DIGITALES VERTRAUEN HERSTELLEN

cscp

gefördert durch

DBU
Deutsche
Bundesstiftung Umwelt

Einleitung

Für Unternehmen bedeutet der digitale Wandel neuen Wettbewerb: um effizientere Produktions- und Geschäftsprozesse, um neue daten- und plattformbasierte Geschäftsmodelle sowie um die Gewinnung und Bindung von – nicht zuletzt – IT-Fachkräften. Dabei ist es wichtig, dass Kund:innen und Verbraucher:innen der Verlässlichkeit, Sicherheit und Fairness bei der Datennutzung und den Entscheidungen von Algorithmen vertrauen. Schwindet dieses Vertrauen, ist der nachhaltige Unternehmenserfolg gefährdet. Infolge der Berichterstattung über moralisch bedenkliche und mitunter illegale Datenerhebungs- und Nutzungspraktiken sowie über groß angelegte Cybersicherheitsprobleme und Datendiebstähle ist die Frage des digitalen Vertrauens auch in breiteren Bevölkerungs- und Konsumentengruppen angekommen. Auch wenn mit der bestehenden Regulatorik wie z. B. der EU-Datenschutzgrundverordnung DSGVO ein Mindeststandard existiert, ist es für Kund:innen und Verbraucher:innen herausfordernd bzw. nur mit hohem Aufwand einsehbar und verständlich, welche Daten von ihnen erhoben, verarbeitet und weitergegeben werden. Wie sie vor nachteiliger oder gar missbräuchlicher Nutzung geschützt werden, bleibt meistens im Dunkeln.[1]

In der Schweiz wurde das weltweit erste *Digital Trust Label* seiner Art entwickelt, dessen Funktion von seinen Entwickler:innen sinnbildlich wie folgt beschrieben wird: „Das digitale Vertrauenssiegel ist eine Kombination aus einem Biosiegel und einer Nährwerttabelle für die digitale Welt. Das Siegel zeigt, dass ein digitaler Dienst verbindliche Kriterien erfüllt, und bietet den Nutzern gleichzeitig mehr Informationen und Transparenz über vier Dimensionen des digitalen Dienstes“.[2] Die folgenden Aktionsfelder und Leitfragen[3] orientieren sich an den vier Dimensionen dieses Labels und ermöglichen Unternehmen, sich strukturiert mit den zugehörigen Nachhaltigkeitschancen bzw. -risiken zu befassen.

1) Dörr, Praxisleitfaden Corporate Digital Responsibility, 2020
2) Swiss Digital Initiative, 2021
3) Mittelstand 4.0-Kompetenzzentrum eStandards, 2021 & Dörr, Praxisleitfaden Corporate Digital Responsibility, 2020

Sicherheit

Wie stellen wir die Sicherheit unserer technischen Systeme z. B. gegen Datendiebstahl, Manipulation oder Bedien- und Konfigurationsfehler sicher?

Datenschutz

Inwieweit gehen unsere Daten- und Persönlichkeitsschutzvorkehrungen über eine compliance-basierte Umsetzung der DSGVO hinaus?

Verlässlichkeit der Services

Sind die gängigen Szenarien für Störungen und Ausfälle der Serviceerbringung bedacht?

Faire Benutzerinteraktion

Wie können wir digitale Produkte und Dienstleistungen gestalten, die wirtschaftlich erfolgreich sind und zugleich grundlegende Werte wie Privatheit, Selbstbestimmung und Fairness stärken?

Aktionsfelder

Sicherheit

Grundlage für das digitale Vertrauen von Kund:innen, Lieferant:innen und der eigenen Belegschaft ist ein zuverlässiges und sicheres IT-System. Cyberangriffe auf Unternehmen sind mehr die Norm als eine Besonderheit. So sind neun von zehn Unternehmen in den letzten 12 Monaten Opfer eines IT-Angriffs geworden.[4] Durch die Verlagerung vieler Tätigkeiten in das Home-Office sind zudem neue vulnerable Schnittstellen zu internen Datensystemen entstanden.[5] Die Folgen für Unternehmen reichen von kleineren Störungen im Betriebsablauf, über Reputationsschäden bis hin zu gesetzlichen Haftungsansprüchen, wenn Kundendaten nicht hinreichend geschützt werden.[6] Die durchschnittlichen Kosten eines erfolgreichen Cyberangriffs betragen für KMU ca. 100.000 Euro. Bei größeren Unternehmen liegen die Kosten mit rund 1 Mio. Euro sogar noch erheblich höher.[7]

