# Datenschutz newsbox

Ausgabe 10 2020



DATAKONTEXT

## Editorial:

Im Dezember 2019 erfuhr die interessierte Datenschutzwelt, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) den Telekommunikationsdienstleister 1&1 Telecom GmbH mit einer Geldbuße in Höhe von 9.550.000 Euro belegt hatte. Der BfDI schrieb dazu, dass er bei der Festsetzung der Höhe der Geldbuße aufgrund des während des gesamten Verfahrens kooperativen Verhaltens von 1&1 Telecom GmbH im unteren Bereich des möglichen Bußgeldrahmens geblieben war.
Das Bußgeldkonzept, auf dessen Grundlage die Höhe der Sanktion wohl berechnet worden war, hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erst im Oktober 2019 veröffentlicht.

Danach erfolge die Bußgeldzumessung in Verfahren gegen Unternehmen in fünf Schritten. Zunächst werde das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach werde der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.) und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.).

Von Anfang an stand insbesondere ein Punkt des Bußgeldkonzepts im Fokus der Kritik. Es wurde bemängelt, dass die Umsatzbezogenheit kein geeignetes Hauptkriterium für die Bußgeldzumessung sei; es sollten vielmehr weitere Faktoren in die Grundberechnung einbezogen werden. Die vorgeschlagene Berücksichtigung des Umsatzes führe zu einem Wertungswiderspruch bei schwerwiegenden Vergehen, begangen von kleinen Unternehmen und kleinen Verstößen von großen Unternehmen. Am 07.10.2020 startete vor dem Landgericht Bonn das erste Verfahren gegen das oben genannte Bußgeld, welches der BfDI verhängt hatte. Unter anderen Punkten ging es in der Verhandlung dann auch tatsächlich um den Aspekt, dass nach dem Modell der DSK kein niedriges Bußgeld für nicht schwerwiegende Vergehen mehr zustande kommen könne und dass im konkreten Fall Unverhältnismäßigkeit vorliege.

Wie das Verfahren auch ausgeht: Das Urteil wird für die Verantwortlichen mehr Vorhersehbarkeit und Klarheit beim Thema Bußgeldbemessung bringen, hofft

Ihr Levent Ferik

DATAKONTEXT

**Impressum**

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

## Datenschutzkonformes KI-Training

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) möchte Unternehmen, die sich mit Künstlicher Intelligenz beschäftigen, mit einem Leitfaden zum Thema unter die Arme greifen.
Der Leitfaden der Bitkom mit dem Titel „Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens" beschäftigt sich insbesondere mit der Herausforderung, das Unternehmen, die Künstliche Intelligenz (KI) entwickeln und einsetzen wollen, sich zwangsläufig mit der Frage konfrontiert sehen, wie die KI mit geeigneten Daten trainiert werden kann.
Da dieses „Trainingsmaterial" in der Regel auch aus personenbezogenen Daten besteht, damit die KI verwertbare Analyseergebnisse liefert, ist es erforderlich, die Anforderungen des Datenschutzes bei der Verwendung dieser Daten zu beachten.
Der Leitfaden des Bitkom geht vor allem unter Schilderung von Anonymisierungs- und Pseudonymisierungsmethoden darauf ein, wie dieses Vorhaben gelingen kann.
Jeweils ein eigenes Kapitel widmet sich der Anonymisierung und Pseudonymisierung medizinischer Textdaten, dem Verfahren der semantischen Anonymisierung sowie Datenschutzrisiken bei Medieninhalten.

*Quelle: Bitkom*

## Policy Paper zu Risiken Künstlicher Intelligenz

Im Forum Privatheit setzen sich Expert*innen aus sieben wissenschaftlichen Institutionen interdisziplinär, kritisch und unabhängig mit Fragestellungen zum Schutz der Privatheit auseinander.
In seiner aktuellsten Veröffentlichung zeigt der Forschungsverbund in einem Policy Paper auf, wie KI die Selbstbestimmung des Menschen fördert oder verletzt – und gibt konkrete Empfehlungen, wie diese geschützt und gestärkt werden kann.
Das Policy Paper analysiert den beschriebenen Themenkomplex vorrangig aus ethischer, rechtlicher und gesellschaftswissenschaftlicher Perspektive und skizziert gesellschaftlichen Handlungsbedarf. Es beginnt mit einer Einführung in die unterschiedlichen Perspektiven auf Selbstbestimmung. Im Anschluss geht es der Frage nach, inwiefern sich KI-Systeme fördernd oder einschränkend auf die Selbstbestimmung von Menschen auswirken können, nennt Beispiele, zeigt Zukunftsperspektiven auf und gibt Empfehlungen. Insgesamt soll das Policy Paper einen Beitrag zur derzeitigen breit geführten Diskussion über die Chancen und Risiken von KI-basierten Technologien leisten.

