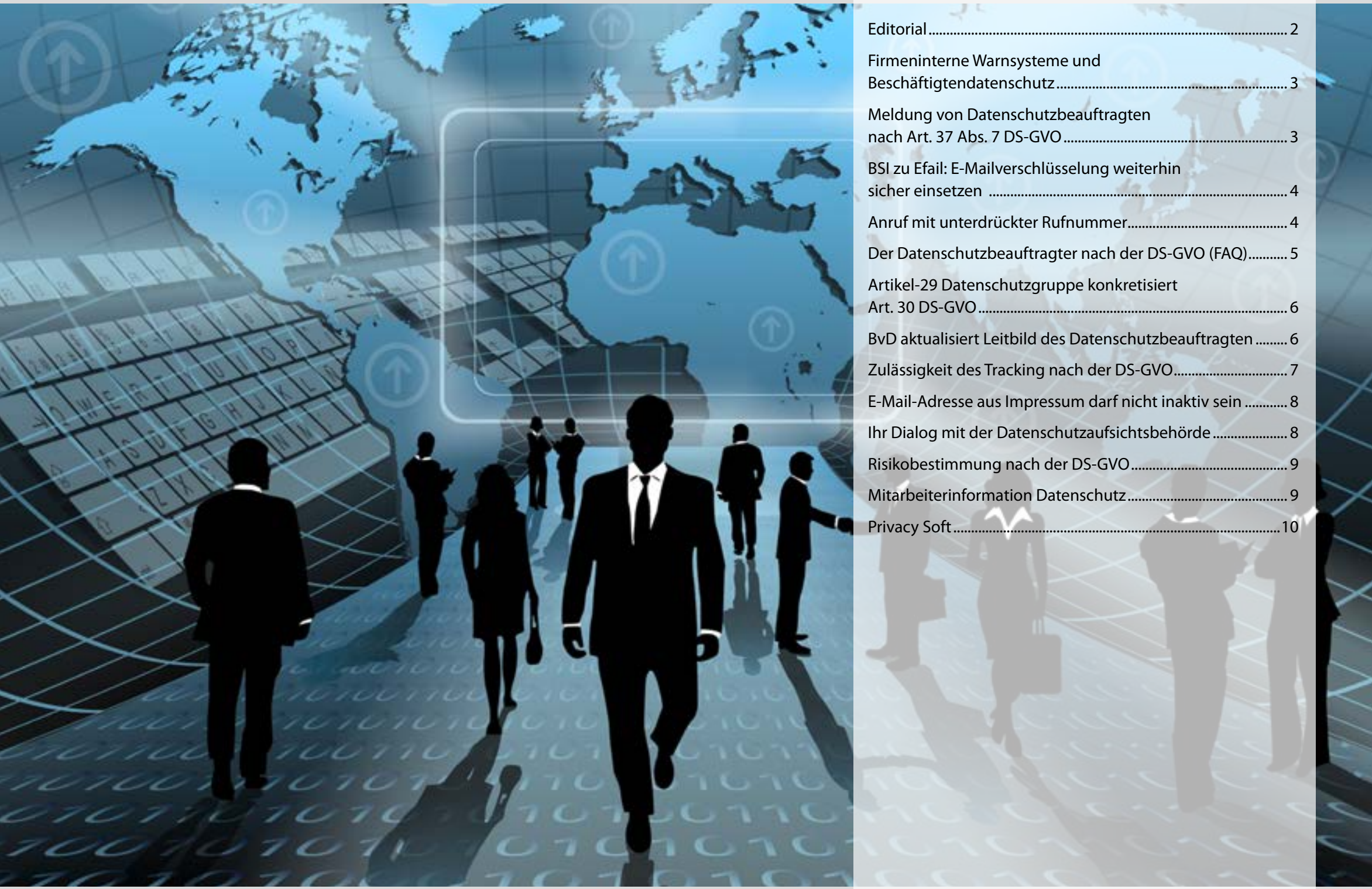
Datenschutz newsbox

Ausgabe 5 2018



DATAKONTEXT

Editorial

„Alles neu macht der Mai, macht die Seele frisch und frei“ heißt es in einem deutschen Volkslied. Und auch in Sachen Datenschutz gibt es anscheinend zum Ausklang des Monats Mai einiges an „digitalem Frühjahrsputz und Reinemachen“ bei der Verarbeitung personenbezogener Daten.
Die DS-GVO warf schon Jahre vor ihrem Wirksamwerden ihre Schatten voraus, aber spätestens mit dem Countdown im Mai scheinen bei Vielen die Nerven blank zu liegen.

