CORRELAID

GOOD CAUSES. BETTER EFFECTS.

Datenschutz und -Ethik

Wie wir verantwortungsbewusst mit Daten umgehen

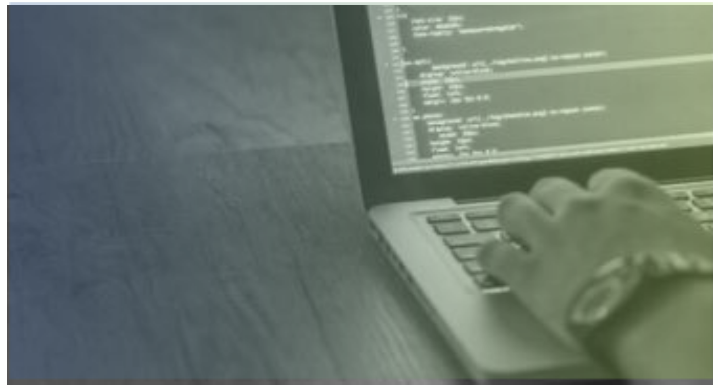
- 2,5h -

Wer wir sind

Wir sind ein deutschlandweites Netzwerk von über 1,700 Datenwissenschaftler:innen, die die Welt durch und mit Daten verbessern wollen.

#MetaWeltretter

Unsere Mission

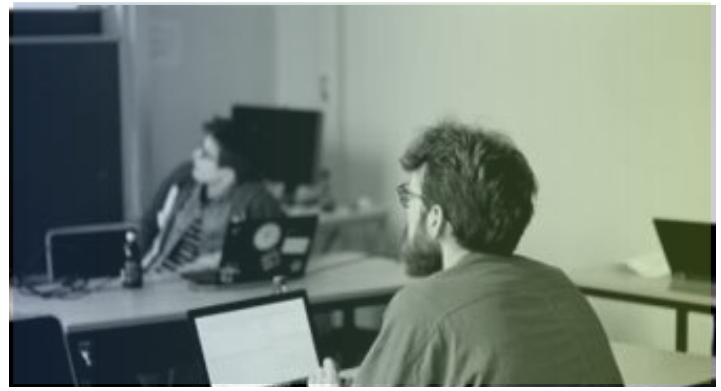


PROJEKTE

Wir führen pro-bono Datenanalyseprojekte für gemeinnützige Organisationen durch.

BILDUNG

Wir vernetzen engagierte sozial denkende Datenanalyst:innen und bieten ihnen Möglichkeiten ihr Wissen anzuwenden und zu erweitern.



DIALOG

Wir treten in den Dialog über den Wert und Nutzen von Daten und Datenanalysen für das Gemeinwohl

Inhalte

Themen	Methodik	Zeitaufwand
Einführung in Datenschutz und Datenethik		60min
Übungsblatt Datenschutz und Datenethik		45min
Q&A Datenschutz und Datenethik (Do, 22.04.21, 18 Uhr)		45min

“Datenschutz ist was Neues!”

Myth Buster
Edition Datenschutz

1977

Erstes Bundesdatenschutzgesetz wird verabschiedet

- Titel: Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung
- Hintergrund: Verwaltungen nutzen beispielsweise im Steuerwesen zunehmen automatisierte Datenverarbeitung
- Zweck: Schutz der Bürger:innen vor Informationsmacht und Privatsphäreneingriffe des Staates

1983

Volkszählungsurteil des Bundesverfassungsgerichts

- Das Recht auf informationelle Selbstbestimmung leitet sich laut dem BVerG aus Art.1 I, der Würde des Menschen, und Art 2. I, das Recht auf freie Entfaltung der Persönlichkeit, her
- Damit ist es ein Fall des allgemeinen Persönlichkeitsrechts
- Um dieses Verständnis wird 1990 auch das BDSG ergänzt

„Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

2006

Aufnahme der Informations-freiheit in das BDSG

Jede natürliche Person hat nun das Recht, sich an den Bundes-beauftragten für Datenschutz und Informationsfreiheit zu wenden, wenn sie der Auffassung ist, dass ihr Recht auf Informationszugang nicht hinreichend beachtet wurde

2016

Datenschutz-Grundverordnung der EU tritt in Kraft

- Nachdem bereits 1995 ein einheitliches Gesetz zum Datenschutz auf EU-Ebene veröffentlicht wurde, passt sich die Gesetzgebung nun Digitalisierung und Globalisierung an
- Seit 2018 gelten nun Auskunfts- und Nachweispflicht – und Verstöße gegen den Datenschutz werden richtig teuer

heute

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Quellen: 27. Januar 1977: Das Bundesdatenschutzgesetz wird verabschiedet, BPD, 27.01.2017, abgerufen am 01.04.21 unter diesem Link.
Leitsätze zum Urteil des Ersten Senats vom 15. Dezember 1983, Bundesverfassungsgericht, 15. Dezember 1983, abgerufen am 01.04.21 unter diesem Link.

Das Recht auf informationelle Selbstbestimmung ergibt sich also aus der Verfassung

Deutscher Bundestag

Parlament

Dem DEUTSCHEN

I. Die Grundrechte

Artikel 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

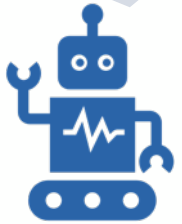
Artikel 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Allgemeines Persönlichkeitsrecht (APR)

Als verantwortungsbewusste Datenwissenschaftler:innen schützen wir die verfassungsrechtlich garantierten Persönlich-keitsrechte (Datenschutz) durch strukturelle Maßnahmen und eine funktionierende IT (Datensicherheit)



CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Quelle: Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 u. 2 Satz 2 des Gesetzes vom 29. September 2020 (BGBl. I S. 2048) geändert worden ist Webauftritt des Deutschen Bundestags, abgerufen am 01.04.21 unter diesem Link.

Die Neuerung durch die DSGVO ist für digital- und datenorientierte Organisationen kein beliebtes Thema

bitkom

Pressebereich › Zwei Jahre DS-GVO: Bitkom zieht durchwachsene Bilanz

Zwei Jahre DS-GVO: Bitkom zieht durchwachsene Bilanz

- **Berg: „Corona zeigt: Unser bislang gut ausbalanciertes System an Freiheits- und Schutzrechten ist aus den Fugen geraten."**
- **8 von 10 Unternehmen sehen Datenschutz als größte Hürde für Einsatz neuer Technologien**

Berlin, 20. Mai 2020 - Seit knapp zwei Jahren gilt die EU-Datenschutz-Grundverordnung. Unternehmen und Organisation haben dadurch u.a. erweiterte Informationspflichten, müssen Verarbeitungsverzeichnisse für Personendaten erstellen sowie Datenschutz schon in Produktionsprozessen berücksichtigen.

