

# Zivilisation im Metaverse: Letzte Chance oder Apokalypse für die digitale Zukunft?

Karin Lange  
die Mobiliar / Data Innovation Alliance

# Was bedeutet Zivilisation?

Gehen Sie auf [menti.com](https://www.menti.com)  
und geben Sie den folgenden  
Code ein:

**5470 6888**

oder scannen Sie den QR-  
Code.



# Zivilisation: Begriffsklärung

Mit dem Begriff Zivilisation beschreibt man die Entwicklung des Zusammenlebens von Menschen, die zu einem möglichst friedlichen und aggressionsfreien Miteinander führen soll. Eine Grundlage dafür ist die Achtung der Grund- und Menschenrechte.

Ein von der Geschichtswissenschaft für vergangene Zivilisationen verwendetes und Synonym ist HOCHKULTUR.

# Ist die Schweiz ein zivilisiertes Land??

Gehen Sie auf [menti.com](https://www.menti.com) und geben Sie den folgenden Code ein:

**6288 7249**

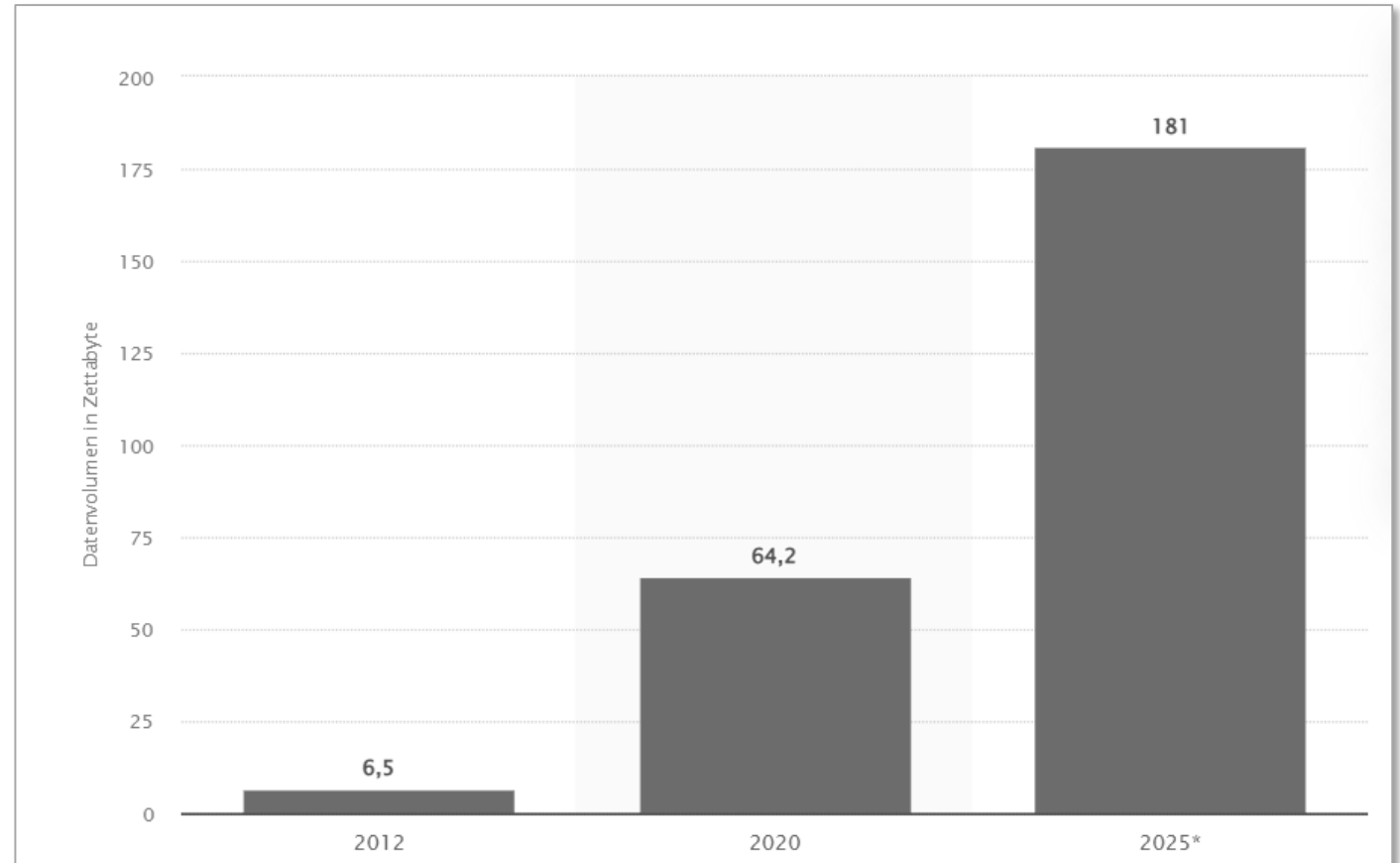
oder scannen Sie den QR-Code.