Macht die DS-GVO tatsächlich Ehemaligen unmöglich Klassentreffen zu organisieren, oder erschwert die Planung zumindest soweit, dass sich das nostalgische Schwelgen in Erinnerungen nach dem 25.05.2018 der Vergangenheit angehören wird?

Hat die DS-GVO zur Folge, dass bald die Bestellung eines Aufgebots im Rahmen der kirchlichen Trauung nicht mehr möglich ist?

Können kleine und innovative Betreiber von Online-Games den Betrieb nicht mehr aufrechterhalten, weil der neue europäische Datenschutz den „Spaß“ vermiest?

Treten demnächst amerikanische Firmen den Rückzug aus Europa an und werden EU-Bürger künftig gar nicht mehr bedienen? Oder ist es gar ganz anders und die Amerikaner finden „unsere DS-GVO“ so prima, dass zumindest 69% der US-Bürger sich „DS-GVO-Schutz“ wünschen?

Können Fotografen bald nicht mehr „vernünftig“ ihrer Arbeit nachgehen? Gilt die DS-GVO auch im Weltraum? Werden Betroffene mit ihren „neuen Betroffenenrechten“ das Tagesgeschäft der Unternehmen zum Erliegen bringen?

Handelt es sich bei den meisten Meldungen zur DS-GVO um Fake-News? Ändert sich ggf. gar nicht so viel mit Wirksamwerden der DS-GVO, wenn der Verantwortliche bereits jetzt schon Datenschutz und Datensicherheit ernst genommen hat?

Essentielle und weniger essentielle Frage scheinen in den letzten Tagen durch das Wirksamwerden der DS-GVO aufgeworfen worden zu sein. Es ist nicht zu erwarten, dass die jetzige Verunsicherung mit dem Stichtag am 25.05.2018 ein Ende finden wird. Fest steht jedoch, dass die DS-GVO bereits jetzt zu einer gewissen natürlichen Selektion führt, was die bislang angebotenen Dienstleistungen angeht, die mit der Verarbeitung personenbezogener Daten zusammenhingen. Das dürfte aber, was die Motivation der DS-GVO angeht, kein Bug, sondern vielmehr ein Feature gewesen sein, meint

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

Firmeninterne Warnsysteme und Beschäftigtendatenschutz

Zu den Entschließungen der letzten Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder gehört auch die Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines. Die Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten zu Whistleblowing-Hotlines auf. Sie soll es den Arbeitgebern und den Interessenvertretungen der Beschäftigten erleichtern, im Unternehmen klare Regelungen zum Umgang mit Whistleblowing-Hotlines zu erreichen.

Firmeninterne Whistleblowing-Hotlines sind Angebote von Unternehmen an ihre Beschäftigten, ein nicht regelkonformes Verhalten anderer Beschäftigter dem Unternehmen zu melden. Mit der Meldung von Verstößen gegen Verhaltenspflichten geht die Verarbeitung von personenbezogenen Daten einher. Für jegliche automatisierte und nichtautomatisierte Verarbeitung von Beschäftigtendaten sind die Datenschutz-Grundverordnung (DS-GVO) und § 26 Bundesdatenschutzgesetz (BDSG) in Verbindung mit Art. 88 DS-GVO anzuwenden. Betroffene Personengruppen sind vor allem die Hinweisgeberinnen und Hinweisgeber sowie die beschuldigten Personen.

Die Aufsichtsbehörden beschränken sich auf die Beurteilung der datenschutzrechtlichen Zulässigkeit der personenbezogenen Datenverarbeitung bei Meldeverfahren unter Einsatz von firmeninternen Whistleblowing-Hotlines nach den Vorschriften der DS-GVO. Die Übermittlung von personenbezogenen Daten in Drittstaaten – beispielsweise aufgrund des US-amerikanischen SarbanesOxley Act (SOX) – ist nicht Gegenstand der datenschutzrechtlichen Beurteilung der vorliegenden Orientierungshilfe. Die Orientierungshilfe richtet sich in erster Linie an die Wirtschaft.

