Geschäftsbereich
Recht, Zentrale Dienste

Nr. 02 / 2020

Newsletter Datenschutz

In dieser Ausgabe:

Industrie- und Handelskammer des Saarlandes
Postanschrift: IHK Saarland │ 66104 Saarbrücken │ Büroanschrift: Franz-Josef-Röder-Straße 9 │ 66119 Saarbrücken
Tel. 0681/9520-0 │ Fax 0681/9520-888 │ E-Mail: info@saarland.ihk.de │ Internet: www.saarland.ihk.de

Einsatz von WhatsApp durch saarländische Kommunen

Die Landesbeauftragte für Datenschutz im Saarland hat Stellung zur Nutzung von WhatsApp durch Gemeinden genommen. Bereits im vergangenen Jahr hat sie die Vereinbarkeit mit den datenschutzrechtlichen Vorschriften überprüft. Mit Ihrer Pressemitteilung regiert das Unabhängige Datenschutzzentrum (UZD) Saarland auf die dazu aktuell geführte öffentliche Diskussion, vgl. Berichterstattung des SR vom 15. Januar 2020 „Piraten kritisieren WhatsApp-Einsatz von Gemeinden“.

Das UZD weist daraufhin, dass im Rahmen der Prüfung keine Verstöße gegen datenschutzrechtliche Vorschriften festgestellt werden konnten. Gleichwohl sei es wichtig darauf hinzuweisen, dass die Vereinbarkeit der in dem Beitrag des SR beschriebenen Verarbeitung von Metadaten durch den Messenger-Dienst mit europäischen Datenschutzvorgaben fraglich ist. Aus datenschutzrechtlicher Sicht stellt sich jedoch die Frage, ob die Kommune für diese datenschutzrechtlich fragwürdige Datenverarbeitung durch WhatsApp (mit)verantwortlich ist.

Anders als etwa im Rahmen des Betriebs einer Facebook-Fanpage „profitiert“ die Kommune nämlich nicht von der Verarbeitung von Metadaten durch WhatsApp. Nach der Rechtsprechung des Europäischen Gerichtshof ist für Fanpage-Betreiber eine (Mit-)Verantwortlichkeit zu bejahen, wenn diesen die von Facebook erhobenen Daten in Form von statistischen Auswertungen, oft auch als Reichweitenanalyse bezeichnet, zur Verfügung gestellt werden, um das eigene Angebot den Präferenzen ihrer Nutzer anpassen und dieses optimieren zu können. WhatsApp stellt den Kommunen allerdings derartige Auswertungen nicht zur Verfügung.

Auch was die technische Umsetzung des WhatsApp-Angebotes bei den Kommunen angeht, konnten keine Verstöße festgestellt werden. Die geprüften Angebote laufen nicht auf einem klassischen Mobilfunkgerät. Vielmehr wird die WhatsApp-Anwendung in einer virtualisierten IT-Umgebung abgeschottet und isoliert betrieben, was einen Zugriff auf das Adressbuch ausschließt. Somit werden WhatsApp durch die Kommune auch keine Telefonnummern oder Kontaktdaten der Bürger zur Verfügung gestellt. Diese haben es vielmehr in der Hand, durch eine eigenverantwortliche Nutzung des Messaging-Dienstes WhatsApp, ihre personenbezogenen Daten an das Unternehmen zu übermitteln und die diesbezüglichen Geschäftsbedingungen zu akzeptieren. Anders wäre dies indes zu beurteilen, wenn die Kommune den Bürger über WhatsApp kontaktiert, ohne dass dem eine vorherige Anfrage des Bürgers vorausgeht.

Ebenfalls geprüft wurde, inwiefern bei der Nutzung von WhatsApp personenbezogene Informationen, die in den Nachrichtentexten und -inhalten enthalten sein können, gegenüber WhatsApp offenbart werden. Die dabei zur Anwendung kommende Ende-zu-Ende-Verschlüsselung, die von WhatsApp in einem Security Whitepaper genauer beschrieben wird, entsprach nach der Bewertung des UZD dem Stand der Technik, sodass davon ausgegangen werden kann, dass technisch sichergestellt ist, dass WhatsApp keine Kenntnis von den Inhalten der Kommunikation zwischen Bürger und Kommune erhält.

