ZE
VE
DI

ShareCast Folge 9

Datenschutz: Daten geben und Rechte behalten

Moderation: Till Seidemann & Konstantin Schönfelder

[Atmo Jingle]

[Opening:] Herzlich Willkommen zu ShareCast, dem Podcast rund ums Datenteilen. Wer teilt Daten mit wem? Warum? Wie? Wie nicht? Und welche neuen Wege gibt es?

[Sprecher 1:] Ja, das Ideal des Teilens ist unser Thema. Datenschutz und die sogenannte Datenschutzgrundverordnung, kurz DSGVO, – also der Schutz als Grenze des Teilens – gehören allerdings auch dazu. Und Datenschutzbausteine begegnen uns überall. Ob wir beim Browsen sogenannten Cookies zustimmen oder sie ablehnen, beim Arztbesuch unterschreiben, dass wir der Verarbeitung unserer Daten zustimmen oder bei einem Update unseres Smartphones in die neuen AGB einwilligen – stets haben wir es mit Datenschutz-Einwilligungen zu tun.

Aber was ist das eigentlich – Datenschutz? Was regelt die so oft genannte Datenschutzgrundverordnung „DSGVO"? Wofür und für wen ist sie wichtig? Und: *Stört* der Datenschutz eigentlich das Teilen oder bringt er sogar Potentiale in Sachen Datenteilen mit sich? Das wollen wir uns genauer ansehen.

Mein Name ist Till Seidemann, ich bin Philosoph und arbeite an der TU Darmstadt. Gemeinsam mit meinem Kollegen Konstantin Schönfelder bin ich Gastgeber der heutigen Folge.

[Sprecher 2:] Hallo, und ich bin Konstantin Schönfelder, Wissenschaftsredakteur am Zentrum für verantwortungsbewusste Digitalisierung an der TU Darmstadt. Till und ich haben diese Folge gemeinsam mit unserer Kollegin Marlin Mayer konzipiert.

Heute beschäftigen wir uns mit einem Thema, das zwar in aller Munde ist – aber es ist auch recht abstrakt: Den rechtlichen Rahmenbedingungen, die regeln, wie wir Daten teilen. Die Datenschutzgrundverordnung, kurz DSGVO, ist eines dieser Gesetze – und sie hat überall dort, wo man Daten ungehindert fließen sehen und verwerten möchte, vielleicht nicht den besten Ruf. Datenschutz verhindert das unbeschwerte Teilen.

Obwohl uns das Kürzel DSGVO mittlerweile ziemlich häufig begegnet und bekannt vorkommt, ist uns nicht immer klar, was es eigentlich genauer besagt. Wir haben daher Sven Hetmank, Wissenschaftlicher Mitarbeiter und Jurist an der TU Dresden gefragt, was die DSGVO ist und für wen sie von Bedeutung ist:

[O-Ton Sven Hetmank:] Vereinfacht kann man sagen, die DSGVO regelt, wann personenbezogene Daten verarbeitet werden dürfen und was dabei zu beachten ist. Wichtig ist, dass es wirklich nur um personenbezogene Daten geht. Also gemeint sind all jene Informationen, die irgendetwas über eine bestimmte oder zumindest bestimmbare Person aussagen. Ja, und warum ist das wichtig, darüber etwas zu wissen? Für jeden Einzelnen, weil man nahezu täglich Daten preisgibt. Wenn man auch nur im Internet surft, ist es wahrscheinlich nicht verkehrt, etwas über seine Rechte zu wissen.