Vor dem Hintergrund gilt eine Dateninventur, mit dem Ziel eine vollständige Übersicht über alle relevanten Datenbestände im Unternehmen zu schaffen, als sinnvoller Startpunkt für eine Sicherheitsstrategie und daraus abgeleitete Maßnahmen.[8] Bei

4) Bitkom, 2021
5) Bitkom, 2020
6) Bitkom, 2021
7) Kaspersky, 2021
8) Cooper, Maitland, Sio, & Wei, 2015

der Zugangskontrolle zu den Systemen, auf denen die Unternehmensdaten verwaltet werden, ist eine Nutzer:innen-Authentifizierung sicherzustellen. Sowohl für die interne als auch die externe Kommunikation ist der Einsatz von Zertifikaten und Kryptographie zu empfehlen. Neben der regelmäßigen Wartung der Hardware und der Aktualisierung der Software sollte ein kontinuierliches Sicherheitsmonitoring und -reporting erfolgen und über einschlägige Störfälle, Angriffe und Sicherheitslücken informieren. Da ein entsprechendes IT-Sicherheitsmanagement limitiert verfügbare Fachexpertise erfordert, sollte die Entscheidung über das In- bzw. Outsourcing der IT bzw. der IT-Sicherheit mit der gebotenen Sorgfalt erfolgen.[9] Gerade weniger IT-erfahrene KMU haben dabei mitunter primär die Sicherheit der selbst verwalteten IT-Infrastruktur im Blick, aber auch smarte Geräte im Büro des Unternehmens bzw. im Home-Office der Mitarbeitenden können Sicherheitslücken darstellen, weil diese häufig geringere Sicherheitsstandards erfüllen.[10]

Schlüsselbegriffe: **Hackerangriffe** **Kryptographie** **Authentifizierung** **Smarte Geräte**

→ GOOD PRACTICE **Sicherheit & Datenschutz bei WEtell**[11]

Der grüne Mobilfunkanbieter WEtell bietet die verschlüsselte Speicherung der Kundendaten an. Das Unternehmen versucht die Anzahl der Dienstleister, mit denen es zusammenarbeitet, so gering wie möglich zu halten. Diese strategische Entscheidung zielt darauf ab, die personenbezogenen Daten vor Zugriffs- und Verarbeitungsrechten Dritter zu schützen. Sowohl in der internen Kommunikation als auch im Service verwendet WEtell Ende-zu-Ende-Verschlüsselung für ein hohes Maß an Datensicherheit.

9) Cooper, Maitland, Sio, & Wei, 2015
10) Dörr, Praxisleitfaden Corporate Digital Responsibility, 2020
11) WEtell, 2021

Unternehmerische Aktivitäten für mehr Datenschutz sind wegen technologischer Abhängigkeiten eng mit den Sicherheitsaspekten der IT-Systeme verbunden. Aus Kundenperspektive ist der Datenschutz ein zentrales Anliegen. Neben der selbstverständlichen Einhaltung gesetzlicher Regelungen wird erwartet, dass Unternehmen darüber hinaus proaktiv tätig werden, also freiwillig die Anforderungen der DSGVO übertreffen.[12] Unternehmen haben diesen Bedarf erkannt und adressieren ihn z. B. mit einem klaren Bekenntnis zum Datenschutz und Maßnahmen wie regelmäßig aktualisierten Risikobewertungen oder der Pseudonymisierung von Daten.[13] Die gesetzlichen Anforderungen der DSGVO sind mit Bezug auf die Speicherung, Nutzung und Weitergabe von personenbezogenen Daten klar abgesteckt. Darüber hinaus sollten Unternehmen Werte und Prinzipien definieren, die den Datenschutz und die zugehörige Kommunikation mit den Kund:innen im Grundsatz vorgeben. Diese sollten sich dann auch in den Datenschutzrichtlinien des Unternehmens wiederfinden und den Kund:innen gut verständlich erläutern, wie Daten gesammelt, gespeichert und genutzt werden. Als besonders wichtig gelten die bereits angesprochene Anonymisierung der Kundendaten, die Angabe der Verwendungszwecke und Angaben zur Dauer der Speicherung. Neben der Einverständniserklärung der Kund:innen sollte das Unternehmen seine Werte und Aktivitäten bezüglich des Datenschutzes auch offen kom-

12) KPMG, 2020
13) Esselmann, Golle, Thiel, & Brink , 2020

munizieren. Ansätze, die über die gesetzlichen Mindestanforderungen hinaus gehen, bieten zunehmend – auch über klassische Anwendungen wie Internetbrowser und Suchmaschinen hinaus – Differenzierungspotential im Wettbewerb und machen sich z. B. an der zunehmenden Anwendung und Verbreitung so genannter Privacy-by-Design-Ansätze bemerkbar, die bereits frühzeitig in der Entwicklungsphase ansetzen.[14] Aspekte, auf die KMU als Auftraggeber beim Einkauf bzw. der Beauftragung von Neuentwicklungen achten können.