Aus datenschutzrechtlicher Sicht ist die Eröffnung einer Kontaktmöglichkeit für Bürger über WhatsApp durch Kommunen daher nicht zu beanstanden. Hiervon getrennt ist jedoch die Frage zu beantworten, ob staatliche Stellen es mit ihrer aus dem Grundgesetz folgenden Schutz- und Gewährleistungspflicht vereinbaren können, wenn sie Dienste eines Dritten in Anspruch nehmen, dessen Geschäftsmodell auf

datenschutzrechtlich fragwürdigen Methoden basiert. Dabei beschränkt sich die Kritik nicht auf bestimmte Messenger- oder Social-Media-Dienste. Dies ist jedoch keine Frage die primär datenschutzrechtlich, sondern vorrangig politisch und gesellschaftlich beantwortet werden muss.

Quelle: PM des Unabhängigen Datenschutzzentrum Saarland vom 16. Januar 2020

Hinweise zum Umgang mit Passwörtern

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat Hinweise zum Umgang mit Passwörtern herausgegeben. Die Anmeldung mittels Nutzername und Passwort stellt eine technisch-organisatorische Maßnahme und oftmals das wesentliche oder gar einzige Sicherheitselement dar, das vor Zugriffen durch Unbefugte schützt.

1. Starke Passwörter wählen

Das Passwort sollte aus zwölf oder mehr Zeichen bestehen. Es sollten sowohl Klein- als auch Großbuchstaben, Ziffern und Satzzeichen enthalten.

Da solche Passwörter schwer zu merken sind, gibt es Eselsbrücken:

a) Die erster-Buchstabe-Methode

Denken Sie sich einen Satz aus, den Sie sich gut merken können und nehmen von jedem Wort den ersten oder einen markanten Buchstaben. Nehmen Sie aber keinen Satz, den jemand anderes leicht erraten kann bzw. verfälschen Sie den Inhalt etwas.

b) Ganzer-Satz-Methode

Der Satz sollte möglichst aus sinnlosen Phantasiewörtern bzw. zufällig aneinandergereihten Wörtern bestehen, aber trotzdem so, dass Sie Ihn sich merken können.

c) Zufällige Passwörter generieren lassen

Einige Browser bieten die Option, zufällige Passwörter zu generieren und von einem Passwort-Safe speichern zu lassen, ohne dass Sie diese sehen. Dies ist oftmals die komfortabelste und einfachste Methode – und auch sicher, solange der Passwort-Safe die Daten gut verschlüsselt ablegt und kein Dritter Zugang dazu erhält.

d) Passwort-Karten und -Schablonen

Passwort-Karten und –Schablonen erleichtern ebenfalls das Finden und Merken von Passwörtern.

2. Passwörter niemals doppelt verwenden

Hacker greifen oft die Sicherheitslücken von Passwortdatenbanken an. Wird das gleiche Passwort für unterschiedliche Dienste verwendet, besteht das Risiko, dass die Angreifen sich unrechtmäßig auch bei anderen Diensten anzumelden oder weitere ähnliche Passwörter (die nur minimal geändert wurden) zu knacken.

3. Passwort-Safe verwenden

Sinnvoll sind sog. Passwort-Safes. Entsprechende Programme gibt es als kostenlose Freie- und Open-Source-Software. Einige Betriebssysteme bieten solche Safes automatisch mit an (z. B. der Schlüsselbund unter MacOS). Viele Web-Browser unterstützen die Speicherung von Passwörtern – diese sollten aber mit einem Master-Passwort abgesichert werden.

