FACHBEITRAG

Die verheerenden Folgen von Datenmissbrauch

Artikel von Felix Rausch · 6. Dezember 2023

Gerade jetzt zur besinnlich(st)en Zeit des Jahres sollten wir uns daran erinnern, warum wir personenbezogene Daten schützen wollen. Nicht allein die Angst vor Sanktionen sollte unser Leitbild des Datenschutzes ausmachen, sondern vielmehr das Risikobewusstsein dafür, warum dieser – gerade im Einzelfall für jeden – so essenziell sein kann. „Wieso beansprucht die DSGVO in Europa so einen hohen Stellenwert? Mal ehrlich: Was kann schon im schlimmsten Fall passieren?“

Der Inhalt im Überblick

Die richtige Motivation für Datenschutz

Fragen, die sich die eine oder der andere zwangsläufig schon einmal gestellt hat, wenn mal wieder eine lästige Datenschutzschulung ansteht oder die datenschutzkonforme Umsetzung von Arbeitsprozessen im Betrieb Kopfschmerzen bereitet. Mehr Sicherheit kann auch Einschränkungen bzw. erheblichen Mehraufwand mit sich bringen. Wenn man angehalten ist, sich selbst einzuschränken sowie seine eigenen und die Daten anderer zu schützen, wäre es aber schon von Vorteil, wenn man wissen oder jedenfalls erahnen könnte, warum man dies so hingebungsvoll tut.

Auch wenn die aufgeworfenen Fragen erst einmal banal klingen mögen, die Antwort darauf erschließt sich nicht auf Anhieb. Jedenfalls nicht in der gesamten Reichweite. Denn die wirklichen schmerzlichen Konsequenzen eines Miss- oder Fehlgebrauchs personenbezogener Daten sind – wie diese selbst – zunächst einmal nicht sofort greifbar. Die daraus resultierenden Gefahren erscheinen erstmal wie ein fernliegendes Phänomen.

Datenmissbrauch: Die unsichtbare Gefahr

In unserem täglichen Leben sind wir normalerweise viel sichtbareren und spürbareren Gefahren ausgesetzt. Wir haben als generell vernunftbegabte Wesen gelernt, dass manche Verhaltensweisen oder Regeln Risiken vorbeugen, welche wir unbedingt vermeiden wollen. So schließen wir beispielsweise die Wohnung ab und unsere Fahrräder an, um Diebstähle zu verhindern, schauen gewissenhaft in alle Richtungen, bevor wir die Straße überqueren, um nicht überfahren zu werden, oder fahren selbst im Auto nicht zu schnell durch die Spielstraße, um andere nicht zu gefährden. Das leuchtet ein. Zumindest den meisten.

Unser geordnetes Zusammenleben basiert zum großen Teil aus diesen Verhaltensregeln, welche sich vielfach auch in strafbewährten Präventivmaßnahmen in Form von Gesetzen widerspiegeln. Abgesehen von Bereichen, in denen ein Hang zur Überregulierung zu spüren ist, liegt die Befolgung der meisten aufgestellten Regeln in unserem eigenen Interesse bzw. dient dem nachvollziehbaren Schutz berechtigter Rechte unserer Mitmenschen. Naja, so sollte es eigentlich sein.

Schutzzweck der DSGVO: Mehr als nur Datenmissbrauch

Um die hochrangige Bedeutung des Datenschutzes in seiner ganzen Dimension zu verstehen, hilft vielleicht erstmal ein kurzer Blick ins Gesetz. Die DSGVO beschreibt ihre Berechtigung in Art. 1 Abs. 2 wie folgt:

> „Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten"

Es geht also um den Schutz unseres Grundrechtes auf informationelle Selbstbestimmung. So weit so klar, aber immer noch nicht wirklich konkret.

Das Recht auf informationelle Selbstbestimmung

Auf europäischer Ebene ist der Schutz personenbezogener Daten ein Grundrecht (Art. 8 GRCh), welches aber immer in Verbindung mit dem Grundrecht auf Privatsphäre (Art. 7 GRCh) gelesen wird. In der deutschen Verfassung ist das Recht auf informationelle Selbstbestimmung hingegen nicht explizit geregelt.

Das Bundesverfassungsgericht hat es in seinem Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) entwickelt und versteht es als eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts.

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

Zur Begründung führt das Bundesverfassungsgericht weiter aus:

> „Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt […] Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."