Dazu erklärt Bitkom-Präsident Achim Berg:

„Die Corona-Krise zeigt, welche herausragende Bedeutung der Datenschutz in Deutschland inzwischen hat. Dabei dominiert der Datenschutz selbst in dieser Krisensituation viele weitere Rechte wie das Recht auf körperliche Unversehrtheit, Versammlungsfreiheit, Gewerbefreiheit oder den Zugang zu schulischer Bildung. So werden einerseits weitgehende Einschränkungen von Grundrechten akzeptiert, gleichzeitig scheiterte die Veröffentlichung einer von vielen Einschränkungen befreienden Tracing-App an Datenschutzbedenken. Schulen können ihren Unterrichtsbetrieb nicht wieder aufnehmen und verlieren zu vielen Schülern einen funktionierenden Kontakt, gleichzeitig wird Lehrern der Einsatz vieler gut funktionierender Videoplattformen mit Hinweisen auf Datenschutzprobleme kategorisch verboten. Offenkundig ist das bislang gut ausbalancierte System an Freiheits- und Schutzrechten mit der DS-GVO aus den Fugen geraten.

„Die Corona-Krise zeigt, welche herausragende Bedeutung der Datenschutz in Deutschland inzwischen hat. Dabei dominiert der Datenschutz selbst in dieser Krisensituation viele weitere Rechte wie das Recht auf körperliche Unversehrtheit, Versammlungsfreiheit, Gewerbefreiheit oder den Zugang zu schulischer Bildung. So werden einerseits weitgehende Einschränkungen von Grundrechten akzeptiert, gleichzeitig scheiterte die Veröffentlichung einer von vielen Einschränkungen befreienden Tracing-App an Datenschutzbedenken. Schulen können ihren Unterrichtsbetrieb nicht wieder aufnehmen und verlieren zu vielen Schülern einen funktionierenden Kontakt, gleichzeitig wird Lehrern der Einsatz vieler gut funktionierender Videoplattformen mit Hinweisen auf Datenschutzprobleme kategorisch verboten. Offenkundig ist das bislang gut ausbalancierte System an Freiheits- und Schutzrechten mit der DS-GVO aus den Fugen geraten."

Achim Berg
Bitkom Präsident

Quelle: Zwei Jahre DS-GVO: Bitkom zieht durchwachsene Bilanz, Krösmann & Weiß, bitkom Presse, 20.05.20, abgerufen am 01.04.21 unter diesem Link.

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Doch trotz aller derzeitigen Hürden sehen die deutschen Unternehmen den Datenschutz positiv

bitkom

Pressebereich › Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen

Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen

- **20 Prozent haben Datenschutz-Grundverordnung inkl. Prüfprozesse umgesetzt**
- **Homeoffice-Tools wegen Datenschutzanforderungen eingeschränkt**
- **Eigene Corona-Apps für Unternehmen kein Thema**

Berlin, 29. September 2020 - Im Pandemiejahr 2020 erschweren Datenschutzanforderungen vielen Unternehmen die Aufrechterhaltung ihres Betriebs. So greifen viele Unternehmen aus Datenschutzgründen nur eingeschränkt oder gar nicht auf digitale Anwendungen zur Zusammenarbeit im Homeoffice zurück. Zudem kämpft die große Mehrheit auch mehr als zwei Jahre nach Geltungsbeginn noch mit der Umsetzung der Datenschutz-Grundverordnung (DS-GVO). Das sind Ergebnisse einer repräsentativen Befragung unter mehr als 500 Unternehmen in Deutschland, die der Digitalverband Bitkom im Rahmen seiner Privacy Conference vorgestellt hat. Demnach hat nur jedes fünfte Unternehmen (20 Prozent) die DS-GVO vollständig umgesetzt und auch Prüfprozesse für die Weiterentwicklung etabliert. Mehr als ein Drittel (37 Prozent) hat die Regeln größtenteils umgesetzt, ähnlich viele (35 Prozent) teilweise. Und 6 Prozent haben gerade erst mit der Umsetzung begonnen. „Die immer noch niedrigen Umsetzungszahlen sind ernüchternd", sagt Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung. „Die Datenschutz-Grundverordnung lässt sich nun einmal nicht wie ein Pflichtenheft abarbeiten. Im Gegenteil: Durch unklare Vorschriften und zusätzliche Anforderungen der Datenschutzbehörden ist aus der DS-GVO ein Fass ohne Boden geworden." Das bestätigen die befragten Unternehmen nahezu einhellig. 89 Prozent meinen: Die Datenschutz-Grundverordnung ist praktisch nicht vollständig umsetzbar.

20 Prozent (!) der Unternehmen haben die DSGVO komplett umgesetzt

89 Prozent der Unternehmen geben an, die DSGVO ist praktisch nicht vollständig umsetzbar

74 Prozent der Unternehmen beklagen eine anhaltende Rechtsunsicherheit

56 Prozent geben an, dass neue innovative Projekte aufgrund der DSGVO scheiterten

23 Prozent verzichtet auch in Zeiten von Home Office wegen der DSGVO auf Kollaborationstools

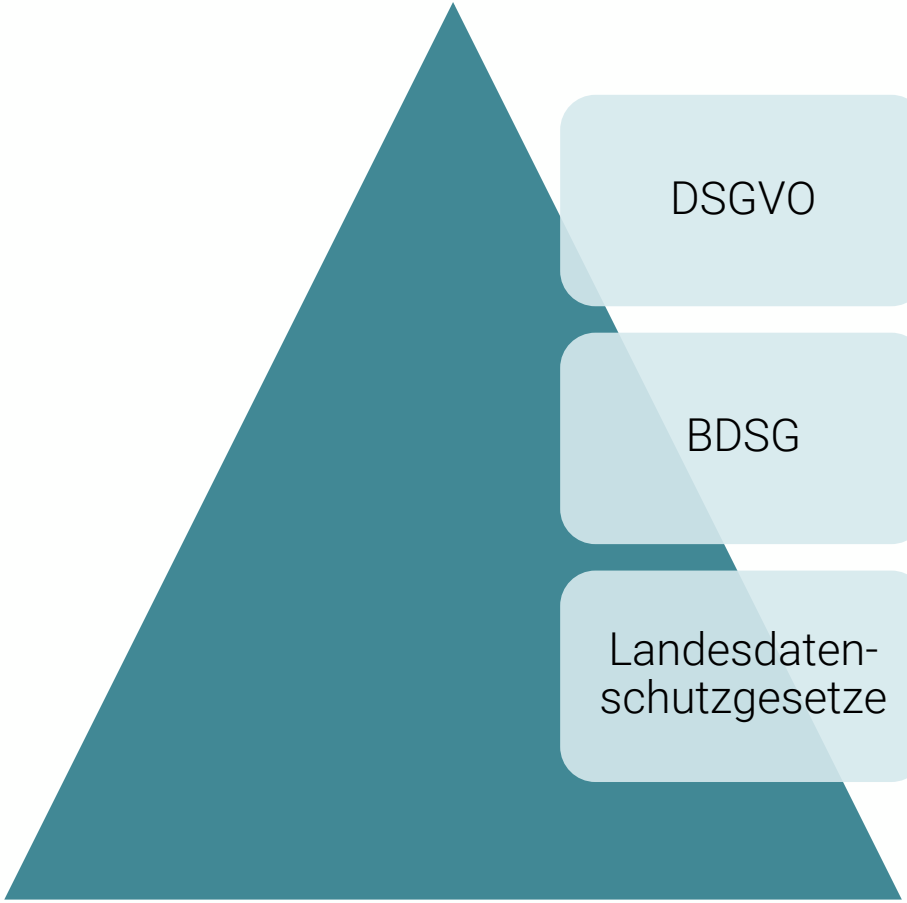
62 Prozent sind überzeugt, dass die DSGVO ein Wettbewerbsvorteil für hiesige Firmen sei

