

# Europäischer Datenschutztag 2022

## Teil 1: Ein Rückblick

*Der Europäische Datenschutztag ist eine Initiative des Europarats ins Leben gerufener Aktionstag für den Datenschutz. Er wird seit dem Jahr 2007 alljährlich um den 28. Januar in allen Mitgliedsstaaten der EU begangen. Dieses Datum wurde gewählt, weil am 28. Januar 1981 die Europäische Datenschutzkonvention unterzeichnet worden war.*

*Ziel des Europäischen Datenschutztages ist es, die Menschen Europas für den Datenschutz zu sensibilisieren. Dies soll durch Aktionen aller mit dem Datenschutz betrauten Organisationen, meistens übernehmen diese Aufgabe die nationalen Datenschutzbehörden, erfolgen.*

*Im Jahr 2008 schlossen sich auch die Vereinigten Staaten und Kanada dieser Initiative der Europäischen Kommission an. Seitdem wird auch in diesen Staaten zeitgleich mit dem Europäischen Datenschutztag der Data Privacy Day begangen.*



Datenschutz ist heutzutage jedem ein Begriff. Das war nicht immer so. Nachfolgend etwas über die Geschichte der Entstehung dieses Grundrechts und welche Rolle der Datenschutz im Zeitalter der Digitalisierung spielt, indem Informationen einfacher und schneller abrufbar sind denn je.

### **1970 – Die Geburtsstunde des Datenschutzes**

Wenn man ehrlich ist, ist 1970 noch gar nicht so furchtbar lange her. Trotzdem gab es erst in diesem Jahr das erste Datenschutzgesetz weltweit. Es war das Bundesland Hessen, das mit dem Hessischen Datenschutzgesetz vom 07. Oktober 1970 die Vorreiterrolle übernahm. Dieses Gesetz behandelte zwar nur die Datenverarbeitung durch öffentliche Stellen, deckte aber ansonsten schon erstaunlich viele Punkte ab, die auch heute noch Kernelemente gesetzlicher Regelungen wie der Datenschutz-Grundverordnung (DS-GVO) oder dem BDSG sind.

### **Das Volkszählungsurteil von 1983**

Elementar für unser heutiges Verständnis des Datenschutzes war aber vor allem das Volkszählungsurteil vom 15. Dezember 1983. Auslöser für dieses Urteil war eine für April bis Mai 1983 geplante Volkszählung in der Bundesrepublik Deutschland. Der Staat wollte im Rahmen der auf dem „Volkszählungsgesetz“ basierenden Volkszählung viele personenbezogene Daten erheben, u.a. detaillierte

Angaben zu Familie und Lebenspartnerschaft, zur Wohnsituation, zu schulischer und beruflicher Ausbildung und Erwerbstätigkeit, zur Stellung im Beruf, zu Arbeitszeit und zum Arbeitsweg.

Hiergegen wurden gleich mehrere Verfassungsbeschwerden erhoben, die letztlich zum Volkszählungs-urteil führten. In diesem wurde nicht nur die Rechtswidrigkeit der geplanten Volkszählung festgestellt und das Volkszählungsgesetz für verfassungswidrig erklärt. Es wurde vor allem das Grundrecht auf informationelle Selbstbestimmung etabliert (als Ausfluss des allgemeinen Persönlichkeitsrechts (Art. 2 Absatz 1 Grundgesetz) und der Menschenwürde (Art. 1 Absatz 1 Grundgesetz). Bund und Länder reformierten daraufhin bestehende Datenschutzgesetze und schafften neue bereichsspezifische Datenschutzgesetze – u.a. auch betreffend der Volkszählung, die dann schließlich 1987 in datenschutz-konformer Ausgestaltung doch noch stattfand.