4. Keine Wörter aus Wörterbüchern verwenden
Angreifer können in kurzer Zeit automatisiert sehr viele Kombinationen durchprobieren. Gute Passwörter sollten daher weder Begriffe oder Begriffskombinationen aus Wörterbüchern enthalten („Sommer2018“) noch solche wiederverwenden. Die einzige Ausnahme sind wirklich sehr lange Passwörter, die aus einer Reihe zufälliger und nicht zusammenhängender Wörter bestehen.

5. Passwörter nicht weitergeben
Passwörter sollen grundsätzlich nicht weitergegeben werden. Ebenso sollen sie nicht per unverschlüsselter E-Mail versendet oder in unverschlüsselten Dokumenten gespeichert werden.

6. Nur bei Kompromittierung ändern
Früher wurde empfohlen, Passwörter in regelmäßigen Abständen zu ändern. Diese Empfehlung gilt heutzutage als überholt, da sie nicht zu mehr Sicherheit führt – sondern nur dazu, dass Nutzer sich diese im Klartext notieren, einfache Passwörter wählen, eine Zahl hoch zählen oder ähnliches. Nur wenn es Anzeichen dafür gibt, dass Passwörter oder Passwort-Hashes in fremde Hände gelangt sind, sollten Nutzer diese ändern.

7. Sichere Passwörter auch auf Smartphones
Auch hier sollten sichere und lange Passwörter gewählt werden. Vierstellige PINs oder Wischgesten sind in der Regel nicht ausreichend. Bei einer biometrischer Authentifizierung ist zu beachten, dass nicht alle Hersteller ein hohes Sicherheitsniveau bieten.

8. Start- bzw. Standard-Passwörter immer ändern
Passwörter, die bei der Registrierung vergeben werden oder die z. B. von Internet-of-Things-Geräten, Fernwartungseinheiten, Software-Paketen und ähnlichem vergeben werden, sind oftmals nicht zufällig sondern bei allen Geräten gleich. Diese müssen Bei der erstmaligen Nutzung sofort geändert werden.

9. Lügen bei Sicherheitsfragen
Viele Dienste fragen Sie für Sicherheitsfragen nach persönlichen Informationen, wie dem Name Ihres ersten Haustieres, dem Geburtsdatum der Mutter oder ähnlichem. Die korrekten Antworten auf solche Fragen sind für Angreifer aus Ihrem Umfeld oder insbesondere bei Personen des öffentlichen Lebens oftmals leicht herauszufinden. Zwingt Sie ein Dienst, solche Sicherheitsfragen zu verwenden: Lügen Sie! Es bietet sich an, wie bei Passwörtern zufällige Angaben zu machen und diese im Passwort-Safe zu speichern.

10. Zwei-Faktor-Authentifizierung aktivieren
Viele Web-Dienste bieten eine so genannte Zwei-Faktor-Authentifizierung (2FA) an. Ist diese aktiviert, müssen Sie bei der Nutzung mit einem neuen Gerät noch einen zweiten Faktor eingeben, so wie das beim Homebanking üblich ist. Dieser zweite Faktor wird auf einem anderen Kommunikationsweg übertragen, daher reicht die Kenntnis des Passworts alleine für einen erfolgreichen Angriff nicht aus.

Auch Diensteanbieter, Hersteller und Entwickler sollten einige Vorgaben beachten. Die Hinweise können Sie hier noch einmal nachlesen.

Quelle: Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg

BayLDA: Datenübertragung bei Windows 10 lässt sich mit der Enterprise-Version deaktivieren

Das Bayerischen Landesamts für Datenschutzaufsicht und der Bayerische Landesbeauftragte für den Datenschutz haben federführend mit einer Facharbeitsgruppe im Dezember 2019 eine Laboranalyse von Windows 10 durchgeführt. Im aktuellen Tätigkeitsbericht des BayLDA werden die Ergebnisse vorgestellt. Ebenfalls beteiligt waren Mitarbeiter von Microsoft (von denen über 10 Personen, überwiegend aus dem technischen Bereich, von Microsoft aus den USA gekommen sind), um alle technischen Fragen zu beantworten. Es wurde ein Testszenario mit einem Windows 10 Rechner, der eine Enterprise-Version (Version 1909) installiert hatte, derart aufgebaut, dass alle Datenflüsse von diesem Rechner noch innerhalb des Labornetzes mittels einer sog. „Man-in-the-Middle-Analyse“ aufgezeichnet wurden. Dabei wurde das System mit von Microsoft offiziell zur Verfügung gestellten Informationen und Tools so konfiguriert, dass das Telemetrielevel „Security“ eingestellt war und möglichst alle Datenflüsse deaktiviert werden konnten.