69 Prozent glauben, dass die DSGVO weltweit Maßstäbe für den Umgang mit Personendaten setzt

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Quelle: Jedes 2. Unternehmen verzichtet aus Datenschutzgründen auf Innovationen, Krösmann & Weiß, bitkom Presse, 29.09.2020, abgerufen am 01.04.21 unter diesem Link.

Um den Datenschutz beachten zu können, müsst Ihr zunächst die für Euch geltende Regelung bestimmen



DSGVO

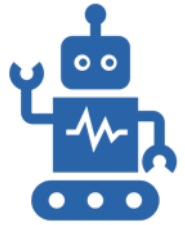
BDSG

Landesdaten-schutzgesetze

Bereichsspezi-fische Gesetze
EG, TKG, TMG

Kirchliche Datenschutz-gesetze

Deutsche Gesetze, die die DSGVO konkretisieren, ergänzen oder modifizieren sind vorrangig zu beachten (Subsidiaritätsprinzip). Durch die Normenhierachie gilt aber bei Auslegungsfragen und Widersprüchen grundsätzlich die DSGVO.



CORRELAID

GOOD CAUSES. BETTER EFFECTS.

Denkaufgabe

Welche Datenschutzrichtlinien gilt für die Evangelische Hochschule Berlin?

- 2 min -

CORRELAID

GOOD CAUSES. BETTER EFFECTS.

Lösung

Hier gibt es grundsätzlich vier Optionen: Die DSGVO (weil keine konkretisierenden Regelungen vorliegen), das Berliner Datenschutzgesetz (BlnDSG), das Berliner Hochschulgesetz (BerlHG) oder das Kirchengesetz über den Datenschutz der evangelischen Kirche in Deutschland (DSG-EKD). Richtig ist Letzteres.

CORRELAID

GOOD CAUSES. BETTER EFFECTS.

Optional: Übung

Findet heraus, welche Datenschutzverordnung für Euer Projekt gilt. Gibt es spezielle Regelungen der Organisation für den Datenschutz?

Art. 1 DSGVO gibt Auskunft darüber, was Sachgegenstand, Ziele und Grenzen der Verordnung sind

Myth Buster
Edition Datenschutz

1 **Gegenstand**

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der **Verarbeitung personenbezogener Daten** und zum freien Verkehr solcher Daten.

2 **Ziele**

Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf **Schutz personenbezogener Daten**.

3 **Grenzen**

Trotzdem soll der **freie Verkehr** personenbezogener Daten in der Unon nicht verboten werden.

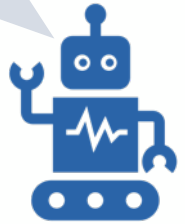
Personenbezogene Daten

Alle Informationen, durch die eine natürliche Person, also Menschen, direkt oder indirekt identifiziert werden oder identifizierbar sind, also durch Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Verarbeitung

Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung, Abgleich, Verknüpfung, Einschränkung, Löschung oder Vernichtung in automatisierten und nicht-automatisierten Vorgängen

Die DSGVO definiert viele Begrifflichkeiten direkt im Gesetzestext. So fallen z.B. auch (teilweise) automatisierte Prozesse unter den Datenschutz.



CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Damit kommen auf Euch sieben Kernpflichten zu

1 **Rechtmäßigkeit**
Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und für Betroffene nachvollziehbar verarbeitet werden

2 **Zweckbindung**
Nur Daten, die einen festgelegten, eindeutigen und legitimen Verarbeitungszweck haben, dürfen für diesen verarbeitet werden

3 **Datenminimierung**
Verarbeitete Daten müssen für den Zweck angemessen und erheblich sowie auf notwendige Maß beschränkt sein

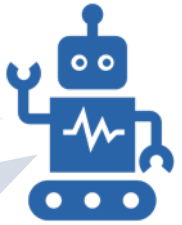
4 **Richtigkeit**
Daten müssen sachlich richtig und aktuell sein. Falsche Daten müssen vor Verarbeitung berichtigt oder gelöscht werden

5 **Datenreduktion**
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie auch noch einen Zweck erfüllen.

6 **Vertraulichkeit**
Daten müssen angemessen durch technische und organisatorische Maßnahmen vor Zugriff und (partiellem) Verlust gesichert sein

7 **Rechenschaft**
Entscheidungsträger:innen sind für die Einhaltung dieser Pflichten verantwortlich und müssen dies nachweisen können.

Daten, die wir langfristig speichern wollen, aber deren Zweck erloschen ist, müssen also anonymisiert werden.



Das ist i.d.R. nach drei Jahren der Fall. Achtung: Für Steuerprüfungen müssen Daten ggf. länger aufgehoben werden.

“Damit wir Daten verarbeiten können, benötigen wir schriftl. Einwilligungen”

Myth Buster
Edition Datenschutz

Verbotsprinzip
Es ist verboten, personenbezogene Daten zu verarbeiten, außer Betroffene haben es erlaubt oder es ist rechtlich notwendig.

Option 1

Betroffene willigen explizit ein

Option 2

Betroffene willigen implizit ein

Option 3

Es existiert eine bes. Rechtsvorschrift

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Myth Buster
Edition Datenschutz

Denkaufgabe

Sind Cookie-Hinweise auf Webseiten notwendig?
Warum?