### **Datenschutz goes Europe**

Bedingt durch das Bedürfnis nach mehr Einheitlichkeit zur Erleichterung des innereuropäischen Verkehrs von Daten wurde 1995 die europäische Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Richtlinie 95/46/EG) erlassen. Diese trug der technischen Fortentwicklung der letzten Jahrzehnte Rechnung, wenngleich auch damals die Technik dem Recht natürlich schon weit voraus war.

2002 folgte dann die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG), auch bekannt als ePrivacy- oder Cookie-Richtlinie, die neue Standards für den Datenschutz im Bereich der Telekommunikation setzte. Dies verursachte 2004 die Novellierung des Telekommunikations-gesetzes in Deutschland. Im Jahr 2009 wurden Teile der ePrivacy-Richtlinie nochmal überarbeitet (Richtlinie 2009/136/EG). Ob diese neuen Vorgaben im deutschen Recht vollständig umgesetzt wurden oder wie diese in Deutschland wirkten, war anschließend für 11 Jahre ein unter Datenschützern beliebtes Diskussionsthema. Der Streit hat sich durch das „Cookie-Einwilligung II“-Urteil des BGH nunmehr erledigt. Entsprechend sah sich der Gesetzgeber gezwungen, in dem im Dezember in Kraft tretenden „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ (Telekommunikation-Telemedien-Datenschutzgesetz) unter anderem die Umsetzung nachzureichen. Die Umsetzung der für die Richtlinie namensstiftende Vorschrift zu Cookies findet sich dann in § 25 TTDSG.

### **Europäische Datenschutz-Grundverordnung (DS-GVO)**

Die am 14. April 2016 vom EU-Parlament verabschiedete und seit dem 25. Mai 2018 anwendbare DS-GVO hat schließlich für eine weitgehende Harmonisierung des Datenschutzes in allen Mitgliedsstaaten gesorgt. Anders als die vorangegangenen Richtlinien gilt sie als Verordnung auch ohne weiteren nationalen Umsetzungsakt unmittelbar in allen Mitgliedstaaten.

Quellen: BfDI Bund, Presseportal BMJ, European Federation of Data Protection Officers, GDD

## Europäischer Datenschutztag 2022

### Teil 2: Warum Datenschutz wichtig ist



#### Was ist Datenschutz – eine Definition

Datenschutz ist ein Begriff, der nicht einheitlich verstanden wird. Er umfasst je nach Perspektive Aspekte wie den Schutz der Privatsphäre, den Schutz vor missbräuchlicher Datenverarbeitung oder die Entscheidungshoheit darüber, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Aus der Sicht des Datenschutzrechtlers betrifft Datenschutz den Schutz des vom Grundgesetz geschützten Rechts auf „informationelle Selbstbestimmung“ bzw. des „Rechts auf Schutz der (eine Person) betreffenden personenbezogenen Daten“ (Art. 8 Abs. 1 der Grundrechtecharta der EU).

Man kann daher den Datenschutz vielleicht am einfachsten als den „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ definieren. So formuliert es etwa der 1. Erwägungsgrund zur DS-GVO. Datenschutz ist also nicht gleichzusetzen mit dem Schutz von Daten an sich (was der Begriff nahelegen könnte). Es geht vielmehr um den Schutz der Grundrechte und Grundfreiheiten der natürlichen Person, die hinter diesen Daten steht. Dementsprechend spricht die DS-GVO auch stets vom Schutz personenbezogener Daten.

#### Unterschied zwischen Datenschutz und Datensicherheit

Damit ist auch schon der zentrale Unterschied zum Begriff der Datensicherheit angesprochen: Denn hier steht gerade die Sicherheit der Daten im Vordergrund, ohne dass es darauf ankäme, ob sie einer konkreten Person zugeordnet werden können. Datensicherheit spielt damit auch bei rein technischen oder wirtschaftlichen Daten eine Rolle, die – insbesondere, wenn sie in den Bereich der Geschäftsgeheimnisse fallen – natürlich ebenfalls eines angemessenen Schutzes bedürfen.