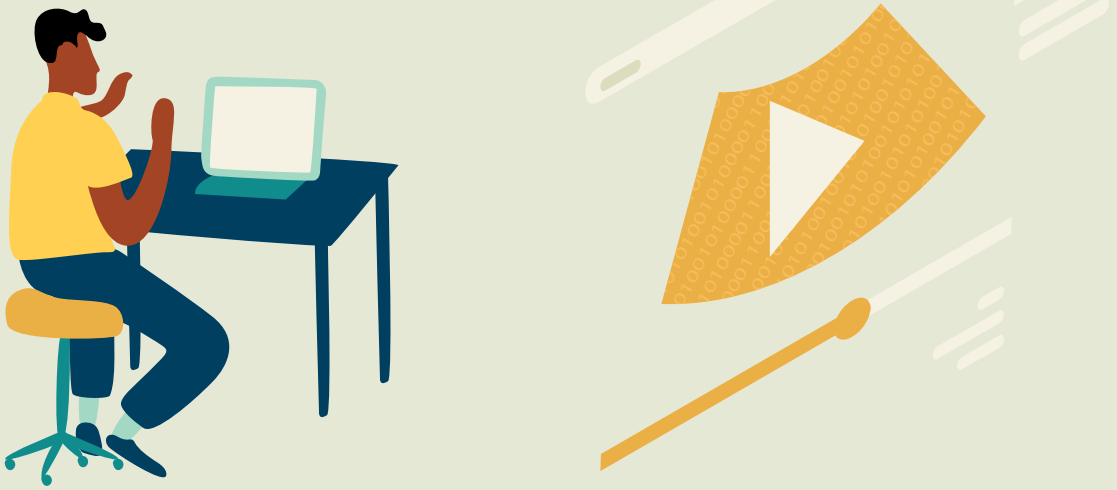
Schlüsselbegriffe: Datenschutzrichtlinien | Einverständniserklärung | Anonymisierung | Privacy-by-Design

→ GOOD PRACTICE **Datenschutz bei WECHANGE[15]**

WECHANGE bietet das Hosting von Online-Communities auf einer Plattform an und ist in einem Genossenschaftsmodell organisiert. Die Communities können die Vergabe von Zugriffsrechten auf der Datenplattform selbst regeln. Neben der direkten Mitbestimmung der Kund:innen beim Schutz der Daten, bietet das Genossenschaftsmodell die Möglichkeit, die üblichen Marktzwänge datengetriebener Geschäftsmodelle zu umgehen.

14) Deloitte, 2021
15) WECHANGE, 2021

Zuverlässigkeit



Digitale Dienstleistungen müssen genauso wie physische Produkte zuverlässig verfügbar sein und funktionieren. Dies gilt umso mehr für geschäftskritische und sicherheitsrelevante IT-Systeme. Gegen eine Unterbrechung oder den Ausfall der Serviceerbringung sind entsprechende Maßnahmen in der IT-Infrastruktur zu implementieren und Echtzeit Back-Ups aufzuzeichnen.[16] Auch unerwünschte Interaktionseffekte der eigenen Services mit anderen Applikationen, Produkten oder Systemen sind in der Design-Phase, bei der Wartung und bei Updates zu berücksichtigen.

Zusammen mit sicheren IT-Systemen und dem Schutz von Kundendaten führt eine reibungslose Interaktion aller Anspruchs- und Interaktionsgruppen mit internen Systemen zu Vertrauen in den digitalen Service.[17]

Schlüsselbegriffe: Nutzererlebnis | Performance | Backups

16) Swiss Digital Initiative, 2021
17) Dörr, Corporate Digital Responsibility, 2020