Bei der Labor-Analyse zeigte sich, dass die Telemetriedaten von einem Windows 10 Rechner mit der Enterprise-Version komplett deaktivierbar sind. Ausschließlich Aufrufe an (Microsoft-)Server, die aktuelle krypto-graphische Zertifikate liefern, waren durch diese Konfiguration nicht abschaltbar, da diese für einen tagesaktuellen sicheren Betrieb eines Windows 10-Systems erforderlich sind. Auch diese Aufrufe können jedoch durch gezielte Systemkonfigurationen unterbunden werden, wenngleich ein solches Vorgehen aus Gründen der Sicherheit keineswegs empfehlenswert ist.

Das BAyLDA sieht insofern für den Umgang mit Telemetriedaten bei Windows 10 Enterprise keinen datenschutzrechtlichen Hinderungsgrund eines Einsatzes dieses Betriebssystems dar, soweit sich das Ergebnis beim realen Einsatz von Windows 10 bei Unternehmen bestätigt.

Quelle: 9. Tätigkeitbericht 2019 des BayLDA

Petitionsausschuss: Mehr Schutz durch ePrivacy-Verordnung

Der Petitionsausschuss des Deutschen Bundestages unterstützt die Zielstellung des Vorschlags der EU-Kommission für eine "Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation" (ePrivacy-Verordnung), ein hohes Schutzniveau für die Vertraulichkeit von Kommunikationsdaten zu schaffen und zugleich den Spielraum für Innovation und digitale Geschäftsmodelle zu sichern sowie die Datensouveränität zu stärken. Er hat beschlossen dem Bundesministerium des Innern, für Bau und Heimat eine Petition zum Thema Datenschutz bei Smartphones "als Material" zu überweisen und sie dem Europäischen Parlament zuzuleiten.

Mit der Petition wird gefordert, Services und Dienste in Deutschland zu untersagen, die Zugriff auf Datenspeicher von Nutzern nehmen und dabei Daten Dritter, beispielsweise über das Auslesen des Adressbuches im Smartphone in Zusammenhang mit der Nutzung eines Messenger-Dienstes, ausspähen und speichern oder sich sogar eine Weitergabe dieser Daten vorbehalten. Zur Begründung heißt es, bestimmte Messenger-Dienste könnten nur dann verwendet werden, wenn den Allgemeinen Geschäftsbedingungen (AGB) und damit dem Auslesen, Speichern und Weiterleiten von Daten aus dem Adressbuch des Nutzers zugestimmt werde. Nichtöffentliche Daten unterlägen jedoch der informationellen Selbstbestimmung und seien

nach dem Bundesdatenschutzgesetz (BDSG) geschützt, heißt es in der Petition. Dienste und Services regelten über solche AGB-Klauseln also einen "regelmäßig rechtswidrigen Zugriff".

In der Begründung zu seiner Beschlussempfehlung macht der Petitionsausschuss darauf aufmerksam, dass Zugriffe auf das Adressbuch eines Nutzers durch einen Messenger-Dienst nur dann datenschutzrechtlich zulässig ist, wenn der Nutzer und die von dem Zugriff auf die Kontaktdaten betroffenen Person eingewilligt hätten oder die Voraussetzungen eines gesetzlichen Erlaubnistatbestandes nach der Datenschutz-Grundverordnung (DSGVO) erfüllt seien. Unbefugte Synchronisation der Kontaktdaten sei damit nicht zulässig und könne unter der DSGVO mit erheblichen Bußgeldern sanktioniert werden, schreiben die Abgeordneten.