Quelle: *LDI NRW*

Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO

Hinsichtlich der Mitteilungspflicht der Kontaktdaten des Datenschutzbeauftragten gem. Art. 37 Abs. 7 DS-GVO an die jeweils zuständige Aufsichtsbehörde hat die LDI NRW ihre Informationen aktualisiert. Die Aufsichtsbehörde teilt mit, dass unterlassene Meldungen der Kontaktdaten der/des Datenschutzbeauftragten während einer Übergangszeit bis zum 31.12.2018 nicht als Datenschutzverstöße verfolgen werden oder geahndet werden. Weiter ist zu erfahren, dass Kontaktdaten, die vor dem 25. Mai 2018 mitgeteilt werden, keine Berücksichtigung finden werden. Vor diesem Zeitpunkt sei eine solche Mitteilung an die LDI NRW nicht erforderlich.
Ab Geltung der EU-Datenschutz-Grundverordnung (25. Mai 2018) jedoch werden Verantwortliche und Auftragsverarbeiter dazu verpflichtet sein, die Kontaktdaten ihrer oder ihres Datenschutzbeauftragten der zuständigen Aufsichtsbehörde mitzuteilen. Für Stellen mit Sitz in Nordrhein-Westfalen ist die LDI NRW zuständige Aufsichtsbehörde. Die deutschen Aufsichtsbehörden arbeiten an einer Lösung zur Umsetzung der Mitteilungspflicht der Kontaktdaten der oder des Datenschutzbeauftragten, so die LDI NRW. Es ist beabsichtigt, eine Möglichkeit zur Online-Meldung über die Homepage der LDI NRW anzubieten, sodass die Mitteilungen auf elektronischem Wege entgegengenommen werden. Welche Daten konkret zu melden sind und weitere Informationen können in den kommenden Monaten auf der Homepage der LDI NRW eingesehen werden.
Die Verfahrensweise der einzelnen Aufsichtsbehörden für das Verfahren aus Art. 37 Abs. 7 DS-GVO ist höchst unterschiedlich. So ist bspw. auf der Seite des Hessischen Datenschutzbeauftragten zu lesen, dass man davon ausgehe, dass Verantwortliche und Auftragsverarbeiter ihrer Mitteilungspflicht innerhalb von drei Monaten nachkommen, sobald das dafür geplante automatisierte Meldeverfahren nutzbar ist. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hingegen bietet jetzt schon die Möglichkeit der Meldung über ein Webformular an.

BSI zu Efail: E-Mailverschlüsselung weiterhin sicher einsetzen

Nach dem ein Forscherteam der FH Münster, der Ruhr-Universität Bochum und der KU Leuven Schwachstellen in den standardisierten E-Mail-Verschlüsselungsverfahren Open Pretty Good Privacy (OpenPGP) und S/MIME entdeckt hat, veröffentlicht das BSI Informationen, um sowohl die Verunsicherung der Nutzer zu beseitigen, als auch Hinweise zu geben, wie die Mail-Verschlüsselung implementiert werden muss, damit sie sicher eingesetzt werden kann.

Nach Angaben des BSI sind die beiden betroffenen Verschlüsselungstechniken die am häufigsten für eine Ende-zu-Ende-Verschlüsselung von E-Mails eingesetzten Verfahren. Während S/MIME bei den meisten E-Mail-Programmen bereits direkt genutzt werden kann, kommt bei OpenPGP meist ein weiteres Programm, wie GPG4Win (Windows), GPG Suite (macOS) oder ein Plug-in für das genutzte E-Mail-Progamm (z. B. Enigmail für Mozilla Thunderbird) zum Einsatz. Die genannten E-Mail-Verschlüsselungsstandards können nach Einschätzung des BSI allerdings weiterhin sicher eingesetzt werden, wenn sie korrekt implementiert und sicher konfiguriert werden. Mittelfristig ist allerdings die Anpassung der beiden Standards und deren Implementierung in den jeweiligen Anwendungen erforderlich, damit die Efail- oder vergleichbare Angriffe auf die E-Mail-Verschlüsselung mit OpenPGP und S/MIME nicht mehr möglich sind.

Nachdem ein Angreifer Zugriff auf verschlüsselte E-Mails eines Opfers erhalten hat, beispielsweise indem eine E-Mail während des Transports oder auf einem E-Mail-Server abgefangen wurde oder Zugriff auf ein E-Mail-Backup bestand, kann dieser die Efail-Schwachstellen ausnutzen. Um die E-Mail-Inhalte im Klartext einsehen zu können, wird eine verschlüsselte E-Mail durch den Angreifer mit aktiven Inhalten manipuliert. Nach der Entschlüsselung durch den Empfänger werden die aktiven Inhalte ausgeführt und der Klartext der E-Mail an einen Server des Angreifers übertragen. Das genaue Angriffsszenario wird von den Forschern auf der Webseite www.efail.de beschrieben.