# Datenproduktion steigt

Prognostiziertes  
Wachstum des  
weltweiten  
Datenvolumens  
(in Zettabyte)

Quelle: Statista 2022



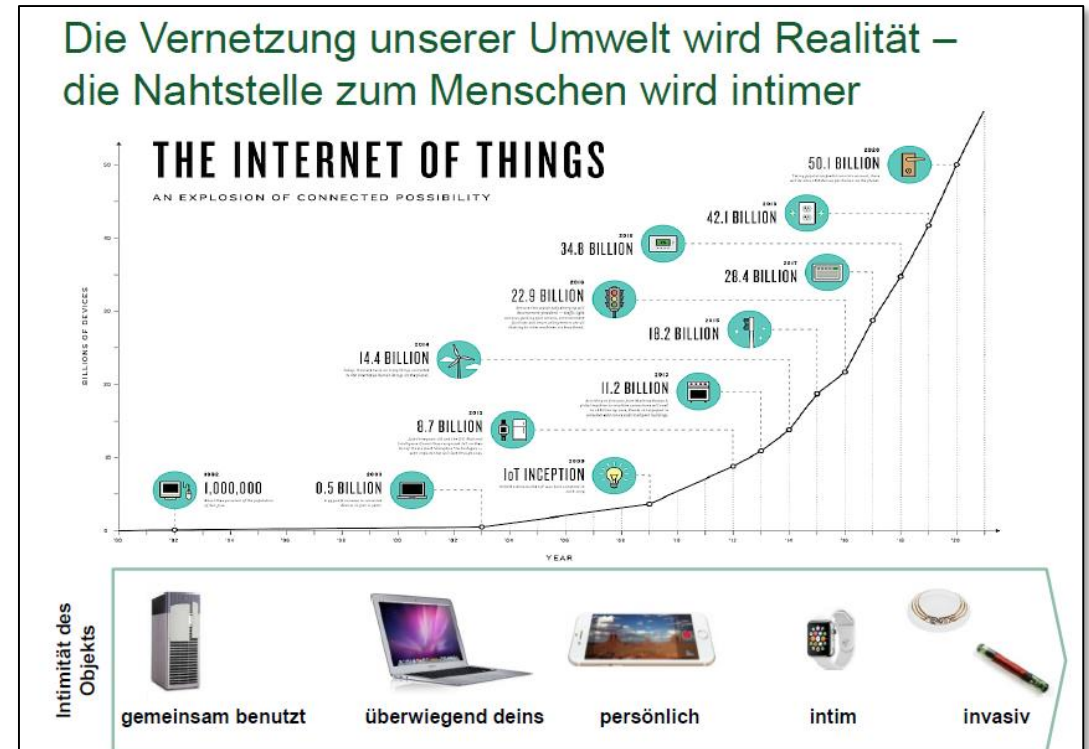
# Datennutzung steigt

## Analoge Welt:

Zweckgebundene Nutzung in Aufwand-Nutzen-orientierten Anwendungsfällen

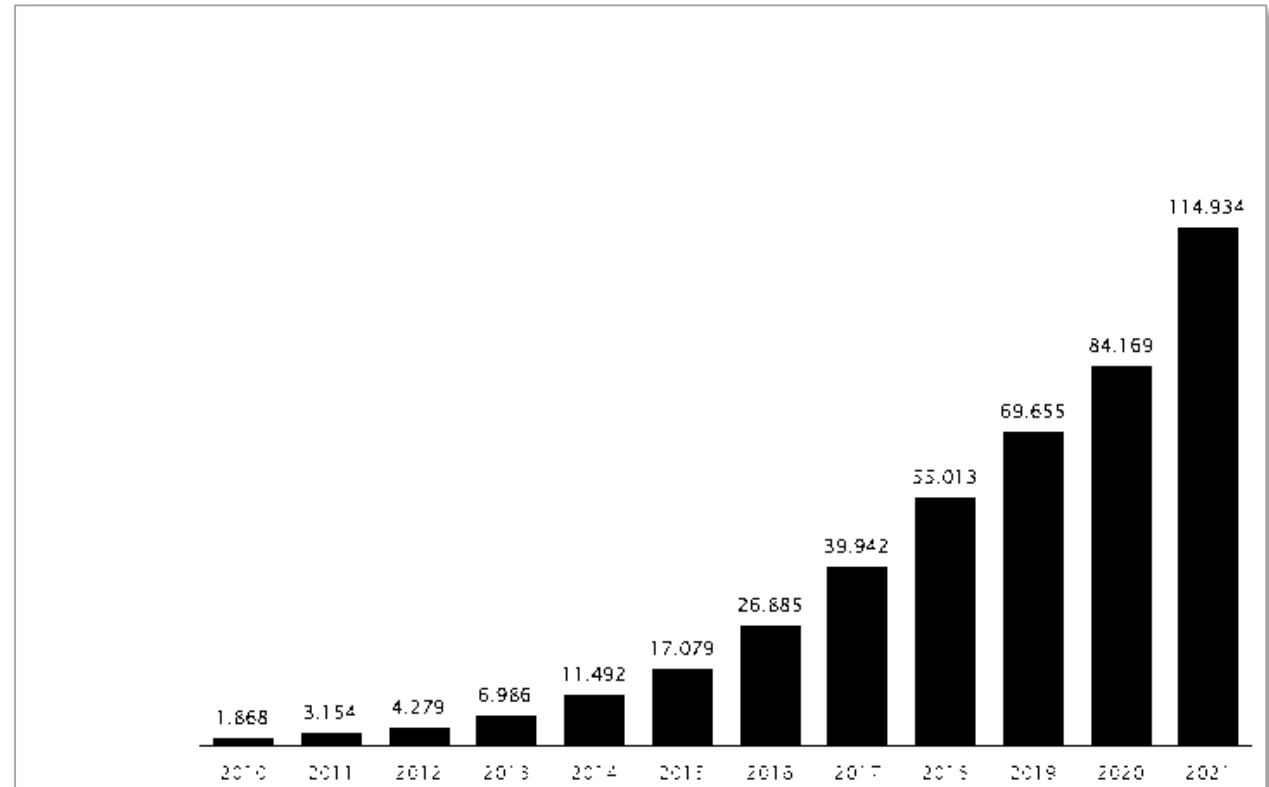
## Digitale Welt:

Zweckentfremdete Nutzung in Trial & Error Versuchsreihen, die auch dem Aufbau von Skills – oder als Trainingsdaten für Datenmodelle dienen



# Datensammeln: ein lohnendes Geschäft

- Ein modernes Auto sammelt schon heute 25 Gigabyte Daten pro Stunde. „Connected Cars“-Services wie die reibungslose Parkplatzsuche exponentiell zunehmen
- Facebook verdiente auch 2020 98.5 Prozent des Gesamtumsatzes mit Werbung .
- Google zapft seine Online-Community an und trainiert sein Deepmind, ähnlich wie Facebook oder Amazon ihre KI-Systeme – und auch Microsoft, IBM oder auch SAP nutzen ihre Software-Lösungen, um an Trainingsdaten für ihre Algorithmen zu kommen.
- Durch das Bereitstellen von Cloud-Speichern haben die „Grossen“ weitere Möglichkeiten, ihre KI mit Daten zu füttern. Unternehmen wie OpenAI (ChatGPT), Spotify, Grammarly und Lensa etc. haben keine Probleme, genügend Menschen zu finden, die ihre Systeme trainieren.



Werbeumsatz Facebook bis 2021 (in Mio. US\$, Quelle: Statista 2022)

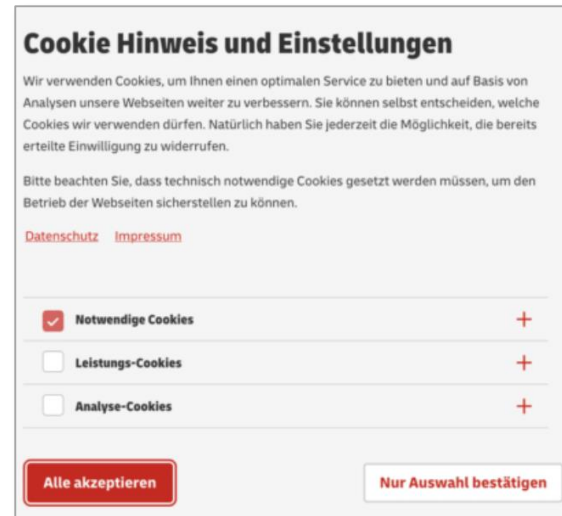
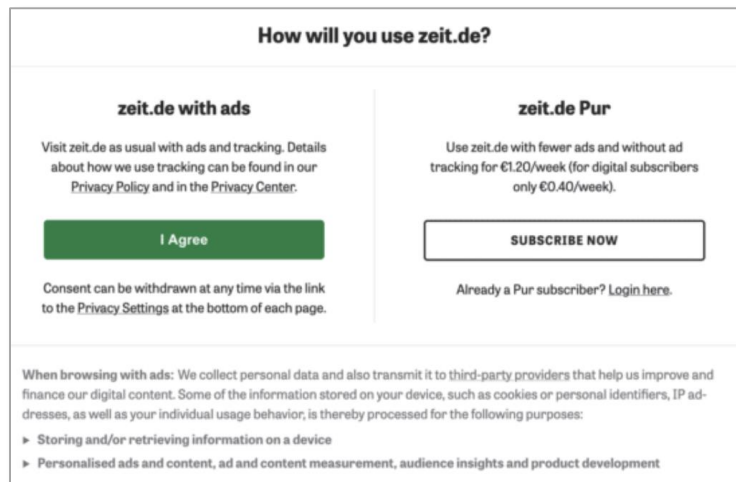
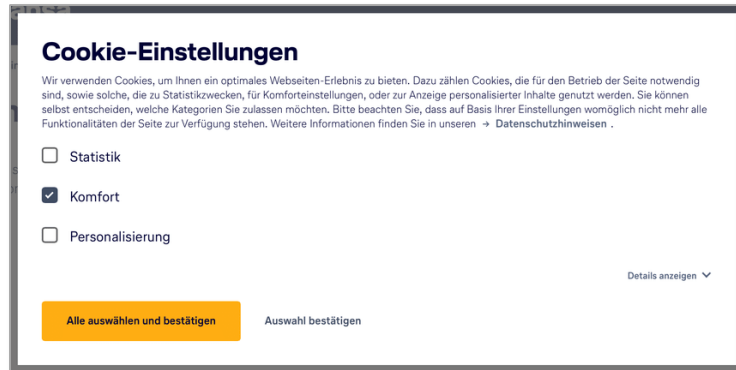
# Daten liefern – kein lohnendes Geschäft

Auf das steigenden Unbehagen der Konsumenten in Bezug auf das Ungleichgewicht beim «Daten zur Verfügung stellen» reagieren die Unternehmen – schliesslich benötigen sie die Daten, um Geld zu verdienen – mit

- vermeintlichen «Rüebli» (Gewinnspiele)
- Nudging (Infos zur «Selbstoptimierung»)
- Tricks (Online-Spiele)
- Fehlinformation/Manipulation (z.B. Einwilligung und Cookies)



# Deceptive Design (Dark Patterns) beim Einwilligungsmanagement



- Deliberate Misdirection (= Bewusste Irreführung)
- Forced Enrollment/Action/Consent (= Erzwungene Einwilligung)
- Confirmshaming (= Einwilligung durch Bloßstellen)
- Click Fatigue (= Klick-Ermüdung)
- Preselection (= Vorauswahl)
- Hidden Information (= Versteckte Informationen)
- Nagging (= Nörgelei)
- etc.