Im Hinblick auf die mit der Petition angeregte Gesetzesänderung habe der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit darauf hingewiesen, dass die DSGVO "unmittelbar anwendbares Unionsrecht" sei, das Anwendungsvorrang vor deutschem Recht genieße, heißt es in der Vorlage. Als Vollharmonisierung des europäischen Datenschutzrechts sei eine abweichende nationale Gesetzgebung grundsätzlich nicht möglich. Eine Öffnungsklausel, die nationale Ausgestaltungen oder Abweichungen ermöglicht, sei in diesem Bereich nicht vorgesehen.

Die ePrivacy-Verordnung, so heißt es weiter, solle durch die anvisierte Gleichstellung der internetbasierten Anbieter mit den herkömmlichen Telekommunikationsdiensten insgesamt die Sicherheit der Kommunikationswege erhöhen, bisherige Rechtslücken schließen und somit für die Rechte von Privatpersonen einen höheren Schutz gewährleisten.

Quelle: Kurzmeldung des Deutschen Bundestages vom 12. Februar 2020

Unzulässige Verwendung eines Mitarbeiterfotos auf Facebook

Verwendet der Arbeitgeber ein Mitarbeiterfoto mit Namensnennung auf seiner Facebookseite, bedarf es hierzu einer schriftlichen Einwilligung des Beschäftigten. Dies entschied das Arbeitsgericht Lübeck im Rahmen eines Prozesskostenhilfeantrages.

Im Rahmen eines Prozesskostenantrags überprüft das Gericht summarisch, ob der Rechtsstreit mit hinreichender Wahrscheinlichkeit Aussicht auf Erfolg hat. Der Antragsteller beabsichtigt gegen seinen ehemaligen Arbeitgeber Klage auf Zahlung von Schmerzensgeld einzureichen. Während seines Arbeitsverhältnisses hatte der Antragsteller seine Zustimmung für einen Aushang mit seinem Bewerbungsbild erteilt Dieser Aushang wurde auch auf Facebook gepostet. In einer an damaligen Geschäftsführer gerichteten E-Mail schrieb der Antragsteller:

"Sollte ich den Arbeitsvertrag bis Mittwoch nicht per Mail erhalten haben, so darf ich Sie bitten, mein Foto von der Website mit der Bezeichnung Pflegedienstleitung zu nehmen auch die Patienten […] darüber in Kenntnis zu setzen, dass es sich um einen Irrtum handelt oder was auch immer sie angeben wollen. Ich möchte nicht, dass in der Öffentlichkeit mit meiner Person in irgendeiner Weise geworben wird, die nicht den Tatsachen entspricht."

Der Aufforderung zur Löschung des Bildes auf der Homepage kam der Arbeitgeber nach, auf Facebook nicht. Erst auf anwaltliche Aufforderung wurde das Bild auf der Facebook-Seite nebst Namen entfernt. Auf die zugleich geltend gemachte Schmerzensgeldforderung reagierte die Antragsgegnerin nicht.

Das Gericht geht davon aus, dass der Anspruch auf Schmerzensgeld dem Grunde nach besteht. Der Facebook-Post mit dem Foto und dem Namen des Antragstellers stellt eine Datenverarbeitung im Sinne der DSGVO dar. Eine Erlaubnis zur Veröffentlichung liegt nicht vor. Insbesondere liegt keine wirksame Einwilligung für die Veröffentlichung mangels Schriftform vor (§ 26 Abs. 2 S. 3 BDSG in der alten Fassung). Die Veröffentlichung von Mitarbeiterfotos in sozialen Netzwerken ist auch nicht durch ein berechtigtes Interesse des Arbeitgebers gedeckt. Weiter führt das Gericht aus, dass maximal 1.000 € als Schmerzensgeld gefordert werden können.

