue Dienste zu entwickeln und innovative Produkte und Services anzubieten. Doch was nützt uns das innovativste Produkt, wenn die Konsument:innen es nicht nutzen wollen, weil sie ihm nicht vertrauen?

Die Lösung liegt in einer tiefgehenden Auseinandersetzung von Anbieter:innen und Entwickler:innen digitaler Dienste mit ethischen Fragen und Fragen des Vertrauens. Dieses Whitepaper bietet Ihnen, basierend auf der Arbeit der Swiss Digital Initiative[1], einen Einstieg in diese Thematik, welche dank der künstlichen Intelligenz und den komplexen Vertrauensfragen, die diese Technologie aufwirft, nur noch mehr an Bedeutung gewinnen wird.

Nach der Lektüre wissen Sie, was sich hinter den Schlagwörtern Digital Trust und Corporate Digital Responsibility verbirgt, wie Sie sich innerhalb Ihrer Organisation diesen Themen annähern können und welche Fragen Sie sich bei der Entwicklung digitaler Dienste stellen sollten.

Quelle: swiss-digital-initiative.org/

1 swiss-digital-initiative.org

Eine Frage des Vertrauens: Die Bedeutung von Digital Trust

Den Stellenwert von Vertrauen kennen wir alle aus dem persönlichen und beruflichen Kontext. Vertrauen ist eine entscheidende **Ressource** in unseren Interaktionen mit anderen Personen und Organisationen. Haben wir Vertrauen, bedeutet das, dass wir mit einer bestimmten Sicherheit davon ausgehen können, dass jemand wirklich tut, was er oder sie sagt. Fehlt uns das Vertrauen, wollen wir uns absichern oder schrecken gar komplett vor einer Interaktion durch. Zum Beispiel gehen wir lieber zu einem Arzt, dem wir vertrauen, während wir bei einem wenig vertrauenswürdigen Arzt oder einer weniger vertrauenswürdigen Ärztin lieber noch eine Zweitmeinung einholen. Ebenfalls verzichten wir bei einer Kaufentscheidung im Zweifel lieber, wenn uns das Produkt oder der Verkäufer oder die Verkäuferin wenig vertrauenswürdig erscheint. Vertrauen ist deshalb für den Unternehmenserfolg ein nicht zu vernachlässigender Faktor.

In unserer Gesellschaft gibt es eine Reihe von Möglichkeiten, das Problem des Misstrauens zu lösen. So müssen wir uns in unserem Alltag die Vertrauensfrage dank Massnahmen der Politik und Wirtschaft nicht ständig stellen. Wenn die Ampel grün ist, können wir ohne Sorge die Strasse überqueren, denn wir vertrauen darauf, dass die Ampeln gut gewartet und gesetzeskonform betrieben werden. Und wir vertrauen darauf, dass sich andere Verkehrsteilnehmende an die Gesetze halten.

In der digitalen Welt sieht es jedoch anders aus. Klar, es gibt zum Beispiel Gesetze zum Datenschutz, aber trotzdem lesen wir immer wieder von Skandalen. Es ist für die Politik schwierig, mit dem rasanten Tempo des technologischen Fortschritts Schritt zu halten. Ausserdem ist gerade für Endnutzer:innen die digitale Welt oft sehr intransparent und schwierig fassbar. Es besteht also umso grösserer Handlungsbedarf.

Deshalb gibt es seit einigen Jahren das Konzept des **Digital Trust**, also des Vertrauens in digitale Dienste. Egal, ob es um das Vertrauen zwischen zwei Firmen oder zwischen einer Firma und ihren Kund:inneen geht: Mit der zunehmenden Bedeutung der Digitalisierung steigt auch die Bedeutung von Digital Trust, insbesondere immer dann, wenn:

- sensible Daten im Spiel sind
- die Konsequenzen der Nutzung eines digitalen Dienstes besonders gross sind
- kaum eine Wahl besteht, ob man einen Dienst nutzen möchte oder nicht
- digitale Dienste zügig und umfassend ausgerollt werden.[2]

