

Nr. 03 / 2021



Newsletter Datenschutz

In dieser Ausgabe:

Double-Opt-In per E-Mail für Einwilligung in Telefonwerbung nicht ausreichend	2
Aushang eines Mietvertrags mit personenbezogenen Daten	3
LfD Niedersachsen: Prüfschema für Datenschutz-Folgenabschätzung.....	3
LfDI Mecklenburg-Vorpommern: Land muss Schutz personenbezogener Daten sicherstellen.....	4
Emotet-Netzwerk stillgelegt	4
Bundeskabinett beschließt Entwurf des Telekommunikation-Telemedien- Datenschutzgesetzes (TTDSG).....	5
Registermodernisierungsgesetz gefährdet Recht auf informationelle Selbstbestimmung	5
VERANSTALTUNGEN.....	7
Reihe: Das digitale Büro	7
„Elektronische Rechnungen: ZUGFeRD, XRechnung und Co.“	7
„Ersetzendes Scannen / Archivierung und Digitalisierung von Steuerunterlagen“ ..	7
„Controlling digital – Digitale Finanzbuchführung als Zukunftsmodell“	7
„Insolvenz und Corona“	7
„Das neue Wohnungseigentumsgesetz – Auswirkungen für Verwalter, Eigentümer, Vermieter und Mieter“	8

Double-Opt-In per E-Mail für Einwilligung in Telefonwerbung nicht ausreichend

Sofern eine Einwilligung durch das sog. Double-Opt-In-Verfahren eingeholt wurde, muss dies entsprechend dokumentiert werden, um den Nachweis der Einwilligungserteilung erbringen zu können.

Die Klägerin ist im Bereich der Versicherungsvermittlung, der Vermögensanlage sowie der Finanzierung tätig. In diesem Zusammenhang betreibt sie telefonische Werbeanfragen. Im August 2018 wandten sich zwei Betroffene an die Beklagte, die Datenschutzaufsichtsbehörde, sie seien von einem Callcenter kontaktiert worden, ohne ihre Einwilligung hierzu erteilt zu haben. Die Beklagte forderte die Klägerin daraufhin dazu auf, Stellung zu nehmen.

Die Klägerin gab an, dass eine Einwilligung in die Telefonwerbung vorliegt. Diese wurde im Rahmen eines Gewinnspiel für Zwecke des Direktmarketings durch ein vollständig durchlaufenes Double-Opt-In-Verfahren eingeholt. Als Beleg wurde der Ausdruck einer Online-Registrierung vorgelegt, in der zusätzlich eine E-Mail-Adresse und der Eingang einer Bestätigungsmail vermerkt waren. Die Eheleute gaben an, die genannte Internetadresse sowie die E-Mailadresse sei ihnen unbekannt. Zudem hätten sie keine Einwilligung in eine Werbeansprache erklärt.

Die Beklagte erließ daraufhin ein Verarbeitungsverbot und ordnete die Löschung der personenbezogene Daten an. Zur Begründung führte sie aus, dass die vorgelegten Dokumente nicht belegten, dass die Eheleute an dem in Frage stehenden Gewinnspiel teilgenommen und in die Verwendung ihrer personenbezogenen Daten für Zwecke der Telefonwerbung eingewilligt hätten. Das Double-Opt-In-Verfahren reiche nicht als Einwilligung aus, da kein notwendiger Zusammenhang zwischen der in einem Online-Teilnahmeformular eingetragenen E-Mail-Adresse und der angegebenen Telefonnummer bestehen müsse. Eine andere Rechtsgrundlage liege nicht vor. Die Werbung mit einem Telefonanruf gegenüber einem Verbraucher sei ohne dessen vorherige ausdrückliche Einwilligung gemäß § 7 Abs. 2 Nr. 2 UWG als unzumutbare Belästigung zu qualifizieren. Diese Einordnung sei auch im Rahmen der datenschutzrechtlichen Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO zu berücksichtigen.

