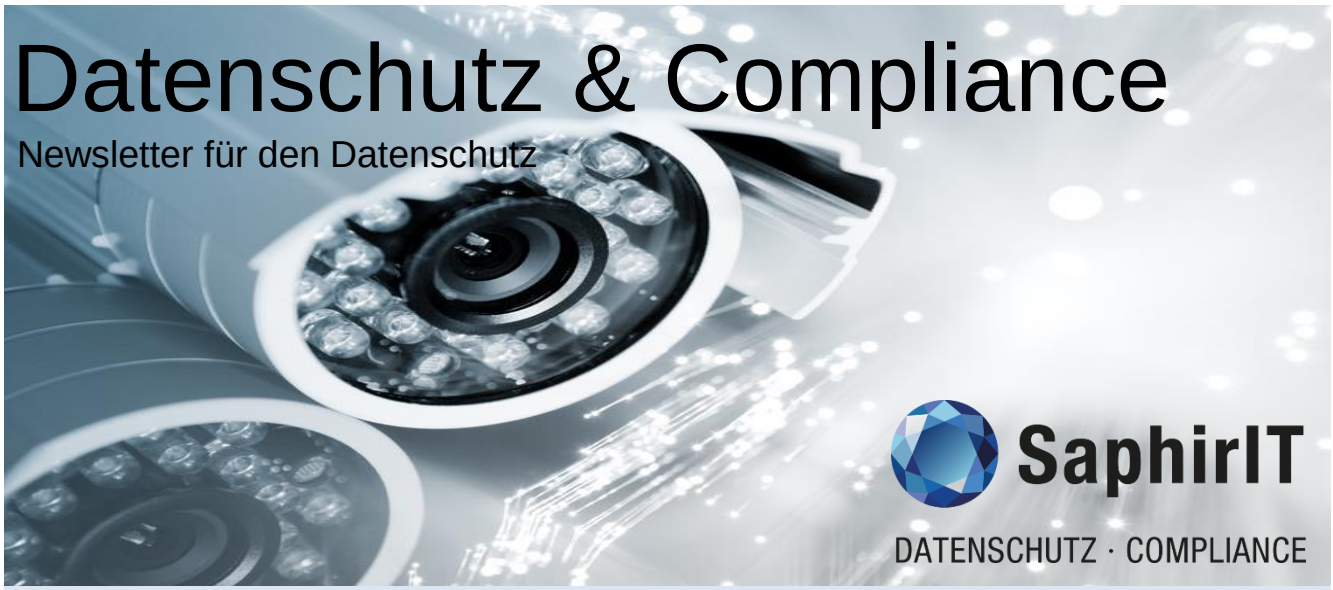


**Ausgabe Mai 2017** | Seite 6-11

INHALT



Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter Mai 2017.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Mit freundlichen Grüßen
*Ihre SaphirIT GmbH*

## Bundestag beschließt neues Bundesdatenschutzgesetz

- Was sich jetzt ändert -

In der Sitzung vom 27.04.2017 hat der Bundestag ein vollständig neues Bundesdatenschutzgesetz (BDSG) beschlossen.
Es tritt damit an die Stelle des seit mehr als 40 Jahren geltenden gleichnamigen Gesetzes.

Zurückzuführen ist das Gesetz auf die ab Mai 2018 europaweit geltende Datenschutzgrundverordnung (DSGVO).

Das Gesetz soll das deutsche Recht an die Vorgaben der DSGVO anpassen.

Warum dieses Gesetz nötig ist, wenn doch die DSGVO als unmittelbar geltendes Recht vorrangig Anwendung findet?

In der DSGVO existieren sogenannte Öffnungsklauseln, diese ermöglichen es den einzelnen Mitgliedsstaaten bestimmte Situationen

konkreter und auf ihr Land angepasst zu regeln. Ferner können diese dadurch die Rechte und Pflichten aus der DSGVO auf nationaler Ebene zusätzlich einschränken.