Die Bedeutung von Digital Trust wurde z. B. auch durch das **World Economic Forum** erkannt, welches ein entsprechendes **Digital Trust Framework** publiziert hat.[3]

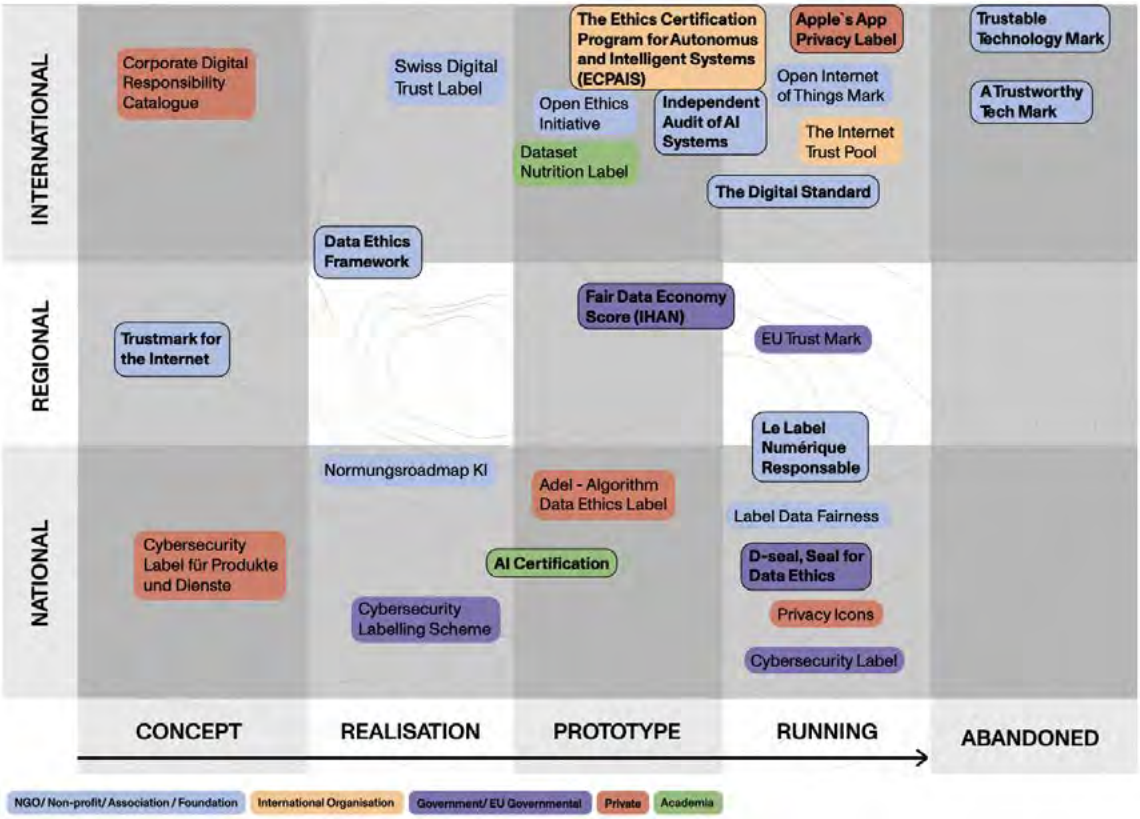
Das WEF reiht sich dabei ein in eine grösser werdende Palette an **Frameworks** und **Initiativen** rund um das Thema Digital Trust. Eine Möglichkeit ist, dass sich Anbieter:innen digitaler Dienste zur Einhaltung gewisser Kriterien verpflichten, wie dies z. B. Salesforce[4] oder Microsoft[5] tun.

Eine weitere Möglichkeit besteht darin, sich bestimmten **Chartas** anzuschliessen, welche typischerweise von Verbänden oder eigens dafür gegründeten Initiativen erarbeitet werden und von Firmen freiwillig übernommen werden. So gibt es z. B. die **Charter of Trust**[6], einen europäischen Zusammenschluss verschiedener Firmen, die sich für einen sicheren und vertrauenswürdigeren digitalen Raum einsetzen wollen.