Das VG Saarlouis hat sich der Ansicht der Beklagten angeschlossen und die Klage abgewiesen. Die im Double-Opt-In-Verfahren erlangte datenschutzrechtliche Einwilligung genüge nicht den Anforderungen an eine Einwilligung. Das Double-Opt-In-Verfahren sei eine praktikable Möglichkeit, um potenziellen Kunden Werbung per E-Mail zukommen zu lassen. Für eine Einwilligung für Werbeanrufe sei das Double-Opt-In-Verfahren nicht geeignet, da kein notwendiger Zusammenhang zwischen der E-Mail-Adresse und der angegebenen Telefonnummer bestehe müsse. So könne es zahlreiche Gründe dafür geben, dass eine falsche Telefonnummer in ein Online-Teilnahmeformular eingetragen werde, wie etwa eine versehentliche oder wissentliche Falsch eingabe. Eine Verifizierung finde nicht statt. Zudem kann die Klägerin nicht den Nachweis führen, dass die betroffenen Personen in die Verarbeitung ihrer personenbezogenen Daten eingewilligt haben.

Die Klägerin kann sich auch nicht auf die Wahrnehmung berechtigter Interessen nach Art. 6 Abs. 1 lit. f DSGVO berufen. Danach ist grundsätzlich die Direktwerbung als berechtigtes Interesse anerkannt. Bei der Interessenabwägung ist insbesondere § 7 Abs. 2 UWG zu berücksichtigen, wonach die Werbung per Telefon gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung als unzumutbare Belästigung zu qualifizieren ist.

Das OVG bestätigte diese Auffassung in der Berufungsinstanz.

OVG des Saarlandes, Beschluss vom 16. Februar 2021, 2 A 355/19

Praxistipp: Sowohl im b2c als auch im b2b-Bereich ist eine vorherige Einwilligung für die werbliche Ansprache per Telefon notwendig. Nicht ausreichend ist es, diese in einem ersten Anruf abzufragen. Mit der Entscheidung des OVG ist auch klargestellt, dass ein Double-Opt-In-Verfahren ebenfalls nicht ausreichend ist, um eine Einwilligung für die Telefonwerbung zu erhalten.

Aushang eines Mietvertrags mit personenbezogenen Daten

Der Betroffene einer rechtswidrigen Datenverarbeitung kann einen datenschutzrechtlichen Unterlassungsanspruch geltend machen. Dies hat das LG Frankfurt a. M. entschieden.

Die Antragstellerin wehrt sich im Wege des einstweiligen Rechtsschutzes dagegen, dass ihre personenbezogenen Daten durch das öffentliche Aushängen des Mietvertrages in einer Vereinsversammlung verbreitet wurden.

Das LG bejahte einen datenschutzrechtlichen Unterlassungsanspruch aus §§ 823, 1004 BGB aufgrund der Verletzung des Rechts auf informationelle Selbstbestimmung. Solche Ansprüche seien nicht durch Art. 79 DSGVO gesperrt. Der Antragsgegner kann sich für die Verwendung der Daten auch nicht auf einen der Gründe in Art. 6 Abs. 1 DSGVO berufen. Der Aushang der Daten des Mietvertrags ist nicht vom Vertragszweck nach Art. 6 Abs. 1 lit. b) DSGVO gedeckt. Dass der Antragsgegner sich auf ein berechtigtes Interesse nach Art. 6 Abs. 1 lit. f) DSGVO berufen könnte, ist weder vorgetragen noch sonst ersichtlich.

LG Frankfurt a.M., Beschluss vom 15. Oktober 2020, 2-03 O 356/20

Praxistipp: Das LG Frankfurt führt mit dem Beschluss seine Rechtsprechungspraxis weiter. Ähnlich hat auch bereits das LG Darmstadt und das LG Wuppertal entschieden.

