NEWS BOX DATENSCHUTZ

AUSGABE
6/2021

INHALTSVERZEICHNIS

DATAKONTEXT

Levent Ferik

EDITORIAL

Es gibt Datenschutz-Interessierte und es gibt Menschen, die nicht genug bekommen können vom Datenschutz. Es gibt Menschen, die sich gerne und beruflich mit dem Thema „Datenschutz" beschäftigen und daneben gibt es Datenschutz-Begeisterte, die auch nach Feierabend nicht davon loskommen.
Wenn Sie also nicht nur die einzelnen Artikel der DS-GVO „anregend" finden, sondern erst bei der Lektüre der passenden Erwägungsgründe entspannen, werden Sie möglicherweise auch Spaß an Datenschutz-Podcasts haben. Diese können Sie nämlich auch dann konsumieren, wenn die Augen schon von der ganzen Leserei entzündet sind. Folgende Angebote lassen sich beispielsweise auch während einer längeren Autofahrt zum Mandanten oder beim Joggen konsumieren.
In die Gedankenwelt des LfDI Baden-Württemberg können Sich mit dem Podcast „Datenfreiheit! – Der LfDI-Podcast" einfühlen.
Uneingeschränkt zu empfehlen sind auch die „Video-Tutorials" des LfDI BW, so zum Beispiel zum Thema „Verzeichnis der Verarbeitungstätigkeiten" und zum Thema „Löschkonzept".

Holger Bleich und Joerg Heidrich führen Sie mit dem Podcast „Auslegungssache" des c't Magazins nicht nur durch die Untiefen des Datenschutzes, sondern des viel breiteren IT-Rechts.

Sehr erfrischend und spannend: Sie lernen bei jedem Podcast nebenbei die Persönlichkeiten Ihrer „Datenschutz-Fiterblase" kennen.
Der auch sonst innovative Dr. Thomas Schwenke (zusammen mit Marcus Richter) hat ebenfalls einen Podcast „Rechtsbelehrung", der seit vielen Jahren Datenschutz-Jünger mit qualitativ überzeugenden und gleichzeitig unterhaltsamen Content versorgt.
Last but not least, ein Neuzugang in der Podcast-Szene: Der 10-Minuten-Talk mit Prof. Schwartmann.
Meinungen, kontroverse Diskussionen und die Einordnung von aktuellen Datenschutz-Themen – das alles bietet in kurzweiligen, rund 10-minütigen Kurztalks der neue DataAgenda Datenschutz Podcast. Mit immer wechselnden Gesprächspartnern aus der deutschen Datenschutzszene bringt Herr Prof. Schwartmann die aktuell spannenden Themen auf den Punkt, verständlich und informativ.
Lassen Sie mich gerne wissen, wenn Sie weitere Empfehlungen haben.
Weiterhin viel Spaß mit dem Datenschutz,