*Quelle: Forum Privatheit / Das Fraunhofer-Institut für System- und Innovationsforschung ISI*

## Generischer Ansatz nach Art. 32 DS-GVO

Unter den vielen Rubriken auf der Seite des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) befindet sich auch die hilfreiche Rubrik „Checklisten zum Datenschutz".
Mit den Veröffentlichungen in dieser Rubrik möchte das BayLDA gerade kleinere Unternehmen, Selbstständige und Freiberufler bei der erfolgreichen Umsetzung der Datenschutzvorschriften unterstützen, in dem die Behörde den eher abstrakt und komplex klingenden Gesetzestext durch Veranschaulichung in den Checklisten greifbarer darstellt. Die aktuellste Handreichungen „Good Practice bei technischen und organisatorischen Maßnahmen", mit dem das BayLDA wichtige Praxismaßnahmen aufzeigen möchte, widmet sich Art. 32 DS-GVO.
Die DS-GVO fordert von Verantwortlichen und Auftragsverarbeitern in Art. 32 DS-GVO ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist. Dabei sollen zur Gewährleistung der Sicherheit der insbesondere die Risiken berücksichtigt werden, die aus einer Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten, der an deren Verarbeitung beteiligten IT-Systeme, Dienste und Fachprozesse hervorgehen können.
Diese Checkliste dient deshalb, so das BayLDA, insbesondere dazu, kleinen und mittleren Unternehmen eine Auswahl an TOM anzubieten, die bei geläufigen Verarbeitungstätigkeiten innerhalb eines Betriebs verwendet werden können. Entsprechend werden häufig in der Praxis adressierte Punkte behandelt wie bauliche Schutzmaßnahmen, Einsatz von mobilen Endgeräten, internetfähige Arbeitsplatzumgebung und Sensibilisierung von Mitarbeitern – dies entspricht einem generischen Ansatz bei IT-gestützten Datenverarbeitungen. Spezialisierte Anwendungen wie vernetzte Fahrzeuge, Künstliche Intelligenz oder Cloud-Computing-Services würden dagegen deutlich spezifischere und teils abweichende Maßnahmen benötigen.

*Quelle: Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)*

## Informationsportal der Stiftung Datenschutz

Die Stiftung Datenschutz wurde 2013 von der Bundesrepublik Deutschland gegründet. Aufgabe der unabhängigen Einrichtung ist die Förderung des Privatsphärenschutzes.
Eine der Aufgaben der Bundesstiftung ist es, die Fähigkeiten der Bevölkerung zum Schutz der eigenen Daten durch Aufklärung und Bildung zu stärken. Mehr Wissen über die konkreten Möglichkeiten eines vorsichtigen Umgangs mit persönlichen Informationen soll dazu geschaffen werden. Das Inkrafttreten der DS-GVO kann als eine Art Zäsur betrachtet werden, was insbesondere Literatur, Handlungsempfehlungen, Orientierungshilfen und aufsichtsbehördlichen Arbeitspapiere angeht.
Viele, auch öffentlich zugängliche Info-Materialien, sind mit Wirksamwerden der DS-GVO zur Makulatur geworden. In den letzten Jahren hat es jedoch unzählige Informationen zur Umsetzung der DS-GVO gegeben, die auch frei zugänglich sind. Verbände, Aufsichtsbehörden und sonstige Fachleute haben sehr viele Informationen zum Thema Datenschutz und speziell zur DS-GVO veröffentlicht. Zunehmend wird es schwieriger, den Überblick über die zur Verfügung stehenden Materialien zu behalten.
Die Stiftung Datenschutz hat nicht nur die zahlreichen frei verfügbaren Informationen aus unterschiedlichen Quellen zusammengetragen, übersichtlich gegliedert und eingeordnet, sondern mittlerweile auch einen beträchtlichen Fundus an eigenen Handreichungen aufgebaut. Das Infoportal besitzt zudem eine brauchbare Suchmaschine mit verschiedenen Filterkriterien, wie bspw. Region, Branche, Kategorie Verfassen etc.