<https://www.deceptive.design/types>

## Daten liefern – kein lohnendes Geschäft

**If you're getting something for free,  
you are the product.**

# Fragwürdige Praktiken in der digitalen Welt

- Anarchistische Geschäftsmodelle (GAFA)
- Aufmerksamkeitsökonomie mit brutalen Vorgehen (Wer am "lautesten" ist, gewinnt)
- Unwahrheiten, Hass und Perversionen werden ungestraft verbreitet
- "customer centricity" ist ein Euphemismus für "Kundenschiessen"
- www ist ein Kriegsraum, in dem immer neue "Waffen" entwickelt werden, um Gebiete für sich zu gewinnen
- Generative AI wird eingesetzt, ohne hinterfragt oder überprüft zu werden
- Machine Learning wird eingesetzt, ohne ausreichend reguliert oder überprüft zu werden

# The Metaverse – das Metaversum

- **Das Metaverse ist ein digitaler Raum, in dem Menschen als Avatare in einer virtuellen Realität miteinander interagieren können.**
- **Diese Realität ist unbegrenzt und hat kein festes Ziel, so wird sie eher als eine Alternative zur "echten" Welt verstanden.**
- **Bisher wurde diese Idee aber noch nicht final umgesetzt.**
  
- **→ Das Rennen um die Dominanz im Metaverse hat begonnen:**
- **der Wettlauf um das Spiel mit einer Milliarde Nutzern**
- **das Rennen um die beste Hardware (VR / AR)**
- **das Rennen um die End-to-End-Infrastruktur selbst**
- **der Wettlauf um den Erfolg in der Metaverse-Ökonomie mit digitalen Währungen, NFTs etc.**



# The Metaverse – das Metaversum

- Nike hat einen virtuellen Store in Decentraland geschaffen, in dem Nutzer virtuelle Turnschuhe und Bekleidung in limitierter Auflage erwerben können
- Gucci hat einen virtuellen Store in Roblox erstellt, in dem Benutzer virtuelle Gegenstände und Zubehör kaufen können.
- Mercedes-Benz hat im Decentraland einen virtuellen Showroom eingerichtet, in dem Nutzer virtuelle Autos erkunden und individuell gestalten können.
- Coca-Cola hat in Decentraland einen virtuellen Verkaufsautomaten geschaffen, an dem Nutzer virtuelle Coca-Cola-Produkte kaufen können..





# The Metaverse – das Metaversum

- Microsoft hat eine virtuelle Welt namens AltspaceVR geschaffen, in der Benutzer virtuelle Veranstaltungen besuchen und Kontakte mit anderen Benutzern knüpfen können.
- Vans hat in Roblox einen virtuellen Skatepark geschaffen, in dem Nutzer skaten und Kontakte knüpfen können.
- Balenciaga hat eine virtuelle Modenschau im Metaverse kreiert, bei der die Nutzer den Models zusehen und virtuelle Kleidung kaufen können.
- Ariana Grande gab 2021 ein virtuelles Konzert in Fortnite, das von Millionen von Spielern besucht wurde.
- TerraZero Technologies Inc. und VentureBeat haben sich zusammengetan, um ein Metaverse-Veranstaltungszentrum in Decentraland zu errichten.



# Exponentielle Entwicklung

## Positive Auswirkungen:

- In Bildung und Ausbildung könnten digital nicht nur dieselben immersiven Erfahrungen produziert werden wie in der realen Welt sondern weitaus weitreichendere.
- Das Metaverse könnte das Gesundheitswesen fundamental revolutioniert werden mit neuen Kanälen um Betreuung und Pflege anzubieten – zu günstigeren Kosten zum Nutzen der Patienten, auch und gerade in ländlichen Gegenden.
- Soziale Interaktion profitiert von lebensechten Begegnungen.
- Neue Geschäftsmodelle und Einnahmequellen werden geschaffen und damit auch neue Arbeitsplätze.
- Wenn nicht mehr soviel gereist werden muss weil virtuell (fast) dasselbe Erlebnis geschaffen werden kann, profitiert die Umwelt.
- Das Potenzial für die Verminderung sozialer Ungleichheit ist da, wenn im Metaverse jeder dieselben Möglichkeiten und Zugang zu Ressourcen erhält

# Exponentielle Entwicklung

## Negative Auswirkungen

**Privatsphäre:** Im Metaverse besteht die Gefahr, dass persönliche Daten noch umfassender erfasst und analysiert werden. Individuen könnten kaum noch ihre Online-Aktivitäten vor neugierigen Blicken abschirmen, was die Privatsphäre erheblich beeinträchtigt. Permanente Überwachung tausender von Parameter (eye tracking, Körperbewegungen als Reaktionen, Schweissanalyse, Verhaltensanalyse, Vorlieben, Abneigungen) wird zu jedem User in ganz grossem Stil möglich.

**Diskriminierung:** Das Metaverse könnte die bestehenden Ungleichheiten verstärken. Menschen könnten aufgrund ihrer Herkunft, ihres Geschlechts, ihrer sexuellen Orientierung oder anderer persönlicher Merkmale diskriminiert werden. Da das Metaverse auf Algorithmen basiert, besteht das Risiko, dass diese bestehende Vorurteile und Stereotypen reproduzieren.

**Gefahr für die Demokratie:** Im Metaverse könnte es schwierig werden, zwischen Wahrheit und Falschheit zu unterscheiden. Falsche Informationen und manipulative Inhalte könnten sich schnell verbreiten und die öffentliche Meinung beeinflussen. Dies könnte die demokratischen Prozesse gefährden und die Grundlage für eine informierte Entscheidungsfindung untergraben.