wünscht Ihnen
Ihr Levent Ferik

Sagen Sie uns Ihre Meinung
kundenservice@datakontext.com

Foto: Robert Kneschke, Adobe Stock

Anspruch auf unentgeltliche Kopie von Examensklausuren nach Art. 15 DS-GVO

Ein Urteil des Oberverwaltungsgerichts dürfte so manchem Examenskandidaten ein Lächeln ins Gesicht zaubern, zumindest denjenigen, die ein Interesse daran haben, Einsicht in die angefertigten Aufsichtsarbeiten und Prüfergutachten zu erhalten – am besten unentgeltlich. Das ist möglich, sagt das Oberverwaltungsgericht und stützt diesen Anspruch auf Art. 15 Abs. 3 DS-GVO. Was war passiert?
Ein in Essen wohnhafter Examensabsolvent hatte im Jahr 2018 erfolgreich an der zweiten juristischen Staatsprüfung teilgenommen und beantragte im Oktober 2018 gegenüber dem Landesjustizprüfungsamt NRW Einsicht in die angefertigten Aufsichtsarbeiten und Prüfergutachten. Zugleich bat er um Übersendung von Kopien auf elektronischem oder postalischem Weg. Das Landesjustizprüfungsamt forderte daraufhin beim Kläger einen Vorschuss für Kopierkosten für insgesamt 348 Seiten in Höhe von 69,70 Euro an. Nachdem sich der Kläger unter Bezugnahme auf die Datenschutz-Grundverordnung geweigert hatte, diesen Betrag zu entrichten, lehnte das Landesjustizprüfungsamt die Übersendung ab.
Auf die Klage des Examensabsolventen hat das Verwaltungsgericht Gelsenkirchen das Land Nordrhein-Westfalen verurteilt, dem Kläger unentgeltlich Kopien der Aufsichtsarbeiten mitsamt Prüfergutachten auf postalischem oder elektronischem Weg zur Verfügung zu stellen.
Die gegen diese Entscheidung eingelegte Berufung hat das Oberverwaltungsgericht nunmehr zurückgewiesen.
Nach Auffassung des OVG kann der geltend gemachte Anspruch auf Zurverfügungstellung einer unentgeltlichen Datenkopie auf Art. 15 Abs. 3 DS-GVO gestützt werden. Daraus folge ein Anspruch auf Zurverfügungstellung einer unentgeltlichen Datenkopie sämtlicher vom Landesjustizprüfungsamt verarbeiteter, den Kläger betreffender personenbezogener Daten, worunter auch die angefertigten Aufsichtsarbeiten mitsamt Prüfergutachten fallen sollen. Weiterhin stellte das OVG fest, dass das Recht aus Art. 15 Abs. 3 DS-GVO insoweit keiner einschränkenden Auslegung auf bestimmte Daten oder Informationen unterliege. Anhaltspunkte für ein rechtsmissbräuchliches Verhalten des Klägers konnte der 16. Senat nicht erkennen. Als weiterer Versagungsgrund für eine unentgeltliche Kopie hätte noch ein unverhältnismäßiger Aufwand aus der Perspektive des Landesjustizprüfungsamts angeführt werden können. Aber auch dieses Argument war nach Wertung des Senats nicht stichhaltig.

Quelle: Oberverwaltungsgericht Nordrhein-Westfalen

Foto: bilderstoeckchen, Adobe Stock

Wissenschaftspreis für Datenschutz und Datensicherheit

Auch in diesem Jahr vergibt die Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) erneut einen Wissenschaftspreis für herausragende wissenschaftliche Arbeiten in den Bereichen Datenschutz und Datensicherheit. Der Preis beträgt 5.000,00 €. Der Preis kann auch zwischen mehreren Arbeiten aufgeteilt werden.
Der Preis soll bevorzugt an Nachwuchswissenschaftler vergeben werden. Es sollen fertiggestellte oder in der Fertigstellung befindliche Abschlussarbeiten oder Doktorarbeiten ausgezeichnet werden. In Betracht kommen neben Arbeiten aus den Rechtswissenschaften, Wirtschaftswissenschaften und der Informatik auch Arbeiten aus anderen Wissenschaftsdisziplinen, in denen Fragen aus den Bereichen Datenschutz und Datensicherheit behandelt werden. Voraussetzung für die Vergabe des Wissenschaftspreises ist die Erfüllung der wissenschaftlichen Exzellenzkriterien.
Die Arbeiten müssen mit Befürwortung des betreuenden Hochschullehrers bei der GDD-Geschäftsstelle bis zum **31. Juli 2021** eingereicht werden.
Nähere Informationen zum Wissenschaftspreis stehen als PDF-Datei und Word-Dokument zum Download zur Verfügung.

NRW hat eine neue Landesbeauftragte für Datenschutz und Informationsfreiheit

Der Landtag von Nordrhein-Westfalen hat am 19. Mai 2021 einstimmig Bettina Gayk zur neuen Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen gewählt. Damit folgt sie auf Helga Block, die im vergangenen Jahr nach fünf Jahren in den Ruhestand gegangen ist. Die Landesbeauftragte für Datenschutz und Informationsfreiheit wird jeweils auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen.
Die Landesbeauftragte wacht über die Einhaltung der datenschutzrechtlichen Vorschriften in Nordrhein-Westfalen. Bürgerinnen und Bürger können sich bei Fragen zum Informationsfreiheitsrecht oder Verstößen gegen den Datenschutz an die Behörde wenden. Die Beauftragte kümmert sich zudem darum, dass Bürgerinnen und Bürger ihr Recht auf freien Zugang zu behördlichen Informationen wahrnehmen können. Daneben berät sie öffentliche und private Stellen bei grundlegenden datenschutzrechtlichen Problemen.
Die neue LDI NRW arbeitete von 2001 bis 2012 unter der Landesdatenschutzbeauftragten Bettina Sokol und Ulrich Lepper als Referatsleiterin und Pressesprecherin.