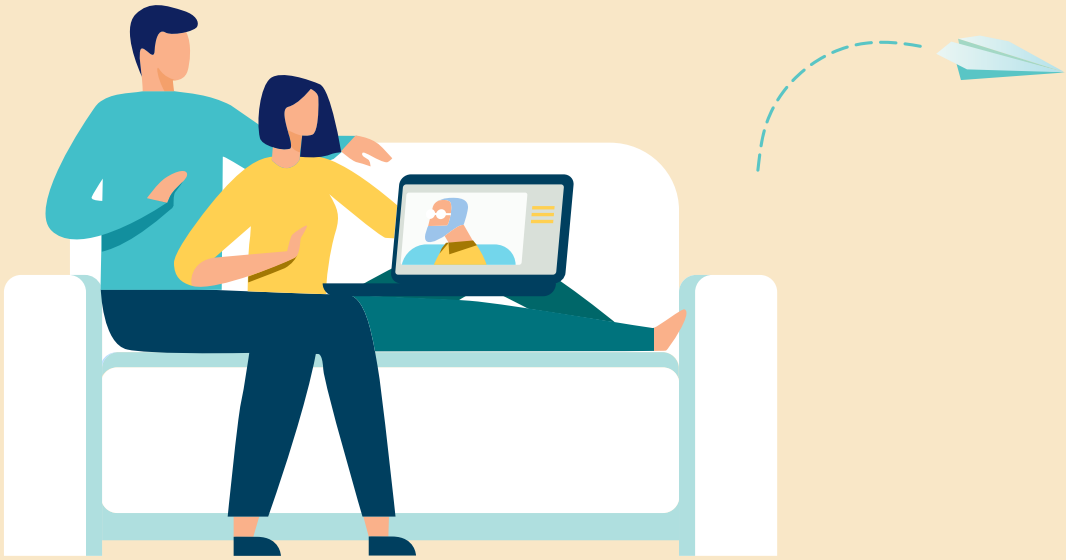
→ GOOD PRACTICE

Cloud Service Plattform für 5G bei der Engineering ITS GmbH[18]

Das Unternehmen bietet eine Cloud-Service-Plattform mit einem Betrieb auf verteilten EDGE Cloud Infrastrukturen für die Entwicklung von digitalen Services in den Bereichen der 5G-Rettungsmobilität und Gesundheit. Durch die Cloud Lösung und hohe Übertragungsraten stehen Echtzeitinformationen zuverlässig im Stream zur Verfügung und vereinfachen die Rettungseinsätze.

18) Bundesverband Digitale Wirtschaft (BVDW) e.V., 2021

Faire Benutzerinteraktion



Kund:innen legen viel Wert auf den Respekt ihrer Privatsphäre und fordern Kontroll- und Verwaltungsoptionen für sie betreffende Daten im Unternehmen ein.[19] Die Stärkung der Daten-Souveränität von Nutzer:innen digitaler Services wird unter dem Begriff Digital Empowerment diskutiert.[20] Neben der Möglichkeit, die Berechtigungen zur Datennutzung besser zu kontrollieren, steht die Berücksichtigung von Anregungen und Beschwerden von Nutzer:innen in einem Dialog auf Augenhöhe im Mittelpunkt. Zudem ist den Abfragen von Kund:innen nach ihren Daten mit Bezug auf die DSGVO möglichst übersichtlich und einfach verständlich nachzukommen, um Nutzer:innen, die geringere digitale Kenntnisse haben, nicht zu überfordern. Auf Websites und in Kundenprofilen sollten die Einstellungen zur Datenspeicherung und -nutzung gut ersichtlich platziert werden und die Voreinstellung nach dem Prinzip der Datensparsamkeit vorkonfiguriert sein.[21] Wenn sich Kund:innen dafür entscheiden mehr Daten zu teilen, sollte auch erklärt und sichtbar gemacht werden, welche Vorteile sich aus Perspektive der Kund:innen daraus ergeben.[22] Digitales Vertrauen kann gestärkt werden, indem neben automatisierten Kommunikationskanälen, bspw. durch Chatbots oder Hotlines, immer auch eine Option zum direkten Gespräch mit Kundenbetreuer:innen besteht. Wenn das Unternehmen automatisierte, algorithmische Entscheidungsprozesse in der Kundeninteraktion nutzt, ist bei der Anwendung auf Diskriminierungsfreiheit und Inklusion aller Nutzer:innengruppen zu achten. Wenn

19) KPMG, 2020
20) Herden, et al., 2021
21) Cooper, Maitland, Sio, & Wei, 2015
22) Dörr, Corporate Digital Responsibility, 2020

diese gar unternehmensintern entwickelt werden, bieten einschlägige, beispielsweise unter dem Begriff Privacy- and Ethics-by Design diskutierte Leitlinien zu ethischer KI eine wichtige Hilfestellung. Für KMU, die KI-basierte Anwendungen von Drittanbietern nutzen, bieten am Markt verfügbare Labels wie das KI-Ethik Label der Bertelsmann Stiftung und VDE eine Hilfestellung.[23]

