



Editorial:.....	2
Praxishilfe zum Gesundheitsdatenschutz	3
Einführung in den Datenschutz (Anzeige).....	3
Aufsichtsbehörde veröffentlicht Muster für Covid-19-Listen	4
Kündigungsschutz des DSB nach BDSG verstößt nicht gegen Art. 38 Abs. 3 DS-GVO	4
Neues DataAgenda-Arbeitspapier zum Datenschutz an Hochschulen während der Corona-Pandemie	4
GDD-Muster für Benennung und Stellenbeschreibung des DSB	5
Datenschutz-Praxishilfen.....	5
DataAgenda Arbeitspapiere (Anzeige).....	5
BBK mit Infos für das Homeoffice und Betreiber von KRITIS .	6
Praxis-Handbuch für die Datenschutz-Folgenabschätzung..	6
DS-GVO: Bußgeld-Liste wächst sukzessiv.....	7
Online-Schulungen für Ihre professionelle Weiterbildung (Anzeige).....	7
Neue BfDI-Broschüre zum Sozialdatenschutz	8
Leitlinien zur Einwilligung bei Internetseiten	8



Editorial:

Die Corona-Krise ist auch ein Treiber und Katalysator für Entwicklungen aus verschiedensten Bereichen. Unternehmen, Schulen und alle anderen Daten verarbeitenden Stellen sind einerseits weiterhin auf gemeinsames Lernen oder gemeinsames Arbeiten angewiesen, müssen jedoch aus nachvollziehbaren Gründen momentan „auf Abstand zueinander“ gehen. Vor allem hier werden schmerzlich Kollaborationstools- und Plattformen vermisst, die nicht nur praxiserprobt und intuitiv sind, sondern auch als rechtlich zulässig anerkannt sind.

Welchen Messenger können Schulen, Lehrer sowie Eltern und Schüler gerade in diesen Zeiten nutzen, um den notwendigen wechselseitigen Informationsfluss aufrechtzuerhalten? Ist **Threema** zulässig? Geht es vielleicht auch mit **WhatsApp**? Muss gar ein Messenger auf Grundlage eines offenen Standards wie **XMPP** („Jabber“) her?

Können Hausaufgaben und deren Lösungen auf OneDrive, Google Drive oder in der Dropbox gespeichert werden? Müssen sich Schulleitungen und Lehrer tatsächlich durch nicht untereinander abgestimmte Leitfäden und

Empfehlungen für Videokonferenz-Systeme, die von diversen Datenschutz-Aufsichtsbehörden veröffentlicht werden, kämpfen, bevor sie sich für eine **Lösung entscheiden**, während ihre zeitlichen Ressourcen woanders sinnvoller eingesetzt werden könnten? Müssen Nicht-Juristen und Menschen, die sich nicht tagtäglich professionell mit Datenschutz beschäftigen, **Handreichungen zu Themen wie Auftragsverarbeitung im Drittland**, Privacy Shield und „datenschutzrechtlich sichere Drittländer“ studieren, bevor sie sicher sein können, sich für das richtige Tool entschieden zu haben?

Dient es der Rechtssicherheit der Nutzer, wenn eine Datenschutz-Aufsichtsbehörde erst eine „Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen“ herausbringt, um diese dann **kommentarlos wieder von ihrer Internetseite** zu nehmen, nachdem sie von einem der kritisierten Anbieter „abgemahnt“ wurde?

Viele Fragen, die sich schon vor der aktuellen Pandemie stellten. Vielleicht sorgt aber der aktuelle Druck dafür, dass auf Fragen dieser Art schneller eine Antwort gefunden wird, hofft

Ihr Levent Ferik

Praxishilfe zum Gesundheitsdatenschutz

Unter der Mitarbeit des GDD-Arbeitskreises „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“ (AK GSW) wurden Praxishilfen zu den Themen „Arbeitsaufwand im Gesundheitsdatenschutz“ sowie „Anforderungen an ein Datenschutz-Cockpit“ erarbeitet und veröffentlicht.