[Sprecher 1:] Die DSGVO regelt also den Umgang mit personenbezogenen, sagen wir: auf unseren Eigennamen zurückführbaren Daten. Das sind zum Beispiel Gesundheitsdaten, über die wir in unserer zweiten Folge von ShareCast gesprochen haben. Aber auch bei Daten aus Geräten, wie zum Beispiel bei den Harvesterdaten, mit denen wir uns in unserer fünften Folge auseinandergesetzt haben, ist die DSGVO relevant. Denn: Auch digitale Arbeitswerkzeuge können mit personenbezogenen Daten in Verbindung stehen – zum Beispiel wenn beim Holzfällen mit großen Maschinen die Harvesterdaten Informationen über den Fahrer der Harvester enthalten. Und generell, das wissen wir alle, geben wir online alltäglich Daten preis: an Unternehmen und vielleicht auch an Behörden. So kommen wir – vielleicht, ohne es explizit zu wissen – täglich mit der DSGVO in Kontakt. Dabei kann es helfen, zu wissen, dass die DSGVO nicht nur etwas ist, dass wir selbst einhalten müssen, sondern: Die DSGVO regelt die Rechte von Datengebenden, an die sich dann auch Datennehmende, Datenverarbeiter, zu halten haben. Die DSGVO steht aber sozusagen nicht für sich alleine, sondern hängt auch noch mit weiteren Rechten zusammen. Anne Lauber-Rönsberg, Professorin für Bürgerliches Recht an der TU Dresden erklärt uns das so:

[O-Ton Anne Lauber-Rönsberg:] Die DSGVO soll sicherstellen, dass jede Person Verfügungsrechte über ihre eigenen Daten hat, auch wenn die natürlich nicht absolut sind, sondern in Einklang gebracht werden müssen mit zum Beispiel dem Recht auf Meinungsfreiheit, Informationsfreiheit. Aber im Ausgangspunkt soll jede Person bestimmen können, wer was über sie weiß und soll eben auch entsprechende Auskunftsansprüche, Kontrollrechte haben. Denn, und das ist eben der zweite Punkt, Datenschutz ist kein Selbstzweck, sondern geht auch einher mit der Ausübung sonstiger Grundrechte. Man könnte zum Beispiel davon abgehalten werden, an politischen Versammlungen teilzunehmen oder seine Meinung frei zu äußern, wenn man nicht weiß, welche Daten darüber erhoben werden und von wem für welche Zwecke verarbeitet werden. Damit[...] ist also Datenschutz auch im weitesten Sinne Grundrechtsschutz.

[Sprecher 2]: Die DSGVO regelt also im weitesten Sinne eine grundrechtliche Freiheit, die wir haben (nämlich über unsere Daten zu verfügen) und sie gibt Betroffenen Auskunftsansprüche und Kontrollrechte über ihre Daten. Was dabei eigentlich geschützt wird, sind also nicht die Daten selbst, sondern die Personen, auf welche sich die jeweiligen Daten beziehen. Hören wir dazu Steffen Augsberg, Professor für Öffentliches Recht an der Justus-Liebig-Universität Gießen:

[O-Ton Steffen Augsberg] Wir schützen eigentlich nicht die Daten. Das klingt so an in der Bezugnahme auf die personenbezogenen Daten. Schützenswert sind im rechtlichen, insbesondere im verfassungsrechtlichen Sinne nicht die Daten als irgendwie immaterielle Güter, Objekte, sondern schützenswert sind natürlich die Menschen, auf die sich diese Daten beziehen. Daraus entstehen Schwierigkeiten. In einem ganz klassischen Sinne sagt man gewissermaßen, jedes Datum, das mit mir verbunden auf mich bezogen ist, soll meiner Kontrolle unterliegen.

[Sprecher 1:] Da der Datenschutz Datengebende schützt, kann er aus dieser Perspektive als ein Gütesiegel für ein sicheres und vertrauenswürdiges Datenteilen betrachtet werden. Dazu hat uns Sven Hetmank erklärt, dass die DSGVO gleich in zweierlei Hinsicht als Pull-Faktor fürs Datenteilen angesehen werden kann:

[O-Ton Sven Hetmank:] Ich denke, da kommen vor allen Dingen zwei Aspekte in Betracht, wie Datenschutz ein Pullfaktor sein kann. Zum einen immer dort, wo Dienstleistungen angeboten und übernommen werden, die man andernfalls selber machen müsste. Also zum Beispiel das Einwilligungsmanagement mit zu übernehmen und anzubieten für die Einwilligungen zu sorgen, die man ja braucht, wenn man mit diesen personenbezogenen Daten arbeiten möchte, oder die Informationspflichten zu übernehmen, die erfüllt werden müssen, oder die Datensicherheit zu gewährleisten, oder bei den Auskunftsrechten zu unterstützen und dergleichen mehr. Und zum anderen kann es auch dort ein Pull-Faktor sein, wo es um Vertrauen geht. Also wenn ich es schaffe, zu gewährleisten, dass die Grundsätze der DSGVO besonders sicher eingehalten werden, dann kann das natürlich auch ein Pull-Faktor sein, weil ich dann dem Anbieter vertraue und darauf vertrauen kann, dass meine Daten DSGVO-konform genutzt werden."

[Sprecher 2:] Datenschutz kann folglich das Datenteilen insofern vorantreiben, als dass Menschen ihre persönlichen Daten erst einmal zurückhalten- Ich teile die Daten dann bereitwilliger, wenn ich Vertrauen darin habe, dass mit den Daten gut umgegangen wird – dass sie also trotz Weitergabe geschützt *bleiben*. Gerade im medizinischen Bereich kann der Datenschutz als ein wichtiges Instrument verstanden werden, um beispielsweise Forschung auf Patientendaten zu ermöglichen. Patienten willigen zu so einer Nutzung zu Forschungszwecken ein, wenn Forschungsprojekte Datensätze beispielsweise ausschließlich anonym oder pseudonym verwenden.

[Atmo Hammer-Gericht]:

[Sprecher 1:] Die DSGVO soll also, kurzgesagt, Datengebenden Transparenz und Kontrollrechte via Einwilligungskonzept über ihre personenbezogenen Daten geben. Wie sieht das aber in der Praxis aus? Haben Datengebende

aufgrund der DSGVO das Gefühl, dass ihre Daten vertrauenswürdig und sicher gemanagt werden? Das SINUS-Institut und YouGov haben dazu 2018 eine repräsentative Umfrage durchgeführt und schreiben zum Ergebnis auf der Website des Sinus-Instituts folgendes:

[Zitator 1:] **„**56% der Deutschen bezweifeln, dass ihre persönlichen Informationen innerhalb und außerhalb des Internets ausreichend geschützt sind. Fast genau so viele (55%) haben das Gefühl, keine Kontrolle über ihre Daten im Internet zu haben. Gleichzeitig sind sich so gut wie alle Deutschen (93%) einig, dass der Schutz persönlicher Daten wichtig ist. 64% finden sogar, dass man diesem Thema gar nicht genug Bedeutung zuschreiben kann. Dagegen finden 29%, dass dem Datenschutz mittlerweile eine zu hohe Wichtigkeit beigemessen wird.“

[Sprecher 2:] Die DSGVO reduziert also Bedenken von Datengebenden. Praktisch sehen wir gleichwohl, dass Datengebende auch trotz der DSGVO die Sorge haben, ob ihre Daten sicher sind. Mehr als die Hälfte der Befragten zweifelt daran, wirklich ein Kontrollrecht über ihre Daten zu haben. Umgekehrt steht die DSGVO allerdings auch bei denjenigen, die Daten erheben und aufbereiten wollen, in der Kritik. Hören wir dazu einmal, was verschiedene Projekte der Datentreuhändercommunity, die das Datenteilen in der Medizin vorantreiben wollen, derzeit darüber denken

[Zitator 2:] „[Wir sehen es] als eine große Herausforderung an, […] eine Praktikabilität reinzubekommen und […] Datenschutz und Technik noch besser zusammenzubringen und intuitiver zu gestalten. Denn gerade wir, die viel mit der praktischen Anwenderseite oder beziehungsweise mit der Computational-Science-/KI-Experten-Seite so zusammenarbeiten, wir merken, dass dann natürlich oft ein totaler Verständnis-Gap vorhanden ist, dass technische Vorgänge von Seiten der technischen Experten als total sicher dargestellt werden. Aber das rechtlich abzubilden, ist das jetzt datenschutzrechtskonform sicher, das ist eben sehr schwierig, so unsere Erfahrung.“