Schlüsselbegriffe: Privacy- and Ethics-by Design | Diskrimierungsfreiheit | KI-Label

→ GOOD PRACTICE **Corporate Digital Responsibility bei Weleda[24]**

Der Naturkosmetikhersteller Weleda hat einen Corporate Digital Responsibility (CDR) Council ins Leben gerufen und 15 ethische Prinzipien zur digitalen Unternehmensverantwortung entwickelt. Im Kontext von fairen Nutzerinteraktion werden z. B. die folgenden ethischen Prinzipien aufgeführt: *Privatsphäre aller Beteiligten schützen und respektieren, Datenverwendung & Algorithmen transparent gestalten und Entscheidungskompetenz beim Menschen belassen.*

23) Leitert, 2020
24) Weleda AG, 2021

Erste Schritte

Verschaffen Sie sich einen Überblick über alle relevanten Datenbestände
Bevor Sie Maßnahmen für digitales Vertrauen einleiten, ist es notwendig, alle personenbezogenen Daten, die das Unternehmen sammelt, zu erfassen und zu kategorisieren. Bewerten Sie hierbei auch die Sicherheitsrisiken die sich aus Datenschnittstellen, Speicherort und Zugriffsrechten der Datensätze ergeben.

Halten Sie Ihr IT-System auf dem aktuellsten Stand und nutzen Sie kostenlose öffentliche Beratungs- und Hilfsangebote
Für das Aktionsfeld Sicherheit können Sie beispielsweise auf das Tool Secure-o-mat[25] oder die Beratungs- und Informationsangebote für Unternehmen des Bundesamts für Sicherheit in der Informationstechnik[26] zurückgreifen.

Berücksichtigen Sie die Interessen verschiedener Anspruchsgruppen in Ihrem Ansatz zur Schaffung und Erhaltung von digitalem Vertrauen:

- *Mitarbeiter:innen* müssen sensibilisiert und ihre Kompetenzen den Anforderungen entsprechend erweitert werden.
- Kund:innen sollten ihr Kundenprofil selber und einfach konfigurieren können und ihnen sollte stets die Möglichkeit zum Direktkontakt mit qualifizierten Ansprechpartner:innen ermöglicht werden.
- *IT-Service Anbieter:* Wie bei der Auslagerung von IT-Funktionen in Cloud Systeme, sind beim Fremdbezug von Daten die Nutzungsbedingungen auf ihre Auswirkungen auf die eigene Datensicherheit und letzten Endes auf das digitale Vertrauen in das Unternehmen hin, zu prüfen. Wie bei einem physischen Produkt besteht die Notwendigkeit eines Data Supply Chain Management[27].
- *Gesellschaft:* Überprüfen Sie Ihre nicht-sensiblen Geschäftsdaten daraufhin, ob es möglich ist, sie für eine öffentliche Nutzung z. B. durch Forschungsinstitute und andere gemeinnützige Organisationen freizugeben und inwieweit Partnerschaften zu den Themen einer nachhaltigen Digitalisierung möglich sind.

→ **IHR ANSPRECHPARTNER** **Mike Tabel**

mike.tabel@cscp.org

25) Transferstelle IT-Sicherheit im Mittelstand, 2021
26) Bundesamt für Sicherheit in der Informationstechnik, 2021
27) KPMG, 2020