LfD Niedersachsen: Prüfschema für Datenschutz-Folgenabschätzung

Das LfD Niedersachsen stellt ein Prüfschema zur Vorab-Bewertung von möglichen Folgen von Datenverarbeitungen zur Verfügung. Denn: Wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, muss eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden.

Mit dem Prüfschema können Datenverarbeiter für ihren Verantwortungsbereich prüfen, ob die Durchführung einer DSFA erforderlich ist. Neben einer Checkliste und einem umfangreichen Glossar der wichtigsten Begriffe enthält das Schema auch Hinweise auf weitere Hilfestellungen zum Thema Datenschutz-Folgenabschätzung. Sie können das Prüfschema [hier](#) herunterladen.

LfDI Mecklenburg-Vorpommern: Land muss Schutz personenbezogener Daten sicherstellen

Zusammen mit dem Landesrechnungshof fordert der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern die Landesregierung in Mecklenburg-Vorpommern dazu auf, den Schutz der von ihr verarbeiteten personenbezogenen Daten sicherzustellen.

Hintergrund sei die Entscheidung des EuGH im Juli 2020, in der der EuGH das Privacy Shield als eine wesentliche Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA für unwirksam erklärt hat. Betroffen seien davon unter anderem Produkte der Firma Microsoft“. Eine rechtskonforme Nutzung dieser Produkte allein auf der Basis von Standarddatenschutzklauseln sei aber aufgrund der vom EuGH aufgestellten Grundsätze nicht möglich. Ohne weitere Sicherungsmaßnahmen würden personenbezogene Daten an Server mit Standort in den USA übermittelt. Dort sähen diverse Vorschriften die Herausgabe der Daten an Behörden und Geheimdienste vor, ohne dass den Betroffenen hinreichende Rechtsschutzmöglichkeiten zur Verfügung stünden.

Kann die Übermittlung personenbezogener Daten nicht unterbunden werden oder ist sie für die Nutzung einer Anwendung oder eines Dienstes funktionsnotwendig, hat die Landesregierung durch geeignete Maßnahmen sicherzustellen, dass entweder der Personenbezug aufgelöst (z.B. durch Anonymisierung) oder die Daten nach dem Stand der Technik verschlüsselt werden. Wenn das nicht geht, ist die Verarbeitung einzustellen oder ein alternatives Produkt einzusetzen, welches die Anforderungen der DSGVO erfüllt.

Quelle: PM des LfDI Mecklenburg-Vorpommern vom 17. März 2021

Emotet-Netzwerk stillgelegt

Die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – und das Bundeskriminalamt (BKA) haben mitgeteilt, dass im Rahmen einer international konzertierten Aktion mit internationalen Strafverfolgungsbehörden die Infrastruktur der Schadsoftware Emotet übernommen und zerstört wurde. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) übermittelt die im Zuge der Beweissicherung ermittelten öffentlichen IP-Adressinformationen von betroffenen Anschlüssen an die für die jeweiligen IP-Netzbereiche zuständigen Netzbetreiber in Deutschland. Internationale IP-Adressen leitet das BSI an die jeweiligen nationalen CERTs weiter. Die Provider werden gebeten, ihre betroffenen Kunden über die Emotet-Infektion zu informieren. Informationen zur Bereinigung betroffener Systeme stellt das [BSI](#) zur Verfügung.

Bundeskabinett beschließt Entwurf des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG)

Das Bundeskabinett hat den vom Bundesministerium für Wirtschaft und Energie (BMWi) vorgelegten [Entwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien \(Telekommunikation-Telemedien-Datenschutzgesetz – TTDSG\)](#) beschlossen.

Ziel des Gesetzes ist es, Rechtsklarheit für den Datenschutz und den Schutz der Privatsphäre in der digitalen Welt zu schaffen.