Foto: Fotolyse, Adobe Stock

Quelle: LDI NRW

14. GDD

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Sommer-Workshop

FÜR DATENSCHUTZBEAUFTRAGTE UND -BERATER SOWIE DATENSCHUTZDIENSTLEISTER

9. bis 11. August 2021

in Timmendorfer Strand

Praxisthemen

- Aktuelle Entwicklungen im Datenschutz
- Anforderungen an einen Beschäftigtendatenschutz
- Richtiger Umgang mit Richtlinien zur Vermeidung von Bußgeldern
- Der Auskunftsanspruch nach Art. 15 DS-GVO
- Die neuen Standarddatenschutzklauseln im Praxischeck
- Binding Corporate Rules – Interne Datenschutzvorschriften für Unternehmen
- Gute Gründe warum man amerikanische Bürosoftware nutzen darf
- Personal Information Management Systeme (PIMS) – Wege zum systematischen Einwilligungs- und Widerspruchsmanagement
- Privacy by Design & Default im Automotive-Umfeld
- Daten in der Corona-Pandemie
- Hacken
- Pandemiebekämpfung mit Apps & Co - Datenschutz als Showstopper?
- Schadensersatz nach DS-GVO: Kleine Preise, aber große Gefahr für Unternehmen?!

Wahrung der Anonymität des Petenten durch die Aufsichtsbehörde

Foto: freshidea, Adobe Stock

Jede Person hat das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, wenn sie glaubt, dass eine bestimmte sie betreffende Datenverarbeitung gegen die DS-GVO verstößt.

Insbesondere wenn sich Beschäftigte wegen vermuteter Datenschutzverstöße an die zuständige Aufsichtsbehörde wenden wollen, bestehen jedoch oftmals Befürchtungen, dass sich ihre Beschwerde negativ auf das Arbeitsverhältnis auswirken könnte.

Die LfD Niedersachsen erläutert in ihrem 26. Tätigkeitsbericht für das Jahr 2020, in welchen Fällen sich Petenten auf die Wahrung der Anonymität verlassen können (S. 78 ff).

Beschwerdeführende können sich nach Angabe der LfD Niedersachsen grundsätzlich auf die Wahrung ihre Anonymität verlassen. Die Behörde gebe den Namen der Beschwerde führenden Person nicht weiter, wenn sie die Verantwortliche zur Stellungnahme auffordere. Die Namensnennung sei jedoch in einigen Fällen nicht vermeidbar. Diese Nennung des Namens sei beispielsweise naturgemäß erforderlich, um dem Verstoß nachgehen zu können, z.B. bei einer behaupteten Verletzung des Auskunftsrechts nach Art. 15 DS-GVO oder anderer Betroffenenrechte.

Auch im Falle der gewährten Akteneinsicht werde die Anonymität weiterhin gewahrt, da der Name des Beschwerdeführenden unkenntlich gemacht werde. Dieses Vorgehen können sogar auf das Urteil des VG Hannover vom 21. Januar 2020 (Az. 10 A 768/19) gestützt werden.

Die LfD macht jedoch darauf aufmerksam, dass die Anonymität des Beschwerdeführenden dann nicht mehr durch die Behörde gewahrt werden könne, wenn die Angelegenheit in ein Ordnungswidrigkeitenverfahren münde. Im Ordnungswidrigkeitenverfahren bestehe ein umfassendes Recht auf Akteneinsicht, sodass eine Beschränkung wegen der Rechte Dritter, anders als im Verwaltungsverfahren, nicht vorgesehen sei.

Quelle: Die Landesbeauftragte für den Datenschutz Niedersachsen

Foto: dp@pic, Adobe Stock

Highlander-Prinzip, Stellvertreter und Hilfskräfte des Datenschutzbeauftragten

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) stellt die Ergebnisse seiner Arbeit aus dem Jahr 2020 vor. In dem am 25. Mai 2021 veröffentlichten 30. Tätigkeitsbericht werden neben diversen datenschutzrechtlichen Einzelfragen auch einige Aspekte zum Tätigkeitsfeld des Datenschutzbeauftragten erläutert.