2 SDI (2021b)
3 WEF (2023) initiatives.weforum.org/digital-trust/framework
4 blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf
5 blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf
6 www.charteroftrust.com

Ausserdem kann man digitales Vertrauen aufbauen, indem man entweder seine Organisation oder einzelne Produkte zertifizieren lässt. Es gibt wenige **Zertifizierungen** auf dem Markt, die sich spezifisch auf das Thema Digital Trust beziehen, z. B. das Digital Trust Label der Swiss Digital Initiative oder das D-Seal[7] aus Dänemark.

Gerade wenn es um die Vertrauenswürdigkeit bestimmter digitaler Technologien wie **künstliche Intelligenz** oder Anwendungen im Bereich des **Internet of Things** geht, gibt es eine Vielzahl an internationalen Projekten, die Firmen helfen können, ihre Produkte möglichst vertrauenswürdig zu gestalten. Die Swiss Digital Initiative hat hierzu einen Bericht und eine interaktive Übersicht erstellt, die frei zugänglich sind.[8]



7 d-seal.eu
8 SDI (2021a) & SDI (2024c)

Fallbeispiel:
Das Digital Trust Label der Swiss Digital Initiative

Möchten wir ein möglichst energiesparsames Auto oder fair gehandelte Lebensmittel kaufen, bieten uns entsprechende Labels eine wichtige Entscheidungshilfe. Das **Digital Trust Label** überträgt diese Hilfe auf die digitale Welt. Es bietet eine einzigartige Zertifizierung für die Vertrauenswürdigkeit eines digitalen Dienstes an. Eine Applikation durchläuft dabei einen unabhängigen Audit, in welchem der **Kriterienkatalog** des Digital Trust Labels überprüft wird.

Dieser Kriterienkatalog wurde in einem mehrstufigen Prozess durch ein internationales **Expertenkomitee** erarbeitet und wurde bis und mit 2024 aktualisiert, um neue technologische und regulatorische Entwicklungen abzubilden, mit dem Ziel, einen hohen Standard sicherzustellen.

Unsere Definition von Digital Trust orientiert sich an den vier Dimensionen:

- **Sicherheit:** Kann mich auf einen bestimmten Sicherheitsstandard verlassen, z. B. verschlüsselte Datenübertragung?
- **Datenschutz:** Wie werden meine Daten geschützt und bearbeitet, wird z. B. meine Einwilligung für die Bearbeitung von Daten eingeholt?
- **Verlässlichkeit:** Wie zuverlässig ist die digitale Anwendung, werden z. B. regelmässige Updates angeboten?
- **Faire Nutzerinteraktion:** Ist der Serviceanbietende transparent in der Kommunikation gegenüber seinen Kund:innen, wird z. B. klargemacht, wenn automatisierte Entscheide getroffen werden?

Das Digital Trust Label bietet sowohl Anbieter:innen digitaler Dienste als auch Endnutzer:innen drei Hauptvorteile:

1. **Einhaltung eines hohen Standards:** Die digitale Anwendung erfüllt die Kriterien des Kriterienkatalogs.
2. **Mehr Transparenz und Information für Nutzer:innen:** Die Nutzer:innen verstehen, was mit ihren Daten geschieht, wenn sie die digitale Anwendung nutzen.
3. **Verantwortungsvolle Unternehmen:** Die Unternehmen zeigen, dass sie ihre Verantwortung gegenüber den Nutzer:innen ihrer digitalen Anwendungen ernst nehmen, und können sich so von ihrer Konkurrenz abheben.