ArbG Lübeck, Beschluss vom 20. Juni 2019, 1 Ca 538/19

Praxistipp: Das Arbeitsgericht legte bei seiner Entscheidung § 26 BDSG in seiner alten Fassung zu Grunde. Seit dem 26. November 2019 sieht § 26 Abs. 3 BDSG vor, dass die Einwilligung schriftlich oder elektronisch erteilt werden kann. Es bleibt abzuwarten, ob und in welcher Höhe das Gericht den Schadensersatz im Hauptsacheverfahren zusprechen wird. Gibt das Gericht der Klage statt, ist damit zu rechnen, dass Arbeitgeber zukünftig immer häufiger mit solchen Ansprüchen von Arbeitnehmern konfrontiert werden.

Sonderkündigungsschutz des Datenschutzbeauftragten

Der Sonderkündigungsschutz des Datenschutzbeauftragten nach § 4f Abs. 3 Satz 5 BDSG in der bis zum 24. Mai 2018 geltenden Fassung (aF) endet mit Absinken der Beschäftigtenzahl unter den Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF. Gleichzeitig beginnt der nachwirkende Sonderkündigungsschutz. Dies entschied das Bundesarbeitsgericht (BAG).

Der Kläger arbeitete bei der Beklagten - einem australischen Bankinstitut, das auch in Deutschland Niederlassungen unterhält - seit dem 1. April 2010 als Director Institutional Banking. Zu diesem Zeitpunkt waren in der Niederlassung neun Beschäftigte tätig, die alle ständig automatisiert personenbezogene Daten verarbeiteten. Mit Schreiben vom 1. Juni 2010 bestellte die Beklagte den Kläger zum Datenschutzbeauftragten. In den Jahren 2010 bis 2015 beschäftigte die Beklagte zwischen zehn und dreizehn, im Jahr 2016 neun Mitarbeiter in der Niederlassung.

2017 kündigte die Beklagte das Arbeitsverhältnis des Klägers ordentlich. Zu diesem Zeitpunkt waren insgesamt acht Arbeitnehmer beschäftigt. Der Kläger beruft sich unter anderem auf seinen Sonderkündigungsschutz aufgrund seiner Benennung zum Datenschutzbeauftragten, wonach er nur außerordentlich gekündigt werden könne.

Das Arbeitsgericht hat festgestellt, dass das Arbeitsverhältnis der Parteien nicht aufgelöst worden ist. Die Berufung der Beklagten wurde zurückgewiesen. Das BAG hat in der Sache an das LAG zurückverwiesen.

Es ist der Auffassung, der Kläger kann sich nicht auf diesen Sonderkündigungsschutz berufen, da die Beklagte bei Zugang der Kündigungen nicht in der Regel mehr als neun Personen (§ 4f Abs.1 BDSG a.F.) ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigte.

Zum Zeitpunkt der Bestellung des Klägers zum Datenschutzbeauftragten bestand für die Beklagte die Pflicht zu einer solchen Bestellung. Er war damit nicht ein bloß „freiwilliger“ Beauftragter für den Datenschutz. Für das Merkmal „in der Regel ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen“, kommt es nicht auf die zufällige tatsächliche Anzahl der Beschäftigten im Zeitpunkt der Bestellung an. Maßgebend ist die Beschäftigungslage, die im Allgemeinen für das Unternehmen kennzeichnend ist. Zur Feststellung der regelmäßigen Beschäftigtenzahl bedarf es deshalb eines Rückblicks auf die bisherige personelle Stärke im Unternehmen und einer Einschätzung der zukünftigen Entwicklung. Zeiten außergewöhnlich hohen oder niedrigen Arbeitsanfalls sind dabei nicht zu berücksichtigen.