Das sog. Highlander-Prinzip: Es kann nur einen geben

Der BayLfD beschäftigt sich mit der Frage, ob es zulässig sei, dass eine bayerische öffentliche Stelle mehrere Datenschutzbeauftragte mit jeweils klar abgegrenzter Zuständigkeit benenne. Die klare Verneinung dieser Fragestellung stützt der BayLfD auf den Wortlaut des Art. 37 Abs. 1 lit. a) DS-GVO. Aus dem Wortlaut könne geschlossen werden, dass ein Verantwortlicher in Erfüllung seiner gesetzlichen Verpflichtung jeweils nur einen Datenschutzbeauftragten benennen kann.
Die Benennung mehrerer Datenschutzbeauftragter durch ein und denselben Verantwortlichen sei rechtlich nicht möglich, da ein solches Vorgehen die Gefahr berge, dass sich insbesondere betroffene Personen zunächst an die „falsche“, weil für ihr jeweiliges Anliegen unzuständige Stelle wenden. Dies würde insbesondere eine effektive Durchsetzung von Betroffenenrechten erschweren. Die hier vorgetragenen Argumente können natürlich nicht nur für bayerische öffentliche Stellen bzw. nicht nur bei öffentlichen Stellen vorgetragen werden.

Stellvertreter, Hilfskräfte und Datenschutzkoordinatoren/Datenschutz-Ansprechpartner

Die Benennung eines stellvertretenden Datenschutzbeauftragten jedoch sieht der BayLfD nicht nur als zulässig, sondern vielmehr sogar als geboten an. Vor dem Hintergrund, dass ein solcher nur im Vertretungsfall, insbesondere bei Urlaub oder Erkrankung des „eigentlich“ benannten Datenschutzbeauftragten, an dessen Stelle tritt, könnten die oben geschilderten Vorbehalte (kein eindeutiger Ansprechpartner in Datenschutzfragen) gar nicht zum Tragen kommen, da ein Stellvertreter des Datenschutzbeauftragten im Vertretungsfalle vollumfänglich in Erscheinung trete. Nach außen hin erkennbare Unklarheiten oder Abgrenzungsfragen hinsichtlich der Zuständigkeiten seien hier nicht zu befürchten. Ferner lasse es die dargestellte Auffassung zu, dass der Datenschutzbeauftragte durch Hilfskräfte bei seiner Aufgabenerfüllung unterstützt werden kann. Ab einer bestimmten Größe der Verantwortung werde dies ohnehin unabdingbar sein. Aus Art. 38 Abs. 2 DS-GVO könne eine solche Unterstützung sogar geschlussfolgert werden. Schließlich habe der Verantwortliche seinem Datenschutzbeauftragten, gemäß Art. 38 Abs. 2 DS-GVO, die zur Aufgabenerfüllung erforderlichen – gegebenenfalls auch personellen – Ressourcen zur Verfügung zu stellen.

Quelle: Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Foto: insta_photos, Adobe Stock

BSI: Informationen für digitalen und sicheren Schulalltag

Es ist zwar primär die Aufgabe des Verantwortlichen, für die Sicherheit der IT-Infrastruktur zu sorgen, jedoch stellen auch schlecht informierte Nutzerinnen und Nutzer ein gewisses Sicherheitsrisiko dar. Nicht nur deshalb sollte IT-Sicherheit auch ein Thema in Lehrerfortbildungen, in der Lehrerausbildung und im Unterricht sein.
Dass es hier Optimierungsbedarf gibt, hat sich gerade vor dem Hintergrund der Corona-Pandemie deutlich gezeigt, als Lehrerinnen und Lehrer ohne größere Vorbereitungszeit „ins kalte Wasser" geworden wurden. Denn das digitale Lehren und Lernen birgt einige Sicherheitsrisiken. Anfang des Jahres wurden beispielsweise Unterrichtsstunden von Unbefugten gekapert oder der Unterricht musste wegen DDoS-Angriffen auf Schulplattformen zeitweise komplett ausfallen.

Seit März 2020 müssen LehrerInnen immer wieder ihren Lehrauftrag vom Klassenraum in eine digitale Umgebung verlegen. Sie sammeln seitdem viele Erfahrungen, insbesondere was die Vermittlung von Lerninhalten auf digitalen Wegen angeht. In diesem Kontext tauchen im Schulalltag aber auch immer wieder Fragen zur IT-Sicherheit auf: Wie kann ich meinen Unterricht per Video vor Scherzen und Störungen schützen? Welche Einstellungen sichern meine SchülerInnen und mich ab? Was mache ich im Notfall?
Vor diesem Hintergrund hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Materialien zur Sensibilisierung von Lehrerinnen und Lehrern zusammengestellt, die sie als Hilfestellung für den grundsätzlichen Basisschutz ihrer Geräte und Daten oder zur Anwendung im Unterricht nutzen können. Das Informationsangebot wird stetig erweitert und hat das Ziel, die Kompetenzen von Lehrerinnen und Lehrern in puncto Cyber-Sicherheit zu stärken und ihnen Tipps für mehr Sicherheit im digitalen Unterricht mit auf den Weg zu geben.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Foto: CrazyCloud, Adobe Stock