*Quelle: Stiftung Datenschutz*

## Die betriebsärztliche Datenverarbeitung

Das Netzwerk Datenschutzexpertise beschäftigt sich in seiner aktuellen Veröffentlichung „Die Datenverarbeitung des Betriebsarztes – Hinweise zum datenschutzgerechten Umgang mit Patientendaten durch Betriebsärzte und betriebsärztliche Dienste“ mit einem Thema, welches nicht sonderlich oft im Rampenlicht des betrieblichen Datenschutzes und insbesondere des Beschäftigtendatenschutzes steht.
Umso weniger nachvollziehbar ist die stiefmütterliche Behandlung des Themas in der Praxis und Literatur, wenn man bedenkt, dass es sich in der Schnittmenge des Medizinrechts und des Datenschutzrechts abspielt, wobei ebenso so viele spannende Fragen des Arbeitsrechts, des Mitbestimmungsrechts und die dort bestehenden spezifischen Regelungen, zur Anwendung kommen.
Daher dürfte die aktuelle Veröffentlichung des Netzwerks Datenschutzexpertise für alle Beteiligten aufschlussreich, wie hilfreich sein, da die Handreichung die rechtlichen Grundlagen ordnet und gleichzeitig eine Vielzahl praktischer Fragestellungen aufgreift. Es werden die wesentlichen anzuwendenden Normen und deren korrekte Anwendung dargestellt.

*Quelle: Netzwerk Datenschutzexpertise:*

## Verunsicherung wegen der Zulässigkeit von Office 365

Die Corona-Pandemie hat das Thema Videokonferenzen, Home-Office und auch die Tools und Anwendungen rund um das Thema stärker ins Rampenlicht gebracht. Damit einhergehend wurde auch die Zulässigkeit von Office 365 und insbesondere von Microsoft Teams immer häufiger hinterfragt. Zuletzt veröffentlichte die Berliner Beauftragte für Datenschutz und Informationsfreiheit Hinweise zu Anbietern von Videokonferenz-Diensten. Im Fokus der Betrachtung standen insbesondere die vertraglichen Bestimmungen der Anbieter Cisco, Google, Zoom und Microsoft.

Vor allem drehte sich die datenschutzrechtliche Prüfung um die Frage, ob die Anbieter rechtskonforme Verträge zur Auftragsverarbeitung nach Art. 28 DS-GVO verwenden. Was die Videofunktion Microsoft Teams angeht, kam die Berliner Beauftragte für Datenschutz und Informationsfreiheit in ihrer Kurzeinschätzung zum Ergebnis, dass die derzeit von Microsoft verwendeten Bestimmungen zur Auftragsverarbeitung nicht rechtskonform sind.

Jetzt hat sich auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) mit der Bewertung seines Arbeitskreises Verwaltung zur Auftragsverarbeitung bei Microsoft Office 365 beschäftigt und das Ergebnis in einer Pressemitteilung mitgeteilt.

Der Arbeitskreis hatte „die dem Einsatz des Produktes Microsoft Office 365 zugrunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft Onlinedienste (Data Processing Addendum / DPA) – jeweils Stand: Januar 2020“ geprüft. Das Papier kommt zu dem Ergebnis, dass auf Basis der genannten Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich ist.

„Wie Anwender und Verantwortliche nun die Aussage bewerten und einordnen sollen, dass die Prüfungsergebnisse nicht in allen Belangen von allen Aufsichtsbehörden mitgetragen werden, bleibt unklar.“ Die Pressemitteilung spricht insoweit nur davon, dass „die Entscheidung der Datenschutzkonferenz mit einer knappen Mehrheit von 9 Stimmen bei 8 Gegenstimmen erging. Gegen die uneingeschränkte Zustimmung haben sich unter anderem die Landesbeauftragten für den Datenschutz Baden-Württemberg, Bayern, Hessen und im Saarland sowie der Präsident des Bayerischen Landesamts für Datenschutzaufsicht ausgesprochen.