- 2 min -

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Myth Buster
Edition Datenschutz

Lösung

Cookie-Hinweise sind generell nicht notwendig. Besonders wenn sie für die Funktionsweise der Seitennutzung relevant sind. Was Ihr aber darüber hinaus über Eure Nutzer:innen sammelt (z.B. Drittseitennutzung), ist natürlich nicht von der konkludenten Einwilligung durch das Klicken auf die Webseite abgedeckt. Best Practice ist es Cookie-Hinweise kurz zu halten und es ist erforderlich eine Opt-Out-Option zu garantieren, die bei Auswahl auch angewählt sein sollte.

Bei der Vielzahl von Rechten hilft es entlang der Data Journey über Datenschutz nachzudenken

1 Fairness

2 Auskunft

3 Berichtigung/Löschung

4 Widerspruch

Vor der Datenerhebung — *Nach der Datenerhebung*

Rechtmäßigkeit, Zweckbindung und Datenminimierung prüfen

- Hinterfragen, welche Daten für welchen Zweck genutzt werden, insb. bei persönlichen Merkmalen und Verarbeitungsverzeichnis erstellen
- Unterscheiden, ob Daten aus tatsächlichen Gründen (Prozessnotwendigkeit, Reporting, Steuer, etc.) oder aus Interesse erhoben werden

Rechenschaft ablegen und Datenrichtigkeit ermöglichen

- Ggf. (digitale) schriftliche Erklärung einsammeln, die u.a. den Zweck der Datenerhebung, das Verfahren, sowie die Speicherdauer beinhaltet
- Anfragen zu Auskunft, Berichtigung und Löschung innerhalb von 30 Tagen bearbeiten (Nachweispflicht)
- Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) beachten

Vertraulichkeit (Datensicherung) gewährleisten

- Dem Risiko angemessene prozessuale und technisch Maßnahmen zur Sicherung der Daten vornehmen (z.B. E-Mail-Verschlüsselung, Passwortschutz, User Management System, doppelte Datensicherung, Verpflichtungserklärungen, …)
- Bei Datenpannen Anzeigepflicht von 72h beachten

Datenminimierung durch Datenaudit sichern

- Namen der Personen durch Pseudonym (z.B. durch eine ID) ersetzen und demographische Daten und Adressdaten löschen, um Feststellung der Identität zu erschweren
- Falls Bezüge zwischen verschiedenen Datensätzen nicht notwendig sind: Anonymisieren (unterliegen nicht der DSGVO)

Best Practices Datenschutz

- Datenschutzerklärung veröffentlichen
- Verarbeitungsverzeichnisse erstellen
- Verantwortlichkeiten festlegen
- Kontaktdaten publizieren
- Datenschutzmgmtsystem einführen
- Maßnahmen überprüfen
- Anonymi-/pseudonymisieren
- Datenaudit etablieren

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

”Zur Anonymisierung reicht es aus, den Namen durch eine ID zu ersetzen”

Myth Buster
Edition Datenschutz

Datenreduktion
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie sie auch noch einen Zweck erfüllen.

Pseudonymisierung

Ein Bezug zur betroffenen Person ist nur unter Zuhilfenahme zusätzlicher Informationen möglich (Art. 5)

Anonymisierung

Es besteht auch mit zusätzlichen Informationen keinerlei Möglichkeit zur Re-Identifikation der natürlichen Person

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Myth Buster
Edition Datenschutz

Denkaufgabe

Wir speichern die Daten von zehn Workshopteilnehmer:innen mit Namen, Kontaktdaten, Alter, Geschlecht und Note. Vor Veröffentlichung löschen wir zur Anonymisierung Name und Kontaktdaten. Ist das ausreichend?

Teilnehmer:innen am 01.04.21	
M – 23 – 2.0	W – 19 – 1.0
M – 25 – 3.0	W – 38 – 5.0
M – 56 – 4.0	W – 43 – 2.0
M – 64 – 2.0	W – 59 – 3.0
M – 36 – 3.0	W – 76 – 4.0

- 2 min -

CORRELAID

GOOD CAUSES. BETTER EFFECTS.

Lösung

Nein. Tatsächlich ließe sich mit der Zuhilfenahme von zusätzlichen Informationen genau bestimmen, wer am Kurs teilgenommen und welche Note erreicht hat. Letztlich ist mit der Informationskombination Geschlecht und Alter eine Re-Identifikation möglich. Deshalb gilt hier auch weiterhin die DSGVO. Eine Veröffentlichung ist also nur mit vorheriger Einwilligung der Teilnehmer:innen erlaubt. Orientierung bietet hier der Umgang mit Zensusdaten: Gem. §16 Bundesstatistikgesetz ändert SAFE die Daten so, dass jede Merkmalskombination mindestens dreimal oder gar nicht mehr auftritt.

Quelle: Nutzerinformation zu SAFE, Statistische Ämter des Bundes, 28.05.14,, abgerufen am 01.04.21 unter diesem Link.

Datensicherung ist komplex, weshalb das Prinzip der doppelten Datensicherung gilt

RECHENZENTRUM IN FLAMMEN

Am Rhein brennt Europas Datenschatz

VON NIKLAS MAAK - AKTUALISIERT AM 13.03.2021 - 14:20

Ein ikonisches Bild: Europas größtes Rechenzentrum geht in Flammen auf, viele Daten sind für immer verloren. Was bedeutet das für uns Internetnutzer?

	Aufwand	Kosten	Übertragung	Sicherung
Analoge Dokumente digitalisieren oder doppelte Ausführung an anderem Ort	◔	◔	◔	Aktenschränke oder –Räume mit Schloss
Lokale Speicher Von Rechnern auf externe Festplatte, internen Server	◔	◔	●	Passwortschutz, sichere Lagerung
Rechenzentren Zusätzliche Datenüber-tragung an externen Standorten (in der EU)	◔	●	◑	Verwaltung der Zugriffsrechte
Cloud Zusätzliche digitale Datenspeicherung im Netz (EU-Anbieter)	◔	◑	●	Verwaltung der Zugriffsrechte

● Hoch ○ Niedrig

Quelle: Am Rhein brennt Europa, Niklas Maak, FAZ online, 13.03.21, abgerufen am 01.04.21 unter diesem Link

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

„Die Nutzung von digitalen Tools von US-Anbietern ist unproblematisch.“

Myth Buster
Edition Datenschutz

Der Europäische Gerichtshof urteilte am 16. Juli 2020, dass auch die US-europäische Vereinbarung (bekannt als Privacy Shield) zur Datenübertragung in die USA unzulässig sei (Schrems II). Vorher hatte es bereits das Safe Harbour Agreement kassiert (Schrems I). Unternehmen sind verpflichtet in jedem Einzelfall zu überprüfen, ob in Drittländern ein angemessenes Datenschutzniveau. vorliegt. Da Behörden auf die Daten US-amerikanischer Unternehmen zugreifen dürfen, ist das bei Nutzung von US-Amerikanischen Tools nicht erfüllt und es drohen Sanktionen - auch wenn sog. Standarddatenklauseln zwischen den Unternehmen getroffen wurden.