Manche Anbieter von E-Mail-Programmen werden jetzt und in den kommenden Wochen Sicherheitsupdates veröffentlichen, die gegen Angriffe über die Efail-Schwachstellen schützen sollen. Wer verschlüsselte E-Mails nutzt, sollte daher alle Sicherheitsupdates für das entsprechende E-Mail-Programm direkt installieren. Unabhängig von der Bereitstellung von Sicherheitsupdates für E-Mail-Clients sind die folgenden Konfigurationsempfehlungen zu beachten.
Das BSI empfiehlt grundsätzlich für mehr Sicherheit bei der E-Mail-Kommunikation auf die Darstellung und Erzeugung von E-Mails im HTML-Format zu verzichten. Insbesondere sollte die Ausführung aktiver Inhalte, also das Anzeigen von E-Mails im HTML-Format sowie das Nachladen externer Inhalte ausgeschaltet werden. So können Nutzerinnen und Nutzer ein Ausspähen des E-Mail-Klartexts über die Efail-Schwachstellen verhindern. Sofern ein E-Mail-Provider über die Einstellungen seiner Webmail-Anwendung dazu die Möglichkeit bietet, sollten auch hier entsprechende Maßnahmen umgesetzt werden.
Um E-Mailverschlüsselung weiterhin sicher einsetzen zu können, müssen Anwender folgende Punkte umsetzen:

- Aktive Inhalte im E-Mailclient müssen deaktiviert werden. Dazu zählt die Ausführung von HTML-Code und das Nachladen externer Inhalte, die oftmals aus Design-Aspekten erlaubt sind.
- E-Mailserver und E-Mailclients müssen gegen unauthorisierte Zugriffsversuche abgesichert werden.

Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

Anruf mit unterdrückter Rufnummer

Fragen des GDD Erfa-Kreises Würzburg:
Stellt es einen unzulässigen Werbeanruf im Sinne des § 102 TKG dar, wenn ein Unternehmen einen säumigen Schuldner mit unterdrückter Rufnummer kontaktiert, um ihn zur Zahlung aufzufordern?

Antworten des BayLDA:
Bei der Anmahnung einer rückständigen Forderung per Telefonanruf, Brief, E-Mail etc., sehen wir in der Verwendung der Kontaktdaten keine werbliche Nutzung von personenbezogenen Daten im Sinne des § 28 Abs. 3 BDSG. Es geht hier bei der Datenverwendung für Mahnungen aus unserer Sicht um eine zulässige Datennutzung im Rahmen der Abwicklung eines Vertragsverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wenn ein Vertragspartner der vereinbarten Leistungspflicht nicht nachkommt.
Wir sind allerdings nicht die zuständige Behörde zu Fragen des Verbots der Rufnummern-Unterdrückung nach § 102 Abs. 2 TKG – das ist die Bundesnetzagentur.

Der Datenschutzbeauftragter nach der DS-GVO (FAQ)

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) existiert erstmals eine europaweit verbindliche verpflichtende Regelung zur Bestellung betrieblicher und behördlicher Datenschutzbeauftragter. Während die EG-Datenschutzrichtlinie (95/46/EG) die Verpflichtung zur Bestellung von Datenschutzbeauftragten lediglich als Alternative vorsah, um die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde entfallen zu lassen, wird sich mit Geltung der DS-GVO ab dem 25. Mai 2018 eine Bestellpflicht erstmals unmittelbar aus dem Europarecht ergeben. Das deutsche Erfolgsmodell der datenschutzrechtlichen Selbstkontrolle hat sich damit auch auf europäischer Ebene durchgesetzt. In Ergänzung zur europarechtlichen (Basis-) Bestellpflicht berechtigt die DS-GVO außerdem über eine Öffnungsklausel die Mitgliedstaaten, weitergehende Bestellpflichten auf nationaler Ebene vorzusehen. Neben den Regelungen über die Bestellpflicht enthält die DS-GVO Regelungen zur Stellung und zu den Aufgaben des Datenschutzbeauftragten, von denen der nationale Gesetzgeber grundsätzlich nicht abweichen darf.

Das neue Bundesdatenschutzgesetz (BDSG-neu), welches am 25. Mai 2018 in Kraft tritt, sieht bei betrieblichen Datenschutzbeauftragten weitergehende Bestellpflichten vor, die in etwa der bisherigen Regelung entsprechen.