## DSK aktualisiert Kurzpapier zum Beschäftigtendatenschutz

Ein spezielles Recht für den Beschäftigtendatenschutz wurde schon zu Zeiten vor Geltung der DS-GVO in wiederkehrender Regelmäßigkeit von vielen von DatenschutzexpterInnen, Personalprofis, Betriebsräten und anderen gefordert. Dies hat sich zwar mit Wirksamwerden der DS-GVO nicht wesentlich geändert, jedoch existiert nach wie vor kein in sich geschlossener Arbeitnehmerdatenschutz. Abgesehen von dem § 26 BDSG, der vom Regelungsgehalt her dem § 32 BDSG-alt recht nahekommt, existieren keine spezielleren datenschutzrechtlichen Normen zum Datenschutz im Beschäftigungsverhältnis.
Der Koalitionsvertrag sieht einen Prüfauftrag zum Beschäftigtendatenschutz basierend auf der Öffnungsklausel in Artikel 88 der DS-GVO vor. Diese Klausel ermöglicht es den EU-Mitgliedstaaten, spezifischere Regulierungen bezüglich des Beschäftigtendatenschutzes selbst zu schaffen. In diesem Sinne hat im Juni 2020 der interdisziplinäre Beirat zum Beschäftigtendatenschutz im Bundesministerium für Arbeit und Soziales (BMAS) seine Arbeit aufgenommen.

Ein Abschlussbericht mit konkreten Empfehlungen soll nach der letzten Sitzung im Dezember 2020 erstellt und Anfang 2021 vorgelegt werden.
Auch das aktualisierte Kurzpapier Nr. 14 – Beschäftigtendatenschutz, welches nun aktualisiert wurde (Stand 24.09.2020), greift als Ausblick das Thema eines eigenständigen Beschäftigtendatenschutzgesetzes auf. Der Ausblick im Kurzpapier Nr. 14 geht davon aus, dass ein solches Beschäftigtendatenschutzgesetz unter anderem das Fragerecht bei der Einstellung von Bewerberinnen und Bewerbern, die Problematik eines Pre-Employment-Screenings, die Grenzen zulässiger Kontrollen von Beschäftigten, die Begrenzung von Lokalisierungen (GPS) und die Verwendung biometrischer Authentifizierungs- und Autorisierungssysteme oder die Nutzung Künstlicher Intelligenz zum Gegenstand haben könnte.

## Datenschutz bei Websites – aktuelle Rechtslage und Ausblick auf das TTDSG

Eine Sonderveröffentlichung von DataAgenda/RDV erläutert die aktuelle Rechtslage in Bezug auf Onlinedatenverarbeitungen im Allgemeinen und Cookies im Besonderen und wagt eine erste Einordnung des Anfang August 2020 geleakten Referentenentwurfs des Bundesministeriums für Wirtschaft (BMWi) für ein Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG), das die Datenschutzvorschriften von TKG und TMG im Vorfeld der Verhandlung der ePrivacy-VO in Deutschland zusammenführen soll.

Der Beitrag wurde gemeinsam von Prof. Dr. Rolf Schwartmann (Leiter der Kölner Forschungsstelle für Medienrecht, Technische Hochschule Köln, Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. sowie Mitglied im Stiftungsrat der European netID Foundation), Kristin Benedikt (Richterin am Verwaltungsgericht Regensburg) und RAin Yvette Reif, LL.M. (stellvertretende Geschäftsführerin der GDD).

Kostenloser Download

# Verbesserungsvorschläge zur DS-GVO

Das Ziel der DS-GVO war die Vollharmonisierung der Regelungen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten der Europäischen Union (EU) sowie eine angemessene Balance zwischen Wirtschafts- und Verbraucherinteressen in Zeiten fortschreitender Digitalisierung. Sie sollte das Grundrecht auf informationelle Selbstbestimmung durch höhere Transparenz und mehr Mitbestimmung der Bürgerinnen und Bürger mit Blick auf ihre Daten stärken. Gleichzeitig sollte die Verordnung einen zukunftsorientierten Rechtsrahmen für datenverarbeitende Unternehmen und innovative Geschäftsmodelle schaffen.

Die DS-GVO sieht selbst ihre eigene regelmäßige Evaluation vor. Vier Jahre nach Inkrafttreten und zwei Jahre nach Geltungsbeginn hat die EU-Kommission im Juni 2020 ihren ersten Evaluationsbericht vorgelegt.