# Exponentielle Entwicklung

## Negative Auswirkungen

**Sicherheitslücken:** Das Metaverse wird wahrscheinlich ein attraktives Ziel für Cyberkriminelle sein. Neue Sicherheitslücken und Schwachstellen könnten ausgenutzt werden, um Nutzerdaten zu stehlen, Betrug zu begehen oder digitale Angriffe durchzuführen.

**Abhängigkeit von Technologie:** Die Abhängigkeit von den technischen Infrastrukturen des Metaversums könnte zu einer Schwächung der Resilienz führen. Störungen oder Ausfälle in der Technologie könnten zu erheblichen Störungen im täglichen Leben führen und ganze Wirtschaftszweige beeinträchtigen.

**Digitale Kluft:** Nicht alle Menschen werden gleichermaßen Zugang zum Metaverse haben. Diejenigen, die aus wirtschaftlichen oder geografischen Gründen keinen Zugang haben, könnten von den potenziellen Vorteilen und Chancen ausgeschlossen werden, was zu einer Vertiefung der digitalen Kluft führt.

**Monopolbildung:** Grosse Unternehmen könnten das Metaverse dominieren und eine monopolartige Kontrolle über die digitale Welt erlangen. Dies könnte den Wettbewerb einschränken, Innovationen hemmen und die Vielfalt der digitalen Ökosysteme verringern.

# Fragwürdige Praktiken heute skalieren morgen im Metaverse!

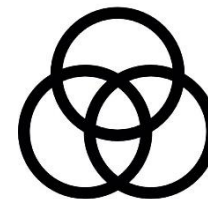
**Der "Sekundärraum", zu dem sich die digitale Welt entwickelt hat, muss sich spätestens mit dem Metaverse zivilisatorischen Kriterien stellen – sonst müssen wir eine Welt akzeptieren, die "barbarisch" werden kann.**

**Wir brauchen eine Zivilisationskampagne!**

**Wir brauchen die Zivilverrechtlichung der digitalen Welt!**

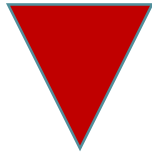
# Ethische Grundsätze wären vorhanden

1. Schutz der Privatsphäre
2. Gleichheit und Nicht-Diskriminierung
3. Informationelle Selbstbestimmung
4. Transparenz
5. Kontrolle der eigenen (digitalen) Identität
6. Solidarität
7. Kontextuelle Integrität
8. Eigentums- und Urheberrecht



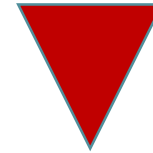
# Status Quo in den meisten Unternehmen

**Gesetz ist Pflicht**



**= must have**

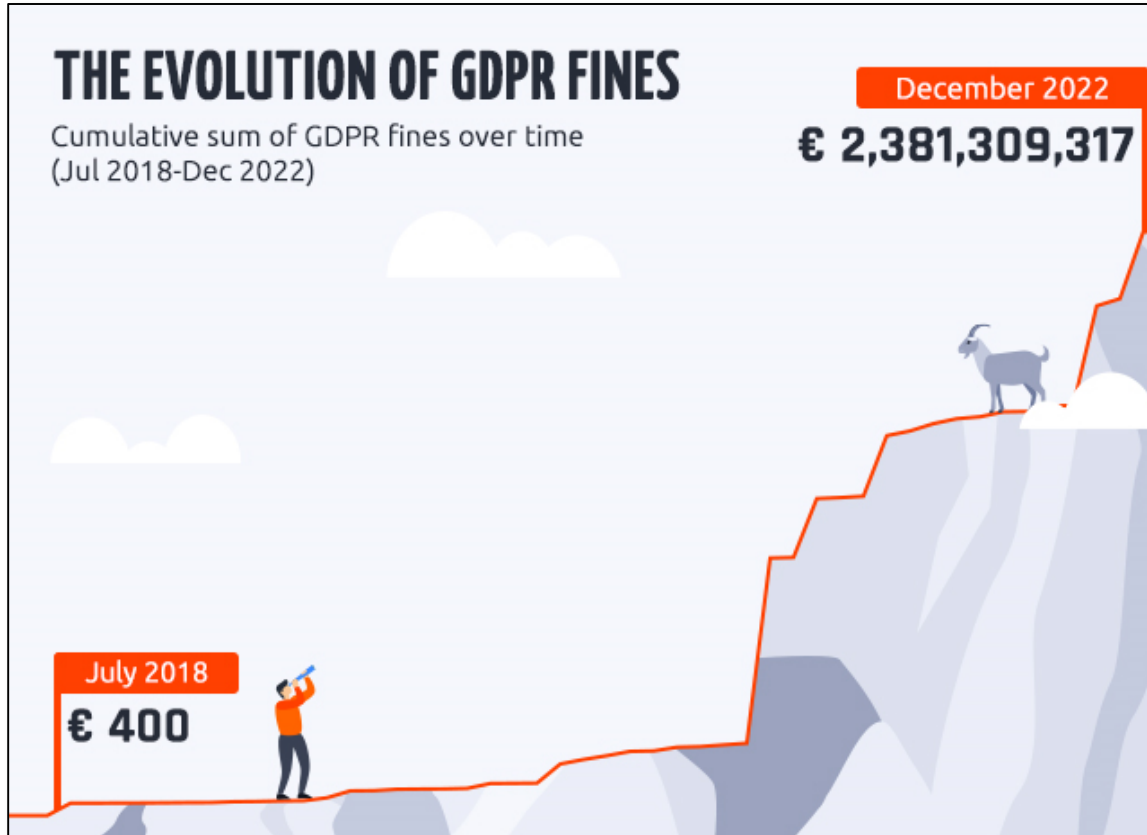
**Ethik ist Kür**



**= nice to have**

- das Gesetz wird immer komplexer und weitreichender
- die Schnittmenge zu ethischem Verhalten wird immer grösser und das Gesetz somit weniger fassbar
- die Konsequenzen aus zwar gesetzestreuem, aber noch nicht gesetzlich geregelterm Verhalten werden potentiell schwerwiegender