[Zitator 3:] „Wir haben vorher *alles* mit dem Datenschutz abgeklärt. Das läuft bei und auch nochmal über die Rechtsabteilung, das sind zwei getrennte Abteilungen bei uns am Uniklinikum, so dass vor Freigabe des Portals auch noch mal ein Test erfolgt, ist das so alles Datenschutz konform? Haben wir da irgendwelche offenen Stellen, die wir hätten erkennen müssen? […] insofern *versuchen wir* alles abzudecken!“

[Sprecher 1:] Praktisch können wir also sagen, ist Datenschutz alles andere als ein Selbstläufer – weder für Datengebende noch für Datennehmende. Dabei, so haben wir gehört, ist es eine Schwierigkeit ein technisches Verständnis über sicheres Datenteilen mit einem rechtlichen Verständnis in Einklang zu bringen. Eine weitere Sorge bei Datennehmende ist, dass, auch wenn man versucht hat, alles noch so gut rechtlich zu bedenken, dennoch immer Fehler passieren können. Professor Thomas Wagner, Leiter des Referenzzentrums für seltene

Erkrankungen an der Uni-Klinik in Frankfurt, berichtet aus seinem Arbeitsalltag und macht weitere Schwierigkeiten deutlich, die der Datenschutz mit sich bringt:

[O-Ton T.O.F. Wagner:] Der Datenschutz verhindert, dass wir uns untereinander austauschen. Wir dürfen, wenn wir den Patienten fragen: Dürfen wir denn ihren Befund aus der Klinik so und so anfordern? Und der Patient dem zustimmt und wir können dem Zentrum, wo wir die Daten gerne her hätten, nachweisen, dass der Patient dem explizit zugestimmt hat, dürfen wir die Daten anfordern. Wir dürften auch natürlich, wenn das Zentrum fragen: Dürften wir die Unterlagen da hinschicken? Und der Patient dem zustimmt, dann dürfen wir das auch, aber es ist alles explizit zustimmungspflichtig und man kann nicht davon ausgehen, dass wenn der Patient Hilfe will, dann kann es ihm egal sein, wo die Hilfe herkommt aus Typ A, aus dem Zentrum A oder aus dem Zentrum B. Nein, wenn er sich ans Zentrum B gewendet hat, dann darf sich nicht Zentrum-A damit befassen."

[Sprecher 2:] Damit personenbezogene Daten erhoben und verarbeitet werden dürfen, müssen die Betroffenen nach der DSGVO „einwilligen". Von Thomas. Wagner haben wir gerade gehört, dass dieses Konzept der Zustimmung, das juristisch auch unter dem Begriff „Einwilligungsmanagement" gefasst wird, in der Praxis aber Probleme mit sich bringt. Dadurch, dass, wie Wagner gesagt hat, „alles explizit zustimmungspflichtig" ist, muss immer wieder aufs Neue eine Zustimmung des Patienten erfolgen. So ist es im Klinikalltag schwierig, einen guten Austausch im Sinne der Patienten durchzuführen und mehr noch: Der Datenschutz verhindert hier, Ressourcen zu bündeln.

[Sprecher 1:]. Zum Einwilligungskonzept der DSGVO gehört es, dass der Zweck, für den die Daten erhoben werden, klar benannt wird und denjenigen, die darin einwilligen sollen, transparent gemacht wird. Dieses Konzept kann man als überholt ansehen, wie uns die Rechtswissenschaftlerin Anne Lauber-Rönsberg erklärt hat:

[O-Ton Anne Lauber-Rönsberg:] Da muss man allerdings auch ganz kritisch sagen, dass dieses Grundkonzept der Einwilligung in vielen Fällen nicht mehr funktioniert. [Eine] Einwilligung ist ja rechtlich gesehen nur dann wirksam, wenn sie informiert und freiwillig erfolgt. Und bei der Vielzahl von Einwilligungen, die wir täglich abgeben, zum Beispiel im Kontext von Cookies, wie gerade diskutiert, ist das ja gar nicht mehr möglich, dass man jedes Mal im Vorhinein auch sich darüber informiert, wer denn dann tatsächlich die Daten zu welchen Zwecken verarbeiten möchte. Und deswegen ist dieses Rechtsinstrument der Einwilligung auch so in die Kritik geraten. Es gibt schon seit längerem Diskussionen darüber, ob man diesen datenschutzrechtlichen Erlaubnistatbestand in irgendeiner Form reformieren oder ändern sollte.

[Sprecher 2:] Die Idee, dass Datengebende durch die DSGVO Kontrolle über ihre Daten haben, läuft also womöglich ein Stück weit ins Leere: Wie sollen wir

diese Kontrolle ausüben, wenn wir bei der Menge an Daten, die wir hinterlassen, keinen Überblick mehr darüber haben, wer welche Daten wo und zu welchem Zweck erhoben, gespeichert oder gar weitergegeben hat? Und was hilft die ganze Einwilligerei, die zwar häufig, aber auch irgendwie blind und nur als „ja“ oder „nein“ erfolgt?
Dass die DSGVO reformbedürftig ist und sozusagen weitergedacht werden muss, haben wir auch in unserem Gespräch mit Steffen Augsberg gehört:

[O-Ton Steffen Augsberg:] Unsere datenschutzrechtlichen Vorgaben stammen aus einer Zeit, wo nicht nur das Internet oder künstliche Intelligenz, [...], sondern auch Datenverarbeitung auf großem elektronischen Wege eigentlich eher so erkennbar, aber noch nicht wirklich vorhanden war. Und darauf in dieser Weise zu reagieren und schon zu sagen, naja, wir schaffen Regelungen, die so allgemein gehalten sind, im positiven Sinne, dass sie sich über die Jahrzehnte hinweg nicht nur in Deutschland bewährt haben, sondern ja auch in gewisser Weise einen Exportschlager dann kreiert haben, weil wir diese Vorstellung vom Datenschutzrecht jetzt [...] in der gesamten Europäischen Union, aber natürlich darüber hinausgehend auch beispielsweise in Brasilien, wo die sich sehr eng an die DSGVO angelehnt haben und anderen Orts vorfinden, das ist schon eine große Leistung. Trotzdem gibt es Spannung. Das gehört, glaube ich, dann auch zur Wahrheit dazu, dass man sagen muss, so sehr man den Hut davor zieht, was da geleistet worden ist und wie zukunftsweisend tatsächlich auch innovationsfördernd das war, so sehr muss man sehen, dass natürlich irgendwelche Friktionen gewissermaßen je älter ein Gesetz ist oder je ältere ein Rechtsprinzip ist, natürlich auch nicht ausbleiben. Insofern sind wir in einer fortwährenden Arbeit des Weiterdenkens, weiter Verbesserns, weiter Überlegens, was man da eigentlich noch zukunftsorientiert anders und optimaler machen könnte.

[Sprecher 1:] Wir sollten die DSGVO also sozusagen nicht in Stein meißeln, sondern weiterdenken – nicht zuletzt auch deshalb, weil sich die Innovationen selbst, auf die sich die Rechtsprechungen beziehen, weiterentwickeln. Die DSGVO und die europäische Datenstrategie sind also keine fertigen Produkte. Auch wenn Vieles darin bedacht ist, wie zum Beispiel auch dass wir unsere Rechte nicht verlieren, wenn wir unsere Daten in andere Länder mit anderen Datenschutzbestimmung übertragen, müssen wir, wie Augsberg sagte, weiter über Rechtsakte wie die DSGVO nachdenken und sie verbessern. Das sieht auch die Juristin Anne Lauber-Rönsberg so. Sie sieht das Thema als Gegenstand eines dynamischen Politikfeldes:

[O-Ton Anne Lauber-Rönsberg:] Also gerade dieses Austarieren von Datenschutz auf der einen Seite, Datennutzung auf der anderen Seite, ist ja ein Prozess, für den man sicherlich auch Zeit braucht. Und hier stellen wir ja auch fest, dass hier durchaus sehr unterschiedliche Wertvorstellungen aus einer globalen Perspektive aufeinanderprallen, dass also zum Beispiel Europa insgesamt eher datenschutzfreundlich ist, während die USA zum Beispiel die Nutzung von personenbezogenen Daten durch Unternehmen ja in viel

weitgehenderen Maße freigeben und erlauben, als dass zum Beispiel das europäische Recht vorsieht.

[Atmo Hammer-Gericht]

[Sprecher 2:] Wir haben gehört, dass es in der Praxis häufig gar nicht so einfach ist, Kontrollrecht über die eigenen Daten auszuüben – nicht zuletzt, da es bei der Menge an Daten, die wir hinterlassen, gar nicht so leicht ist, zu wissen, wer welche Daten von uns wo und zu welchem Zweck gespeichert oder verwendet hat. Dazu hat Steffen Augsberg darauf hingewiesen, dass auf Informationsfreiheit abzielende Auskunftsersuche zu personenbezogenen Daten gerade aus Datenschutzgründen zurückgewiesen werden:

[Steffen Augsberg:] [D]ie Informationsfreiheit ist ja eigentlich eine moderne Anforderung transparenter Verwaltung oder überhaupt transparenten, hoheitlichen Handelns. Wir entfernen uns davon, dass man eine spezifische Begründung geben muss, sondern sagen, eigentlich soll unser Staat uns Bürgern gegenüber so durchsichtig wie möglich sein. Und dann kommt sofort das Problem, Durchsichtigkeit kann auch immer andere Rechte beeinträchtigen Und ein zentraler Aspekt dabei ist der Datenschutz. Und deshalb werden Informationsfreiheitsanträge nicht sehr selten zurückgewiesen, damit, dass man sagt, hier sind personenbezogene Daten dritter betroffen und aus Datenschutzgründen kann diese Anfrage nicht beantwortet werden.

[Sprecher 1:] Steffen Augsberg wirkt in einem Datentreuhandprojekt mit, das an der Schnittstelle von Datenschutz und informationeller Selbstbestimmung operiert:

[O-Ton Augsberg:]: Die Idee wäre jetzt zu sagen, durch den Datentreuhänder kann dieser Personenbezug insoweit reduziert werden, dass Anfragen beantworten werden können, ohne dass dafür datenschutzrechtliche Beeinträchtigungen vorgenommen werden müssten.

[Sprecher 2:] Das Konzept, das DaGarIn für Datentreuhänder erarbeitet, vermittelt genauer gesagt zwischen den behördlichen Interessen und den Interessen von Auskunftsersuchenden. Dabei bringt er beider Interessen dadurch in Zusammenhang, dass er die angefragten Daten von ihrem Personenbezug befreit, sodass einerseits Verwaltungen die Daten ohne datenschutzrechtliche Bedenken teilen können, und andererseits Betroffene Auskunft über ihre Daten erhalten und damit ihr Recht auf informationelle Selbstbestimmung ausüben können. Wie so ein Datentreuhandmodell – es heißt „transaktionsbasiert“ – genauer funktioniert, schauen wir uns in unserer zehnten Folge von ShareCast an und verabschieden uns für heute.

[Sprecherin 1:]: In der nächsten Folge werfen wir einen Blick in die Schweiz und zeigen, wie unser Nachbar die herausforderungen des Datenteilens auf seine Weise gestaltet, ohne Mitglied in der EU zu sein.

Mehr Infos zum Thema und weiterführende Links finden Sie in den Shownotes zur Folge.
Mein Name ist Till Seidemann

[Sprecher 2]: Und ich bin Konstantin Schönfelder. Danke fürs Zuhören und bis zur nächsten Folge.

[Atmo Jingle]: ShareCast - der Podcast rund ums Datenteilen

This work is licensed under CC BY-NC-ND 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/