Das TTDSG enthält Datenschutzbestimmungen, die bisher im Telekommunikationsgesetz (TKG) und im Telemediengesetz (TMG) enthalten waren. Es führt so den Telekommunikationsdatenschutz und den Telemedienschutz in einem neuen Gesetz zusammen. Dabei nimmt das Gesetz notwendige Anpassungen an die europäischen Vorgaben der Datenschutzgrundverordnung (DSGVO) und der ePrivacy-Richtlinie vor und soll für eine Stärkung der unabhängigen Datenschutzaufsicht sorgen.

Im Hinblick auf den Schutz der Privatsphäre beim Speichern und Auslesen von Informationen auf Endgeräten, insbesondere Cookies, sowie die Rechtsprechung des Europäischen Gerichtshofes dazu, erfolgt die Aufnahme einer Regelung zum Einwilligungserfordernis, die eng am Wortlaut der Vorgaben der ePrivacy-Richtlinie orientiert ist. Das Setzen eines Cookies soll also grundsätzlich der Einwilligung des Nutzers bedürfen.

Die Aufsicht über die Datenschutzbestimmungen des TKG bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten soll zukünftig umfassend, d. h. auch im Hinblick auf die Verhängung von Bußgeldern, durch den Bundesbeauftragten oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) als unabhängige Datenschutzaufsichtsbehörde erfolgen.

Das Gesetz ist erforderlich, da ein Inkrafttreten der ePrivacy-Verordnung frühestens in zwei Jahren erwartet wird. Im März soll der Entwurf im Bundesrat und auch schon im Bundestag beraten werden; es gilt als eilbedürftig.

Registermodernisierungsgesetz gefährdet Recht auf informationelle Selbstbestimmung

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) warnt eindringlich vor der Verabschiedung des Registermodernisierungsgesetzes in der derzeitigen Fassung. Das Gesetz sieht den Einsatz der Steuer-Identifikationsnummer (Steuer-ID) als zentrales Ordnungsmerkmal in der öffentlichen Verwaltung vor, um den Datenaustausch zwischen Behörden zu erleichtern. Nachdem schon der Bundestag Ende Januar das Gesetz angenommen hat, ist nun die abschließende Beratung im Bundesrat vorgesehen.

Die DSK hatte bereits 2019 und 2020 erhebliche verfassungsrechtliche Kritik an diesem Vorhaben geäußert und auf die damit verbundenen Risiken hingewiesen. Durch die Schaffung eines solchen einheitlichen und verwaltungsübergreifenden Personenkennzeichens – auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch – besteht die Gefahr einer missbräuchlichen Verknüpfung personenbezogener Daten und der Erstellung umfassender Persönlichkeitsprofile.

Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang der geplanten Regelung zeigt das Potenzial der möglichen missbräuchlichen Verwendung. In über 50 Registern soll die Steuer-ID als zusätzliches Ordnungsmerkmal aufgenommen werden. Auf diese Weise könnten beispielsweise Daten aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden.

Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern.

Diese stellen zwar sicher, dass nur autorisierte Behörden die erforderlichen Daten Ende-zu-Ende-verschlüsselt übermitteln, allerdings bieten sie keinen ausreichenden Schutz vor einer missbräuchlichen Zusammenführung der Daten zu einer Person aus unterschiedlichen Registern. Zudem verzichtet das Gesetz für einen nicht unerheblichen Teil der Übermittlungen auch noch auf diese Sicherungen. Darüber hinaus sollten sich die Sicherheits- und Transparenzmaßnahmen des Gesetzesentwurfs auch auf den Steuerbereich erstrecken, in dem fortan ebenfalls das neue allgemeine Personenkennzeichen verwendet wird.

Die ausgedehnte Verwendung der Steuer-ID als einheitliches Personenkennzeichen steht zudem im Widerspruch zu ihrer ursprünglichen Funktion für rein steuerliche Sachverhalte. Nur aufgrund dieser Zweckbestimmung konnte sie bislang als verfassungskonform angesehen werden.

Die DSK hatte demgegenüber „sektorspezifische“ Personenkennciffren gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren. Dieses Modell wird in Österreich seit vielen Jahren erfolgreich praktiziert und könnte auch in Deutschland mit vertretbarem Aufwand eingeführt werden.