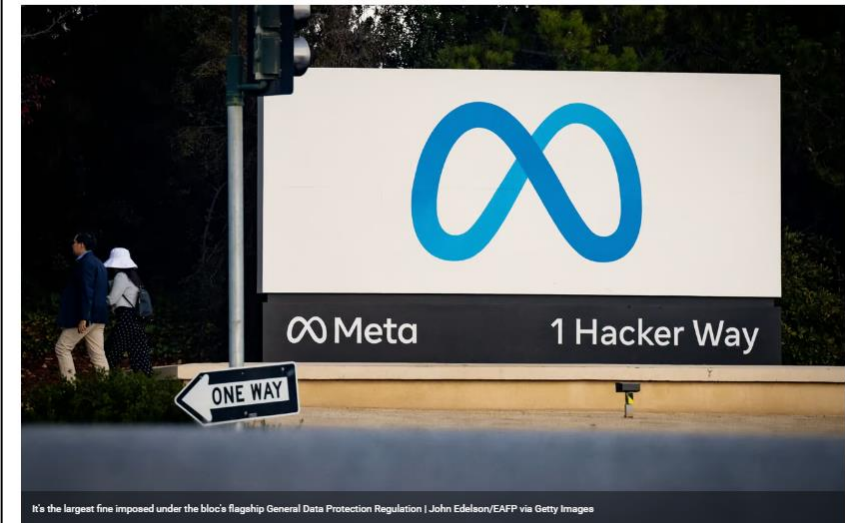
# GDPR kann teuer werden



<p><b>amazon</b></p> <p>1. Amazon – €746 million (\$677 million)</p> <p>Amazon's gigantic GDPR fine, announced in the company's July 2021 earnings report, is nearly 10 times bigger than the previous record. The full reasons behind the fine haven't yet been confirmed, but we know the cause has to do with cookie consent.</p> <p>And this isn't the first time Amazon has been punished due to the way it collects and shares personal data via cookies. In late 2020, France fined Amazon €35 million after the tech giant allegedly failed to get cookie consent on its website.</p> <p>How the fine could have been avoided: It's tempting to force users to "agree" to cookies—or make opting out of cookies difficult—to collect as much personal data as possible. But regulators have shown some serious appetite for enforcing the EU's cookie rules recently. If Amazon had obtained "freely given," informed, and unambiguous opt-in consent before selling cookies on its users' devices, the company probably could have avoided this huge GDPR fine.</p>	<p><b>WhatsApp</b></p> <p>2. WhatsApp – €225 million (\$255 million)</p> <p> mere months after Amazon's colossal GDPR fine knocked Google off the number one GDPR fine spot, WhatsApp pushed Google into third place with a penalty nearly five times as large as the search giant's previous record. Ireland slammed WhatsApp with a €225 million GDPR penalty after claiming that the messaging service had failed to properly explain its data processing practices in its privacy notice.</p> <p>Ireland is not known for issuing large fines, cookie being the European home of nearly every US-based big tech firm. And even this penalty arrived only after other EU data protection authorities used the "disproportionate" mechanism to argue that it should have been higher. So what did WhatsApp do wrong? It's complicated, and the company is appealing the decision.</p> <p>But it boils down to WhatsApp's alleged failure to explain its legal basis for certain data processing — "legitimate interests."</p> <p>How the fine could have been avoided: The Irish DPA said that WhatsApp's somewhat opaque privacy notice was at fault here—the company should have provided privacy information in an easily accessible format using language its users could understand. If you're relying on "legitimate interests," you must make sure you explain what those interests are in respect of each relevant processing operation.</p>	<p><b>Google</b></p> <p>5. Google LLC – €60 million (\$68 million)</p> <p>This Jan 6 fine against Google's California headquarters came alongside the CNIL's €90 million penalty against the search giant's European establishment (see fine number 3, above). That larger sanction was linked against Google's non-compliant selling of cookies on the YouTube platform.</p> <p>Google LLC was hit with this €60 million blow on the same day for precisely the same reason—but in relation to its search website rather than its video-sharing platform.</p> <p>How the fine could have been avoided: The latecomer in both Google cases is clear: make sure it's as easy for your users to accept cookie consent as it is for them to refuse it.</p>
<p><b>Google</b></p> <p>3. Google Ireland – €90 million (\$102 million)</p> <p>The French data protection authority (the CNIL) hit Google Ireland with this substantial fine on Jan 6, 2022. The fine relates to the way Google's European arm implements cookie consent procedures on YouTube. The Google Ireland fine was one of two fines issued as part of the same decision, with the other being levied against California-based Google LLC, which operates Google Search.</p> <p>So what's the issue? In a nutshell, the CNIL said that Google should have made it easier for YouTube users to refuse cookies. YouTube asks cookies on our devices to track our online activity for marketing purposes. It's easy to accept cookies on YouTube, but harder to refuse them. The CNIL noted that refusing cookies required a user to make several clicks, whereas accepting cookies required just one click.</p> <p>The CNIL justified the relatively high fine by pointing to the large number of people using YouTube and the huge profits that Google derives from the service. But not a minute passed Google ran its EU operations out of Ireland! How come the Irish regulator didn't dethrone this fine?</p> <p>The reason, the CNIL contended, is that cookie regulation primarily falls under the ePrivacy Directive, not the GDPR, so regulators can take direct action against website operators in their jurisdiction rather than referring everything back to the organizations' "main establishment." But the decision still qualifies as a "GDPR fine" because it's the GDPR that determines how website operators obtain consent.</p> <p>How the fine could have been avoided: Under the GDPR, consent must be "freely given," usually easy to accept or refuse, if you can accept w</p>	<p><b>facebook</b></p> <p>4. Facebook – €60 million (\$68 million)</p> <p>Facebook's second largest GDPR fine (excluding its WhatsApp fine, above) came from the French data protection authority, the CNIL, on Jan 6, 2022. The social media giant earned this €60 million penalty owing to its ongoing failure to obtain proper cookie consent from its users.</p> <p>The issue here mainly related to the unclear way in which Facebook provided a cookie opt-out. Like with Google (see above and below), accepting cookies on Facebook is a piece of cake—just click "accept," including them is a little more complicated.</p> <p>How the fine could have been avoided: The CNIL drew attention to how Facebook's cookie consent interface seemed to offer no option except "Accept Cookies," even when it appeared that users were actually refusing them. The CNIL reflected that this language "necessarily generates confusion and that the user may have the feeling that it is not possible to refuse the deposit of cookies and that they have no way to manage it. Such a confusion may cause users to have a false sense of security and to click on the 'accept' button without understanding the consequences of their choice."</p>	<p><b>Google</b></p> <p>6. Google – €50 million (\$56.6 million)</p> <p>Google's fine, levied in 2019 and finalized after an unsuccessful appeal in March 2020, was the largest on record until August 2021.</p> <p>The case related to how Google provided privacy notice to its users—and how the company requested their consent for personalized advertising and other types of data processing.</p> <p>How the fine could have been avoided: Google should have provided more information to users in consent policies and granted them more control over how their personal data is processed.</p>
<p><b>facebook</b></p> <p>7. H&amp;M – €35 million (\$41 million)</p> <p>On October 5, 2020 the Data Protection Authority of Hamburg, Germany, fined clothing retailer H&amp;M €35,236,100.16 – the second-largest GDPR fine ever imposed at the time.</p> <p>H&amp;M's GDPR violations involved the "monitoring of several hundred employees." After employees took vacation or sick leave, they were required to attend a return-to-work meeting. Some of those meetings were recorded and accessible to over 50 H&amp;M managers.</p> <p>Senior H&amp;M staff gained "a broad knowledge of their employees' private lives... ranging from rather harmless details to family issues and religious beliefs." This "detailed profile" was used to help evaluate employees' performance and make decisions about their employment.</p> <p>How the fine could have been avoided: H&amp;M appears to have violated the GDPR's principle of data minimization by collecting and processing more data about people's health and</p>	<p><b>"Biggest" Fines der letzten 24 Monate</b></p>	