Ein Absinken der Beschäftigtenzahl unter den Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF während der Tätigkeit als Beauftragter für den Datenschutz führt dazu, dass dessen Sonderkündigungsschutz nach § 4f Abs. 3 Satz 5 BDSG aF entfällt, ohne dass es eines Widerrufs der Bestellung durch den Arbeitgeber bedarf. Dies folgt aus der Auslegung der Norm. Der Wortlaut der Regelung spricht stark für die Annahme, dass ein Sonderkündigungsschutz nur besteht, wenn im Zeitpunkt des Zugangs der Kündigung die Voraussetzungen für die verpflichtende Bestellung eines Beauftragten für den Datenschutz vorliegen. § 4f Abs. 3 Satz 5 BDSG aF knüpft an eine gegenwärtige Pflicht zur Bestellung an („Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen“). Maßgeblich sind die objektiven Verhältnisse im Zeitpunkt des Zugangs der Kündigungserklärung. Besteht keine Verpflichtung mehr zur Bestellung eines Datenschutzbeauftragten, bedarf es außerdem nicht mehr des Schutzes der Unabhängigkeit seiner Stellung. Vergleichbar ist dies mit dem Amt als Betriebsratsmitglied. Das Amt des Betriebsrats endet, wenn die Zahl der ständig beschäftigten Arbeitnehmer des Betriebs nicht nur vorübergehend auf unter fünf Arbeitnehmer absinkt und damit die Voraussetzungen für die Bildung eines Betriebsrats entfallen. Der besondere Kündigungsschutz nach § 15 Abs. 1 Satz 1 KSchG besteht nur während der Amtszeit des Betriebsrats.

Das BAG stellt weiter fest, das nach Beendigung des Amtes der nachwirkende Sonderkündigungsschutz beginnt. Danach ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, sofern kein wichtiger Grund besteht.

Praxistipp: Auch in der Neufassung des BDSG ist ein Sonderkündigungsschutz für den Datenschutzbeauftragten vorgesehen. Diese Regelung ist stark umstritten. Eingewandt wird, dass der deutsche Gesetzgeber keine Regelungskompetenz dafür hat. Im Übrigen gilt der Sonderkündigungsschutz ausdrücklich nur, wenn die Benennung eines Datenschutzbeauftragten verpflichtend ist (§ 38 Abs. 2 BDSG).

VERANSTALTUNGEN

„Richtig kündigen!?“
Montag, 16. März 2020, 18.00 - 20.00 Uhr, Raum 1, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken

Herr Rechtsanwalt Dr. Kai Hüther, Fachanwalt für Arbeitsrecht, Kanzlei Rapräger, Saarbrücken, wird im Rahmen seines Vortrages vorstellen, wie die Formalien bei einer Kündigung in den Griff zu bekommen sind. Außerdem geht er auf die Besonderheiten ein, wenn der bzw. die zu Kündigende im Ausbildungsverhältnis steht oder sich in der Mutterschutz- oder Elternzeit befindet.

Die Teilnehmerpauschale (inkl. MwSt.) beträgt 25,00 € pro Person für IHK-Mitglieder und 30,00 € für Nichtmitglieder.

Anmeldungen **bis 13. März 2020** unter E-Mail: veranstaltungen@saarland.ihk.de

„Rund um die BGB-Gesellschaft“
Donnerstag, 26. März 2020, 18.00 - 20.00 Uhr, Raum 1, IHK Saarland, Franz-Josef-Röder-Str. 9, 66119 Saarbrücken.

Frau Dr. Carmen Palzer, Kanzlei DR. PALZER | BERGER, Saarbrücken, gibt Ihnen einen praxisgeprägten Einblick in das Recht der BGB-Gesellschaft. Als potenziell betroffener Unternehmer sollte man wissen, welche Handlungsinstrumente das Gesetz an die Hand gibt, falls keiner oder nur ein unvollständiger Gesellschaftsvertrag geschlossen wurde. Und vor allem: was im Gesellschaftsvertrag geregelt werden kann - oder auch soll.

Die Teilnehmerpauschale (inkl. MwSt.) beträgt 25,00 € pro Person für IHK-Mitglieder und 30,00 € für Nichtmitglieder.

Anmeldungen **bis 25. März 2020** 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 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