10 Missverständnisse zum Thema „Anonymisierung"

Der Europäische Datenschutzbeauftragte und die spanische Datenschutz-Aufsichtsbehörde haben ein gemeinsames Papier über 10 Missverständnisse im Zusammenhang mit Anonymisierung veröffentlicht.
Die technologischen Entwicklungen der letzten Jahre haben die Nachfrage nach hochwertigen Daten stetig erhöht, so die Autoren des Papiers. In diesem Zusammenhang würden sowohl öffentliche als auch private Stellen die Anonymisierung als Mittel zur gemeinsamen Nutzung von Daten in Betracht ziehen, ohne dabei die Grundrechte des Einzelnen zu verletzen. Mit der wachsenden Popularität der Anonymisierung habe sich jedoch auch einige Missverständnisse in Bezug auf die Anonymisierung verbreitet.

Weiter auf DataAgenda lesen

Internationaler Datentransfer: Koordinierte Prüfung durch Aufsichtsbehörden

In seiner Schrems-II-Entscheidung hat der EuGH festgestellt, dass Übermittlungen in die USA nicht länger auf Basis des sogenannten Privacy Shields erfolgen können. Der Einsatz der Standarddatenschutzklauseln für Datenübermittlungen in Drittstaaten ist nur noch unter Verwendung wirksamer zusätzlicher Maßnahmen ausreichend, wenn die Prüfung des Verantwortlichen ergeben hat, dass im Empfängerstaat kein gleichwertiges Schutzniveau für die personenbezogenen Daten gewährleistet werden kann. Das Urteil des EuGH erfordert in vielen Fällen eine grundlegende Umstellung lange praktizierter Geschäftsmodelle und -abläufe.

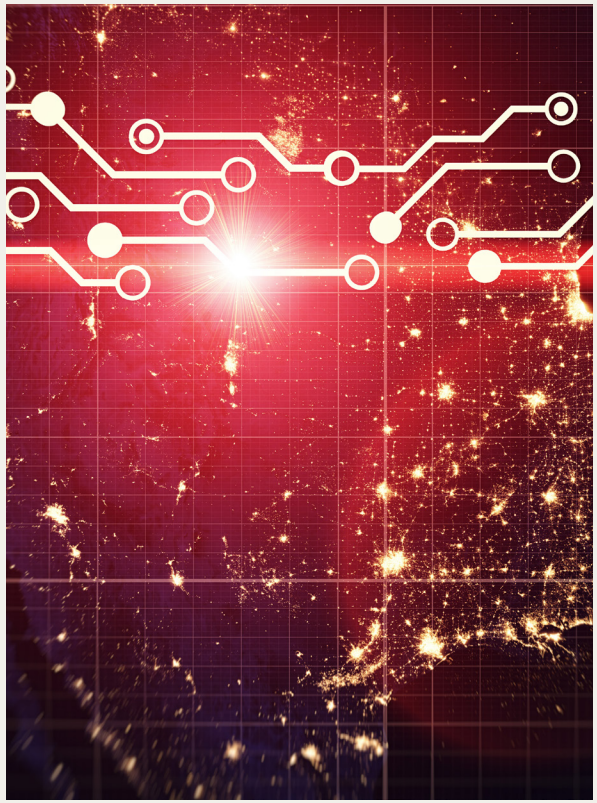


Foto: Jürgen Fälchle, Adobe Stock

Weiter auf DataAgenda lesen

25.000 EUR Bußgeld für automatische E-Mail-Weiterleitung

Foto: ra2 studio, Adobe Stock

Die Datenschutz-Aufsichtsbehörde in Norwegen hat ein Bußgeld in Höhe von 25.000 EUR gegen ein nicht namentlich benanntes Unternehmen verhängt. Grund war die Anordnung der automatischen Weiterleitung von E-Mails vom Postfach eines Mitarbeiters an einen gemeinsamen E-Mail-Firmenaccount.

Der Name des Unternehmens wurde nicht öffentlich bekannt gemacht, um die Identitäten der Mitarbeiter zu schützen.

Der Fall wurde durch eine Beschwerde eines Mitarbeiters ins Rollen gebracht, der feststellen musste, dass sein Arbeitgeber eine automatische E-Mails-Weiterleitung hatte einrichten lassen.