Quelle: Judgement of the Court (Grand Chamber), EuGH, veröffentlicht auf dem Webauftritt des EuGH am 16.07.20, abgerufen am 01.04.21 unter diesem Link

DSGVO-konforme Tools haben ihren Serverstandort in der EU und/oder sind Tools von EU-Anbietern

Vertraulichkeit
Daten müssen angemessen durch technische und organisatorische Maßnahmen vor Zugriff und (partiellem) Verlust gesichert sein

Option 1

DSGVO-konforme Tools wählen[1]

Option 2

Eigene Tool oder Tool-Instanzen hosten[2]

Option 3

Binding Corporate Rules (BCR) abschließen

Quelle: Judgement of the Court (Grand Chamber), EuGH, veröffentlicht auf dem Webauftritt des EuGH am 16.07.20, abgerufen am 01.04.21 unter diesem Link

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Welche Tools können wir also noch nutzen?

Kommunikation

Videokonferenzen

BigBlueButton, alfaview

Newsletter

CleverReach, rapidmail

Terminplanung

nuudel – nicht speicherndes Termintool

Kollaboration

Chats

Mattermost, WECHANGE

Cloud

Nextcloud, ownCloud, idgard by uniscon - A member of TÜV

Daten

Erhebung

LimeSurvey, KoBoToolbox

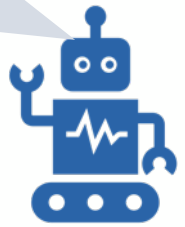
Speicherung

SeaTable, MEINVEREIN, PostgreSQL

Analyse

python, RStudio, Metabase

Dies ist nur eine beispielhafte Auswahl von DSGVO-konformen Tools zum Selber-Hosten und als SaaS-Lösung! Mehr Tools gibt es u.a. auf den Seiten der Berliner Datenschutzbeauftragten.



Auch Ihr seid zur Einhaltung des Datengeheimnisses ggü. Eurem Projektpartner und der DSGVO verpflichtet

Darüber hinaus sollten wir bedenken, welche ethischen Abwägungen für unsere Arbeit relevant sind

Flexibilität

Wir garantieren, dass unsere Volunteers und NPOs ihre Zeit für die Arbeit an Projekten frei einteilen können

Pragmatismus

Wir kreieren in unserer Arbeit praktische Lösungen, die tatsächlichen Mehrwert schaffen und nachhaltig sind

Wertschätzung

In unserer Arbeit bringen wir anderen Menschen und Ansichten Anerkennung entgegen und lernen voneinander

Diversität

Wir achten bei unserer Arbeit auf die Integration aller Menschen im Sinne des Art. 3 GG und allen Organisationen, die ihre Arbeit diesen Menschen widmen

Wissens-management

Wir teilen unser Wissen innerhalb und außerhalb unserer Organisation in Formaten und Formulierungen, die für die Allgemeinheit zugänglich und verständlich sind

Selbst-bestimmung

Wir unterstützen unsere Volunteers und Projektpartner:innen in ihren individuellen Entscheidungsfindungen

Das äußert sich u.a. in den folgenden Handlungsempfehlungen

- Wir sollten prinzipiell *immer* überlegen sollte, ob das **Problem überhaupt durch Technologie** gelöst werden oder Technologie positiv dazu beitragen kann.
- Falls es notwendig ist, sozio-demographische Merkmale zu erheben, sollte eine **Selbstidentifikation von Betroffenen** umfangreich möglich sein. Diese ist ggf. um die selbst eingeschätzte Fremdidentifikation zu ergänzen.
- Falls es notwendig ist, sozio-demographische Merkmale in Analysen zu nutzen, sind Daten auf **(historische) Verzerrungen** zu prüfen
- Datenverarbeitungen, die zu **Diskriminierung, insb. der Einschränkung von Möglichkeiten der freien Persönlichkeitsentfaltung, führen oder anderweitig politisiert werden könnten**, sind der Ethikbeauftragten vorzulegen (Bsp. Untersuchung der Polizeikriminalstatistik zu Täter:innenprofilen)
- Bei der Datenverarbeitung sind wir transparent und geben Betroffenen bei Erhebung **umfangreich Auskunft** und **erklären ausführlich die Funktionsweise von Datenlösungen**
- Wir lizenzieren digitale Produkte als Nutzende und Veröffentlichende auf Basis von **CC BY 4.0**, also als **Open Source mit Autor:innenkreditierung**

Unsere ethischen Werte basieren auf den Ideen der Charta der digitalen Grundrechte…

CHARTA DER DIGITALEN GRUNDRECHTE DER EUROPÄISCHEN UNION

(überarbeitete Fassung 2018)

VORWORT

DIESER ENTWURF einer Digital-Charta ist in der Überzeugung entstanden, dass die Debatten um Grundrechte im digitalen Zeitalter zu einem Ergebnis führen müssen. Wir wollen die bestehenden Grundrechte stärken und konkretisieren.

WIR, DIE AUTORINNEN UND AUTOREN, halten dies für notwendig, weil sich mit der technologischen Entwicklung neue Herausforderungen und staatliche Aufgaben ergeben.

DIESE entstehen etwa durch neue Formen der Automatisierung, Vernetzung, künstliche Intelligenz, Vorhersage und Steuerung menschlichen Verhaltens, Massenüberwachung, Robotik und Mensch-Maschine-Interaktion sowie Machtkonzentration bei staatlichen und nichtstaatlichen Akteuren.

DIE DIGITAL-CHARTA ist ein politisches Manifest in Gestalt eines gesetzesähnlichen Textes. Sie enthält neben Vorschlägen für künftige Grundrechte auch Staatszielbestimmungen und mögliche Aufträge an den europäischen Gesetzgeber, die alle zusammen die Größe der Herausforderung umreißen und die Bedeutung der Bürgerrechte im digitalen Zeitalter betonen sollen.

NACH INTERNEN UND ÖFFENTLICHEN DISKUSSIONEN legen wir hiermit den überarbeiteten Entwurf einer Charta vor, der in der Öffentlichkeit weiter reifen soll. Wir setzen uns dafür ein, dass damit ein gesellschaftlicher und politischer Prozess entsteht, der in ein bindendes Grundrechte-Dokument mündet.