Wer von Datensicherheit spricht, meint damit den Schutz von Daten vor gewissen Sicherheitsrisiken wie etwa der Manipulation, dem Verlust oder der unberechtigten Kenntnisnahme. Hier geht es also nicht um die Zulässigkeit oder die rechtskonforme Ausgestaltung einer konkreten Datenverarbeitung (von personenbezogenen Daten), sondern um die generelle Frage, welche Maßnahmen zum Schutz der Daten getroffen werden müssen. Hierzu gehört dann u.a. die Umsetzung durch geeignete technische und organisatorische Maßnahmen, die auch das Datenschutzrecht erfordert.

#### Warum ist Datenschutz - insbesondere für Unternehmen - wichtig?

Wie eben erwähnt geht es beim Datenschutz letztlich um den Schutz von Grundrechten und der Selbstbestimmung natürlicher Personen. Angesichts der massenhaften Datenverarbeitungen, die unsere digitale Lebenswirklichkeit bereits heute stetig steigend mit sich bringt, kann dieser Schutz

nicht hoch genug geschätzt werden. Und für Unternehmen gilt: Mangelhafter Datenschutz wird früher oder später dazu führen, dass sie in den Fokus der Öffentlichkeit oder gar der Datenschutzaufsichtsbehörden geraten. Die Bedrohung durch potenzielle Bußgelder ist dabei ebenso real wie diejenige eines ernsthaften Reputationsschadens und vor allem, weil ein Datenschutzverstoß heute kostspielig sein kann.

### **Bußgelder und Schadensersatz**

Über aktuelle (Millionen-)Bußgelder kann man sich mittlerweile leicht im Internet informieren. Wer den Datenschutz ernst nimmt, gerät weniger in Gefahr, überhaupt ein Bußgeld zu kassieren. Oder dieses wird zumindest – im Fall der Fälle – weit geringer ausfallen. Denn die DS-GVO sagt zur Höhe einer Geldbuße, dass sie in jedem Einzelfall wirksam und abschreckend sein soll – aber eben auch verhältnismäßig. Wer entsprechende Anstrengungen beim Datenschutz vorweisen kann, darf daher auf eine erheblich geringere Buße hoffen.

Unzureichender Datenschutz kann aber auch Auslöser für monetäre Ansprüche von Privatpersonen sein. So besagt Art. 82 Abs. 1 DS-GVO ausdrücklich: „Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“

### **Datenschutz rückt ins öffentliche Bewusstsein**

Mit zunehmender Sensibilisierung der Öffentlichkeit für das Thema Datenschutz wird zudem ein potenzieller Imageschaden sogleich wahrscheinlicher wie empfindlicher. Gerade in der Digitalwirtschaft, wo der Konkurrent oft nur einen Mausklick entfernt ist, ist auch die wirtschaftliche Bedeutung des Bekanntwerdens von Verstößen gegen den Datenschutz, nicht zu unterschätzen. Oder andersherum: Ein besonders sensibler, datenschutzkonformer Umgang mit den Daten der Kunden kann ein echter Wettbewerbsvorteil werden.

Immer mehr Beachtung findet der Datenschutz auch bei Unternehmenskäufen. Für den Unternehmenswert ist auch der Umgang mit personenbezogenen Daten (nicht zuletzt denjenigen der Kunden) von immer größerer Bedeutung. Außerdem nimmt auch der Wert der im Unternehmen vorhandenen Daten immer weiter zu. Wer heutzutage den Datenschutz vernachlässigt, schadet dem Wert des Unternehmens und damit seinen Anteilseignern.