Gerade in Zeiten einer weitreichenden Digitalisierung staatlicher Verarbeitungsprozesse kommt es darauf an, diese auf Strukturen aufzusetzen, die sicherstellen, dass auch bei gegebenenfalls veränderten Rahmenbedingungen das Recht auf informationelle Selbstbestimmung verlässlich gewährleistet wird.

Quelle: PM des UDZ Saarland vom 25. Februar 2021

VERANSTALTUNGEN

Reihe: Das digitale Büro

Wie führte ich das digitale Büro rechtssicher? Eine Frage, die sich viele Unternehmen stellen. Gemeinsam mit der Steuerberaterkammer des Saarlandes wollen wir im Rahmen unserer unentgeltlichen Webinar-Reihe darauf Antworten geben. Ihr Referent ist: Herr Guido Badjura, DATEV eG, Düsseldorf. Wir freuen uns über Ihre Teilnahme an den einzelnen oder allen Terminen.

„Elektronische Rechnungen: ZUGFeRD, XRechnung und Co.“

Mittwoch, 21. April 2021, 17.00 bis 19.00 Uhr, Onlineveranstaltung

Anmeldungen bis 20.04.2021 unter E-Mail: veranstaltungen@saarland.ihk.de oder per [Direktlink](#).

„Ersetzendes Scannen / Archivierung und Digitalisierung von Steuerunterlagen“

Montag, 28. Juni 2021, 17.00 bis 19.00 Uhr, Onlineveranstaltung

Anmeldungen bis 27.06.2021 unter E-Mail: veranstaltungen@saarland.ihk.de oder per [Direktlink](#).

„Controlling digital – Digitale Finanzbuchführung als Zukunftsmodell“

Dienstag, 2. November 2021, 17.00 bis 19.00 Uhr, Onlineveranstaltung

Anmeldungen bis 01.11.2021 unter E-Mail: veranstaltungen@saarland.ihk.de oder per [Direktlink](#).

„Insolvenz und Corona“

Donnerstag, 22. April 2021, 14.00 - 16.00 Uhr, Onlineveranstaltung

Die zu Beginn der Corona-Pandemie ausgesetzten Insolvenzantragspflichten für bestimmte zahlungsunfähige und überschuldete Unternehmen ist derzeit bis zum 30.4.2021 ausgesetzt. Die Verlängerung bedeutet, dass die Insolvenzgründe und auch die Insolvenzantragspflichten selbst in Kraft bleiben. Lediglich die Pflicht zur Antragstellung wurde unter bestimmten Bedingungen für bestimmte insolvenzreife Unternehmen ausgesetzt.

Deshalb ist jeder Unternehmer gut beraten, die Insolvenzgründe zu kennen und zu überwachen, insbesondere wenn es darum geht, rechtzeitig die Weichen in Richtung außergerichtliche bzw. gerichtliche Sanierung zu stellen. Die Regelungen des COVID-19-Insolvenzaussetzungsgesetzes sowie die Insolvenzgründe sind Gegenstand des Webinars.

Referent: Herr Rechtsanwalt Dr. Michael Bach, Heimes und Müller Rechtsanwälte, Saarbrücken

Anmeldungen bis 21.04.2021 unter E-Mail: veranstaltungen@saarland.ihk.de oder per [Direktlink](#).

**„Das neue Wohnungseigentumsgesetz – Auswirkungen für Verwalter, Eigentümer, Vermieter und Mieter“
Donnerstag, 06.05.2021, 14:00 - 16:00 Uhr, Onlineveranstaltung**

Referent: RA Dr. Gerhard Kallenborn, STOPP | PICK | ABEL | KALLENBORN, Saarbrücken

Anmeldungen bis 01.11.2021 unter E-Mail: veranstaltungen@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 Dr. Frank Thomé, 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