Nun kommen wir der Sache schon etwas näher. Die Kernaussage ist also, dass sich der einzelne Bürger nur dann wirklich frei entfalten kann, wenn er nicht das Gefühl haben muss, unfreiwillig von irgendeiner Seite bewertet oder gar abgewertet zu werden und hierdurch ggf. Nachteile zu erfahren.

Abwehrrechte gegen den Staat

Ohne die weiteren Hintergründe des Volkszählungsurteils zum wiederholten Mal im Detail durchzugehen, lässt sich doch aber erstmal festhalten, dass es bei dem Recht auf informationelle Selbstbestimmung in erster Linie um ein Abwehrrecht des Bürgers gegen den Staat und seine Institutionen geht. Datenschutz ist also Grundrechtsschutz und damit integraler Bestandteil des modernen Rechtsstaates.

Deswegen ist u.a. das Ausspähen privater Daten aus einem staatlichen Interesse heraus strengen Beschränkungen unterworfen. Viel staatliche Maßnahmen wurden auf den höchstrichterlichen Prüfstand gestellt und für unzulässig erklärt (z.B. präventive Rasterfahndung, „großer Lauschangriff" und Vorratsdatenspeicherung). Die Verhinderung eines umfassenden „orwell'schen" Überwachungsstaates dürfte oberste Priorität haben. Keine Frage.

Mit steigendem Überwachungsdruck sinkt in der Regel auch die Bereitschaft, sich so frei zu verhalten, wie man es sich vielleicht eigentlich wünscht. Dazu gesellt sich eine gewisse Ambivalenz. Nämlich die Diskrepanz zwischen Sicherheit und Freiheit. Einerseits will sich die Bevölkerung in ihrem Lebensumfeld sicher fühlen und dürfte sich gerade in bedrohlichen Situationen beispielsweise über eine Kameraüberwachung oder die Verhinderung eines Terroranschlages erleichtert zeigen.

Andererseits wäre es auch ein unangenehmes Gefühl, zu wissen, dass der Staat oder andere Einrichtungen einen bei jeder Gelegenheit, „auf Schritt und Tritt" über die Schulter schauen. Auch dann, wenn man eigentlich „nichts zu verbergen" hat. Mit dem zunehmenden Gefühl, beobachtet zu werden, steigt auch die Angst, womöglich ungewollt gegen gewisse Verhaltensregeln und Gesetze zu verstoßen. Eine Angst allerdings, welche zumindest in Deutschland der größte Teil der Bevölkerung nicht (mehr) haben wird. Gerade auch wegen der hohen Bedeutung des Datenschutzes in Deutschland. In manch anderen Ländern sieht es allerdings ganz anders aus.

Verantwortung für Freiheitsrechte der Betroffenen

Nur was haben private Einrichtungen und Unternehmen sowie ihre einzelnen Mitarbeiter damit am Hut? Die DSGVO erlegt auch ihnen zum Schutz der Daten umfangreiche Pflichten auf. Und das muss auch so sein. Denn der Staat hat durch seine Gesetze sicherzustellen, dass nicht von ihm selbst, sondern auch von keinem anderen das Recht auf informationelle Selbstbestimmung in erheblichen Umfang verletzt wird.

Wer personenbezogene Daten verarbeitet, sollte bei der Einhaltung von Datenschutz und -sicherheit bedenken, welche Konsequenzen ein gezielter Missbrauch von Daten im schlimmsten Fall mit sich bringen kann. Und hiermit sind nicht nur Tracking und personalisierte Werbung gemeint, welche v.a. Unternehmen durch Auswertung personenbezogener Daten einseitig große finanzielle Vorteile einbringen. Bei der DSGVO geht es um mehr. Wesentlich mehr. Nämlich um verehrende persönliche Konsequenzen.

Hier bringt der Erwägungsgrund 75 der DSGVO Licht ins Dunkle. Denn hier werden die tatsächlichen Gefahren bei der Verarbeitung personenbezogener Daten für die Rechte und Freiheiten der Betroffenen aufgezählt, welche materielle oder immaterielle Schäden führen können:

- Identitätsdiebstahl oder -betrug,
- Diskriminierung aufgrund religiöser oder weltanschaulicher Überzeugungen und sexueller Vorlieben,
- Rufschädigung sowie erhebliche wirtschaftliche oder gesellschaftliche Nachteile,
- Bewertung von Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben oder Interessen,
- Verlust der Vertraulichkeit von Berufsgeheimnissen.