Mit der Geltung der DS-GVO gehen auch viele Neuerungen für das Berufsbild der Datenschutzbeauftragten einher. Datenschutzbeauftragte werden weiterhin für viele Behörden und Unternehmen eine zentrale Rolle einnehmen, zumal sie diese dabei unterstützen, die Einhaltung der neuen Regelungen zu gewährleisten. Datenschutzbeauftragte werden zukünftig erheblich dazu beitragen, ein effizientes Datenschutz-Managementsystem in der Behörde oder im Unternehmen zu implementieren. Sie sind darüber hinaus wichtige Vermittler zwischen den Beteiligten, wie z. B. Aufsichtsbehörden, Betroffenen und Behörden bzw. Unternehmen.

Die Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen hat die häufigsten Fragen rund um das Thema in dem Papier „Häufig gestellte Fragen zum Datenschutzbeauftragten (FAQ)“ zusammengefasst und stellt diese nun zum Abruf bereit. Darin werden bspw. folgende Fragen beantwortet:

- Wer muss einen Datenschutzbeauftragten benennen?
- Können mehrere Verantwortliche einen gemeinsamen Datenschutzbeauftragten benennen?
- Welche Besonderheiten gelten für die Pflicht zur Benennung eines Datenschutzbeauftragten bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs?
- In welcher Form ist ein Datenschutzbeauftragter zu benennen?
- Kann eine juristische Person als Datenschutzbeauftragte benannt werden?
- Können auch externe Datenschutzbeauftragte benannt werden?
- Welche Voraussetzungen muss der Datenschutzbeauftragte erfüllen?
- Wo müssen die Kontaktdaten des Datenschutzbeauftragten genannt werden?
- Darf ein Datenschutzbeauftragter zusätzlich andere Aufgaben haben? (Interessenkonflikt)
- Welche Ressourcen müssen dem Datenschutzbeauftragten zur Verfügung gestellt werden, damit dieser seine Aufgaben ordnungsgemäß erfüllen kann?
- Haben Datenschutzbeauftragte einen besonderen Kündigungsschutz?
- Ist der Datenschutzbeauftragte persönlich verantwortlich für die (Nicht-)Einhaltung der DS-GVO bzw. der JI-RL?
- Welche Rolle spielt der Datenschutzbeauftragte bei der Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO bzw. Artikel 27 JI-RL?
- Welche Rolle hat der Datenschutzbeauftragte beim Verarbeitungsverzeichnis?

Quelle: *LDI NRW*

Artikel-29 Datenschutzgruppe konkretisiert Art. 30 DS-GVO

Die Artike-l29-Datenschutzgruppe konkretisiert in ihrem letzten Positionspapier vom 19.04.2018 die Anforderungen, die aus Artikel 30 DS-GVO (Verzeichnis von Verarbeitungstätigkeiten) erwachsen. Dabei nimmt sie Bezug auf Erwägungsgrund 13 der DS-GVO. Dort lautet es sinngemäß, dass die DS-GVO, um der besonderen Situation der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen, eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen enthält, die weniger als 250 Mitarbeiter beschäftigen. Artikel 30 Abs. 5 DS-GVO trägt diesem Gedanken Rechnung.
Er besagt, dass die in den Absätzen 1 und 2 des Artikels 30 DS-GVO genannten Pflichten nicht für Unternehmen oder Einrichtungen gelten, die weniger als 250 Mitarbeiter beschäftigen, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.
Auf Grund einer hohen Anzahl von Fragen von Unternehmen, die die Artikel-29 Datenschutzgruppe zu dieser in Absatz 5 geregelten Ausnahme erhalten hat, möchte die Artikel-29 Datenschutzgruppe hervorheben, dass die Ausnahmeregelungen in Art. 30 Abs. 5 DS-GVO alternativ zu betrachten sind. Bereits das Auftreten eines der Kriterien löst eine Pflicht zur Führung der Aufzeichnung der Verarbeitungstätigkeiten aus. Damit wird die Privilegierung von Unternehmen mit weniger als 250 Mitarbeiter wieder hinfällig, wenn die von ihnen vorgenommene Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt, oder eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 gegeben ist.

Der Umstand, dass Mitarbeiterdaten regelmäßig verarbeitet werden, wenn diese denn vorhanden sind, führt in der Regel dazu, dass die Ausnahme aus Art. 30 Abs. 5 DS-GVO in den allermeisten Fällen nicht greift.
Die Artikel 29-Datenschutzgruppe hebt hervor, dass die Aufzeichnung der Verarbeitungstätigkeiten ein sehr nützliches Mittel ist, um eine Analyse der Auswirkungen einer bestehenden oder geplanten Verarbeitung zu unterstützen. Die Aufzeichnung erleichtere die sachliche Beurteilung des Risikos der Verarbeitungstätigkeiten eines für die Verarbeitung Verantwortlichen oder Verarbeiters in Bezug auf die Rechte des Einzelnen sowie die Ermittlung und Umsetzung geeigneter Sicherheitsmaßnahmen zum Schutz personenbezogener Daten – beides Schlüsselkomponenten des im GDPR enthaltenen Grundsatzes der Rechenschaftspflicht.
Für viele Kleinst-, Klein- und Mittelbetriebe sei es unwahrscheinlich, dass die Aufzeichnung der Verarbeitungstätigkeiten eine besonders große Belastung darstelle.

