

Nr. 04 / 2019



Newsletter Datenschutz

In dieser Ausgabe:

LfDI NRW: Empfehlung zum Schutz von E-Mails	2
LfDI Baden-Württemberg: Ratgeber zum Beschäftigtendatenschutz	3
Europäischer Datenschutzausschuss fordert ambitionierte E-Privacy Verordnung	3
EuGH-Generalanwalt: Einwilligung für Cookies Pflicht	4
Erstes Bußgeld in Polen sorgt für Kontroverse	5
VERANSTALTUNGEN	6
Sprehtag „CE-Kennzeichnung von Maschinen und Anlagen“	6
„1 Jahr DSGVO“	6
„Tag der IT-Sicherheit 2019“	6
„Haftungsrisiken von GmbH-Geschäftsführern“	6
„Die elektronische Betriebsprüfung - Datenquellen, Archivierung, Prüfung und Analyse “	6

LfDI NRW: Empfehlung zum Schutz von E-Mails

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LfDI) hat Empfehlungen zur sicheren Kommunikation per E-Mail veröffentlicht. Die Empfehlungen wurden unter dem Vorbehalt späterer Anpassungen gegeben. Die Datenschutzkonferenz (DSK) hat angekündigt, ebenfalls eine Empfehlung zu erarbeiten.

E-Mails bestehen grundsätzlich aus den Inhaltsdaten wie Text und Anhänge und Metadaten wie Absender und Empfänger, Datum und Betreff. Beide können personenbezogene Daten beinhalten. Deshalb ist bei der Übermittlung von E-Mails grundsätzlich zwischen einer Verschlüsselung auf Inhaltsebene und einer Verschlüsselung auf Transportebene zu unterscheiden.

1. Inhaltsebene

Nach Angaben des LfDI kommen für die Verschlüsselung des Inhaltes in erster Linie zwei Standards infrage: S/MIME und OpenPGP. S/MIME und OpenPGP sind sogenannte Ende-zu-Ende-Verschlüsselungen. Dies bedeutet, dass die Nachricht auf dem System des Absenders verschlüsselt und auf dem System des Empfängers entschlüsselt wird. Damit liegt sie auf dem Übertragungsweg niemals im Klartext vor. Beide Standards unterstützen auch digitale Signaturen.

2. Transportebene

Von der Verschlüsselung des Inhaltes werden jedoch nicht die Metadaten erfasst. Diese liegen bei der Übertragung weiterhin im Klartext vor. Anders bei einer Verschlüsselung auf Transportebene. Dabei werden sowohl Meta- als auch Inhaltsdaten auf der Verbindung zwischen Mail-Client und Server bzw. zwischen verschiedenen Mail-Servern verschlüsselt. Dadurch wird sichergestellt, dass die Mail bei der Übermittlung nicht von Dritten gelesen werden kann.

Das LfDI empfiehlt, bei der Wahl der Transportverschlüsselung folgende Punkte zu beachten:

- Die Transportverschlüsselung sollte entsprechend der Technischen Richtlinie „BSI TR-03108 Sicherer E-Mail-Transport“ implementiert sein. Abweichungen von der Richtlinie sind statthaft.
- Bei besonders schutzwürdigen Daten (z.B. Kontobewegungsdaten, Finanzierungsdaten, Daten zum Gesundheitszustand, Beschäftigtendaten) ist eine alleinige Transportverschlüsselung möglicherweise nicht ausreichend. Zusätzliche technische und organisatorische Maßnahmen, wie z. B. eine Ende-zu-Ende-Verschlüsselung können geboten sein.
- Der Betreff der E-Mail sollte keine personenbezogenen Daten enthalten.