Die Weiterleitung erfolgte auf Anordnung des Arbeitgebers, eine automatische Weiterleitung von seinem E-Mail-Konto auf ein gemeinsames Firmen-E-Mail-Konto einzurichten. Für die Anordnung und die Weiterleitung gab der Arbeitgeber betriebliche Gründe an.

Nach einer Untersuchung der Angelegenheit kam die norwegische Datenschutzbehörde zu dem Schluss, dass dem Unternehmen eine Rechtsgrundlage für die Weiterleitung von E-Mails fehlte. Diese Anordnung und Weiterleitung erfolgte unter Verletzung der Vorschriften über den Zugriff des Arbeitgebers auf E-Mail-Konten und anderes elektronisches Material. Ebenso ließ sich die Maßnahme auch mit den Anforderungen der DS-GVO nicht in Einklang bringen.

Auf dieser Grundlage hat die Datenschutzbehörde das Unternehmen angewiesen, seine internen Kontrollverfahren und Richtlinien für den Zugriff auf die E-Mails der Mitarbeiter zu verbessern. Darüber hinaus wurde das Unternehmen zur Zahlung von 25.000,00 EUR verurteilt, weil die Weiterleitung des E-Mail-Verkehrs des Beschwerdeführers ohne eine rechtliche Grundlage erfolgt sei.

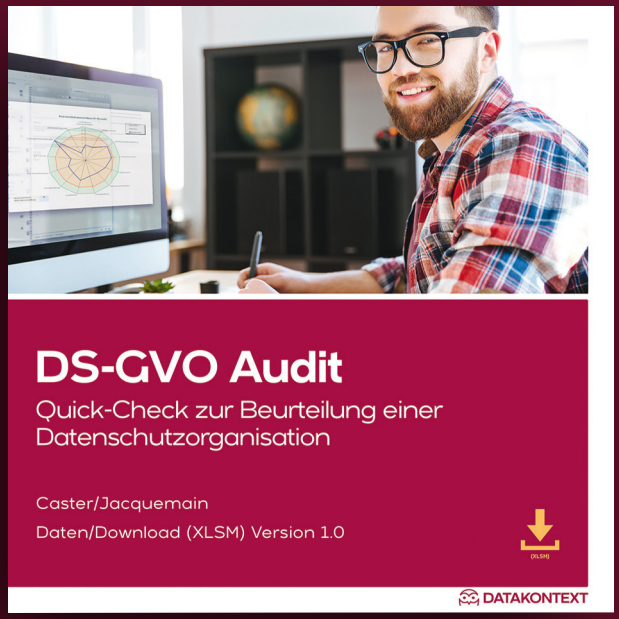
Quelle: European Data Protection Board

Ihr ständiger Begleiter im Datenschutz-Management.

NEU

Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren.

Datenschutz-organisationen prüfen und beurteilen mit begrenztem Zeitaufwand.



Datenschutz Excel-Tools

Bestellen Sie direkt unter: **datakontext.com**

DATAKONTEXT

Foto: Gorodenkoff, Adobe Stock

BSI bietet Selbst-Check für Informationssicherheit

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2020 legte das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die Cyber-Sicherheitsbehörde des Bundes einen umfassenden und fundierten Überblick über die Bedrohungen Deutschlands, seiner Bürgerinnen und Bürger und seiner Wirtschaft im Cyber-Raum vor.

Demnach bleibt die IT-Sicherheitslage in Deutschland angespannt. So verwendeten Angreifer Schadprogramme für cyber-kriminelle Massenangriffe auf Privatpersonen, Unternehmen, Behörden und andere Institutionen, aber auch für gezielte Angriffe.

Dass Cyber-Kriminelle schnell auf gesellschaftlich relevante Themen und Trends reagieren, zeigen unterschiedliche Angriffe unter Ausnutzung der COVID-19-Pandemie. Hier wurden beispielsweise Phishing-Kampagnen, CEO-Fraud und Betrugsversuche mit IT-Mitteln beobachtet. So gelang es Betrügern beispielsweise, Soforthilfe-Maßnahmen zu missbrauchen, indem sie die Antragswebseiten amtlicher Stellen täuschend echt nachahmten.

Mit dem sog. ExPress Informationssicherheits Check (EPIC) stellt das BSI ab sofort eine web-basierte Selbstüberprüfung zur Beurteilung des Status der Informationssicherheit für Behörden und Unternehmen zur Verfügung. Diese können mit dem Instrument eigenständig identifizieren, an welchen Stellen die Informationssicherheit ihrer Institution optimiert werden kann.