Quelle: *Europäische Kommission*

BvD aktualisiert Leitbild des Datenschutzbeauftragten

Vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. existiert ein Papier zum beruflichen Leitbild des Datenschutzbeauftragten. Der BvD weist in diesem Papier auch darauf hin, dass die beruflichen Kriterien einem dynamischen Wachstum unterliegen und unter Berücksichtigung neuer Erfahrungen sowie neuer Erkenntnisse auch regelmäßig anzupassen und weiterzuentwickeln sind.

Der Ausschuss erarbeitet Qualitätsstandards für den Beruf der Datenschutzbeauftragten. Das berufliche Leitbild der Datenschutzbeauftragten entwickelt er weiter und passt es kontinuierlich an aktuelle rechtliche und technische Entwicklungen an. Die vorliegende 4. Auflage integriert die neuen Anforderungen durch die europäische Datenschutz-Grundverordnung (DS-GVO) an die Qualifikationen der Datenschutzbeauftragten. Das Leitbild zum Datenschutzbeauftragten ist zweisprachig (Deutsch/Englisch).

Auf der Seite der iapp (The International Association of Privacy Professionals) finden sich Hinweise, wie der iapp die Fähigkeiten, Kenntnisse und Background des Datenschutzbeauftragten generell und insbesondere im Lichte der DS-GVO einschätzt. Es ist ersichtlich, dass die aufgestellten Kriterien sich nicht in jedem Punkt mit dem Leitbild des BvD decken.

Zulässigkeit des Tracking nach der DS-GVO

Nach Auffassung der DSK stellt der 4. Abschnitt des TMG keine Umsetzung der ePrivacy-Richtlinie dar und genießt deswegen keinen Anwendungsvorrang als spezialgesetzliche Regelung für die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste auf Grundlage des Art. 95 DS-GVO. Die GDD stimmt mit der DSK überein, dass für die Beurteilung der Rechtmäßigkeit der Reichweitenmessung und des Einsatzes von Tracking-Mechanismen ab dem 25.5.2018 ausschließlich die DS-GVO einschlägig ist. Folglich kommen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Diensteanbieter von Telemedien Art. 6 Abs. 1, insbesondere lit. a, b und f DS-GVO in Betracht. Technisch notwendige Verarbeitungen für die Bereitstellung eines Dienstes sind unstrittig nach Art. 6 Abs. 1 lit. b oder f DS-GVO zulässig. Divergenz besteht hingegen hinsichtlich der Rechtsgrundlage beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Der Auffassung der DSK nach ist das Tracking von Nutzern wie z.B. durch Analysetools wie Google Analytics oder durch Werbetracker nur noch durch eine explizite Einwilligung des Nutzers legitimiert, auch wenn es lediglich in pseudonymisierter Form erfolgt. Werbung stellt jedoch nach der DS-GVO grundsätzlich ein berechtigtes Interesse im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO dar, dass dem Regelungsverständnis der DS-GVO nach, jedenfalls grundsätzlich nicht von einer Einwilligung abhängig ist.
Wenn nach ErwG. 47 DS-GVO die Direktwerbung ein berechtigtes Interesse des werbenden Unternehmens sein kann, muss in der Konsequenz auch das Tracking von Nutzerverhalten als weniger stark in das Persönlichkeitsrecht eingreifende Maßnahme grundsätzlich zulässig sein.
Danach dürften Cookies im Rahmen der Werbung, die keine sensiblen Daten betreffen und nicht auf Personenbezug schließen lassen (wie sie derzeit nach § 15 Abs. 3 TMG gestattet sind), ein berechtigtes Interesse der datenverarbeitenden Unternehmen darstellen. Die Anzeige etwaiger zielgerichteter Werbung ist in der Regel transparent für die betroffene Person. Insofern bestehen gerade bei pseudonymer Nutzung der personenbezogenen Daten der betroffenen Person für die Zwecke des Online-Marketings und der Online-Werbung keine Bedenken, im Rahmen des Art. 6 Abs. 1 lit. f DS-GVO die Abwägung zu Gunsten des Verantwortlichen zuzulassen. Entscheidend für die Zulässigkeit nach Art. 6 Abs. 1 lit. f DS-GVO ist, welche Ziele bei der Datenverarbeitung verfolgt werden. Sofern Daten in Verbindung mit Personendaten von Nutzern gebracht werden oder Daten über ein umfassendes Werbenetzwerk hinweg erhoben werden, lässt sich die Beeinträchtigung des Betroffenen als erheblich qualifizieren. Die beim Online-Tracking webseiten- und sogar geräteübergreifend erstellten Nutzungsprofile sind nicht derart schwerwiegend, dass sie „die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“. Durch die Pseudonymisierung wird den schutzwürdigen Interessen der Nutzer Rechnung getragen.
Die Kommentierung dieser Thematik von Schwartmann/Klein finden Sie im Heidelberger Kommentar der DS-GVO/BDSG ab Rn. 138 ff. frei abrufbar hier.