Arbeitshilfe „Gemeinsame Empfehlung hinsichtlich des Arbeitsaufwands im Gesundheitsdatenschutz“

Die Arbeitshilfe „Gemeinsame Empfehlung hinsichtlich des Arbeitsaufwands im Gesundheitsdatenschutz“ stellt grundsätzlich den vollständigen Arbeitsaufwand für alle datenschutzrechtlichen Fragen dar, d.h. kumulativ der Aufwand aller Personen, die sich mit datenschutzrechtlichen Fragestellungen beschäftigen (z. B. IT-Mitarbeitende, die eine datenschutzrechtliche Dokumentation erstellen). Dabei wird eine professionelle Aufgabenerfüllung mit entsprechender Fachkenntnis vorausgesetzt. Eventuell notwendige Einarbeitungszeiten von nicht ausgebildeten Personen stehen nicht im Fokus dieser Arbeitshilfe und müssen gesondert betrachtet werden.

Die Empfehlungen sollen Verantwortlichen in der Gesundheitsversorgung helfen, den Aufwand resp. Arbeitsbedarf abzuschätzen, um so die benötigten personellen Ressourcen einplanen und bereitzustellen zu können. Daher werden die Empfehlungen in „Vollbeschäftigtenäquivalent“ (englisch „full time equivalent“ oder abgekürzt FTE) angegeben, wobei davon ausgegangen wird, dass eine FTE einer Arbeitszeit von 40 Stunden/pro Woche entspricht. Die Empfehlungen beruhen auf im Alltag erworbenen Erfahrungswerten; wissenschaftliche Untersuchungen zu dem aus dem Datenschutzrecht entstehenden Aufwand erfolgten bisher leider nicht, obwohl dies sicherlich ein spannendes Untersuchungsthema sein könnte.

Arbeitshilfe „Anforderungen an ein Datenschutz-Cockpit“

Die Arbeitshilfe „Anforderungen an ein Datenschutz-Cockpit“ wurde entwickelt, um eine bes-

sere Übersichtlichkeit im operativen Datenschutz herzustellen. In IT-Systemen fehlt regelhaft eine Möglichkeit, schnell einen Überblick zu Fragen des Datenschutzes zu erhalten. Diese Praxishilfe enthält einen Anforderungskatalog, aus dem Hersteller von IT-Systemen ein Pflichtenheft ableiten und so entsprechende Funktionalitäten in ihre Systeme einbauen können.

Beide Praxishilfen können Sie im Word-, Pdf-, Epub- oder Azw3-Format kostenfrei auf den Seiten (www.gesundheitsdatenschutz.org) der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS) e.V. herunterladen.

>>> Die Praxishilfe „Gemeinsame Empfehlung hinsichtlich des Arbeitsaufwands im Gesundheitsdatenschutz“ finden Sie hier

>>> Die Praxishilfe „Anforderungen an ein Datenschutz-Cockpit“ können Sie hier abrufen.

Anzeige



Einführung in den Datenschutz

Mitarbeiter schulen via E-Learning.

- ✓ Rechtssicher gemäß DS-GVO
- ✓ von einem Experten entwickelt
- ✓ Dauer: 45 Minuten
- ✓ Abschlusszertifikat
- ✓ auch in englischer Sprache verfügbar

Jetzt informieren:
datakontext.com/eLearning

**E-Learning in
TV-Studioqualität**

Aufsichtsbehörde veröffentlicht Muster für Covid-19-Listen

Um Infektionsketten und Ausbrüche von SARS-CoV-2 (Covid-19) schnellstmöglich zu erkennen und einzugrenzen, müssen etwa Frisöre, Kosmetikstudios aber auch Gaststätten und Cafés die Besuche ihrer Gäste oder Kunden dokumentieren.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern stellt auf ihrer Internetseite Formulare und Muster für die verschiedenen Branchen zur Verfügung, damit Infektionsschutz und Datenschutz gleichermaßen gewahrt werden können.

Die Landesbeauftragte empfiehlt alle Listen in Papierform zu führen, um die Verfahren zunächst möglichst einfach zu halten. Eine digitale

Erfassung könnte zu mehr Aufwand bei der Erfüllung datenschutzrechtlicher Vorgaben führen. Änderungen aufgrund neuer Bestimmungen oder Abstimmungen mit anderen Behörden behält sich die Aufsichtsbehörde vor und weist darauf hin, dass Betroffenenrechte grundsätzlich innerhalb von vier Wochen bearbeitet werden müssen. Diese Frist könne in Ausnahmefällen um weitere zwei Monate verlängert werden. Die betroffene Person müsse dann aber über die Gründe für die Fristverlängerung unterrichtet werden.