## EU hits Meta with record €1.2B privacy fine

Tech giant transferred Europeans' data to the US unlawfully, Irish privacy regulator said.



It's the largest fine imposed under the bloc's flagship General Data Protection Regulation | John Edelson/EAFP via Getty Images

BY CLOTHILDE GOJJARD AND MARK SCOTT

MAY 22, 2023 | 10:50 AM CET | 4 MINUTES READ

# GDPR wird durchgesetzt

Show  entries Search:

	ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
	<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	<input type="text" value="Filter Column"/>		<input type="text" value="Filter Column"/>	
	ETid-1448	 FRANCE	2022-10-17	20,000,000	Clearview AI Inc.	Art. 6 GDPR, Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 31 GDPR	Insufficient fulfilment of data subjects rights	<a href="#">link</a> <a href="#">link</a>
	ETid-1268	 GREECE	2022-07-13	20,000,000	Clearview AI Inc.	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 27 GDPR	Non-compliance with general data processing principles	<a href="#">link</a>
	ETid-1190	 UNITED KINGDOM	2022-05-18	9,000,000	Clearview AI Inc.	Art. 5 (1) a), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 22 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles	<a href="#">link</a> <a href="#">link</a>
	ETid-1098	 ITALY	2022-02-10	20,000,000	Clearview AI Inc.	Art. 5 (1) a), b), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 27 GDPR	Non-compliance with general data processing principles	<a href="#">link</a> <a href="#">link</a>
	ETid-1035	 GERMANY	2020	10,000	Clearview AI Inc.	Art. 58 (1) GDPR	Insufficient cooperation with supervisory authority	<a href="#">link</a>

[Home](#) [License](#) [Privacy](#) [Imprint](#)

# Wie können wir das Metaversum "zivilisieren"?

- **Senkung der technischen Zugangsbarrieren:** Kompatibilität und Open Data.
- **Senkung der sozialen Zugangsbarrieren:** Zugang nicht nur für Menschen mit Hochleistungscomputern und teurem VR-Equipment.
- **Förderung von Vielfalt und Inklusion:** Das Metaverse sollte so gestaltet sein, dass es Vielfalt und Inklusion fördert, damit sich jeder willkommen und wertgeschätzt fühlt.
- **Umsetzung von Cybersicherheitsmassnahmen:** Wie bei jeder digitalen Plattform sind Cybersicherheitsmassnahmen essentiell, um Nutzerdaten vor Cyberangriffen zu schützen.
- **Schutz der Privatsphäre der Nutzer:** Das Metaverse sammelt riesige Datenmengen über Nutzerverhalten, Präferenzen und Interaktionen, die für verschiedene Zwecke genutzt werden können.

