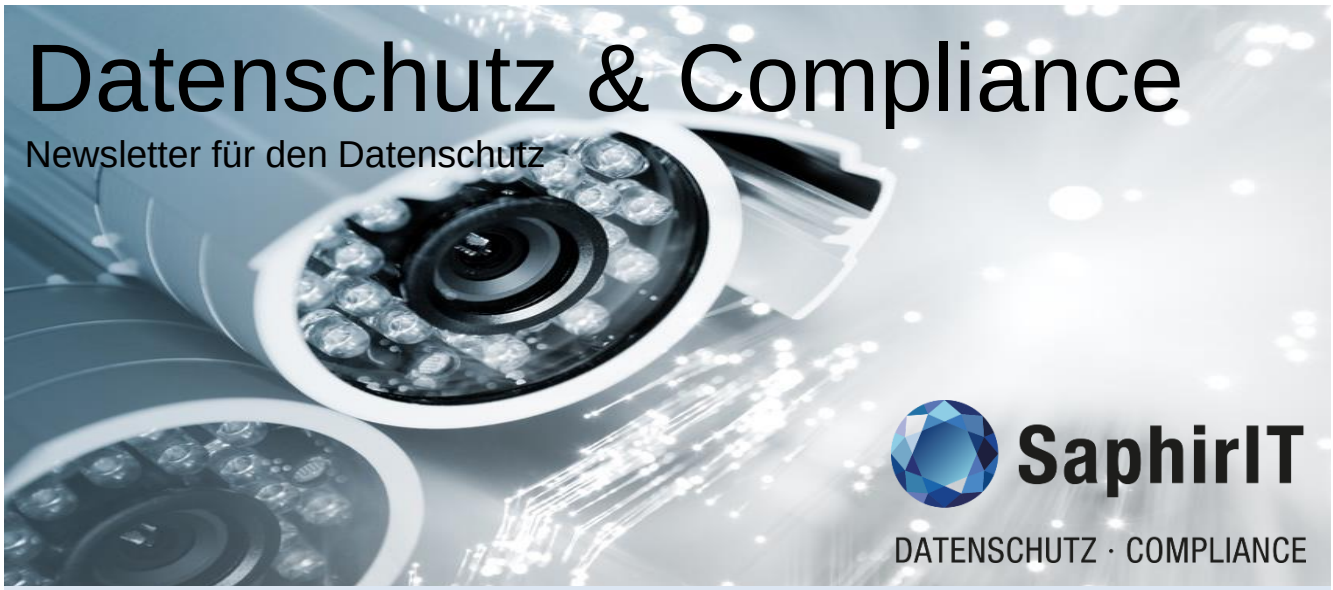

Ausgabe Dezember 2020 | Seite 194 - 199

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Dezember 2020.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Wir wünschen Ihnen und Ihrer Familie ein schönes Weihnachtsfest und einen guten Start in das neue Jahr 2021. Bleiben Sie gesund.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

DSK zum Einsatz von Windows 10 und zur Bedeutung verschlüsselter Kommunikation

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im Rahmen ihrer 100. Zusammenkunft in einem Beschluss festgehalten, dass Unternehmen und Behörden beim Einsatz der Enterprise-Edition von Windows 10 die Übermittlung personenbezogener Daten unterbinden können, wenn sie die Telemetriestufe „Security“ nutzen.

Bei der Enterprise Software handelt es sich um eine für Großkunden optimierte Version der Software.

Die Enterprise Edition von Windows 10 war im IT-Labor der Landesbeauftragten für den Datenschutz Niedersachsen in verschiedenen Szenarien getestet worden. Es zeigte sich, dass unter bestimmten Voraussetzungen keine

Telemetriedaten an Microsoft übermittelt wurden.

Die Landesbeauftragte für den Datenschutz Niedersachen Barbara Thiel sagte hierzu, dass man mit diesen Feststellungen einen wichtigen Schritt gemacht habe, damit Verantwortliche Windows 10 datenschutzkonform einsetzen könnten. Sie sei sehr froh, dass sich die Datenschutzkonferenz auf eine gemeinsame Linie einigen konnte.