Die Empfehlungen des LfDI können Sie hier nachlesen:

https://www.lfdi.nrw.de/mainmenu_Aktuelles/Inhalt/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand.html

Quelle: LfDI Nordrhein-Westfalen

LfDI Baden-Württemberg: Ratgeber zum Beschäftigtendatenschutz

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BaWü) hat einen Ratgeber zum Beschäftigtendatenschutz veröffentlicht. Dieser liegt nunmehr in der 3. Auflage vor. Der Ratgeber zeigt im ersten Teil die rechtlichen Regelungen in der DSGVO und dem BDSG auf. Im zweiten Teil sind Fälle aus der Praxis zusammengestellt. Sie finden den Ratgeber hier:

<https://www.baden-wuerttemberg.datenschutz.de/ratgeber-zum-beschaefigtendatenschutz-3-auflage/>

Praxistipp: Informationen zum Beschäftigtendatenschutz hält auch unser Infoblatt → **D10** „[Beschäftigtendatenschutz nach der DSGVO](#)“ unter der **Kennzahl 2158** bereit.

Europäischer Datenschutzausschuss fordert ambitionierte E-Privacy Verordnung

Der Europäische Datenschutzausschuss (EDSA) hat den europäischen Gesetzgeber aufgefordert, die bereits seit langem diskutierte E-Privacy Verordnung schnellstmöglich zu verabschieden. Diese müsse in Ergänzung der Datenschutz-Grundverordnung (DSGVO) ein hohes Schutzniveau für die Daten im Bereich der elektronischen Kommunikation garantieren.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, stellte als einer der Mitinitiatoren der Stellungnahme klar: "Die E-Privacy-Verordnung sollte ursprünglich zeitgleich mit dem Anwendungsbeginn der DSGVO im letzten Mai in Kraft treten. Es ist eine Sache, diese zugegebenermaßen ambitionierte Frist nicht halten zu können. Das entschuldigt aber nicht den Umstand, dass seit über einem Jahr inhaltlich keine wirklichen Fortschritte erzielt werden konnten, sondern stattdessen versucht wird, das angestrebte Datenschutzniveau abzusenken. Gerade in dem hochsensiblen Bereich der elektronischen Kommunikation benötigen wir eine starke Regelung. Deshalb muss die E-Privacy Verordnung zwingend so ausgestaltet werden, dass das Schutzniveau sowohl der aktuellen E-Privacy-Richtlinie als auch der DSGVO mindestens gehalten und - wo nötig - erweitert wird. Zudem muss klargestellt werden, dass den Datenschutzaufsichtsbehörden bei der Aufsicht über die Verarbeitung personenbezogener Daten auch unter der E-Privacy-Verordnung sämtliche in der DSGVO vorgesehenen Kompetenzen zukommen."

Die E-Privacy-Verordnung ist neben der DSGVO das zweite große Gesetzgebungsvorhaben zur Reform des europäischen Datenschutzrechts. Sie soll die aktuell noch geltende E-Privacy-Richtlinie ablösen und den Datenschutz bei der elektronischen Kommunikation regeln. Insofern stellt sie eine bereichsspezifische Ergänzung und Konkretisierung der Datenschutzvorgaben in der DSGVO dar.

Ein erster Entwurf der Verordnung wurde von der Europäischen Kommission bereits im Januar 2017 vorgelegt. Das Europäische Parlament positionierte sich im Oktober 2017 zum Gesetzentwurf. Lediglich der Europäische Rat konnte sich nach mittlerweile zweijähriger Debatte noch nicht auf eine gemeinsame Linie einigen.

Quelle: PM des Bundesbeauftragten für den Datenschutz und die Informationssicherheit vom 14. März 2019

EuGH-Generalanwalt: Einwilligung für Cookies Pflicht

2017 hat der [BGH](#) (Beschl. v. 5.10.2017 - I ZR 7/16) dem EuGH die Frage vorgelegt, ob für das Setzen eines Cookies eine ausdrückliche Einwilligung erforderlich ist. Der Generalanwalt beim EuGH hat nun seine Schlussanträge vorgelegt (EuGH, Schlussanträge des Generalanwalts vom 21.03.2019, Rs. C-673/17).