PRÄAMBEL

IM BEWUSSTSEIN, DASS

die Anerkennung der angeborenen Würde und der gleichen und unveräußerlichen Rechte aller Menschen die Grundlage von Freiheit, Gerechtigkeit und Frieden in der Welt bildet,

die zunehmende Digitalisierung zur Veränderung der Grundlagen unserer Existenz führt,

es im digitalen Zeitalter zu enormen Machtverschiebungen zwischen Einzelnen, Staat und Unternehmen kommt,

im digitalen Zeitalter eine zivilgesellschaftliche Debatte entstanden ist und weitergeht,

Grundrechte und demokratische Grundprinzipien im digitalen Zeitalter auf neue Herausforderungen und Bedrohungen treffen,

technischer Fortschritt stets im Dienste der Menschheit zu stehen hat,

die Gestaltung der digitalen Welt auch eine europäische Aufgabe sein muss, damit es im europäischen Verbund gelingt, Freiheit, Gerechtigkeit und Solidarität im 21. Jahrhundert zu erhalten;

IN ANERKENNUNG

der Allgemeinen Erklärung der Menschenrechte,

der Europäischen Menschenrechtskonvention,

der Charta der Grundrechte der Europäischen Union,

der Grundrechts- und Datenschutzstandards der Europäischen Union und ihrer Mitgliedstaaten;

FEST ENTSCHLOSSEN,

Grundrechte und demokratische Prinzipien auch in der digitalen Welt durch die Herrschaft des Rechts zu schützen,

staatliche und nichtstaatliche Akteure auf eine Geltung der Grundrechte in der digitalen Welt zu verpflichten,

auf diese Weise das Fundament einer rechtsstaatlichen Ordnung im digitalen Zeitalter zu schaffen,

das Digitale nicht als Quelle der Angst, sondern als Chance für ein gutes Leben in einer globalen Zukunft zu erfassen;

ERKENNT DIE UNION DIE NACHSTEHEND AUFGEFÜHRTEN RECHTE, FREIHEITEN UND GRUNDSÄTZE AN:

ART. 1 (WÜRDE)

Die Würde des Menschen ist auch im digitalen Zeitalter unantastbar. Sie ist zu achten und zu schützen. Keine technische Entwicklung darf sie beeinträchtigen.

ART. 2 (FREIHEIT)

Jeder hat ein Recht auf freie Information und Kommunikation. Es beinhaltet das persönliche Recht auf Nichtwissen.

ART. 3 (GLEICHHEIT)

(1) Jeder Mensch hat das Recht auf eine gleichberechtigte Teilhabe in der digitalen Sphäre. Es gilt das in der Europäischen Grundrechte-Charta formulierte Diskriminierungsverbot.

(2) Die Verwendung von automatisierten Verfahren darf nicht dazu führen, dass Menschen vom Zugang zu Gütern, Dienstleistungen oder von der Teilhabe am gesellschaftlichen Leben ausgeschlossen werden. Dies gilt insbesondere im Bereich Gesundheit, Schutz vor elementaren Lebensrisiken, Recht auf Arbeit, Recht auf Wohnen, Recht auf Bewegungsfreiheit und bei Justiz und Polizei.

ART. 4 (MEINUNGSFREIHEIT UND ÖFFENTLICHKEIT)

(1) Jeder Mensch hat das Recht, in der digitalen Welt seine Meinung frei zu äußern. Eine Zensur findet nicht statt.

(2) Dieses Recht findet seine Schranken in den Vorschriften der allgemeinen Gesetze.

(3) Betreiber öffentlicher Diskursräume tragen Verantwortung für den Schutz der Meinungsfreiheit. Sie haben die Beachtung der in dieser Charta aufgeführten Grundrechte und Pflichten nach Maßgabe der Gesetze zu gewährleisten.

ART. 5 (AUTOMATISIERTE SYSTEME UND ENTSCHEIDUNGEN)

(1) Ethisch-normative Prinzipien dürfen nur vom Menschen aufgestellt, und Entscheidungen, die in Grundrechte eingreifen, nur von Menschen getroffen werden.

(2) Automatisierte Entscheidungen müssen von natürlichen oder juristischen Personen verantwortet werden.

(3) Die Kriterien automatisierter Entscheidungen, etwa bei Profilbildung, sind offenzulegen.

(4) Wer einer automatisierten Entscheidungen von erheblicher Bedeutung für seine Lebensführung unterworfen ist, hat Anspruch auf unabhängige Überprüfung und Entscheidung durch Menschen.

(5) Entscheidungen über Leben, körperliche Unversehrtheit und Freiheitsentzug dürfen nur von Menschen getroffen werden.

(6) Der Einsatz von künstliche Intelligenz und Robotik in grundrechtsrelevanten Bereichen muss gesellschaftlich begleitet und vom Gesetzgeber reguliert werden.

ART. 6 (TRANSPARENZ)

(1) Jeder Mensch hat das Recht auf Zugang zu Informationen staatlicher Stellen. Der Schutz insbesondere personenbezogener Daten ist zu gewährleisten. Das Transparenzgebot gilt auch gegenüber Privaten, die öffentliche Aufgaben wahrnehmen.

(2) Hinweisgeber, die Informationen über Fehlverhalten einer Organisation offenlegen, sind angemessen zu schützen.

ART. 7 (PRIVATSPHÄRE, VERTRAULICHKEIT UND DATENSCHUTZ)

(1) Jeder Mensch hat das Recht auf den Schutz seiner Daten und die Achtung seiner Privatsphäre.

(2) Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke beim Betroffenen erhoben und verarbeitet werden, wenn hierfür eine gesetzliche Grundlage besteht. Die Datenverarbeitung muss sicher, fair, transparent und nach dem Stand der Technik gestaltet werden.

(3) Rechte auf Löschung, Berichtigung, Widerspruch, Information und Auskunft sind zu gewährleisten.

(4) Jeder Mensch hat das Recht auf digitalen Neuanfang. Dieses Recht findet seine Grenzen in den berechtigten Informationsinteressen der Öffentlichkeit.

(5) Jeder Mensch hat das Recht, in seiner Wohnung frei und unbeobachtet zu leben.

(6) Jeder Mensch hat das Recht, seine Daten und Kommunikationen durch Wahl geeigneter Mittel gegen Kenntnisnahme Dritter zu schützen.

(7) Eine anlasslose Überwachung findet nicht statt.

(8) Die Einhaltung dieser Rechte wird von unabhängigen Stellen überwacht.

ART. 8 (SICHERHEIT INFORMATIONS-TECHNISCHER SYSTEME)

Die Unversehrtheit, Vertraulichkeit und Integrität informationstechnischer Systeme und Infrastrukturen ist sicherzustellen und angemessen technisch und organisatorisch zu gewährleisten.