### **Warum ist Datenschutz im Privatleben wichtig?**

Wenn es nicht möglich ist zu wissen oder zu beeinflussen, welche Informationen über einen selbst gespeichert, verwendet oder weitergegeben werden, wird der Einzelne sein Verhalten entsprechend anpassen, um nicht durch abweichende Verhaltensweisen aufzufallen. Das wiederum führt zu einer Beeinträchtigung der individuellen Entfaltungschancen des Einzelnen und darüber hinaus auch zu einer Beeinträchtigung des Gemeinwohls. Denn ein freiheitlich demokratisches Gemeinwesen zeichnet sich auch durch die Selbstbestimmung seiner Bürger aus.

So argumentierte bereits das BVerfG im Volkszählungsurteil aus dem Jahre 1983. Heute, wo jeder von uns tagtäglich, mal mehr, mal weniger freiwillig, Daten von sich im Internet und anderswo preisgibt, gelten diese Gedankengänge umso mehr. Nur sind wir heute nicht nur der Datensammelei der eigenen Staatsmacht ausgesetzt, sondern auch derjenigen kommerzieller Player, deren einziges Ziel die Steigerung von Profit ist. Wenn diese Unternehmen nicht durch den Datenschutz reglementiert würden, gäbe es so etwas wie Datenhoheit oder Datensouveränität nicht mehr. Der gläserne Bürger bzw. Nutzer wäre längst Realität. Dass wir alle, entgegen einem gern zitierten Satz, sehr wohl etwas zu verbergen haben, sollten wir uns häufiger ins Gedächtnis rufen. Jedenfalls dann, wenn wir auch zukünftig unsere Entscheidungen selbst treffen und dies nicht den großen Internetkonzernen oder Werbenetzwerken überlassen wollen.

Wie man sich gegen Datenkraken und andere digitale Bösewichte zur Wehr setzen kann, illustrieren z.B. die „Kurze Anleitung zur digitalen Selbstverteidigung“ der Digitalen Gesellschaft oder auch das „Kleine Einmaleins der digitalen Selbstverteidigung“ von „netzpolitik“ sehr gut.

## **Datenschutz: Als Exportschlager zum weltweiten Trend**

Die DS-GVO stellt auch über 3 Jahre nach ihrem „Inkrafttreten“ die Wirtschaft weiter vor erhebliche Herausforderungen. Zugleich aber loben viele die DS-GVO als Exportschlager oder datenschutzrechtlichen Goldstandard, sehen Europa aufgrund der DS-GVO in einer Vorreiterrolle. Aufgrund der Vernetzung der globalen Wirtschaft wird die Einhaltung der DS-GVO weltweit immer wichtiger. Zudem treffen die Verpflichtungen aus der DS-GVO aufgrund des Markttortprinzips des Art. 3 Abs. 2 DS-GVO Unternehmen oft auch dann, wenn diese gar nicht in der EU sitzen.

So ist es nur konsequent, dass immer mehr Staaten neue Datenschutzgesetze verabschieden, die sich weitgehend oder zumindest hinsichtlich zentraler Prinzipien an der DS-GVO ausrichten. Als derzeit relevanteste seien genannt Kaliforniens Consumer Privacy Act (CCPA), das Datenschutzgesetz Brasiliens (Lei Geral de Proteção de Dados), die Überarbeitung des japanischen Datenschutzgesetzes (APPI) oder Chinas neues Datenschutzgesetz aus diesem Jahr.

Eine Anpassung ihrer nationalen Gesetze in Richtung der DS-GVO ist für Drittstaaten aber auch deshalb interessant, weil sie so die Chancen auf einen Angemessenheitsbeschluss der Kommission erhöhen und dadurch die Wirtschaftsbeziehungen mit der EU verbessern können. Derzeit befindet sich die Prüfung eines Angemessenheitsbeschlusses für Südkorea auf der Zielgeraden.

## **Datenschutz schreibt Geschichte**

So sehr man sich auch an einzelnen Regelungen der DS-GVO oder an deren Auslegung durch die Aufsichtsbehörden reiben mag, ihr internationaler Erfolg zeigt, wie überfällig die robuste Novellierung des Datenschutzrechts und dessen weitgehende Vereinheitlichung in Europa war – und in vielen Regionen der Welt weiterhin ist. Datenschutz ist gerade in unserer digitalen Welt, die zukünftig noch viel digitaler und datengetriebener sein wird, die Grundlage für unser selbstbestimmtes Leben.