Da das Gesetz als zustimmungsbedürftig eingestuft wurde, muss sich auch der Bundesrat damit befassen und zustimmen. Es steht ihm offen das Gesetz anzunehmen, oder den Vermittlungsausschuss anzurufen. Die erforderliche Zustimmung gilt jedoch nach letzten Verhandlungen als sicher.

Sobald das Gesetz verabschiedet wurde und in Kraft tritt, werden wir gesondert ausführlich berichten.

Vorab nur so viel:

Insbesondere die Bußgelder und Anforderungen an Unternehmen in Sachen Transparenz, Dokumentation und Haftung steigen bzw. entsprechen den Vorschriften der DSGVO.

So werden beispielsweise in Zukunft Bußgelder von bis zu 20 Millionen Euro oder 4 % des globalen Umsatzes – je nachdem welcher Betrag höher ist – verhängt. Einzig Verstöße, die allein das deutsche Recht betreffen sind bei einem Bußgeldbetrag von 50.000 Euro gedeckelt.

Auch in Sachen Schadensersatz ändert sich einiges. Unternehmen können dann auch wegen Nichtvermögensschäden zur Rechenschaft gezogen werden, was für Unternehmen zu erheblichen wirtschaftlichen Risiken führen kann. Die umfassenden Dokumentationspflichten die die DSGVO vorsieht, werden durch das BDSG nicht reduziert.

Insbesondere in Anbetracht dieser Entwicklungen ist es umso wichtiger einen datenschutzrechtlich konformen Standard in seinem Unternehmen gewährleisten zu können, sodass oben genannte Folgen gar nicht erst auftreten.

Sprechen Sie uns gerne an, sollten Sie sich unsicher sein, ob bei Ihnen datenschutzrechtlich Bedenken bestehen.

# Datenschutzverstoß durch Mitarbeiter

- außerordentliche Kündigung -

Dem aktuellen Fall liegt folgender Sachverhalt zu Grunde: Eine Mitarbeiterin einer Behörde, die seit 34 Jahren dort beschäftigt war, hatte in den vergangenen Jahren aus privatem Interesse mehrere hundert Melderegisterabfragen vorgenommen. Die Betroffenen waren größtenteils Personen aus ihrem Umfeld. So zum Beispiel die Tochter ihres Freundes, oder die Ex-Frau eines Bekannten.

Als dem Arbeitgeber die unbefugten Registerabrufe bekannt wurden, sprach er der Mitarbeiterin die außerordentliche Kündigung aus. Die Mitarbeiterin ging gerichtlich gegen die Kündigung vor und gab vor ihr sei ein Datenschutzverstoß nicht bewusst gewesen und sie habe zudem keine bösen Absichten gehabt.

Das Landesarbeitsgericht stufte schlussendlich die Beweggründe der Mitarbeiterin als Schutzbehauptung ein. Im Rahmen der Interessenabwägung seien auf Seiten der Klägerin nur noch ihr Lebensalter und die Beschäftigungsdauer zu berücksichtigen.

Datenschutzverstöße seien höher zu gewichten als die langjährige Beschäftigung in der Behörde und die Tatsache, dass die Abfragen ausschließlich zu privaten Zwecken erfolgten. Dem LAG zufolge sei die Verletzung datenschutz- und melderechtlicher Vorschriften als wichtiger Kündigungsgrund im Sinne des § 626 BGB „an sich“ geeignet.

Die Kündigungsschutzklage der Arbeitnehmerin wurde abgewiesen.

Das Gericht stellte im Laufe des Prozesses jedoch fest, dass die Datenverarbeitungsanlagen durch den Arbeitgeber nicht ausreichend geschützt waren. Die Mitarbeiter konnten jederzeit ohne Angabe eines Betreffs oder Aktenzeichens Daten abrufen.