ART. 9 (WAHLEN)

Das Recht, an öffentlichen Wahlen und Abstimmungen teilzunehmen, darf nicht an die Nutzung digitaler Medien gebunden werden.

ART. 10 (FREIER ZUGANG)

(1) Jeder Mensch hat das Recht auf freien und gleichen Zugang zu Kommunikations- und Informationsdiensten, ohne dafür auf grundlegende Rechte verzichten zu müssen.

(2) Dieser Zugang ist flächendeckend, angemessen und ausreichend zu gewährleisten.

(3) Jeder Mensch hat das Recht auf eine nichtpersonalisierte Nutzung digitaler Angebote. Einschränkungen dürfen nur auf gesetzlicher Grundlage stattfinden.

ART. 11 (NETZNEUTRALITÄT)

Netzneutralität ist diskriminierungsfrei zu gewährleisten.

ART. 12 (PLURALITÄT UND WETTBEWERB)

(1) In der digitalen Welt sind Pluralität und kulturelle Vielfalt zu fördern.

(2) Interoperabilität und offene Standards sind zu fördern und zu bevorzugen.

(3) Marktmissbräuchliches Verhalten ist wirksam zu verhindern.

ART. 13 (BESONDERS SCHUTZBEDÜRFTIGE PERSONEN)

Kinder, Heranwachsende, benachteiligte und besonders schutzbedürftige Menschen genießen in der digitalen Welt spoziellen Schutz. Ihre Teilhabe an der digitalen Welt ist zu fördern und ihr Zugang zu elementaren Gütern und Dienstleistungen zu gewährleisten.

ART. 14 (BILDUNG)

Jeder Mensch hat ein Recht auf Bildung, die ein selbstbestimmtes Leben in der digitalen Welt ermöglicht. Dieses Ziel besitzt einen zentralen Stellenwert in den Lehrplänen von Bildungseinrichtungen.

ART. 15 (ARBEIT)

(1) Der digitale Strukturwandel ist nach sozialen Grundsätzen zu gestalten.

(2) Im digitalen Zeitalter ist effektiver Arbeitsschutz und Koalitionsfreiheit zu gewährleisten.

ART. 16 (IMMATERIALGÜTER)

(1) Jeder Mensch hat das Recht auf Teilhabe am kulturellen Leben und am wissenschaftlichen Fortschritt und dessen Errungenschaften.

(2) Jeder Mensch hat das Recht auf Schutz der geistigen und materiellen Interessen, die aus der Schaffung und Verbreitung von immateriellen Gütern erwachsen. Dies muss in Ausgleich gebracht werden mit den Interessen der Allgemeinheit, dem technischen Fortschritt und den kreativen Prozessen in Gesellschaft, Wirtschaft, Wissenschaft und Kunst.

ART. 17 (GELTUNGSBEREICH)

(1) Diese Charta gilt für die Organe, Einrichtungen und sonstigen Stellen der EU und ihrer Mitgliedsstaaten.

(2) Die Rechte und Prinzipien dieser Charta gelten auch gegenüber nichtstaatlichen Akteuren. Dabei ist eine Abwägung mit den Grundrechten dieser Akteure vorzunehmen.

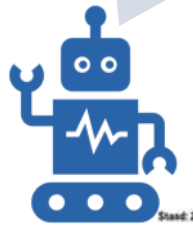
ART. 18 (SCHLUSSBESTIMMUNGEN)

(1) Die Auslegung der in dieser Charta enthaltenen Rechte obliegt in letzter Instanz dem Europäischen Gerichtshof.

(2) Jede Einschränkung der Ausübung der hier anerkannten Rechte muss gesetzlich vorgegeben sein, dem Grundsatz der Verhältnismäßigkeit entsprechen und den Wesensgehalt dieser Rechte achten. Es gelten im Übrigen Artikel 52 bis 54 der EGC.

Stand: 25. April 2018

Es gibt eine dt. Datenethik-kommission!



Quelle: Charta der digitalen Grundrechte der EU (Entwurf), ZEIT-Stiftung Ebelin und Gerd Bucerius, 25.04.2018, abgerufen am 01.04.21 unter diesem Link

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

Besonders wichtig finden wir die folgenden Artikel:

Freiheit

ART. 2 (FREIHEIT)

Jeder hat ein Recht auf freie Information und Kommunikation. Es beinhaltet das persönliche Recht auf Nichtwissen.

Diskriminierungsverbot

ART. 5 (AUTOMATISIERTE SYSTEME UND ENTSCHEIDUNGEN)

(1) Ethisch-normative Prinzipien dürfen nur vom Menschen aufgestellt, und Entscheidungen, die in Grundrechte eingreifen, nur von Menschen getroffen werden.

(2) Automatisierte Entscheidungen müssen von natürlichen oder juristischen Personen verantwortet werden.

(3) Die Kriterien automatisierter Entscheidungen, etwa bei Profilbildung, sind offenzulegen.

(4) Wer einer automatisierten Entscheidungen von erheblicher Bedeutung für seine Lebensführung unterworfen ist, hat Anspruch auf unabhängige Überprüfung und Entscheidung durch Menschen.

ART. 3 (GLEICHHEIT)

(1) Jeder Mensch hat da
tigte Teilhabe in der digitalen Sphäre. Es gilt das in der Europäischen Grundrechte-Charta formulierte Diskriminierungsverbot.

(2) Die Verwendung von automatisierten Verfahren darf nicht dazu führen, dass Menschen vom Zugang zu Gütern, Dienstleistungen oder von der Teilhabe am gesellschaftlichen Leben ausgeschlossen werden. Dies gilt insbesondere im Bereich Gesundheit, Schutz vor elementaren Lebensrisiken, Recht auf Arbeit, Recht auf Wohnen, Recht auf Bewegungsfreiheit und bei Justiz und Polizei.

Inklusion

ART. 13 (BESONDERS SCHUTZBEDÜRFTIGE PERSONEN)

Kinder, Heranwachsende, benachteiligte und besonders schutzbedürftige Menschen genießen in der digitalen Welt speziellen Schutz. Ihre Teilhabe an der digitalen Welt ist zu fördern und ihr Zugang zu elementaren Gütern und Dienstleistungen zu gewährleisten.

ART. 14 (BILDUNG)

Jeder Mensch hat ein Recht auf Bildung, die ein selbstbestimmtes Leben in der digitalen Welt ermöglicht. Dieses Ziel besitzt einen zentralen Stellenwert in den Lehrplänen von Bildungseinrichtungen.

Quelle: Charta der digitalen Grundrechte der EU (Entwurf), ZEIT-Stiftung Ebelin und Gerd Bucerius, 25.04.2018, abgerufen am 01.04.21 unter diesem Link

Tolle Ressourcen rund um das Thema Datenverarbeitung gibt es bei CfE…

Welche der folgenden (Selbst-) Bezeichnungen trifft am ehesten auf Sie zu?