Wie man unschwer aus der Aufzählung ersehen kann, geht es bei dem Schutz personenbezogener Daten also um nichts Geringes als um die Sicherung elementarer und existentieller Werte:

> „Datenschutz schützt keine Daten, sondern den Menschen!"

Das Gespür für Datenmissbrauch

Nicht nur die versehentliche Falschverarbeitung, Veröffentlichung oder Löschung von personenbezogenen Daten kann gravierende Folgen für die Betroffenen nach sich ziehen. Viel schlimmer wird es, wenn die Daten mit eindeutiger Schädigungsabsicht von unbekannten Dritten erbeutet und im Darknet an Datenbroker „vertickt werden". Werden personenbezogene Daten benutzt, um damit kriminelle Handlungen zu begehen, spricht man von Datenmissbrauch.

In einer digital vernetzten Welt, in der Daten allgegenwärtig sind, nimmt die Bedrohungslage durch IT-Angriffe (u.a. Phishing, Trojaner, Spyware oder Malvertising) für Privatpersonen, Wirtschaft und Staat laut des Lageberichts der IT-Sicherheit in Deutschland des Bundesamtes für Sicherheit in der Informationstechnik stetig weiter zu.

Die Gefahren für unsere bürgerliche Existenz lassen sich wohl am besten anhand markanter Beispiele vor Augen führen. Hierfür beleuchten wir die möglichen Folgen von Identitätsdiebstahl und Betrug, Rufschädigung bzw. Diskriminierung und Arbeitsplatzverlust.

Identitätsdiebstahl – der perfide Missbrauch von Identitäten

Öffentliche Stellen, aber vor allem auch Unternehmen sammeln eine Vielzahl von personenbezogenen Daten, darunter Namen, Geburtsdaten, Adressen und Sozialversicherungsnummern. Einmal in die falschen Hände geraten, können Kriminelle unter fremden Namen betrügerische Transaktionen durchführen, Warenkäufe tätigen und Kredite aufnehmen und somit das Leben Einzelner in Scherben legen.

Die Betroffenen erfahren meist erst vom Identitätsdiebstahl, wenn sie entweder in ihrem Briefkasten oder E-Mail-Postfach Rechnungen, Inkasso-Schreiben oder gerichtliche Mahnbescheide entdecken. Auch wenn die Schufa-Auskunft überraschenderweise Schuldeneinträge enthält und Unternehmen plötzlich die Bonität in Zweifel ziehen, könnte dahinter möglicherweise ein Identitätsdiebstahl stecken.

Was bedeutet Identitätsdiebstahl?

Durch die zunehmende Digitalisierung avancierte Identitätsdiebstahl – oder auch Identitätsklau – in den letzten Jahren zu einem der bedeutendsten Cybergefahren der heutigen Zeit. Die Agentur der Europäischen Union für Cybersicherheit (kurz: Enisa) definiert Identitätsdiebstahl wie folgt:

> „Identitätsdiebstahl oder Identitätsbetrug ist die illegale Verwendung der personenbezogenen Daten eines Opfers durch einen Betrüger, um sich als diese Person auszugeben und einen finanziellen und andere Vorteile zu erzielen"

Verbraucherschutz zeigt sich besorgt über die Zunahme von Identitätsdiebstahl

Den Verbraucherschutzzentralen zufolge gibt es etliche Beispiele für den Missbrauch von Verbraucherdaten:

- Kriminelle nutzen die Daten, um beispielsweise Hörbücher oder Lizenzschlüssel für Software ein- und anschließend weiterzuverkaufen oder unberechtigt teure Streaming, Premium-Online-Dienste oder Dating-Portal-Abonnements abzuschließen.
- Unbefugte kaufen im Namen der ahnungslosen Betroffenen bei Onlinehändlern ein oder schließen mit ergaunerten Identitäten Mobilfunkverträge ab.

Wie sich aus Erlebnisberichten Betroffener erfahren lässt, ist dies in den allermeisten Fällen nur der Beginn einer nervenaufreibenden und belastenden Zeit, welche sich schlimmstenfalls über Jahre hinweg hinziehen kann. Die Betroffenen müssen sich nämlich in aller Regel erstmal der realen Gefahr erwehren, zu Unrecht verklagt oder zu einer Zahlung verurteilt zu werden. Auch strafrechtliche Konsequenzen können drohen. Unschuldig einer Straftat verdächtigt. Das Lieblingsthema von Hitchcock-Filmen.