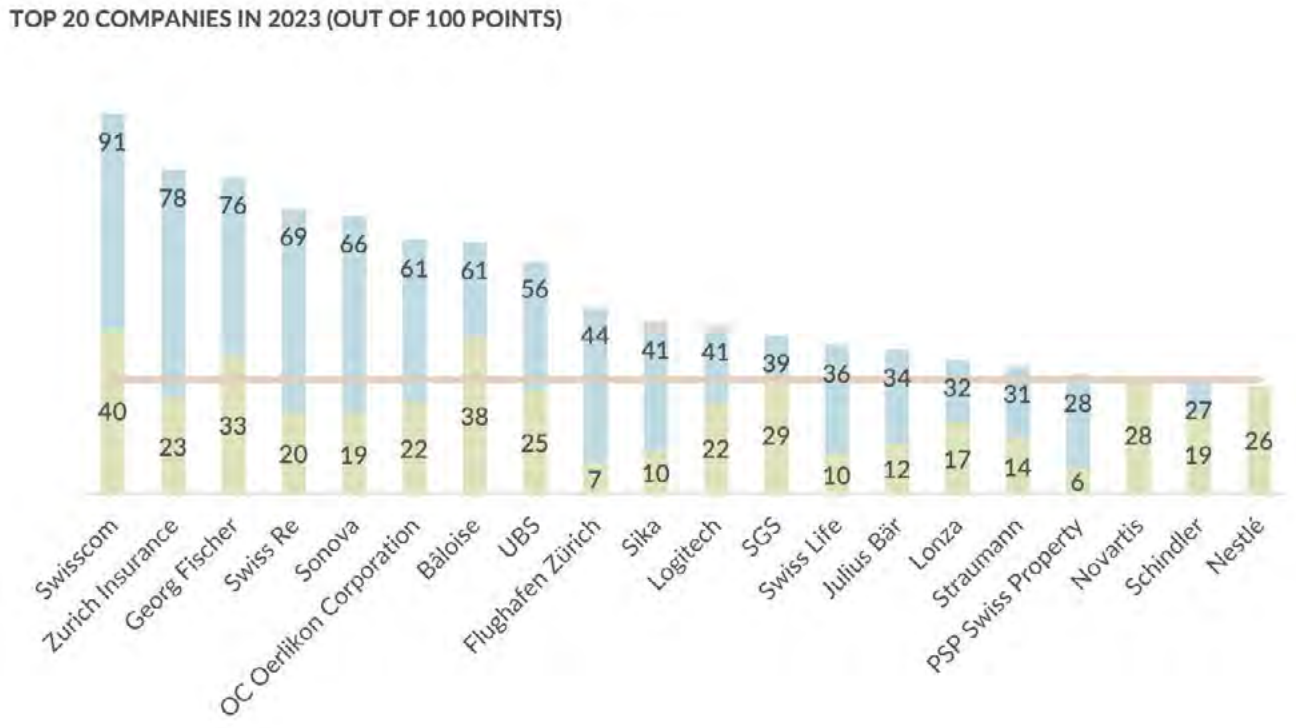
Mehr Informationen unter: swiss-digital-initiative.org

Vertrauenswürdige Digitalisierung: Corporate Digital Responsibility

Eng verwandt mit dem Thema Digital Trust ist das Thema Corporate Digital Responsibility (CDR). Ähnlich wie beim Thema Corporate Social Responsibility geht es hier darum, das Bewusstsein für die Auswirkungen der Digitalisierung zu schärfen.

Auch hier geht es um Frameworks und Chartas, denen man als Unternehmen folgen kann. Beispiele sind das CDR Manifesto[9] oder die Charta für den ethischen Umgang mit Daten von SWICO[10], sowie entsprechende Weiterbildungs- und Beratungsangebote z. B. durch das Centre for Digital Responsibility.[11]