Quellen: BfDI Bund, Presseportal BMJ, European Federation of Data Protection Officers, GDD

# Europäischer Datenschutztag 2022

## Tipps zum Datenschutz im Alltag



*Die Geschichte des Datenschutzes ist mit der DS-GVO um ein wesentliches Kapitel fortgeschrieben worden. Sie zu einer Erfolgsgeschichte zu machen, liegt in unser allen Händen. Jeder einzelne von uns kann mit seinem Verhalten und seiner Haltung daran mitschreiben. Hier 10 Tipps, was wir zum Datenschutz und zur Sicherheit der Daten tagtäglich beitragen können:*

### 10 Tipps zum Datenschutz im Alltag

- 1 Lassen Sie keine Unterlagen mit personenbezogenen Daten offen liegen (Verträge, Bewerbungsunterlagen etc.). Weder auf dem Schreibtisch – auch im Home-Office! – auch nicht am Drucker oder Kopierer.
- 2 Müssen Sie Papierdokumente mit personenbezogenen Daten vernichten, nutzen Sie den Shredder oder die Datentonne und nicht nur den normalen Papierkorb.
- 3 Sperren Sie Ihren PC oder Ihren Laptop, wenn Sie Ihren Schreibtisch – egal, ob im Büro oder am heimischen Arbeitsplatz – verlassen. Mit einer Tastaturkombination ist das schnell erledigt (meist Windows-Taste + L).
- 4 Wählen Sie sichere Passwörter (mind. 12 Zeichen, Klein- und Großbuchstaben, Ziffern und Satzzeichen). Kleben Sie diese nicht an den Bildschirmrand oder unter die Tastatur, geben Sie diese auch nicht weiter – auch nicht an Kolleginnen und Kollegen.
- 5 Geben Sie beim Telefonieren im Zug oder beim Arbeiten am Laptop/Tablet im Café keine Geschäftsgeheimnisse, Kundendaten u.Ä. öffentlich preis.
- 6 Vorsicht bei E-Mails mit Links, die z.B. nach Log-in-Daten fragen. Das könnten Phishing-Mails sein. Sie greifen Zugangsdaten ab und können mit Schadsoftware „verseucht“ sein. Vorsicht auch bei E-Mails mit Anhängen. Sie können ebenfalls Schadsoftware enthalten.
- 7 Veröffentlichen Sie Fotos von Kollegen und Kolleginnen oder externen Dritten, aber auch nicht von Freunden und Freundinnen nicht ungefragt in sozialen Netzwerken oder auf der Homepage.
- 8 Nutzen Sie für personenbezogene Daten möglichst gemeinsame Speicherorte, statt eigene Kopien und Listen zu führen. Zugriff dürfen nur die Kolleginnen und Kollegen darauf haben, die mit den Daten tatsächlich arbeiten müssen.
- 9 Melden Sie ungewöhnliche Vorgänge. Das können abhandengekommene Daten oder etwa eine verlorener USB-Stick mit Kundendaten sein. Oder stellen Sie ungewöhnliche Vorgänge an Ihrem Computer, dann wenden Sie sich an die zuständigen Stellen. Fallen Ihnen ungewöhnliche Vorgänge im Gebäude aufm z.B. fremde Personen die alleine unterwegs sind? Sprechen Sie diese an und begleiten Sie sie zum Empfang.
- 10 Erhalten Sie Auskunftersuchen, möchten also z.B. Kunden genau wissen, welche personenbezogenen Daten in unserem Hause verarbeitet werden, so leiten diese Nachricht unverzüglich an Ihren Datenschutz-Koordinator oder Datenschutzbeauftragten weiter.