Vor allem, wenn zum Beispiel gleich mehrere Verträge unter falschen Namen abgeschlossen wurden und überdies vielleicht sogar eine erste Teilforderung gutgläubig bezahlt wurde, wird es für Betroffene immer schwerer werden, den Durchblick und einen ruhigen Kopf zu behalten. Die Abwehr unberechtigter Forderungen ist in jedem Fall nicht nur mühsam, sondern vielfach auch finanziell und psychisch zermürbend. Der Grund dafür ist simpel. Den Betroffenen wird schlichtweg nicht geglaubt. Die Gläubiger sehen sich erstmal im Recht.

> „Inkasso-Firmen prüfen nicht, ob die Forderungen gerechtfertigt sind oder nicht, das würde ihr Geschäft schmälern. Auf Einwände von Verbraucherinnen und Verbrauchern wird nicht reagiert und pauschal an den Rechnungssteller verwiesen"

Die Verbraucherschutzzentralen raten daher zusätzlich dazu, unbedingt Strafanzeige zu stellen, die eigene Bank zu informieren, die Schufa mit einzubeziehen und ggf. unter Hinzuziehung von IT-Fachläuten alle Passwörter zu ändern. Und das am besten auf einmal.

Identitätsdiebstahl hat langwierige Konsequenzen

Die Angelegenheit ist nur meistens eben nicht mit der Strafanzeige erledigt. Die Verfahren der Ermittlungsbehörden können sich je nach Kapazitäten und Aufkommen nicht selten über Monate hinziehen. Monate, in denen die Betroffenen gleichzeitig immer wieder die Forderung abzuwehren und weitere rechtliche Schritte zu verhindern versuchen.

Der Druck erhöht sich vor allem dann, wenn bereits fälschlicherweise ein negativer Schufa-Eintrag vorgenommen wurde, und die Betroffenen beispielsweise wegen der Anmietung einer neuen Wohnung oder eines Vertragsabschlusses (z.B. mit einem Energieversorger) dringen auf einen positiven Score angewiesen sind. Zwar steht dem Betroffenen nach der DSGVO das Recht auf Löschung unrichtig gespeicherter Daten gegen die Auskunftei zu. Wie sich im Fall der Schufa zeigt, kann sich die Löschung aber sehr lange ziehen.

Wer bei so etwas neben dem ohnehin schon bestehenden Alltagsstress nicht irgendwann aufgibt oder durchdreht, muss schon überragenden Ehrgeiz und Nerven aus Stahl haben; alternativ einen guten Anwalt und das nötige Kleingeld.

Enkeltrick 2.0 und andere Betrügereien

Das „kriminelle Genie" ersinnt immer wieder neue Szenarien, in denen es uns in trügerischer Sicherheit wiegen und auf Glatteis führen kann. Besonders gerne in Momenten der Überforderung und Unachtsamkeit schlägt es zu und trifft häufig die gutgläubigen, arglosen, besorgten und unerfahrenen Menschen unter uns. Und damit sind selbstverständlich nicht nur ältere Mitbürger gemeint.

> „Hallo papa das ist meine neue nummer kannst du diese speichern und mir auf WhatsApp schreiben? Lg"

Wer so eine SMS bekommt und gar keine Kinder hat oder diese noch zu jung für ein Handy sind und gerade neben einem auf den Boden mit Bauklötzen spielen, der wird wahrscheinlich nicht nur wegen der Rechtschreibfehler stutzig. In diesen Fällen sind der Betrugsversuch und die Masche also schnell aufgedeckt: Die Betrüger versuchen einen erst einmal zu isolieren und dann mit einer rührseligen Masche an schnelles Geld bzw. die jahrelang angesparten Rücklagen zu kommen.

Mehr Informationen bieten größeres Potenzial für Betrug

Je mehr Informationen den Betrügern über das anvisierte Opfer dabei zur Verfügung stehen, umso glaubhafter wird es aber. Und dann schlägt die gestellte Falle zu. Wenn den Betrügern z.B. Alter des Kindes, das Geschlecht, der Name und der Wohnort bekannt sind, dürfte es schon nicht mehr so leichtfallen, den Trick auf Anhieb zu durchschauen und einen kühlen Kopf zu behalten.