Auch das Thema Corporate Digital Responsibility ist in der Schweiz noch relativ neu, gewinnt aber zunehmend an Bedeutung. Die Anlagestiftung **ethos** recherchiert seit einigen Jahren zur Thematik und untersucht jährlich Schweizer Unternehmen daraufhin, ob sie sich mit der Thematik auseinandersetzen und wie sie das tun. Die Ergebnisse (siehe Grafik) zeigen, dass definitiv noch Luft nach oben besteht. So hält der letztjährige Bericht fest, dass eine steigende Zahl von Firmen an der Umfrage teilnimmt und auch immer aktiver öffentlich zum Thema CDR kommuniziert. Allerdings wollen sich erst wenige Firmen klare Prinzipien beim ethischen Einsatz von künstlicher Intelligenz geben und die Resultate fallen je nach Wirtschaftssektor recht unterschiedlich aus. Es zeichnet sich ein wachsender Graben ab zwischen Firmen, die sich früh mit der Thematik beschäftigt haben und entsprechende Fortschritte zeigen, und anderen Firmen, welche das Thema bisher noch nicht angegangen sind.[12]



9 corporatedigitalresponsibility.net
10 www.swico.ch/de/news/detail/swico-lanciert-eine-charta-fur-den-ethischen-umgang-mit-daten
11 digitalresponsibility.ch/ueber-uns
12 www.ethosfund.ch/sites/default/files/2024-01/CDR%20Study_%202023_EN_FINAL_3.pdf

2022 hat die Swiss Digital Initiative zusammen mit IMD Lausanne ein Corporate Digital Responsibility Starter Kit und einen Bericht erarbeitet, die einen Einstieg in die Materie erlauben.[13] Eine Auseinandersetzung mit den Auswirkungen der Digitalisierung ist nötig, da die Allgegenwärtigkeit und die schnelle Anpassungsfähigkeit digitaler Technologien komplexe Fragen aufwerfen. Dabei geht Corporate Social Responsibility über den Umweltaspekt hinaus, auch wenn dieser sehr wichtig ist und z. B. beim **Institut du Numérique Responsable** im Zentrum steht, welches u. a. einen Fragebogen zur Evaluation des Umweltimpacts der eigenen IT entwickelt hat.[14]

Breiter gedacht befasst sich Corporate Digital Responsibility mit den folgenden Dimensionen:

- **Soziales:** Wie wirkt sich die Nutzung digitaler Technologien auf die Gesellschaft und auf unsere Kunden aus? Hier geht es z. B. um Themen wie Datenschutz oder Privatsphäre, aber auch die Autonomie des Individuums. Schliessen wir gewisse Gruppen durch digitale Dienste aus?
  Beispiel: Wenn bei Die Mobiliar ein Versicherungsantrag, der online eingereicht und digital verarbeitet wird, abgelehnt wird, hat der Kunde, die Kundin die Möglichkeit, mit einem Versicherungsberater zu sprechen, um den Prozess zu verstehen.
- **Wirtschaft:** Hier geht es um den wirtschaftlichen Impact von digitalen Technologien, welche ein Unternehmen nutzt, z. B. den Einfluss von Automatisierung und künstlicher Intelligenz auf den Arbeitsmarkt. Geben wir ökonomische Vorteile durch die Nutzung digitaler Technologien an die Wirtschaft weiter?
  Beispiel: Das Pharmaunternehmen Weleda hat sich dazu verpflichtet, Roboter und Automatisierung nicht in einer Weise einzusetzen, die zu Arbeitsplatzverlust führt, und will stattdessen betroffene Mitarbeitende weiterbilden oder umschulen.
- **Technologie:** Hier geht um die verantwortungsvolle Entwicklung neuer Technologien durch ein Unternehmen. Entwickeln wir z. B. ein KI-System, ohne dabei auf Bias oder Diskriminierung zu achten, oder könnten unsere Produkte missbraucht werden, z. B. für deep fakes?
  Beispiel: Die Deutsche Telekom hat sich bereits früh betriebsinterne Regeln für einen ethischen Umgang und der Entwicklung von künstlicher Intelligenz gegeben.
- **Umwelt:** Hier geht es um das, was umgangssprachlich unter Nachhaltigkeit verstanden wird: um den Einfluss digitaler Technologien auf die Umwelt. Recyclen wir unsere IT-Geräte und versuchen wir möglichst, unsere Datenzentren mit nachhaltiger Energie zu betreiben?
  Beispiel: UBS hat sich im Rahmen ihrer Nachhaltigkeitsziele verpflichtet, den Energiebedarf der IT zu minimieren, und setzt hierbei auf Sensoren in Rechenzentren, um diese möglichst effizient zu betreiben.