E-Mail-Adresse aus Impressum darf nicht inaktiv sein

Kommerzielle Betreiber von Webseiten sind nach dem Telemediengesetz dazu verpflichtet, ihren Kunden eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation zu ermöglichen – zum Beispiel, für Fragen zum Vertrag oder zu den angebotenen Produkten. Dafür müssen sie eine E-Mail-Adresse angeben.

Google darf auf Kunden-Anfragen, an die im Impressum genannte E-Mail-Adresse, nicht mit einer automatisch erzeugten Standardantwort reagieren, die Verbraucherinnen und Verbraucher lediglich auf Hilfeseiten und andere Kontaktmöglichkeiten verweist. Das hat das Kammergericht Berlin nach einer Klage des Verbraucherzentrale Bundesverbands (vzbv) gegen den Internetkonzern entschieden und bestätigt damit die Entscheidung des Landgerichts.

Die von Google im Impressum genannte Adresse entpuppte sich allerdings als „toter Briefkasten“. Kunden, die eine E-Mail an support.de@google.com schickten, bekamen eine automatisch generierte Antwort mit dem Hinweis: „Bitte beachten Sie, dass aufgrund der Vielzahl von Anfragen E-Mails, die unter dieser E-Mail-Adresse eingehen, nicht gelesen und zur Kenntnis genommen werden können.“ Google verwies in der Antwort-Mail vor allem auf seine Hilfeseiten, über die „gegebenenfalls“ auch Kontaktformulare erreichbar seien.

Das Gericht schloss sich der Auffassung des vzbv an, dass dieser Umgang mit Kundenanfragen gegen das Telemediengesetz verstößt. Die Angabe einer E-Mail-Adresse, bei der erklärtermaßen ausgeschlossen sei, dass Google vom Inhalt der eingehenden E-Mails Kenntnis erlangt, ermögliche keine individuelle Kommunikation. Diese werde im Gegenteil verweigert. Auch mit einem für alle Fälle von Anfragen vorformulierten Standardschreiben werde das Kommunikationsanliegen des Kunden letztlich nur zurückgewiesen.

Die Richter stellten auch klar: Kontaktformulare, Online-Hilfen und Nutzerforen ersetzen nicht die gesetzlich vorgeschriebene Möglichkeit, dass sich der Kunde per E-Mail an das Unternehmen wenden kann.

Das Urteil des Kammergerichts ist noch nicht rechtskräftig. Wegen der grundsätzlichen Bedeutung der Rechtssache hat das Gericht die Revision beim Bundesgericht zugelassen.