Auch wenn die Kündigung des Arbeitgebers in diesem Fall gerechtfertigt war, kann es aufgrund der mangelnden Einhaltung der Datenschutzvorschriften für ihn jedoch zu Konsequenzen kommen.

Es ist denkbar, dass eine den Rechtsreit verlierende Klägerin sich wegen der im Rechtstreit festgestellten Datenschutzverstöße an die Landesdatenschutzbehörde wendet.

Solche Ordnungswidrigkeiten können gemäß § 43 Abs. 3 Alt. 2 BDSG dann mit einer Geldbuße von bis zu 300.000 EUR geahndet werden.

Des Weiteren kann sich auch das Gericht gemäß § 19 Niedersächsisches Datenschutzgesetz (NDSG) jederzeit an die Landesbeauftrage oder den Landesbeauftragten wenden (ähnliche Vorschriften sind in den jeweiligen Datenschutzgesetzen der anderen Bundesländer auch zu finden).

Gemäß § 9 BDSG sind Arbeitgeber dazu verpflichtet die technisch und organisatorisch erforderlichen Maßnahmen vorzunehmen, um personenbezogene Daten vor ungerechtfertigter Kenntnisnahme, Manipulation oder Verlust zu schützen.

Dies gilt nicht nur für den unbefugten Zugriff Dritter, sondern auch der eigenen Mitarbeiter.

Mitarbeiter sollten dementsprechend geschult werden, um für das Thema sensibilisiert zu werden und notwendige Programme zur Aufzeichnung von Zugriffen auf bestimmte Programme sollten überwacht und protokolliert werden.

Gerne helfen wir Ihnen einen ordnungsgemäßen Datenschutz in Ihrem Unternehmen sicherzustellen und alle erforderlichen Maßnahmen zu treffen, denn immer häufiger führt gerade das Nicht-Handeln zu Verstößen mit arbeitsrechtlichen und auch strafrechtlichen Konsequenzen für das Unternehmen (LAG Berlin-Brandenburg, Urteil vom 01.09.2016, Az. 10 SA 192/ 16).

## Vorstellungsgespräch per Skype

- Datenschutzrechtlich unzulässig? -

Vergangenen Monat veröffentlichten die Beauftragten für den Datenschutz und die Informationsfreiheit der Länder Berlin und Nordrhein-Westfalen ihren aktuellen Tätigkeitsbericht. In diesem nahmen sie unter anderem Stellung zum Einsatz moderner Auswahlinstrumente im Bewerbungsverfahren.

Speziell ging es auch darum, ob ein Vorstellungsgespräch per Skype zulässig ist.

Bewerbungsgespräche nehmen viel Zeit in Anspruch, insbesondere, wenn Unternehmen aus einer Vielzahl von Bewerbern auswählen müssen. Hinzu kommen durchaus Unternehmen die an internationalen Bewerbern interessiert sind. Gerade unter diesem Gesichtspunkt scheint ein Bewerbungsprozess mittels technischer Unterstützung eine Möglichkeit zu sein, die für Unternehmen an Attraktivität gewinnt, gerade um von der Notwendigkeit einer Anwesenheit vor Ort abzusehen.

Rechtlich gesehen stellten die Beauftragten für den Datenschutz allerdings fest, dass es keine Rechtsgrundlage für den Einsatz solcher Techniken gebe. Weder das Bundesdatenschutzgesetz, noch eine Einwilligung des Bewerbers würden den Einsatz technischer Mittel im Bewerbungsprozess rechtfertigen.

§ 32 Abs. 1 des Bundesdatenschutzgesetzes regelt, dass es für die konkrete Datenerhebung darauf ankommt, ob diese zwingend für den Bewerbungsprozess erforderlich ist. Es reicht demnach nicht aus, wenn die Datenerhebung das Verfahren erleichtert oder generell dafür geeignet ist.

Eine Einwilligung zu einem solchen Verfahren müsste auf der freien und informierten Entscheidung der Betroffenen beruhen. Regelmäßig sei diese in einem Bewerbungsprozess jedoch nicht anzunehmen.