Quelle: [Die Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern](#)

Kündigungsschutz des DSB nach BDSG verstößt nicht gegen Art. 38 Abs. 3 DS-GVO

Mit Urteil vom 19.02.2020 (2 Sa 274/19) hat das LAG Nürnberg festgestellt, dass die nationalen Regelungen, wonach ein interner Datenschutzbeauftragter nur aus wichtigem Grund gekündigt und nur aus wichtigem Grund von seinem Amt abberufen werden kann (§ 38 Abs. 2 i. V. m. § 6 Abs. 4 BDSG), mit Art. 38 Abs. 3 Satz 2 DS-GVO vereinbar sind.

Die Kündigung des Arbeitsverhältnisses eines Datenschutzbeauftragten sei unzulässig, es sei denn, dass Tatsachen vorliegen, die den Arbeitgeber zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach einer wirksamen Abberufung als Datenschutzbeauftragter gelte dies noch für ein Jahr weiter (§§ 38 Abs. 2, 6 Abs. 4 Satz 3 BDSG). Dieser Sonderkündigungsschutz gelte auch bereits in der Probezeit.

Dieser besondere Kündigungsschutz auf nationaler Ebene verstoße nicht gegen Art. 38 Abs. 3 Satz 2 DS-GVO. Nach dieser Vorschrift dürfe

der Datenschutzbeauftragte wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Zwar sei davon auszugehen, dass die DS-GVO als EU-Verordnung unmittelbar und zwingend im Sinne einer Vollharmonisierung gelte und nicht lediglich Mindeststandards setze („Mindestharmonisierung“). Die Mitgliedstaaten dürften somit von ausdrücklichen Vorgaben der DS-GVO nur insoweit abweichen, wie dies die DS-GVO ausdrücklich oder durch Auslegung ermittelbar zulasse, und im Übrigen die Vorgaben der DS-GVO lediglich konkretisierten. Eine ausdrückliche Öffnungsklausel für den nationalen Gesetzgeber, einen besonderen Kündigungsschutz für Datenschutzbeauftragte zu regeln, finde sich in der DS-GVO nicht. Allerdings ergebe die Auslegung, dass die DS-GVO spezifisch arbeitsrechtliche Regelungen für den Datenschutzbeauftragten zulasse, soweit der Schutz nicht hinter der DS-GVO zurückbleibe.

LArbG Nürnberg, Urteil v. 19.02.2020 – 2 Sa 274/19

Neues DataAgenda-Arbeitspapier zum Datenschutz an Hochschulen während der Corona-Pandemie

Die Corona-Pandemie hat Auswirkungen auf nahezu jeden Lebensbereich. Genauso wie die Wirtschaft und Verwaltung soll auch das Leben an Universitäten und Hochschulen nicht zum Erliegen kommen. Unter Verwendung digitaler Möglichkeiten lassen sich die Lehre, aber unter gewissen Anforderungen auch die Prüfungen digital abhalten. Dabei müssen jedoch datenschutzrechtliche Anforderungen angemessen und funktionierend umgesetzt sein.

Das neue Arbeitspapier zeigt, was beim digitalen Prüfen rechtlich zu beachten ist. Im digitalen Semester sind Hochschulen nicht nur organisatorisch gefragt. Die Ausarbeitung erklärt welche rechtlichen Spielräume bestehen und wie Lösungen in der gegenwärtigen Praxis aussehen könnten.

GDD-Muster für Benennung und Stellenbeschreibung des DSB

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) existiert erstmals eine europaweit verbindliche und verpflichtende Regelung zur Benennung betrieblicher und behördlicher Datenschutzbeauftragter .

Während die EG-Datenschutzrichtlinie (95/46/EG) die Verpflichtung zur Benennung von Datenschutzbeauftragten lediglich als Alternative vorsah, um die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde entfallen zu lassen, ergibt sich mit der Geltung der DS-GVO erstmals eine Benennungspflicht unmittelbar aus dem Europarecht. Das deutsche Erfolgsmodell der datenschutzrechtlichen Selbstkontrolle hat sich damit auch auf europäischer Ebene durchgesetzt. In Ergänzung zur europarechtlichen (Basis-) Benennungspflicht berechtigt die DS-GVO außerdem über eine Öffnungsklausel die Mitgliedstaaten dazu, weitergehende Benennungspflichten auf nationaler Ebene vorzusehen. Von dieser Regelungsmöglichkeit hat der deutsche Gesetzgeber mit § 38 Bundesdatenschutzgesetz (BDSG) Gebrauch gemacht. Neben den Regelungen über die Benennungspflicht enthält die DS-GVO Regelungen zur Rechtsstellung und zu den Aufgaben des Datenschutzbeauftragten, von denen der nationale Gesetzgeber nicht abweichen darf.

Die Gesellschaft für Datenschutz und Datensicherheit hatte bereits Anfang 2019 eine Praxishilfe zum Thema „**Datenschutzbeauftragter nach der DS-GVO**“ der Allgemeinheit zur Verfügung gestellt (Praxishilfe I). Die Praxishilfe I gibt dem Interessierten einen Überblick über die Regelungen zur Benennung von Datenschutzbeauftragten sowie deren Aufgaben und Stellung.

Mit der neuesten Publikation rundet die GDD dieses Themengebiet ab, in dem sie ein Muster zur **Benennung und Stellenbeschreibung** für Datenschutzbe-

auftragte zur Verfügung stellt. Die GDD empfiehlt der Benennung zum/zur Datenschutzbeauftragten eine Stellenbeschreibung beizufügen, die Aufgaben und Stellung des jeweiligen Datenschutzbeauftragten im Einzelnen und bezogen auf die individuellen Besonderheiten beim Verantwortlichen bzw. Auftragsverarbeiter beschreibt.

Ziel sei es, die rechtlichen Vorgaben zu Aufgaben und Stellung des Datenschutzbeauftragten, unter Berücksichtigung von Größe und Organisation der benennenden Stelle sowie der Komplexität der Datenverarbeitung, zu konkretisieren.

Quelle: GDD e.V.

Anzeige

Datenschutz-Praxishilfen

DataAgenda Arbeitspapiere



Monatlich aktuelle und tiefgehende Praxishilfen zum Umgang mit dem Datenschutzrecht

Ob Cookies, Brexit oder Personenfotografie – die DataAgenda Arbeitspapiere helfen Ihnen, Datenschutz-Themen DS-GVO-konform in der Praxis umzusetzen. Mit unseren Musteraushängen, Tabellen und Fact Sheets sind Sie für jede Herausforderung gewappnet.

»Zu den DataAgenda Arbeitspapieren

BBK mit Infos für das Homeoffice und Betreiber von KRITIS

Die Eindämmung des Corona-Virus liegt in der Zuständigkeit der Bundesländer, dort vor allem in den für Gesundheit zuständigen Ressorts. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übernimmt eine Beratungsfunktion für den Krisenstab des BMI / BMG, steht im Austausch mit den Innenministerien der Länder und stellt seine Produkte, Fähigkeiten und Informationsmöglichkeiten zur Lageunterstützung nach Bedarf und in Abstimmung mit den zuständigen Stellen zur Verfügung.

In diesem Zusammenhang hat das BBK zahlreiche Leitfäden veröffentlicht, die auch mittelbar den Bereich der IT-Sicherheit adressieren.

Mit dem Leitfaden „**COVID-19: Interne Kommunikation im Krisenmodus**“ gibt das BBK auch eine Handlungsempfehlung mit Schwerpunkt Homeoffice heraus. Mit der darin enthaltenen Checkliste möchte das BBK Führungskräften und auch Mitarbeitenden in einem Unternehmen oder einer Behörde helfen, ihre Kommunikation im Krisenmanagement zu überprüfen und gegebenenfalls aktiv steuernd in Kommunikationswege und -kanäle einzugreifen. Diese Checkliste richtet sich vorrangig an Organisationen, bei denen eine Vielzahl von

Mitarbeitenden lagebedingt im längeren und dauerhaften „Homeoffice“ ist. Mit dem Begriff Homeoffice bezieht sich das BBK auf das Arbeiten von zu Hause aus, unabhängig davon, ob die Mitarbeitenden einen regulären Homeoffice-Arbeitsplatz haben oder nun situationsbedingt ohne weitere Vorkehrungen mit ihren dienstlichen und z.T. auch privaten Geräten bestmöglich ihr Arbeitspensum daheim absolvieren.

Eine weiteres Papier mit dem Titel „**COVID-19: Übersicht Kritischer Dienstleistungen**“ stellt eine Sammlung nützlicher Links für Betreiber von KRITIS dar. Darin sind sektorspezifische Hinweise und Informationen mit KRITIS-Relevanz enthalten. Um die Transparenz zu aktuellen Entwicklungen in den einzelnen Sektoren im Kontext kritischer Infrastrukturen zu verbessern, enthält die Übersicht Sektoren, Branchen und kritische Dienstleistungen sowie eine Auswahl der im Rahmen der Corona-Lage sektorspezifisch veröffentlichten Leitlinien, Empfehlungen und sonstiger relevanter Hinweise.

Quelle: *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)*

Praxis-Handbuch für die Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (DSFA) soll gem. Art. 35 DS-GVO eine umfassende Risikobewertung von Datenverarbeitungsvorgängen ermöglichen.

Wer personenbezogene Daten verarbeitet und dadurch die Rechte von Personen gefährden könnte, muss seit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung (DS-GVO) eine Datenschutz-Folgenabschätzung durchführen. Dabei handelt es sich um eine systematische Risikoanalyse, die bereits vor Inbetriebnahme einer Datenverarbeitung zu erstellen ist und zum Ziel hat, etwaige Gefahren zu erkennen, diese in ihrer Tragweite zu bewerten und geeignete Abhilfemaßnahmen zu ergreifen.

Das Fraunhofer-Institut für System- und Innovationsforschung ISI, gefördert mit Mitteln des Bundesministeriums für Bildung und For-

schung, hat ein Praxishandbuch (AuthorInnen: Martin, Nicholas; Friedewald, Michael; Schiering, Ina; Mester, Britta A.; Hallinan, Dara;) mit dem Titel „Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO – Ein Handbuch für die Praxis“ veröffentlicht.

Dieses Praxishandbuch gibt eine knappe Einführung in die Vorgaben der DS-GVO an die Datenschutz-Folgenabschätzung und die damit verbundenen Ziele. Es erläutert die Voraussetzungen für die erfolgreiche Durchführung und erläutert Schritt für Schritt, wie eine Datenschutz-Folgenabschätzung in fünf Phasen praktisch umgesetzt werden kann.

Das ebook ist unter nachfolgender URL kostenlos abrufbar: <http://publica.fraunhofer.de/documents/N-586394.html>

DS-GVO: Bußgeld-Liste wächst sukzessiv

Mit der seit 25. Mai 2018 anwendungspflichtigen Datenschutz-Grundverordnung (DS-GVO) hat der Datenschutz radikal an Bedeutung gewonnen. Grund dafür ist nicht etwa eine grundlegend veränderte Regulierung der Verarbeitung personenbezogener Daten, sondern ganz maßgeblich der erhöhte Bußgeldrahmen.

Sah das alte Bundesdatenschutzgesetz (BDSG) nur Bußgelder bis zu einer Höhe von 300.000 Euro vor, so erlaubt die DS-GVO den Aufsichtsbehörden bereits beim ersten Verstoß, wie etwa einer Datenverarbeitung ohne Rechtsgrundlage oder einer fehlenden Informationspflicht, ein Bußgeld von bis zu 20 Mio. Euro zu verhängen. Dabei spielt es keine Rolle, wie groß das Unternehmen ist. Jede datenverarbeitende Stelle – ob ein kleiner Verein oder ein mittelständisches Unternehmen – ist damit diesen extremen Bußgeldern potenziell ausgesetzt.

Inzwischen hat die DS-GVO in vielen Unternehmen ihren Projektstatus verloren und ist erfolgreich, wenn auch sicher noch nicht abschließend, umgesetzt. Einige Betriebe haben aber die sicherlich nicht immer angemessene Aufregung rund um die DS-GVO im Mai 2018 an sich vorbeiziehen lassen und keine Anpassungen an diesen neuen EU-Rechtsakt vorgenommen. Da die ersten Bußgelder, die regelmäßig als Argumentationshilfe bemüht wurden, zunächst auf sich warten ließen, freuten sich die untätigen Unternehmen wahrscheinlich schon über die Kostenersparnis durch die fehlende DS-GVO-Umsetzung und verfielen dem Glauben, dass die Gefahr der hohen Bußgelder nur theoretischer Natur war.

In den knapp zwei Jahren DS-GVO ist die Bußgeld-Liste aber nun doch sukzessive gewachsen und sowohl die Anzahl der verhängten Bußgelder als auch die Bußgeldhöhen sind durchaus beachtlich. Mit 1 & 1 (Telekommunikationsanbieter) und der Deutschen Wohnen (Immobilienwirtschaft) sind in Deutschland zwei bekannte, wenn auch nicht führende Unternehmen, mit Bußgeldern in Millionenhöhe sanktioniert worden. Auch in anderen EU-Mitgliedstaaten gab es bereits Bußgelder in Millionenhöhe.