Quelle: *Verbraucherzentrale Bundesverband e.V.*

Risikobestimmung nach der DS-GVO

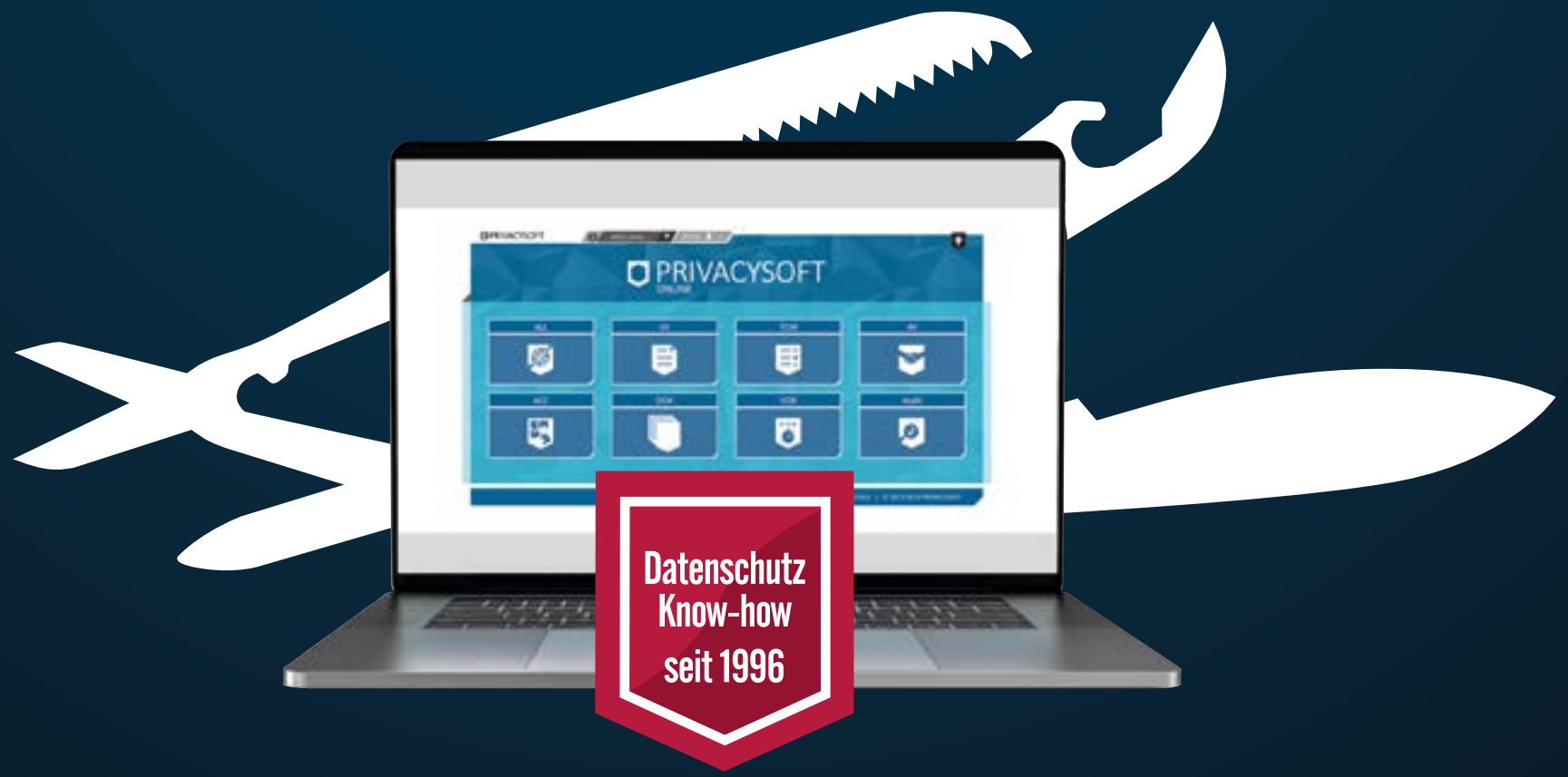
Die Datenschutzkonferenz ist der Zusammenschluss der unabhängigen Datenschutzbehörden des Bundes und der Länder. Die 95. Konferenz fand am 25. und 26. April in Düsseldorf statt. Der jährlich wechselnde Vorsitz richtet die Sitzungen der Datenschutzkonferenz aus und vertritt die Konferenz nach außen. Im Rahmen der Konferenz sind einige Kurzpapiere ausgearbeitet worden. Darunter auch das Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen".
Der Begriff „Rechte und Freiheiten natürlicher Personen" ist in der Datenschutz-Grundverordnung zentral. Die Verordnung stellt den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen in den Mittelpunkt. Der Begriff ist zudem wesentlich für die Frage, wann eine Datenschutz-Folgenabschätzung und eine vorherige Konsultation der Aufsichtsbehörde durchzuführen ist.
Ziel des verabschiedeten Kurzpapieres ist es, das Risiko im Kontext der Datenschutz-Grundverordnung zu definieren und aufzuzeigen, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Die Eindämmung von Risiken durch Ergreifen geeigneter technischer und organisatorischer Maßnahmen ist nicht Gegenstand des Papiers.

Das Kurzpapier ist hier abrufbar.

Quelle: *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.



DAS DSB-MULTI-TOOL FÜR DEN DATENSCHUTZ NACH EU-DSGVO

Datenschutzdokumentation | Vorlagen und Checklisten | Vorgangsmanagement | Online-Schulungen

Projekt 29 GmbH & Co. KG | Ostengasse 14 | 93047 Regensburg | www.privacysoft.de