Literatur

- Bitkom e.V. (2021). Wirtschaftsschutz 2021. Abgerufen am 2. Dezember 2021 von *https://www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf*
- Bitkom e.V. (2020). Bitkom zum Lagebericht der IT-Sicherheit. Abgerufen am 2. Dezember 2021 von *https://www.bitkom.org/Presse/Presseinformation/Bitkom-zum-Lagebericht-der-IT-Sicherheit*
- Bundesamt für Sicherheit in der Informationstechnik. (2021). Abgerufen am 2. Dezember 2021 von Unternehmen und Organisationen: *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html;jsessionid=31370348EC56FDBD9CC5EC93463C0CF9.internet482*
- Bundesverband Digitale Wirtschaft (BVDW) e.V. (2021). Corporate Digital Responsibility Award 2021 Shortlist. Abgerufen am 2. Dezember 2021 von *https://www.cdr-award.digital/shortlist-2021/#1637058464203-4-2*
- Cooper, T., Maitland, A., Sio, J., & Wei, K. (2015). Accenture - Guarding and Growing personal data value. Abgerufen am 2. Dezember 2021 von *https://www.yumpu.com/en/document/read/42457948/accenture-guarding-and-growing-personal-data-value-narrative-report*
- Deloitte. (2021). Privacy by Design - Setting a new standard for privacy certification. Abgerufen am 2. Dezember 2021 von *https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF*
- Dörr, S. (2020). Von Corporate Digital Responsibility. Abgerufen am 2. Dezember 2021 von *https://wiseway.de/wp-content/uploads/2020/11/Dr_Saskia_Doerr_CDR_final.pdf*
- Dörr, S. (2020). Praxisleitfaden Corporate Digital Responsibility. Berlin, Heidelberg: Springer.
- Esselmann, F., Golle, D., Thiel, C., & Brink , A. (2020). Corporate Digital Responsibility – Unternehmerische Verantwortung als Chance für die deutsche WIrtschaft. Garching: Zentrum Digitalisierung Bayern.
- Herden, C., Allio, E., Cakici, A., Cormier, T., Deguelle, C., & Gambhir, S. (2021). Corporate Digital Responsibility. NachhaltigkeitsManagementForum 29 (1), 12-29.
- KPMG. (2020). The new imperative for corporate data responsibility. Abgerufen am 2. Dezember 2021 von The new imperative for corporate data responsibility: *https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf*
- Kaspersky. (2021). Abgerufen am 2. Dezember 2021 von How businesses can minimize the cost of a data breach: *https://www.kaspersky.com/blog/it-security-economics-2020-part-2/*
- Leitert, S. (2. April 2020). Bertelsmann Stiftung und VDE stellen neues KI-Ethik-Label vor. Abgerufen am 2. Dezember 2021 von *https://corporate-digital-responsibility.de/article/neues-ki-ethik-label/*
- Swiss Digital Initiative. (2021). The Digital Trust Label by the Swiss Digital Initiative. Abgerufen am 2. Dezember 2021 von *https://www.swiss-digital-initiative.org/digital-trust-label/*, zuletzt aktualisiert am 06.08.2021
- Transferstelle IT-Sicherheit im Mittelstand. (2021). TISiM - Sec-O-Mat. Abgerufen am 2. Dezember 2021 von *https://www.sec-o-mat.de/*,
- WECHANGE. (2021). Über uns. Abgerufen am 2. Dezember 2021 von *https://wechange.de/cms/genossenschaft/*
- WEtell. (2021). Datenschutz. Abgerufen am 2. Dezember 2021 von *https://www.wetell.de/vision/datenschutz/*
- Weleda AG. (2021). Die digitale Unternehmensverantwortung der Weleda AG. Abgerufen am 2. Dezember 2021 von *https://sway.office.com/v72SfTyDzBpQvvo0?ref=Link*

Impressum

Herausgeber

Collaborating Centre on Sustainable Consumption and Production (CSCP) gGmbH
Das Collaborating Centre on Sustainable Consumption and Production (CSCP) ist ein internationaler, gemeinnütziger Think and Do Tank mit Sitz in Wuppertal, der mit politischen Entscheidungsträger:innen, Unternehmen, Partnerorganisationen und der Zivilgesellschaft an einem guten Leben in den planetaren Grenzen arbeitet. Mit diversen Projekten sowohl auf lokaler, nationaler als auch internationaler Ebene setzen wir uns im Einklang mit dem Europäischen Grünen Deal dafür ein, die Potentiale der Digitalisierung als Wegbereiter für die sozial-ökologische Transformation unserer Wirtschaft und Gesellschaft zu heben.

Autoren Arne von Hofe & Mike Tabel
Layout Eva Rudolf (CSCP)
Grafiken basierend auf: © by shutterstock / Viktoria Kurpas, © by shutterstock / alexdndz, © by shutterstock / GoodStudio, © by shutterstock / Rawpixel.com, © by shutterstock / TatiVovchenko, © by shutterstock / mangsaabguru, © by shutterstock / Unitone Vector

Kontakt *arne.vonhofe@cscp.org*

Bitte die Publikation folgendermaßen zitieren:
von Hofe, A. & Tabel, M. (2022): „Charta für nachhaltige Digitalisierung“, Collaborating Centre on Sustainable Consumption and Production (CSCP)

Wuppertal, Januar 2022

Gefördert durch die Deutsche Bundesstiftung Umwelt (DBU)

Deutsche
Bundesstiftung Umwelt