13 swiss-digital-initiative.org/corporate-digital-responsibility
14 institutnr.org

Umsetzung

Sowohl bei Digital Trust als auch bei Corporate Digital Responsibility ist es wichtig, diese Themen zur Chefsache zu erklären und in der gesamten Organisation zu leben.

Ein Framework zu identifizieren, was bei über 160 verschiedenen Dokumenten gar nicht so einfach ist,[15] kann dabei nur der erste Schritt sein. Um die beiden Themen erfolgreich in einer Organisation umzusetzen, braucht es neben management attention auch einige weitere Erfolgsfaktoren:

- **Digital Trust & CDR als *enabler* sehen:** Diese Themen ernst zu nehmen ist mit Aufwand verbunden. Doch statt dies als weitere Regulierungs- oder Compliance-Übung zu sehen, sollte man sich vor Augen führen, dass es sich um Investitionen in die Zukunft handelt. Firmen, die glaubwürdig Digital Trust und CDR umsetzen, können davon bei ihrer Kundschaft und anderen Beziehungen profitieren.
- **Transparenz & Aufklärung:** Selbst, wenn man sich nicht zertifizieren lassen möchte oder ein Framework anwendet, so kann man mit klarer Kommunikation schon viel erreichen. Wie gehen wir mit Daten um? Zu welchen Zwecken wollen wir digitale Technologien einsetzen? Verstehen wir, unsere Mitarbeitenden und unsere Kund:innen die entsprechenden Risiken?
- **Klein beginnen, dann aufbauen:** In den meisten Firmen sind die Themen Digital Trust und CDR noch nicht klar verortet. So gibt es z. B. erst wenige Organisationen, die eine Position des *Chief Trust Officers* geschaffen haben. Deshalb können diese Themen am Anfang etwas überfordern. Man kann aber bereits auf Stufe eines Produktentwicklungsteams ein Umdenken anstossen und sich mit den nötigen ethischen Fragestellungen auseinandersetzen.

Quellen

a. SDI (2019). *User Study Digital Trust in Switzerland.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2023/12/User-Study-Digital-Trust-in-Switzerland.pdf

b. SDI (2021b). *Digital Trust Whitepaper.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2023/12/Digital-Trust-Whitepaper.pdf

c. SDI (2021a). *Labels and Certifications for the Digital World.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2023/12/Labels-and-Certification-for-the-Digital-World.pdf

d. SDI (2022a). *Second Public Consultation.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2023/12/Second-Public-Consultation.pdf

e. SDI (2022b). *Co-Development Report.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2023/12/Co-Development-report.pdf

f. SDI (2023). *Digital Trust Guide.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2023/11/2023_Digital-Trust-Guide_Final.pdf

g. SDI (2024a). *Digital Trust Label Criteria Catalogue.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2024/05/2024-Digital-Trust-Criteria-Catalogue-2.pdf

h. SDI (2024b). *Digital Trust Label Interpretation Guidelines.* Retrieved from swiss-digital-initiative.org/wp-content/uploads/2024/04/2024_DTL_Criteria-Interpretation-Guidelines.pdf

i. SDI (2024c). *Overview of Digital Trust Initiatives.* Retrieved from airtable.com/appScluR9PDVE7fE3/shrJXQG1zNQlGaVR9

j. McKinsey (2022). *Why digital trust truly matters.* Retrieved from www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

k. Workday (2024). *Closing the AI trust gap – key findings.* Retrieved from forms.workday.com/en-us/other/closing-the-ai-trust-gap/form.html?eid=enus_pr_pr_wd_wds_cxoedu_ig_23.5595&productfocus=wds&aud=cxoedu&assetype=ig&assetid=23.5595&pblr=wd&step=step1_default

15 Global AI Ethics Inventory von AlgorithmWatch: inventory.algorithmwatch.org