Abschließend könne ein datenschutzkonformer Einsatz von Windows 10 jedoch nicht garantiert werden. Es handele sich einerseits um eine Momentaufnahme, da Windows 10 laufend weiterentwickelt werde, zum anderen seien noch immer Fragen zur Datenübermittlung unbeantwortet.

Verantwortliche müssten mit vertraglichen, technischen oder organisatorischen Maßnahmen sicherstellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfinde. Insbesondere gelte dies für den Einsatz der Pro- und Home-Editionen, in denen die Telemetriestufe derzeit nicht auf „Security“ gesetzt werden kann.

Die Datenschutzkonferenz fordert, dass in allen von Microsoft angebotenen Editionen diese Möglichkeit bestehen müsse. Dazu würden die Aufsichtsbehörden weiter das Gespräch mit Microsoft suchen.

Verschlüsselung als essentielle Voraussetzung für Digitalisierung

Sehr klar lehnte die Datenschutzkonferenz die Forderungen des EU-Rats ab, Sicherheitsbehörden und Geheimdiensten den Zugriff auf Inhalte verschlüsselter Kommunikation zu ermöglichen. Die DSK betonte eine sichere und vertrauenswürdige Verschlüsselung sei essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung.

Die DSK führt hierzu aus, dass bei einer Umsetzung der Vorschläge des Rates der Europäischen Union eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört würde. Die Ermittlungsmöglichkeiten von Sicherheitsbehörden würden dadurch nicht nachhaltig und effektiv verbessert.

Die Sicherheitsbehörden verfügten bereits über sehr weitreichende Befugnisse wie die Quellen-Telekommunikationsüberwachung, von der jedoch kaum Gebrauch gemacht werde.

Beschluss der Konferenz abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf

„Bring Your Own Device" – Dürfen Arbeitgeber die Geräte ihrer Arbeitnehmer untersuchen?

In einigen, gerade jüngeren Unternehmen, dürfen Mitarbeiter häufig ihre eigenen Geräte für berufliche Zwecke nutzen. Gerade in der Start-Up-Szene ist dies ein häufig gewähltes Mittel um Kosten zu sparen. In größeren Unternehmen wird dagegen meist streng zwischen privaten und dienstlichen Geräten getrennt.

Dabei stellt sich die Frage, was passiert, wenn es zu einem Sicherheitsvorfall kommt? Kann der Arbeitgeber die privaten Geräte seiner Mitarbeiter durch die IT untersuchen lassen?

Auf den Geräten werden zwangsläufig viele personenbezogene Daten und Geschäftsgeheimnisse oder wenigstens sensible Zahlen verarbeitet.

Um eine sichere Verarbeitung gewährleisten zu können müssen sich Unternehmen schon ziemlich viel einfallen lassen. Nicht selten mahnen Datenschutzbeauftragte stets streng private und dienstliche Geräte voneinander zu trennen.

Kommt es zu einem Datenschutzvorfall, so ist der Verantwortliche gemäß Art. 33 und 34 Datenschutzgrundverordnung (DSGVO) in der Pflicht, den Vorfall aufzuklären. Die Aufsichtsbehörde muss informiert werden und ggf. auch der Betroffene.

Die Untersuchung eines dienstlichen Gerätes zur Aufklärung eines Vorfalls ist in der Regel kein Problem. Anders jedoch bei „Bring Your Own Device" (BYOD) Geräten.

Die privaten Geräte stehen im Eigentum der Arbeitnehmer. Diese können durchaus ein Interesse daran haben, dass der Arbeitgeber nicht auf das Gerät zugreifen kann um dieses zu untersuchen.

Verpflichtet sind Arbeitnehmer grundsätzlich nicht ihr Gerät herauszugeben. Zwar kann das Beweisstück behördlich beschlagnahmt werden, das dürfte in den meisten Fällen, in denen kurze Fristen eingehalten werden müssen, aber eher nicht in Betracht kommen.

Bei Datenschutzvorfällen muss ein Unternehmen schnell handeln und Datenschutzverstöße innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde melden.