Zum Sachverhalt:

Um an einem von einem Unternehmen veranstalteten Gewinnspiel teilnehmen zu können, musste der Nutzer bei zwei Ankreuzfeldern ein Häkchen setzen bzw. entfernen, bevor er die Schaltfläche für die Teilnahme betätigen konnte. Dabei musste er in einem nicht angekreuzten Pflichtfeld seine Zustimmung erteilen, von „einigen Sponsoren und Kooperationspartnern“ mit Werbeangeboten kontaktiert zu werden. In einem zweiten Feld, das bereits vorangekreuzt war, konnte der Nutzer seine Einwilligung in die Setzung von Cookies auf seinem Computer geben. Eine Teilnahme am Gewinnspiel war auch möglich, wenn das Häkchen in diesem Ankreuzfeld nicht gesetzt wurde. Darüber erhielt der Nutzer jedoch keine Information.

Nach Ansicht des Generalanwalts macht es keinen Unterschied, ob durch das Setzen der Cookies personenbezogene Daten gespeichert werden oder nicht. Entscheidend ist, dass „Informationen“ gespeichert werden. Er hat weiter ausgeführt, dass es nicht ausreicht, wenn die Einwilligungserklärung des Nutzers vorformuliert ist und der Nutzer aktiv widersprechen muss, falls er mit der Verarbeitung der Daten nicht einverstanden ist. Unklar ist nämlich, ob ein solcher vorformulierter Text gelesen und verstanden wurde. Die Einwilligung muss zudem gesondert abgegeben werden. Das heißt, es ist nicht ausreichend, wenn die Einwilligung durch das Anklicken der Schaltfläche für die Teilnahme an dem Online-Gewinnspiel erklärt wird. Die Teilnahme an einem Gewinnspiel und die Erteilung einer Einwilligung können nicht Teil derselben Handlung sein. Darüber hinaus muss der Nutzer ausreichend darüber informiert, ob und, wenn ja, in welchem Umfang sich die Erteilung seiner Einwilligung auf die Entfaltung seiner Aktivität im Internet auswirkt. Er wurde nicht ausreichend darüber informiert, dass die Teilnahme am Gewinnspiel nicht davon abhängig ist, dass das zweite Ankreuzfeld angeklickt wird.

Bezüglich der Frage, welche Informationen der Diensteanbieter dem Nutzer über die Cookies geben muss, antwortete der Generalanwalt, dass der Diensteanbieter über die Funktionsdauer der Cookies und die Frage, ob Dritte auf die Cookies Zugriff erhalten, informieren muss.

Die Schlussanträge des Generalanwalts finden Sie [hier](#).

Praxistipp: Die Schlussanträge des Generalanwalts sind für den Gerichtshof nicht bindend. Es bleibt abzuwarten, wie der EuGH entscheidet. Schließt sich der EuGH den Schlussanträgen an, sind Betreiber von Internetseiten gehalten, aktiv die Einwilligung für die Setzung von Cookies einzuholen. Eine vorangekreuzte Checkbox reicht nicht mehr aus.

Erstes Bußgeld in Polen sorgt für Kontroverse

Die polnische Aufsichtsbehörde hat der polnischen Tochtergesellschaft der EU-weit agierenden Aktiengesellschaft Bismode AB ein Bußgeld in Höhe von 220.000 € auferlegt. Grund ist der Verstoß gegen die Informationspflichten nach Art. 14 DSGVO. Das verhängte Bußgeld bietet nun die Grundlage für eine breite Diskussion, wann die Informationspflicht sich als unverhältnismäßig aufwändig für den Verantwortlichen herausstellt. Die progressive Partei Wiosna hat den polnischen Premierminister aufgefordert, die Sanktionen nach der DSGVO sofort für ein Jahr auszusetzen und über die korrekte Anwendung der DSGVO-Bestimmungen zu informieren.

Das Unternehmen verarbeitet über 7 Mio. Datensätze aus öffentlich zugänglichen Quellen, wie etwa das Handelsregister oder dem Zentralregister der Wirtschaftlichen Tätigkeit. Gesammelt werden auch Daten von Personen, die ihre Wirtschaftstätigkeit ausgesetzt oder aufgegeben haben. Die gesammelten Daten wurden für kommerzielle Zwecke genutzt.