Anruf vermeintlicher Ärzte aus dem Krankenhaus oder von Polizisten lösen dann zudem größte Sorgen aus. Sie suggerieren eine besondere Dringlichkeit und setzen schnellen Handlungsbedarf voraus. Es bleibt in dieser unbekannten Situation weniger Zeit zum Nachdenken und Nachfragen. Gute Voraussetzungen, jemand hinters Licht zu führen.

Kein Wunder also, dass sich die Fälle versuchter, aber auch vollendeter sog. Betrugsfälle im Jahr 2023 nach Aussagen der Polizei massiv erhöht haben. Nicht auszudenken, welche Konjunktur der Enkeltrick 2.0 erst haben könnte, wenn sich mithilfe Künstlicher Intelligenz im Handumdrehen Stimmen klonen lassen.

Der „falsche Handwerker"

Gesetzt den Fall, dass Betrüger beispielsweise aufgrund fehlgeleiteter/abgefangener E-Mails von geplanten Handwerker- oder Technikerbesuchen zuhause Wind bekommen, ist es durchaus nicht ganz abwegig, dass sie die Betroffenen anschreiben, einen früheren Termin ausmachen und sich somit selbst zu einem persönlichen Hausbesuch einladen.

Wer mit dem Besuch rechnet, lässt auch schnell den falschen Handwerker rein ohne sich vorher einen Ausweis zeigen zu lassen. Der Wasserhahn tropft weiter, während sich die Goldmünzensammlung über einen neuen Besitzer freuen darf. Bitter!

„Fake-President-Attack"

Daneben hat sich mittlerweile ein weiteres neues Phänomen herausgebildet. Bei einer sog. „Fake-President-Attack" (auch CEO-Fraud genannt) geben sich Betrüger regelmäßig als Unternehmensvorstand aus und veranlassen Mitarbeiter offenbar mit dem nötigen Nachdruck, die Zahlungsverkehrsberechtigungen besitzen oder Stammdaten in der Finanzbuchhaltung ändern können, Transaktionen auszulösen. Manchmal in Millionenhöhe. Ähnlich funktionieren auch die „Payment-Diversion-Fälle".

Datenmissbrauch: Stigma und Scham

Betrug ist allerdings nicht die einzige Möglichkeit, um mit Datenmissbrauch an Geld zu kommen. So schrecken Kriminelle als probates Mittel zur eigenen Einkommensaufbesserung auch nicht vor sexueller Erpressung (sog. Sexortion) zurück. Hier machen sich diese die vermeintliche Scham anderer zu Nutze. Nicht jeder Mensch möchte, dass seine im Privaten ausgelebten sexuellen Fantasien öffentlich werden.

Und wenn es nicht ums Geld geht, dann muss eben der gute Ruf dran glauben. Und dies geschieht oftmals gar nicht absichtlich. Bei Comedy-Sketchen herzlich belacht, dürfte es im realen Leben weitaus unangenehmer sein, wenn beispielsweise an der Kasse eine Durchsage zu dem Kondompreis erfolgt. Oder das bestellte Sexspielzeug versehentlich beim Nachbarn landet oder die Sprechstundenhilfe einen im Wartezimmer der Arztpraxis mit Vor- und Nachnamen aufruft, um das Rezept für ein bestimmtes Medikament am Empfang abzuholen.

Peinlich kann es auch werden, wenn es eine Behörde vergeigt. So hatte das Berliner Gesundheitsamt während der Corona-Pandemie per E-Mail bis zu 150 Teilnehmende einer schwulen Sexparty im Berghain nicht nur vor einem Covid-19-Fall gewarnt. Es hatte gleich auch alle Betroffenen aus Versehen in CC geoutet. Auweia, der Klassiker unter den Datenschutzpannen! Was für den einen eine willkommene Dating-Möglichkeit geboten hat, dürfte für den anderen ganz und gar nicht mehr feierlich gewesen sein: Stigma und Scham!

Rufschädigung

Die Verbreitung von rufschädigenden Gerüchten und (Halb-)wahrheiten kann manchen dazu dienen, die Betroffenen in der Öffentlichkeit zu beschämen und herabsetzen. Bezweckt ist damit, den Ruf und das Ansehen des anderen durch ehrverletzende Äußerungen nachhaltig zu schaden (üble Nachrede gem. § 186 oder § 188 StGB). Folge daraus sind nicht selten:

- Existenzgefährdung bis hin zu beruflichem und finanziellem Ruin,
- nachhaltige Beschädigung des öffentlichen Ansehens (Rufmord),
- oder eine reale Gefahr physischer Übergriffe.