In diesen Fällen sitzt der Arbeitgeber am kürzeren Hebel und hat keine schnelle Möglichkeit auf das Gerät zuzugreifen.

Ist eine Nutzung von BYOD-Geräten trotz datenschutzrechtlicher Bedenken dennoch gewollt, bedarf es einer vernünftigen Strategie. Technische und organisatorische Maßnahmen können das Risiko jedenfalls mindern.

Technisch ist insbesondere an sog. Containerlösungen zu denken. Diese ermöglichen es private von beruflichen Daten zu trennen. Zusätzlich sollten Informationen, die auf den Geräten verarbeitet werden, nur auf Netzwerklaufwerken des Unternehmens gespeichert werden.

Aber auch Zugriffe aus der Ferne zum Zwecke IT-Forensischer Untersuchungen sind wichtig. Ein solcher Zugang muss auch rechtlich belastbar sein. Erforderlich ist dazu der Abschluss einer tauglichen Nutzungsvereinbarung. Sofern der Arbeitnehmer dem Arbeitgeber ein solches Nutzungsrecht nicht einräumen möchte, so muss der Arbeitgeber ihm ein Gerät stellen, da das Unternehmen ansonsten ein Problem mit der erforderlichen Freiwilligkeit bekommt.

Es ist bei einer IT-Forensischen Untersuchung nicht vermeidbar, dass auch private personenbezogene Daten mitverarbeitet werden. Bezogen auf diese Daten rechtfertigt nur eine wirksame Einwilligung das Vorgehen, die eine Freiwilligkeit voraussetzt.

Fazit

Bei BYOD bestehen grundsätzlich eine Reihe von datenschutzrechtlichen Problemen, die gelöst werden müssen. Diese sind auch durchaus umfangreich.

Ein Unternehmen sollte sich genau überlegen, ob die Kostenersparnis des BYOD-Modells die Nachteile bezüglich der datenschutzrechtlichen Vorkehrungen aufwiegt. Wenn ja, müssen genaue Nutzungsregeln aufgestellt werden, um Konfliktsituationen aus dem Weg zu gehen.

Ungewollte Datenweitergabe an sämtliche Wohnungseigentümer – nicht immer Schadensersatz bei unerwünschter Datenweitergabe

Das Landgericht Landshut hatte sich mit der Frage zu beschäftigen, ob gegen eine Hausverwaltung und den externen Datenschutzbeauftragten ein Schadensersatzanspruch nach Art. 82 Abs. 1 Datenschutzgrundverordnung (DSGVO) besteht. Es ging dabei um die Weitergabe von Daten des Klägers aufgrund eines Legionellenbefalls im Haus.

Einer der Wohnungseigentümer war der Kläger. Er machte einen Anspruch gegen die Hausverwaltung und den externen Datenschutzbeauftragten geltend.

Die Hausverwaltung hatte aufgrund eines Legionellenbefalls, der auch die Wohnung des Klägers betraf, Einladungen zur Eigentümerversammlung unter anderem mit folgender Tagesordnung versendet:

,,Informationsblätter zum Umgang mit der Trinkwasseranlage, Merkblatt für die Inspektion und Wartung von Bauteilen für Trinkwasserin-

stallationen sowie die Historie der Trinkwasseranlagen als auch die nächsten Beprobungstermine sind der Einladung beigefügt.

Folgende Untergemeinschaften sind von einem Befall (ab 101 Kb) betroffen:

…“

Auch der Kläger und seine Wohnung wurden in der Mitteilung aufgeführt. Die Einladung wurde an sämtliche ca. 97 Wohnungseigentümer versandt.

Der Kläger forderte die Hausverwaltung erfolglos auf, die Daten für die durchzuführende Eigentümerversammlung zu entfernen oder unkenntlich zu machen.

Der Kläger ging davon aus, dass die Veröffentlichung seiner Daten ohne seine Zustimmung einen Verstoß gegen Art. 6 DSGVO darstelle. Ihm sei dadurch sowohl ein materieller, als auch ein immaterieller Schaden entstanden – sein Ruf sei geschädigt.