Nach Art. 13, 14 DSGVO sind Unternehmen verpflichtet, über die Datenverarbeitung zu informieren. Das polnische Unternehmen kam dieser Informationspflicht nur gegenüber den Unternehmen und Personen nach, von denen die E-Mail-Adressen vorlagen. So wurde nur ein Bruchteil der Betroffenen informiert.

Die Aufsichtsbehörde sah darin eine Nichterfüllung der Informationspflichten nach Art. 4 DSGVO. Das Bereitstellen der Informationen auf der Internetseite sei nicht ausreichend, da die betroffenen Personen keine Kenntnis von der Verarbeitung durch das Unternehmen hätten. Der Betroffene habe auch keinen Anhaltspunkt, auf der Internetseite danach zu suchen. Die Aufsichtsbehörde sah zudem eine vorsätzliche Verletzung, da dem Unternehmen bewusst war, dass Betroffene, von denen nur eine Postadresse oder eine Telefonnummer vorlag, nicht informiert werden.

Das polnische Unternehmen beruft sich darauf, dass es einen unverhältnismäßigen Aufwand bedeuten würde, alle per Post zu informieren. Die Aufsichtsbehörde ließ dieses Argument nicht geltend. Die Informationserteilung sei zumutbar gewesen.

VERANSTALTUNGEN

Sprechtage „CE-Kennzeichnung von Maschinen und Anlagen“

Dienstag, 14. Mai 2019, ab 8:30 Uhr, Raum 4, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Anmeldungen bis 13. Mai 2019 unter E-Mail: carine.messerschmidt@saaris.de.

„1 Jahr DSGVO“

Donnerstag, 23. Mai 2019, 18.00 - 20.00 Uhr, Raum 1-3, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Referenten: Rechtsanwalt Hubert Beeck und Rechtsanwältin Jennifer Hohmann, Homburg

Anmeldungen **bis 22. Mai 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de.

“Tag der IT-Sicherheit 2019”

Donnerstag, 06. Juni 2019, 09:15 - 18:00 Uhr, Saalbau, IHK Saarland, Franz-Josef-Röder-Straße 9, 66119 Saarbrücken,

Anmeldungen **bis 05. Juni 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de.

„Haftungsrisiken von GmbH-Geschäftsführern“

Dienstag, 18. Juni 2019, 18.00 Uhr - 20.00 Uhr, Raum 1, Saalgebäude, IHK Saarland, Franz-Josef-Röder-Straße 9, 66119 Saarbrücken.

Referentin: Rechtsanwältin Nicole Wartenphul, Abel und Kollegen, Rechtsanwälte, PartGmbH, St. Ingbert,

Anmeldungen **bis 17. Juni 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de

“Die elektronische Betriebsprüfung - Datenquellen, Archivierung, Prüfung und Analyse ”

Donnerstag, 12. September 2019, 18:00 Uhr, Raum 1, IHK Saarland, Franz-Josef-Röder-Straße 9, 66119 Saarbrücken,

Referent: Guido Badjura, DATEV eG

Anmeldungen **bis 11. September 2019** unter E-Mail: sabine.lorscheider@saarland.ihk.de.

Verantwortlich und Redaktion:

Ass. iur. Heike Cloß, Tel.: (0681) 9520-600, Fax: (0681) 9520-690

E-Mail: heike.closs@saarland.ihk.de

IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Ihre Ansprechpartnerinnen:

Ass. iur. Heike Cloß

Tel.: (0681) 9520-600

Fax: (0681) 9520-690

E-Mail: heike.closs@saarland.ihk.de

Ass. iur. Kim Pleines

Tel.: (0681) 9520-640

Fax: (0681) 9520-690

E-Mail: kim.pleines@saarland.ihk.de

Impressum:

IHK Saarland, vertreten durch Präsident Dr. jur. Hanno Dornseifer und Hauptgeschäftsführer Dipl.-Volkswirt Dr. Heino Klingen, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken, E-Mail info@saarland.ihk.de, Tel. + 49 (0) 6 81/95 20-0, Fax + 49 (0) 6 81/95 20-8 88, UST.- Ident.- Nummer: DE 138117020