Im Zeitalter des Internets kann sich eine Rufschädigung in Sekundenschnelle verbreiten, wie zum Beispiel dieses Jahr der Fall Schönbohm gezeigt hat.

Wenn persönliche – evtl. stigmatisierte – Daten in der Öffentlichkeit preisgegeben werden, kann dies zu erheblichen Schäden führen. So werden manche „Jugendsünden oder Kavaliersdelikte" erst Jahre später im Kollektiv bestraft.

Diskriminierung

Leider leben wir Zeiten, in der manche Teile unserer Gesellschaft – sei es wegen ihrer politischen Ansichten, ihrer Herkunft, Religion, sexuellen Ausrichtung, Geschlecht oder Erkrankung – nicht nur benachteiligt, sondern verbal angegriffen – nein sogar massiv angefeindet werden. Und es bleibt nicht nur beim Shitstorm und der Netzhetze.

Menschen, die sich bereits in der virtuellen Welt einem solchen Hass anderer ausgesetzt sehen, dürften größte Angst davor haben, dass ihre Adresse und die Adresse von Verwandten oder Bekannten öffentlich bekannt werden und sie möglicherweise Opfer von Übergriffen werden. Wie sich an einem aktuellen Beispiel des Antisemitismus in Deutschland zeigt, können plötzlich aufflammende Konflikte in der Welt für manche Bevölkerungsgruppen ungeahnte Gefahren für Leib und Leben bedeuten. Dies gilt aber auch für Muslimfeindlichkeit. Oder Homophobie oder Aggressionen gegen Personen des öffentlichen Lebens. Die Aufzählung aller potenziell gefährdeter Bevölkerungsgruppen würde hier den Rahmen sprengen.

Datenmissbrauch und Datenpannen können also Diskriminierung nicht nur ermöglichen, sondern diese auch erheblich verstärken. Unternehmen, die unrechtmäßig personenbezogene Daten verwenden, könnten aus finanziellen Interessen unethische Praktiken anwenden, um Personen aufgrund ihres Geschlechts, ihrer Rasse oder anderer sensibler Merkmale zu benachteiligen und auszugrenzen.

Arbeitsplatzverlust

Fast jeder Arbeitgeber wäre durch automatisierte Datenergebung und eine strukturierte Sammlung personenbezogener Daten theoretisch in der Lage, über seine Mitarbeiter sensible Daten zu sammeln, von Verhaltens- und Leistungsbeurteilungen bis zu Gesundheitsinformationen. Datenmissbrauch am Arbeitsplatz kann zu schwerwiegenden Konsequenzen führen, einschließlich Diskriminierung, Mobbing und Arbeitsplatzverlust.

Und dies umfasst nicht nur die (heimliche) Überwachung der Mitarbeiter mittels Videoaufnahmen. Namhafte Unternehmen setzen z.B. Projektmanagement-Software ein, um die Effizienz zu steigern und gleichzeitig ineffiziente Mitarbeiter aufzuspüren. In manchen Fällen führte dies in der Vergangenheit zu einer Mitarbeiteraussortierung am Fließband. Der Überwachungsdruck am Arbeitsplatz ist nicht zu unterschätzen.

Jüngstes und unrühmliches Beispiel für die unzulässige Datenerhebung von Mitarbeitern abseits der düsteren Großkonzernwelt ist ein Dienstleister der Stiftung Humboldt Forum. Dieser sammelte sensible Daten über Angestellten in der Probezeit. Dabei wurde auch festgehalten, wenn sich Angestellte einer Psychotherapie unterzogen oder daran interessiert zeigten, einen Betriebsrat zu gründen. Unter anderem wegen dieser Negativliste hatte die Berliner Datenschutzbeauftragte Bußgelder in Höhe von insgesamt 215.000,00 EUR gegen den Dienstleister verhängt.

Bedeutung des Arbeitnehmerdatenschutzes

Wie man sieht, stellt der Beschäftigtendatenschutz in der DSGVO und BDSG (LDSG) sicher, dass personenbezogene Daten Angestellter angemessen geschützt werden und dass Verstöße dagegen Konsequenzen haben.