Zudem habe ein potentieller Käufer seiner Wohnung aufgrund der Information über den Befall, abgesagt.

Der Kläger behauptete zudem, dass der externe Datenschutzbeauftragte den Verstoß innerhalb des E-Mail-Verkehrs eingeräumt habe und ein Schuldanerkenntnis demnach vorliege, aus welchem dieser nun hafte.

Das Landgericht Landshut wies die Klage ab.

Dem Kläger stehe kein Schadensersatzanspruch zu.

Gemäß Art. 82 Abs. 1 DSGVO kann jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist einen Anspruch auf Schadensersatz gegenüber dem Verantwortlichen oder dem Auftragsverarbeiter geltend machen.

,,Die Nennung der Wohnung des Klägers sowie die Nennung des Namens des Klägers als Eigentümer der Wohnung und auch die Nennung des KBE-Wertes stellen keinen Verstoß gegen die Vorgaben der DSGVO dar. Die Nennung erfolgte sowohl bei der Übersendung der Tagesordnung als auch in der streitgegenständlichen Eigentümerversammlung durch die Beklagte zu 1) als Verwalterin ausschließlich gegenüber den weiteren Wohnungseigentümern der streitgegenständlichen Wohnungseigentümergemeinschaft.“

Zwar sei zu berücksichtigen, dass die DSGVO auch innerhalb einer Wohnungseigentümergemeinschaft zur Anwendung komme, jedoch sei die Hausverwaltung vertraglich verpflichtet gegenüber den Eigentümern und der Wohnungseigentümergemeinschaft den gesetzlichen und vertraglichen Pflichten einer Hausverwaltung nachzukommen.

Gemäß §§ 13 und 14 WEG haben andere Wohnungseigentümer einen Anspruch darauf zu erfahren, in welchen Wohnungen ein Legionellenbefall vorliege.

Es hätten demnach, so das Gericht, die Voraussetzungen des Art. 6 Abs. 1 lit. b und c DSGVO als Rechtsgrundlage für die Datenverarbeitung vorgelegen.

Danach ist eine Datenverarbeitung rechtmäßig, wenn diese für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, erforderlich ist.

Ein materieller Schaden, aufgrund des Abrückens eines Interessenten als Käufer für seine Wohnung, liege nicht vor. Den Kläger hätten als Verkäufer einer Wohnung bei einem vorliegenden Legionellenbefall gegenüber dem Käufer ohnehin Aufklärungsplichten getroffen, da die durch die Legionellen auslösbare Legionärskrankheit einen lebensgefährlichen Verlauf nehmen könne.

Auch ein immaterieller Schadensersatzanspruch sei unbegründet, da der Betroffene nachweisen müsse, dass ihm ein spürbarer Nachteil entstanden sei. Zudem müsse die Beeinträchtigung objektiv nachvollziehbar mit gewissem Gewicht für die persönlichen Belange gewesen sein.

Letztlich habe der Kläger auch gegen den externen Datenschutzbeauftragten keinen Schadensersatzanspruch. Der externe Datenschutzbeauftragte sei kein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er sei nicht für die Handlungen des Verantwortlichen verantwortlich. Für das Schuldanerkenntnis fehlt es ohnehin an der erforderlichen Schriftform.

Konsequenz des Urteils

Dieses Urteil verdeutlicht, dass alleine die Verletzung des Datenschutzrechts noch nicht zwingend einen Schadensersatzanspruch begründet.

Ein begründeter Schadensersatzanspruch muss vielmehr weitere Voraussetzungen erfüllen.

Dem Betroffenen muss ein spürbarer Nachteil entstanden sein. Zudem muss eine objektiv mit gewissem Gewicht erfolgte Beeinträchtigung von „persönlichkeitsbezogenen Belangen“ vorliegen.

Für sog. Bagatellverstöße, die zu keiner ernsthaften Beeinträchtigung führen und bloß für „individuelle Unannehmlichkeiten“ sorgen, ist kein Schadensersatz zu zahlen (LG Landshut, Urt. v. 06.11.2020, Az. 51 O 513/20).

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