Wie dem Berliner Tätigkeitsbericht letztlich zu entnehmen ist, ist der Einsatz von Skype in Vorstellungsgesprächen demnach unzulässig. Die Daten der Nutzer und somit der Bewerber würden für 90 Tage auf den Servern von Microsoft gespeichert. Diese konkrete Datenübermittlung sei für das Zustandekommen von Beschäftigungsverhältnissen nicht erforderlich.

Anders sehe es in dem Fall aus, wenn das Skype Gespräch vom Bewerber selbst angeboten wird. Von einer Einwilligung kann dann ausgegangen werden. Jedoch stellt sich hier dann das Problem, ob bei den Mitarbeitern des Unternehmens die für das Bewerbungsgespräch zuständig sind auch von einer wirksamen Einwilligung ausgegangen werden kann. Im Zweifelsfall eher nicht.

Welche Bedeutung einem solchen Tätigkeitsbericht zuzumessen ist, lässt sich daran erkennen, dass dieser Aufschluss darüber gibt, in welchen Bereichen in den letzten zwei Jahren vermehrt Prüfungen der Aufsichtsbehörden durchgeführt worden sind.

Auch wenn der Tätigkeitsbericht erkennen lässt, dass die Anforderungen an die Erforderlichkeit und Freiwilligkeit sehr hoch sind, wird es grundsätzlich aber insbesondere auf den konkreten Einzelfall ankommen.

Sollten Sie in Ihren Bewerbungsverfahren Video- oder auch beispielsweise Sprachanalysen nutzen wollen, muss zuvor eine ausführliche datenschutzrechtliche Prüfung erfolgen, um festzustellen, ob die beabsichtigten Maßnahmen zulässig sind.

Nicht nur müssten umfangreiche Schutzmaßnahmen für die Bewerber getroffen werden, sondern insbesondere die Punkte Transparenz, Löschfristen und Berechtigungskonzepte berücksichtigt werden.

Jede Datenaufzeichnung im Bewerbungsprozess muss demnach einer Verhältnismäßigkeitsprüfung unterzogen werden, ob nicht ein milderes Mittel gegeben sein könnte, um den gewünschten Zweck zu erreichen.

Sollten Sie in Ihrem Unternehmen Fragen bezüglich spezieller Bewerbungsverfahren oder zur generellen Aufbewahrung von Bewerberdaten haben stehen wir Ihnen jederzeit für Rückfragen zur Verfügung.

# „Recht auf Vergessen“ gilt nicht für Einträge im Gesellschaftsregister

Mit Urteil vom 09.03.2017 hat der Europäische Gerichtshof (EuGH) die Pflicht der Handelskammern verneint, persönliche Daten zu anonymisieren oder zu entfernen.

Bezug nahmen sie dabei auf das sogenannte „Recht auf Vergessen“. Dieses gelte demnach nicht für Einträge in Gesellschafts- oder Handelsregistern.

Im vom EuGH entschiedenen Fall ging es um einen im Baugewerbe tätigen Italiener, welcher sich gegen eine Eintragung im nationalen Gesellschaftsregister wehrte. Er trug vor, aus dem Eintrag ließe sich entnehmen, dass er selbst Geschäftsführer einer insolventen und später liquidierten Gesellschaft gewesen war. Er vertrat die Auffassung die Eintragungen seien für ihn geschäftsschädigend gewesen und hätten entfernt oder zumindest anonymisiert werden müssen.

Die Register haben laut EuGH jedoch grundsätzlich die Aufgabe für Rechtssicherheit zu sorgen.

Eine starre Löschfrist lehnte das Gericht daher ab. Es sei auf die unterschiedlichen Verjährungsfristen der Mitgliedsstaaten Rücksicht zu nehmen, weshalb allein diese die Fristen bestimmen müssten.



SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de