Das BSI betrachtet diese Möglichkeit vor allem in Pandemie-Zeiten mit stark eingeschränkten Möglichkeiten zur Durchführung von Vor-Ort-Prüfungen als ein Vorteil. Darüber hinaus könne der EPIC sinnvoll mit anderen Dienstleistungen des BSI rund um das Thema Sicherheitsprüfungen kombiniert werden, um zum Beispiel im Vorfeld einer IS-Revision oder eines IS-Penetrationstests grundlegende Aspekte der Informationssicherheit zu analysieren.

Der Check basiert auf umfangreichen Erfahrungswerten der IS-Revision des BSI und gliedert sich in 32 Fragen, die in sechs Themenfeldern (Sicherheitsmanagement, Organisation und Personal, Infrastruktur, IT-Systeme, Netzwerke sowie Anwendungen) gruppiert sind.

Durch die Beantwortung der Fragen soll eine Sensibilisierung für das Thema Informationssicherheit erfolgen und potenzielle Mängel aufgezeigt werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik

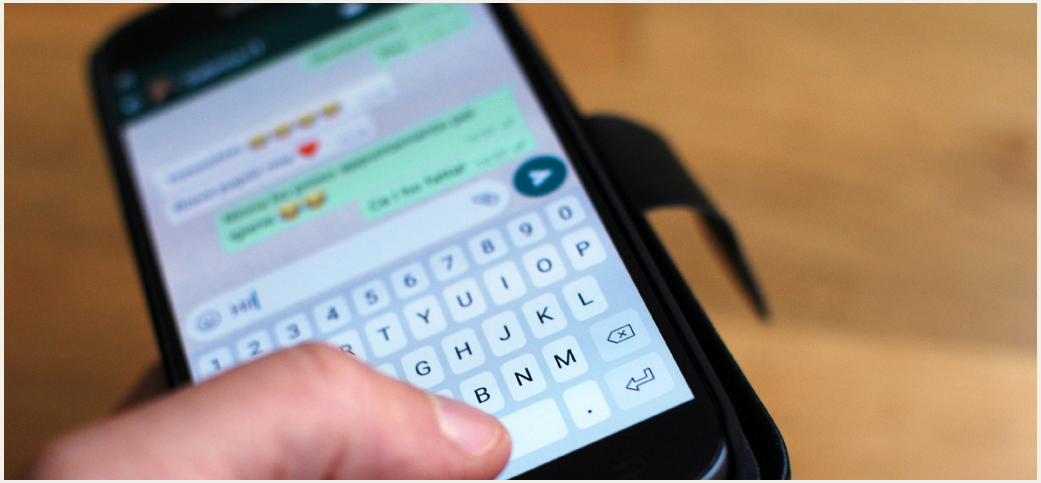


Foto: Sara Michilin, Adobe Stock

Keine Weitergabe von Nutzerdaten aus WhatsApp an Facebook?