Nach Auffassung von Prof. Dr. Alexander Roßnagel und Dr. Christian Geminn, den Autoren des Werks „Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht“ geht der Bericht aber nicht auf Schwachstellen und Verbesserungsvorschläge ein, sondern befasst sich allein mit der Umsetzung der DS-GVO in der Praxis. Damit ignoriere sie die vielen Vorschläge zur Verbesserung von Mitgliedstaaten, Unionsorganen und aus der Zivilgesellschaft, so die beiden Autoren. In dem Buch „Datenschutz-Grundverordnung verbessern“ macht die Autoren 33 , ihrer Auffassung nach, leicht umsetzbare Vorschläge.

Das Buch führt nach zwei Jahren Erfahrung mit der Datenschutz-Grundverordnung eine Evaluation aus Verbrauchersicht durch und präsentiert 33 einfache konkrete Vorschläge, Ihren Text zu verbessern, um Ihre Ziele besser zu verwirklichen. Daneben erörtert es konzeptionelle Schwächen der Verordnung und entwickelt Vorschläge für Lösungen, die Ihren Schutzauftrag erfüllen.

Die Idee der beiden Autoren ist, dass die wiederkehrenden Evaluationen der Verordnung dazu beitragen können, Mängel zu beseitigen und eine Evolution des EU-Datenschutzrechts zu bewirken.

## LDI NRW klärt auf: Zweck ändernde Zugriff auf Corona-Listen

In Zusammenhang mit der Coronakrise ist die Kontaktdatenerfassung von großem Interesse, um Infektionsketten aufzudecken und zu unterbrechen. Sofern die Erfassung nach einer gesetzlichen Vorgabe oder aufgrund einer behördlichen Anordnung erforderlich ist, ist sie zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 Satz 1 lit. c, Abs. 3 Datenschutz-Grundverordnung zulässig.
Eines separaten Einverständnisses des Betroffenen nach Art. 6 Abs. 1 Satz 1 lit. a), Art. 7 DS-GVO bedarf es dann nicht mehr, so die Feststellung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) in einer aktuellen Meldung. Vor dem Hintergrund einer schwindenden Akzeptanz für das Ausfüllen dieser Listen in der Bevölkerung, macht die LDI NRW aber auch auf darauf aufmerksam, ob und inwiefern Zugriffe von Strafverfolgungsbehörden auf diese Informationen zulässig sein können.
Die Zulässigkeit des Zugriffs auf die Corona-Kontaktlisten durch die Strafverfolgungsbehörden im Rahmen von strafrechtlichen Ermittlungsverfahren richte sich insbesondere nach der Strafprozessordnung (StPO). Sobald die Polizei von einem Anfangsverdacht einer Straftat Kenntnis erlange, sei sie nach dem Legalitätsgrundsatz verpflichtet, den Sachverhalt zu erforschen.
Sowohl Polizei und Staatsanwaltschaft dürften grundsätzlich sämtliche Ermittlungen durchführen, die aufgrund der Intensität ihres Grundrechtseingriffs nicht spezielle Eingriffsbefugnisse verlangen. Von einem derart gesteigerten Grundrechtseingriff könne aber im Fall des Zugriffs auf die Corona-Kontaktlisten regelmäßig nicht ausgegangen werden. Deshalb sei ein Zugriff auf Gästelisten auf Grundlage der Ermittlungsgeneralklausel grundsätzlich möglich.
Die LDI NRW macht aber darauf aufmerksam, dass die Einsicht in die Corona-Kontaktlisten, davon abhängt, ob die Erforderlichkeit und die Verhältnismäßigkeit dieser Zugriffe bejaht werden können. Erforderlich und verhältnismäßig sei ein Zugriff auf die Corona-Listen in der Regel nicht zur Aufdeckung von Kleinkriminalität, sondern lediglich zur Verfolgung erheblicher Straftaten, so die LDI NRW weiter.
Bei überschießenden Zugriffen und diese Anforderungen nicht beachtenden Verwendung der Corona-Listen, bestünde die Gefahr, dass die Akzeptanz in der Bevölkerung für die Erfassung der Kontaktdaten weiter sinke. Eine Konsequenz der Ablehnung in der Bevölkerung könne dann sein, dass nicht wahrheitsgemäße Angaben gemacht würden.

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW)