NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

AUSGABE
12/2021

DATAKONTEXT


Levent Ferik

EDITORIAL

Es gibt einen „E-Mail-Dienst“ dessen Kosten sich auf ca. 1.000,- EUR pro Nachricht summieren und trotzdem (oder eher gerade deswegen) wird er wohl bald gänzlich eingestellt. Auch wenn Sie zu den vielen Millionen gehören, die den Dienst nicht genutzt haben, ahnen Sie es vielleicht trotzdem, um welchen Dienst es geht.

Rund 6.000 Nachrichten hat die Bundesverwaltung nach Berechnungen des Bundesrechnungshofs wohl zwischen 2016 und 2019 über den rechtssicheren E-Mail-Dienst De-Mail versandt. Aufbau und Betrieb der entsprechenden Plattform kosteten den Bund bis 2020 „mindestens 6,5 Millionen Euro“, haben die Prüfer des Bundesrechnungshofes mit spitzem Bleistift zusammengerechnet. Erwartet wurden für diesen Zeitraum übrigens 6 Millionen De-Mails und Einsparungen in Höhe von 3,5 Mio. Euro. Heraus kam eine „Einsparung“ in Höhe von knapp 3.500 Euro. Im Jahr 2014 hatte die Bundesregierung das Ziel ausgegeben, De-Mail als Standardverfahren der Bundesverwaltung zu etablieren. In der Erwartung des BMI sollte De-Mail als elektronisches Pendant zur Briefpost in der Bundesverwaltung etabliert werden.

Wie man besser mit finanziellen Ressourcen und vor allem mit Steuergeld umgehen kann, zeigt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Kurz vor Nikolaus gab der BfDI in einem Newsletter die Veröffentlichung von zwei Kinderbüchern, aus der nicht nur Eltern und Kindern geläufigen PIXI-Reihe, bekannt: „Pixi Wissen – Was ist Datenschutz?“ sowie „Pixi Buch – Das ist privat!“. Auch wenn der Run auf die Bücher nicht so groß war, dass die Aktion zu einer ungewollten DoS-Attacke ausartete, musste der BfDI kurz nach der Veröffentlichung seines Newsletters vermelden, dass durch die hohe Zahl der Bestellungen Verzögerungen bei der Auslieferung zu erwarten sind.

Und falls sich jemand tatsächlich fragt, ob Publikationen des BfDI und Pixi-Bücher zusammenpassen, sollte sich den Erwägungsgrund 38 der DS-GVO anschauen. Wer hingegen auch bei dem Wort Weihnachten nur an die DS-GVO und der Vereinbarkeit von geschäftlicher Weihnachtspost mit dem Datenschutz denkt, dem wird vielleicht hier geholfen.
In diesem Sinne, frohe Weihnachten und ein gesundes, neues Jahr wünscht Ihnen Ihr

Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: ryanking999, Adobe Stock

Handreichung und Präventionsprüfung zu Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern (v.a. durch Verschlüsselung) und eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines Lösegelds (engl. ransom). Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Mai 2021 ein Papier zum Thema „Ransomware – Bedrohungslage, Prävention & Reaktion 2021“ veröffentlicht und auf den Umstand hingewiesen, dass sich in den letzten Jahren die Bedrohungslage durch Ransomware deutlich verschärft hat. Nach den Erfahrungswerten des BSI zahlen Opfer in vielen Fällen das geforderte Lösegeld, da der Leidensdruck für die Betroffenen extrem hoch ist. Dieser Erfolg der Täter führe dazu, dass mittlerweile Kapazitäten aus dem „Banking-Trojaner-Geschäft“ abgezogen werden und die Botnetze nun Ransomware verteilen.

Das BSI stellt in dem oben genannten Dokument neben einer kurzen Darstellung der Bedrohungslage konkrete Hilfen für die Prävention und die Reaktion im Schadensfall bereit.

Daher überrascht es nicht, dass sich aktuell auch das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) dieser Problematik angenommen hat und das Thema aus der Perspektive einer Datenschutz-Aufsichtsbehörde vorantreiben möchte. Anlässlich der enorm gestiegenen Gefährdungslage im Internet führt das BayLDA Prüfungen durch, um grundlegende Sicherheitslücken oder Mängel in der IT-Organisation aufzuzeigen und Verantwortliche somit noch vor einem Vorfall hinsichtlich des Bedarfs an durchzuführenden Maßnahmen hinzuweisen. Die Behörde weist auf den vorbeugenden Charakter der Datenschutzkontrollen hin, stellt aber gleichzeitig fest, dass seit der Anwendbarkeit der DS-GVO, neben der bereits existierenden gesetzlichen Verpflichtung, für ein ausreichendes Sicherheitsniveau im Umgang mit personenbezogenen Daten zu sorgen, auch grundsätzlich die Möglichkeit besteht, bei (gravierenden) Verstößen gegen die Sicherheit der Verarbeitung nach Art. 32 DS-GVO Geldbußen zu verhängen.

Die sog. „Ransomware Präventionsprüfung“ richtet sich naturgemäß an private Wirtschaftsunternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden in Bayern, jedoch dürfte der Blick in die vom BayLDA veröffentlichten Prüfdokumente auch für Verantwortliche in anderen Bundesländern ein gutes Hilfsmittel sein, den von einer Aufsichtsbehörde als notwendig erachteten SOLL-Zustand mit dem im Unternehmen bestehenden IST-Zustand abzugleichen und zu überprüfen, ob die technischen und organisatorische Maßnahmen nach Art. 32 DS-GVO ausreichend sind, einen Basisschutz gegen Ransomware-Angriffe zu gewährleisten.

Die Prüfunterlagen können hier abgerufen werden:

Praxisthemen:

- ✓ Vorlageverfahren EuGH
- ✓ Aktuelle Entwicklungen in der nationalen und europäischen Bußgeldpraxis
- ✓ Arbeitsaufwand im Datenschutz quantifizieren – am Beispiel Gesundheitswesen
- ✓ „Garantien" im Datenschutz – aktueller Stand zu Verhaltensregeln nach Art. 40 DS-GVO
- ✓ Datenschutz bei Microsoft
- ✓ TTDSG – Anforderungen und Herausforderungen für die Praxis
- ✓ Tracking auf Webseiten
- ✓ Nutzung von Videokonferenzlösungen außereuropäischer Anbieter

24.–25.01.2022
online

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Foto: PixPartout, Adobe Stock

Telekommunikations-Telemediendatenschutz-Gesetz (TTDSG) in Kraft getreten

Zum 01.12.2021 ist das neue TTDSG in Kraft getreten. Ziel der Neuregelung ist die erforderliche Anpassung der Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) an die Datenschutz-Grundverordnung (DS-GVO) sowie die – bereits lange ausstehende – Umsetzung der e-Privacy-Richtlinie (RiLi 2002/58/EG in der durch die RiLi 2009/136/EG geänderten Fassung).

Das hat zur Folge, dass es seit dem 01.12.2021 ein neues TKG gibt. Das bisherige TMG besteht in einer gekürzten Fassung fort. In beiden Gesetzen werden keine Datenschutzvorschriften mehr enthalten sein. Auch hier gibt es bzgl. der praktischen Relevanz noch Unsicherheiten bei den Unternehmen:

- Für wen gelten die Regelungen des TTDSG?
- Unter der bisherigen Rechtslage wurden von der herrschenden Meinung auch Arbeitgeber als geschäftsmäßige TK-Anbieter eingestuft, sofern diese die private Nutzung der betrieblichen Kommunikationsmittel erlauben. Ist das immer noch so?
- Welche praktische Relevanz haben die neuen Bestimmungen für „normale“ Unternehmen und öffentliche Stellen, sofern diese Cookies im Rahmen des Websitebetriebs einsetzen?
- Sind die Datenschutz-Aufsichtsbehörden überhaupt zuständig für den Vollzug des TTDSG?

Mit diesen und anderen Fragen beschäftigt sich die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und stellt auch weiterführende Informationen zum TTDSG in er GDD-Praxishilfe „Das neue TTDSG im Überblick“ bereit, die hier abgerufen werden kann.

Auch die Datenschutz-Aufsichtsbehörden haben mittlerweile einige Orientierungsleitfäden und FAQs zum Thema veröffentlicht:

1. Berliner Beauftragte für Datenschutz und Informationsfreiheit
2. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt Hamburg
3. Die Landesbeauftragte für den Datenschutz Niedersachsen
4. Sächsischer Datenschutzbeauftragter

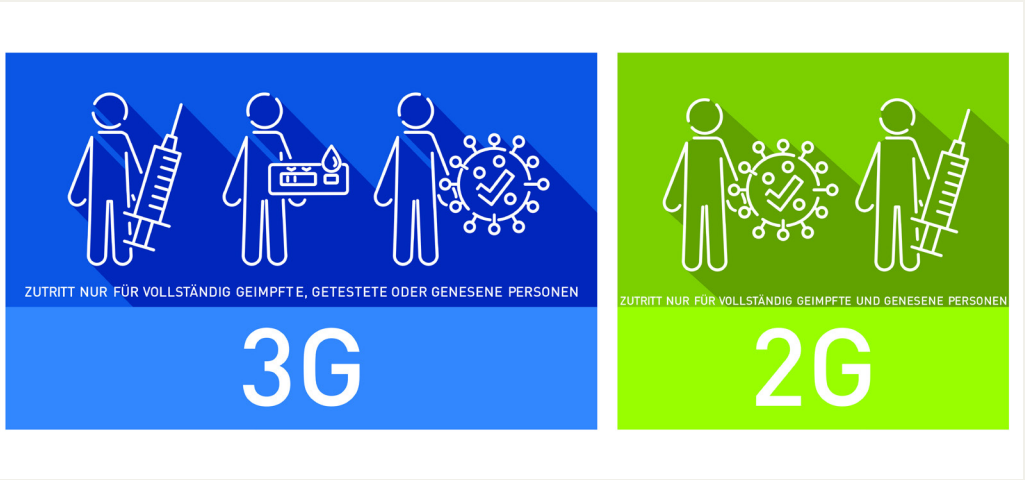

Foto: Fiedels, Adobe Stock

Umsetzung der 3G-Regelung – Hinweise und Orientierung

Nach wie vor bestehen bei den Verantwortlichen Unsicherheiten bzgl. der praktischen Umsetzung der 3G-Regelungen und vor dem Hintergrund datenschutzrechtlicher Anforderungen auch Unsicherheiten im Hinblick auf die Umsetzbarkeit der Regelungen. In Anbetracht unterschiedlicher Organisationsstrukturen bieten offizielle Informationsquellen nicht immer die für die verantwortliche Stelle passenden Best Practices. Daher sollen nachfolgend einige Links und Anlaufstellen genannt werden, die eine gute erste Orientierung und auch weiterführende Hinweise bieten:

1. Bundesministerium für Arbeit und Soziales (BMAS) – Fragen und Antworten Betrieblicher Infektionsschutz

Erste Anlaufstelle für eine Orientierung und Informationsquelle der ersten Stunde dürfte die Seite des BMAS sein, die zudem regelmäßig aktualisiert wird. Die Hinweise gehen auch auf datenschutzrechtliche Fragestellungen ein.
Erreichbar unter:

2. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)

Abfragen von Gesundheitsdaten durch Arbeitgeber_innen?
3G-Nachweis im Beschäftigtenverhältnis (§ 28b Abs. 1 und 3 IfSG) Orientierungshilfe des LfDI

3. Der Bayerische Landesbeauftragte für den Datenschutz

FAQ-Sammlung zur Verarbeitung von 3G/3G plus/2G im Beschäftigtenverhältnis (Stand 11.11.2021)

4. Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Aktuelle Kurz-Information 38: 3G-Zutrittsregel im bayerischen öffentlichen Dienst

5. Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Verarbeitung des COVID-19-Impfstatus im bayerischen öffentlichen Dienst Arbeitspapier

Weiter auf DataAgenda lesen

Foto: bluedesign & Daniel Berkmann, Adobe Stock

GDD äußert sich zu Datenschutz im Koalitionsvertrag

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. nimmt die am 24.11.2021 erfolgte Veröffentlichung des Koalitionsvertrags 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90/Die Grünen und den Freien Demokraten (FDP) zum Anlass, um die wesentlichen Aussagen zum Thema Datenschutz herauszuarbeiten:
Im Koalitionsvertrag setzen sich SPD, Bündnis 90/Die Grünen und FDP für eine bessere Kohärenz des Datenschutzes ein. Dazu soll die europäische Zusammenarbeit verbessert und der Datenschutzkonferenz im Bundesdatenschutzgesetz rechtlich verbindliche Beschlüsse ermöglicht werden.

Weiter auf DataAgenda lesen

E-LEARNING
Mitarbeiter online sensibilisieren:
In 45 Minuten Datenschutzrisiko mindern

nur 14,90 € (netto) Einstiegspreis pro Schulung

Jetzt kostenlos testen:
elearning-mit-zertifikat.de

UNIVADO
DATAKONTEXT

Foto: denisismagilov, Adobe Stock

Handreichung Videokonferenzsysteme – Hinweise zur praktischen Nutzung

Beim Thema Videokonferenzsysteme gibt es auch Ende des Jahres 2021 nach wie vor Unsicherheiten bei den Nutzern und insbesondere den Verantwortlichen. Der Bedarf an diesen war nie gänzlich weg und ist mit Beginn der 4. Corona-Welle und der teilweise gesetzlichen verordneten Homeoffice-Pflicht größer denn je.
Daher dürfte es die meisten Verantwortlichen als eine gute Unterstützung empfinden, dass der LfDI Baden-Württemberg eine aktuelle Handreichung zu diesem Dauerbrenner veröffentlicht hat. Die aktuelle Publikation „Handreichung Videokonferenzsysteme – Hinweise zur praktischen Nutzung“ soll Unternehmen, Behörden und Vereine bei der Auswahl geeigneter Videokonferenz-Dienste unterstützen. Es gibt einen auf das Wesentliche beschränkten Überblick über die rechtlichen und technischen Datenschutz-Anforderungen, beschreibt einige gängige Anbieter und stellt tabellarisch eine Übersicht an Eigenschaften der Softwares und Dienste dar. Das formulierte Ziel des LfDI BW: Wer Videokonferenzen veranstalten möchte, soll sich orientieren können, was unterschiedliche Systeme leisten und welche „Baustellen“ es gibt.
Dabei betrachtet der LfDI BW die grundsätzlich in drei Varianten betreibbaren Alternativen:

1. Das System wird auf Basis eigener Infrastruktur und Software vollständig selbst betrieben, oder der Verantwortliche greift dabei auf einen Dritten zurück, der die Videokonferenz (VK) als externer IT-Dienstleister mitsamt Hard- und/ oder Software anbietet.
2. Aktuell greifen die meisten Verantwortlichen auf die zweite Möglichkeit, einen Online-Dienst (Software as a Service) zurück. Diese Fallgestaltung untersucht der LfDI näher und gibt Empfehlungen zu den einschlägigen rechtlichen und technischen Fragestellungen, wobei er eine Reihe von verbreiteten Online-Dienste-Anbietern näher betrachtet.
3. Anstatt das Videokonferenzsystem selbst zu betreiben oder von einem Dienstleister nach eigenen Vorstellungen betreiben zu lassen, gibt es auch die Möglichkeit, bestehende Online-Dienste zu verwenden.

Da die größten und bekanntesten Anbieter von Videokonferenzprodukten ihren Firmensitz allerdings in den USA haben und dort (zumindest teilweise) die personenbezogenen Daten der Teilnehmenden als auch der Organisatoren einer Videokonferenz verarbeiten, geht die Handreichung auch auf die spezielle Drittlandproblematik ein. Bei Datenübermittlungen in die USA oder andere Drittstaaten sind die Anforderungen des Kapitels V der DS-GVO einzuhalten.

Foto: vanillya, Adobe Stock

Abdingbarkeit des Art. 32 DS-GVO

Eine als Vermerk veröffentlichte Publikation des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) fand bereits April 2021 in Datenschutzkreisen einige Beachtung.
Darin beschäftigte sich der HmbBfDI mit der Frage, ob betroffene Personen in ein niedrigeres Schutzniveau einwilligen können, als rechtlich geboten ist. Es gehe dabei um die Frage, ob oder inwieweit es sich bei den Vorgaben des Art. 32 DS-GVO um zwingende, nicht zur Disposition der betroffenen Person stehende Vorgaben handele. Die Frage, ob Art. 32 DS-GVO zwingendes, nicht zur Disposition stehendes Recht darstellt, sei besonders praxisrelevant, weil dies teilweise mit dem Argument bejaht werde, dass die DS-GVO einen europäischen Mindeststandard des Systemdatenschutzes schaffen wolle.

Auf der anderen Seite würde es jedoch eine erhebliche Beschränkung der Entscheidungsfreiheit der betroffenen Personen bedeuten, wenn eine Verarbeitung ihrer personenbezogenen Daten, die sie ausdrücklich wünschen, mit Verweis auf den Systemdatenschutz nicht durchgeführt werden kann. Als praxisrelevantes Beispiel werden in dem Vermerk Arztpraxen, Steuerberater oder Anwälte genannt, bei denen ein undifferenziertes Festhalten an dieser Auffassung dazu führen würde, dass die Auskünfte oder die Übermittlung dringend benötigter Unterlagen per einfacher E-Mail nicht durchgeführt würden, da sie befürchten müssten, Art. 32 DS-GVO zuwiderzuhandeln, selbst wenn die betroffene Person ausdrücklich in die unsichere Übermittlungsart einwilligt hat.

Mit dieser Fragestellung hat sich nunmehr auch die DSK beschäftigt und hat ihre Sichtweise in einem Beschluss (vom 24. November 2021) veröffentlicht. Darin kommt sie zu folgenden Ergebnissen:

1. Die vom Verantwortlichen nach Art. 32 DS-GVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen.
2. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO ist nicht zulässig.
3. Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.
4. Kapitel V der DS-GVO (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) bleibt hiervon unberührt.

Gesellschaft für Datenschutz und Datensicherheit e. V.

GDD-Praxishilfe „Die Datenschutz-Richtlinie“ veröffentlicht

Unternehmen, Vereine und Behörden sind nach der DS-GVO verpflichtet, jederzeit nachweisen zu können, dass und wie sie die gesetzlichen Datenschutzanforderungen umsetzen (Rechenschaftspflicht oder Accountability).
In der Praxis stellt sich allerdings die Frage, wie dieser Nachweis zu führen ist, etwa im Fall der Prüfung durch die Aufsichtsbehörde, im Rahmen eines Datenschutzaudits oder bei der Prüfung des Auftragsverarbeiters durch den Auftraggeber. Gelebter Datenschutz in einer Organisation wird zudem nur möglich, wenn den dort Tätigen klar ist, was ihre Aufgaben und Pflichten sind. Klare und auf das Wesentliche reduzierte interne Regelungen tragen insofern dazu bei, Haftungsrisiken für den Verantwortlichen zu reduzieren sowie (Handlungs-)Sicherheit für die Beschäftigten zu schaffen.
Um das Datenschutzmanagement einer Organisation zu dokumentieren, hat sich die Erstellung und Einführung von Leit- und Richtlinien zum Datenschutz bewährt. Während Leitlinien die Datenschutzziele einer Organisation in ihren Grundzügen beschreiben, geben Richtlinien den Rahmen zur Umsetzung konkreter Maßnahmen zur Erreichung dieser Ziele vor. Mit Blick auf die Accountability ist insbesondere die Inkraftsetzung von Datenschutz-Richtlinien ein zentrales Mittel, um den Nachweis eines aktiven Datenschutzmanagements innerhalb einer Organisation erbringen zu können. Sinnvollerweise sollten Datenschutz-Richtlinien einer Datenschutz-Leitlinie vorangestellt werden, welche die Bedeutung des Datenschutzes unterstreicht, Ziele definiert und die gesamte Organisation auf die Einhaltung der gesetzlichen sowie internen Datenschutzvorgaben verpflichtet.
Die neue GDD-Praxishilfe liefert Begriffsdefinitionen, formuliert Anforderungen an Inhalt und Form interner Datenschutzvorgaben und beschreibt die Zuständigkeiten für den Erstellungs-, Prüfungs- und Freigabeprozess. Sie soll als Hilfe zur Selbsthilfe dienen und Anleitung zur Erstellung individueller interner Regelwerke sein.
Die neue GDD-Praxishilfe liefert Begriffsdefinitionen, formuliert Anforderungen an Inhalt und Form interner Datenschutzvorgaben und beschreibt die Zuständigkeiten für den Erstellungs-, Prüfungs- und Freigabeprozess. Sie soll als Hilfe zur Selbsthilfe dienen und Anleitung zur Erstellung individueller interner Regelwerke sein.
Die Praxishilfe können Sie hier downloaden.
Alle Praxishilfen finden Sie hier.

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

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

GDD-BASIS-SCHULUNG TEIL 1

Einführung in den Datenschutz für die Privatwirtschaft

07.–11.02.2022 I Köln
14.–15.02. + 17.–18.02. + 22.02.2022 I Online
29.11.–03.12.2021 I Köln
RA Andreas Jaspers, Thomas Müthlein,
Prof. Dr. Rolf Schwartmann

Schwerpunkte:

- ✓ Einführung in das Datenschutzrecht
- ✓ Arbeitnehmerdatenschutz
- ✓ Kundendatenschutz und Fallübungen
- ✓ Umsetzung des Datenschutzes in der Praxis

Jetzt anmelden: **www.datakontext.com**

GDD DATAKONTEXT