Diese Liste orientiert sich an den geografischen Bezügen und Selbstbezeichnungen von zahlenmäßig großen Gruppen in Deutschland und Berlin, sowie an den nach der UN-Antirassismuskonvention schutzwürdigen Gruppen. Da sich diese Bezeichnungen mit der Zeit ändern, fragen wir danach, welche „am ehesten" für Sie passend erscheinen.
Die Liste ist nicht vollständig und kann im letzten Feld – auch durch andere Schreibweisen – ergänzt werden.
Mehrfachantworten sind möglich.

- ☐ Weiß
- ☐ Person of Colour
- ☐ Schwarz
- ☐ Jüdisch
- ☐ Russischsparchig jüdisch
- ☐ Muslimisch
- ☐ Sinti oder Roma
- ☐ Afrodeutsch
- ☐ Arabisch
- ☐ Asiatisch-Deutsch
- ☐ Polnisch-Deutsch
- ☐ Russlanddeutsch
- ☐ Türkisch-Deutsch
- ☐ Für mich treffen andere Selbstbezeichnungen zu und zwar:

Frage 1:

Was wollen wir wissen und welche Daten benötigen wir dafür?

Frage 2:

Wie werden die tatsächlich benötigten Daten erhoben?

Quelle: Daten für die vielfältige Gesellschaft, Citizens for Europe, 2019, abgerufen am 01.04.21 unter diesem Link

CORRELAID
GOOD CAUSES. BETTER EFFECTS.

…und auch bei uns findet Ihr Inspiration

Disclaimer:
In der folgenden Umfrage fragen wir Daten zu Dir und Deiner bisherigen Berufserfahrung ab. Dabei erheben wir Deinen Namen und Deine Kontaktdaten, damit unsere Projektmanager:innen Dich kontaktieren können. Nach erfolgreicher Ausschreibung werden diese Daten auch mit dem Projektteam innerhalb unserer Organisation geteilt.

Bei einer Umfrage hast Du gemäß der DSGVO das Recht auf Auskunft sowie Löschung Deiner personenbezogenen Daten. Du kannst diese Einwilligungserklärung jederzeit widerrufen. Schreib hierzu einfach eine E-Mail an datenschutz@correlaid.org. Nach erfolgtem Widerruf werden Deine Daten gelöscht.

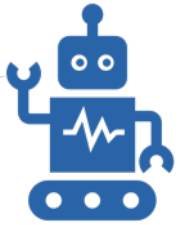
* 4. Was ist dein Geschlecht?
Hinweis: Da wir bei CorrelAid nach dem Grundprinzip von Geschlechtergleichberechtigung arbeiten, ist diese Frage für uns besonders wichtig.

- ◯ Weiblich
- ◯ Männlich
- ◯ Non-binary
- ◯ Das möchte ich nicht angeben
- ◯ Mein Geschlecht ist:

Hier geht es zu unseren Ethikrichtlinien, …

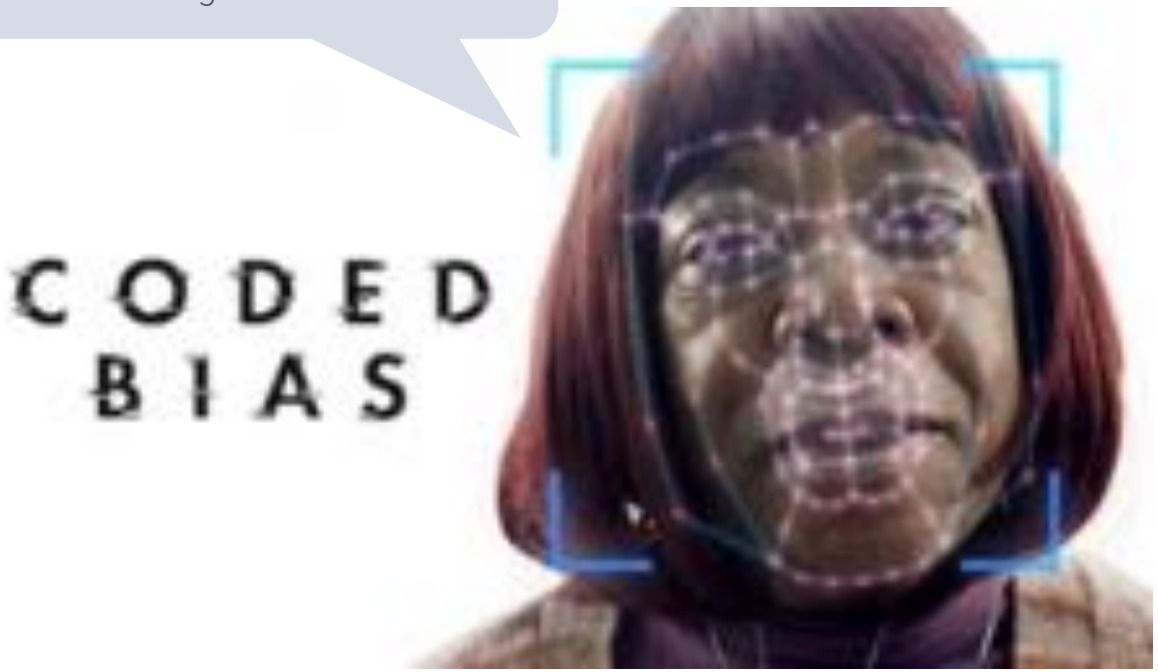
zum Code of Conduct und…

zu den Kontaktdaten des Datenschutzbeauftragten!



Als Abend- und Filmempfehlung ist auch die neue Netflixdokumentation ‘Coded Bias’ zu erwähnen

‚Data is a reflection of our history, The past dwells within our algorithms.‘



Codierter Bias entsteht durch…

a) Stichproben/Daten, die nicht repräsentativ oder verzerrt sind

b) Algorithmen, die sozio-demographische Variablen oder deren Proxies nutzen ohne auf Fairness überprüft zu werden

Das kann neben der Förderung von Vorurteilen in der Gesellschaft für vulnerable Gruppen, u.a. Frauen und BPoCs, konkrete strukturelle Benachteiligung bedeuten:

- Kein oder geringerer Zugang zum Finanz- und Arbeitsmarkt und Technologien
- Targeted Advertising von zweifelhaften Produkten oder Dienstleistungen
- Racial Profiling und Surveillance durch Sicherheitsbehörden

Quelle: Coded Bias, Shalini Kantayya, Netflix, 2020, abgerufen am 05.04.21 unter diesem Link