Art. 66 DS-GVO (Dringlichkeitsverfahren) ist kein Artikel, der dem Datenschutz-Interessierten häufig begegnet. Darin ist normiert: *„Unter außergewöhnlichen Umständen kann eine betroffene Aufsichtsbehörde, abweichend vom Kohärenzverfahren nach Artikel 63, 64 und 65 oder dem Verfahren nach Artikel 60, sofort einstweilige Maßnahmen mit festgelegter Geltungsdauer von höchstens drei Monaten treffen, die in ihrem Hoheitsgebiet rechtliche Wirkung entfalten sollen, wenn sie zu der Auffassung gelangt, dass dringender Handlungsbedarf besteht, um Rechte und Freiheiten von betroffenen Personen zu schützen. Die Aufsichtsbehörde setzt die anderen betroffenen Aufsichtsbehörden, den Ausschuss und die Kommission unverzüglich von diesen Maßnahmen und den Gründen für deren Erlass in Kenntnis.“*
Die Anwendung des Art. 66 DS-GVO soll also auch nach dem Willen des Verordnungsgebers eher die Ausnahme sein. Das verdeutlicht auch Erwägungsgrund 138, der im zweiten Satz ausführt, dass in anderen Fällen von grenzüberschreitender Relevanz das Verfahren der Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden zur Anwendung gelangen soll, und die betroffenen Aufsichtsbehörden auf bilateraler oder multilateraler Ebene Amtshilfe leisten und gemeinsame Maßnahmen durchführen können, ohne auf das Kohärenzverfahren zurückzugreifen.
Nun hat der Hamburgische Beauftragte für Datenschutz (HmbBfDI) und Informationsfreiheit auf dieses Instrument zurückgegriffen, als er eine Anordnung erließ, die es Facebook verbietet, personenbezogene Daten von WhatsApp zu verarbeiten, soweit dies zu eigenen Zwecken erfolgt.
Anlass sind die seit geraumer Zeit kritisierten Bedingungen von WhatsApp mit denen die Befugnisse zur Datenverarbeitung formal erneuert und künftig inhaltlich erweitert werden sollen.
Darin, so der HmbBfDI, lasse sich WhatsApp insbesondere weitreichende Befugnisse für eine Datenweitergabe an Facebook einräumen.
Nach Auswertung des gegenwärtigen Sachstands fehle für eine Verarbeitung durch Facebook zu eigenen Zwecken, ungeachtet der von WhatsApp derzeit eingeholten Zustimmung zu den Nutzungsbedingungen, eine ausreichende rechtliche Grundlage, führt der HmbBfDI als Erklärung für seine Anordnung weiter aus. Die Bestimmungen zur Datenweitergabe fänden sich verstreut auf unterschiedlichen Ebenen der Datenschutzerklärung, sie seien unklar und in ihrer europäischen und internationalen Version schwer auseinanderzuhalten.

Aufgrund des beschränkten Zeitrahmens der Anordnung im Dringlichkeitsverfahren von lediglich drei Monaten werde der HmbBfDI eine Befassung durch den Europäischen Datenschutzausschuss (EDSA) beantragen, um eine Entscheidung auf europäischer Ebene herbeizuführen.

DATA AGENDA
PODCAST

Der **10-Minuten-Talk**
mit Prof. Schwartmann

Folge #1

Schrems II und die Folgen für die Nutzung von Bürosoftware (wie z.B. MS Teams) in Deutschland

Dr. Brink

Folge #2

Ein Gesetz gegen das Cookie-Dilemma – Das Telekommunikation-Telemedien-Datenschutz-Gesetz" – TTDSG

Thomas Jarzombek MdB

Folge 1: Schrems II und die Folgen für die Nutzung von Bürosoftware (wie z.B. MS Teams) in Deutschland

Zum Ende des Schuljahres gehen die Schulen in Deutschland wieder in den Regelunterricht. Homeschooling per Videokonferenz ist damit hoffentlich erst einmal Vergangenheit. Wenn es wieder dazu kommt, müssen Schulen den Datenschutz in den Griff bekommen. Aufsichtsbehörden sprechen in dieser Situation teilweise sogar von Bußgeldern für staatliche Schulen. Darüber, warum das rechtlich nicht möglich ist und was auch Unternehmen fast ein Jahr nach der Schrems-II-Entscheidung des Europäischen Gerichtshofes in Sachen Datenschutz beachten müssen, spricht Rolf Schwartmann spricht mit **Dr. Stefan Brink**, dem Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg. Zum Podcast bitte hier klicken.

Folge 2: Ein Gesetz gegen das Cookie-Dilemma – Das Telekommunikation-Telemedien-Datenschutz-Gesetz" – TTDSG

Seit Ende Mai 2021 ist das TTDSG beschlossene Sache. Der Gesetzgeber in Deutschland hat damit die Regelungen zum Datenschutz und zum Fernmeldegeheimnis im Bereich der Telekommunikation sowie der Telemedien in einem Gesetz zusammengefasst. Das Gesetz passt die Bestimmungen zum Onlinedatenschutz an die Vorgaben der DS-GVO und der ePrivacy-RL an und schließt damit bis zum Inkrafttreten der ePrivacy-Verordnung in Deutschland eine wichtige Regelungslücke. Wie kam es zum TTDSG? Was kann in der Praxis verändern werden? Und was nutzt es Nutzern und der Onlinewirtschaft? Rolf Schwartmann im Gespräch mit **Thomas Jarzombek (MdB)**, Beauftragter für die Digitale Wirtschaft und Start-ups des Bundesministeriums für Wirtschaft und Energie sowie Koordinator für Luft- und Raumfahrt der Bundesregierung. Zum Podcast bitte hier klicken.

Weitere Folgen unter DataAgenda.de/podcast

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

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

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Hans-Günter Böse, 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