Auch die Mitarbeitenden in einem Unternehmen sollten deswegen sensibel mit personenbezogenen Daten umgehen und sich der Bedeutung des Datenschutzes bewusst sein. Datenschutzkoordinatoren und -beauftragte spielen eine entscheidende Rolle dabei, sicherzustellen, dass Datenschutzbestimmungen eingehalten werden.

Virtuelle Welt und reale Risiken durch Datenmissbrauch

Datenmissbrauch ist keine abstrakte Bedrohung; es sind reale und allgegenwärtige Gefahren, denen wir und unsere Mitmenschen ausgesetzt sind, wenn wir den Datenschutz vernachlässigen. Dies kann schwerwiegende Konsequenzen für Einzelpersonen nach sich ziehen. Für Unternehmen, die darin verwickelt sind, können die wegen Datenmissbrauchs oder wegen einer Datenpanne verhängten Bußgelder und die darauffolgenden Schadensersatzforderungen mitunter verheerend sein.

Letztendlich ist Datenschutz und die Einhaltung der DSGVO aber nicht nur eine gesetzliche Anforderung, sondern eine moralische Verpflichtung, um die Privatsphäre und die Rechte jedes Einzelnen zu wahren und die Gefahren des Datenmissbrauchs abzuwehren. Das mag nicht jeden von uns zu jeder Zeit gleichermaßen betreffen. Aber wie auch z.B. im Gesundheitswesen gilt der Schutz in erster Linie denjenigen, welche besonders angreifbar und schützenswert sind. Datenschutz ist eine Gemeinschaftsaufgabe.

Autor:in

Felix Rausch
Rechtsanwalt

Weitere Beiträge von mir · Diesen Beitrag teilen

Beitrag kommentieren

Fehler entdeckt oder Themenvorschlag? Kontaktieren Sie uns anonym hier.

Klicken Sie hier, um den Kommentarbereich anzuzeigen.

Das könnte Sie auch interessieren

- Kein Datenschutz für Datensünder!
- Elektronischer Personalausweis geht in die zweite Runde
- Wie unsere Bewegungsdaten bei Geheimdiensten landen
- ArbG: Missbrauch von Kundendaten führt zu außerordentlicher Kündigung

Datenmissbrauch Datenschutz Datenschutzpanne Diskriminierung Identitätsklau permanente Überwachung Startseite

Whistleblowing

Kostenloses Webinar zum neuen Hinweisgeberschutzgesetz
News · 22. November 2023

Whistleblowing im Unternehmen: Wichtige Fragen beantwortet
Fachbeitrag · 19. Juli 2023

Hinweisgeberschutzgesetz: Das müssen Unternehmen nun tun
Fachbeitrag · 16. Mai 2023

Mehr zum Thema

Bußgeld

Top 5 DSGVO-Bußgelder im November 2023
News · 4. Dezember 2023

Wann liegt eine meldepflichtige Datenpanne vor?
Fachbeitrag · 2. November 2023

Top 5 DSGVO-Bußgelder im Oktober 2023
News · 1. November 2023

Mehr zum Thema

Auf Dr. Datenschutz schreiben Mitarbeiter der intersoft consulting, die als Experten für Datenschutz, IT-Sicherheit und IT-Forensik international Unternehmen beraten.

Erfahren Sie mehr zu unseren Leistungen:
Externer Datenschutzbeauftragter

Wir suchen Datenschutzberater (m/w/d):
Jobangebote anzeigen

- ✓ täglich oder wöchentlich per E-Mail
- ✓ kostenlos und jederzeit abbestellbar

Bitte wählen: ☐ Täglich ☐ Wöchentlich

Hier E-Mail-Adresse eingeben *

Ihre E-Mail-Adresse wird nicht an Dritte weitergegeben und zu keinem anderen Zweck verwendet. Weitere Informationen finden Sie in unserer Datenschutzerklärung.

Diese Seite teilen

Wenn Ihnen dieses Angebot gefällt, freuen wir uns über eine Empfehlung:

Dr. Datenschutz
intersoft consulting services

Ansprechpartner zur Verfügung.

Hier kontaktieren

aufbereitet.

DSGVO-Gesetz.de

Wie gefällt Ihnen diese Website?

★★★★★ Ø 4.5 / 636 Bewertungen