# Wie können wir das Metaversum "zivilisieren"?

**Schaffung rechtlicher Rahmenbedingungen:** Es bedarf klarer rechtlicher Rahmenbedingungen, die den Datenschutz und die Privatsphäre im Metaversum regeln

**Aufklärung der Nutzer:** Die Aufklärung der Nutzer über Datensicherheit und Datenschutz ist unerlässlich, um sicherzustellen, dass sie die Risiken verstehen und angemessene Massnahmen zum Schutz ihrer Daten ergreifen.

**Entwicklung neuer Technologien:** Tools und Services, die Anwendern beim Datenschutz helfen oder Entwicklern bei der Priorisierung von Datensicherheit und Datenschutz helfen, Metaverse zivilisierter zu machen.



Und wer kümmert sich darum?  
Wie kriegen wir das hin?



# Und wer kümmert sich darum? Wie kriegen wir das hin? Wer ist in der Verantwortung?

Institute for Ethics and Emerging Technologies <https://ieet.org/>

Center for Humane Technology <https://www.humanetech.com/>

Partnership on AI <https://partnershiponai.org/>

The IEEE Global Initiative <https://standards.ieee.org/industry-connections/ec/autonomous-systems/>

AI4People <https://www.eismd.eu/ai4people/>

AI Now Institute <https://ainowinstitute.org/>

AlgorithmWatch <https://algorithmwatch.ch/de/>

Responsible Metaverse Alliance <https://responsiblemetaverse.org/>

# Wer trägt die Verantwortung für die Zivilisierung der digitalen Welt(en)?

Gehen Sie auf [menti.com](https://www.menti.com) und geben Sie den folgenden Code ein:

**39 69 56**

oder scannen Sie den QR-Code.



Reue ist Verstand, der zu spät  
kommt.

---

(Ernst Freiherr von Feuchterleben)

# Stories: Leben im Metaverse

## **Geschichte 1: Sexuelle Diskriminierung im Metaverse**

Emma lebt in einem Land, das im Metaverse eine restriktive politische Agenda verfolgt. Obwohl sie talentiert und motiviert ist, findet sie keine angemessenen Beschäftigungsmöglichkeiten. Im Metaverse wird sie wiederholt sexuell diskriminiert, da die politischen Regeln und Richtlinien des Landes diskriminierende Verhaltensweisen tolerieren. Emma erlebt Belästigung und Ausgrenzung, was ihre Erfahrungen im Metaverse stark beeinträchtigt. Sie fühlt sich machtlos, da die Politik ihre Situation nicht verbessert und sie daran hindert, ihr volles Potenzial auszuschöpfen.

## **Geschichte 2: Das Monopol und das Verschwinden der Demokratie im Metaverse**

Im Laufe der Zeit haben einige grosse Unternehmen im Metaverse ihre Stellung weiter gefestigt und ein nahezu uneinnehmbares Monopol errichtet. Diese Unternehmen beherrschen die Infrastruktur und Dienstleistungen des Metaversums und können dadurch die Spielregeln bestimmen. Sie nutzen ihre Macht, um politische Entscheidungen zu beeinflussen und schliesslich die Demokratie zu untergraben. Durch Lobbyarbeit und wirtschaftlichen Druck gelingt es ihnen, ihre eigenen Interessen über die der Gesellschaft zu stellen. Die Bürger verlieren das Vertrauen in die demokratischen Institutionen, da diese von den Unternehmen kontrolliert werden.

# Stories: Leben im Metaverse

## **Geschichte 3: Zunahme von cyberkriminellen Angriffen im Metaverse**

Im Metaverse, das eine immer grössere Rolle im Alltag der Menschen spielt, nimmt die Anzahl und Intensität von cyberkriminellen Angriffen exponentiell zu. Im Vergleich zu heute verursachen diese Angriffe zehnmal so hohe Schäden. Die fortgeschrittene Technologie im Metaverse bietet Cyberkriminellen neue Möglichkeiten, Zugang zu sensiblen Daten zu erhalten, Identitäten zu stehlen und Betrug zu begehen. Die Schäden belaufen sich auf Milliarden von Dollar, während die Opfer mit den Konsequenzen kämpfen und das Vertrauen in die Sicherheit des Metaversums schwindet.

## **Geschichte 4: Innovation und Datenschutz im Metaverse**

Im Metaverse gibt es strenge Regulierungen zum Schutz von Daten und zur Nutzung von Künstlicher Intelligenz (KI). Dies führt zu einer Welt, in der Privatsphäre-Verletzungen verpönt sind und AI ausschließlich zum Wohl der Allgemeinheit eingesetzt wird. Dank dieser starken Regulierung entsteht eine Umgebung, in der Innovation gefördert wird. Ein Beispiel dafür ist ein revolutionäres medizinisches Forschungsprojekt, das auf aggregierten, anonymisierten Daten basiert. Die Kombination von AI-Analysen und Datenschutzbestimmungen ermöglicht es Wissenschaftlern, Krankheitsmuster zu erkennen, personalisierte Behandlungen zu entwickeln und medizinische Durchbrüche zu erzielen. Ähnliche Innovationsbeispiele gibt es in den Bereichen nachhaltige Energie und Bildung, da Datenschutz und das Gemeinwohl Vorrang haben.