So soll etwa Google in Frankreich 50 Mio. Euro für rechtswidrige Datenverarbeitungen und mangelnde Transparenzpflichten bezahlen. Die genannte Bußgeldhöhe von 20 Mio. Euro kann nämlich sogar überschritten werden, wenn vier Prozent des Vorjahreskonzernumsatzes die 20 Mio. Euro überschreiten. Unabhängig von der Risikohaftigkeit der mit der Kerntätigkeit des Unternehmens verbundenen Datenverarbeitung befinden sich in jeder Personalabteilung jedes Unternehmens besonders sensible und damit besonders schützenswerte Daten. Gerade die von der DS-GVO verlangten, dem Risiko der Verarbeitung dieser Daten angemessenen technischen und organisatorischen Maßnahmen (TOMs) wurden von vielen Unternehmen bis heute nicht implementiert. Dass die zwei deutschen Bußgelder in Millionenhöhe gerade auf solche Mängel zurückzuführen sind, wird sicher ein Umdenken zur Folge haben.

Anzeige



GDD-Datenschutz-Akademie goes digital:

Online-Schulungen für Ihre professionelle Weiterbildung

■ live ■ interaktiv ■ dialogorientiert

Alle digitalen Angebote finden Sie unter:
www.datakontext.com/online-angebote

Neue BfDI-Broschüre zum Sozialdatenschutz

Durch die DS-GVO wird auch im Bereich des Sozialrechtes der Datenschutz gestärkt. Der Bundesgesetzgeber hat das Sozialgeheimnis und die zentralen Vorschriften des Sozialdatenschutzes im Zehnten Buch Sozialgesetzbuch (SGB X) sowie die übrigen Fachgesetze den vorrangigen europäischen Vorgaben angepasst.

Die Zulässigkeit der Verarbeitung von Sozialdaten unterliegt einem besonders komplexen gesetzlichen Gefüge. Neben der vorrangig anzuwendenden DS-GVO finden sich viele ergänzende Regelungen im SGB X, aber auch als bereichsspezifische Regelungen in den Büchern der einzelnen Sozialversicherungszweige (SGB III, V, VI, VII, XI) oder in anderen Gesetzen wie beispielsweise dem Wohngeldgesetz, dem Bundeskindergeldgesetz oder Teilen des Bundeselterngeld- und Elternzeitgesetzes.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) möchte mit dem der Broschüre „**Info 3 – Sozialdatenschutz – Die Bürger und ihre Daten im Netz der sozialen Sicherheit**“ dazu beitragen, die Datenschutzbestimmungen des Sozialrechts transparent zu machen und Sozialversicherte über ihre Rechte informieren. Die Info 3 richtet sich also vor allem an Bürgerinnen und Bürger, aber auch an Mitarbeiterinnen und Mitarbeiter von Sozialversicherungsträgern.

Stand: April 2020

Quelle: *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*

Leitlinien zur Einwilligung bei Internetseiten

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) informiert darüber, dass der Europäische Datenschutzausschuss (EDSA) seine Leitlinien zur Einwilligung in die Nutzung von Internetseiten aktualisiert hat. Als eine besonders praxisrelevante Bewertung in den Leitlinien dürfte die Meinung des Ausschusses zu bewerten sein, dass der Zugang zu einem Web-Service nicht abhängig von der Erlaubnis in das Setzen von sogenannten Cookies sein darf. Auch die bloße Weiternutzung einer Seite soll nicht als wirksame Einwilligung angesehen werden.

„Es gibt immer noch Internetseiten, die durch Ihren Aufbau den Nutzenden Tracking aufdrängen. Die aktualisierten Leitlinien machen

erneut deutlich, dass Einwilligungen nicht erzwungen werden können. Die meisten Cookie-Walls und die Annahme, dass das Weitersurfen eine Einwilligung bedeutet, widersprechen dem Aspekt der Freiwilligkeit und verstoßen gegen die Datenschutz-Grundverordnung. Ich wünsche mir, dass Verantwortliche daraus die richtigen Schlüsse ziehen und endlich datenschutzfreundliche Alternativen anbieten“, so der BfDI in seiner Pressemitteilung.

Quelle: *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen?
Dann tragen Sie sich unverbindlich und kostenlos ein unter www.datakontext.com/newsletter