

Datenschutz & Compliance

Newsletter für den Datenschutz



SaphirIT

DATENSCHUTZ · COMPLIANCE

Ausgabe März 2021 | Seite 210 - 214

INHALT

SEITE 210

BSI plant Mindeststandards für Videokonferenzen

SEITE 211

LfD Mecklenburg-Vorpommern fordert Behörden zum Verzicht von Microsoft auf

SEITE 213

Schmerzensgeldanspruch nach der DSGVO – Europäischer Gerichtshof muss entscheiden

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter März 2021.

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

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

BSI plant Mindeststandards für Videokonferenzen

Das Bundesamt für Sicherheit in der Informationstechnik hat den Entwurf eines Mindeststandards für sichere Videokonferenzen zur Kommentierung veröffentlicht.

Auch wenn seit nunmehr einem Jahr die Nutzung von Videokonferenztools erheblich an Bedeutung gewonnen hat, herrscht noch immer Unsicherheit darüber welche Programme und Tools tatsächlich datenschutzkonform ein-

gesetzt werden können und welcher man sich lieber nicht bedienen sollte.

Viele Videokonferenzprogramme haben zwar Anpassungen bezüglich des Datenschutzes gemacht, bei vielen Programmen liegt das Problem allerdings eher darin, dass die Programme von amerikanischen Unternehmen betrieben werden und daher häufig auch eine

Datenübertragung in die Vereinigten Staaten nicht verhindert werden kann.

Die nun erstellten Mindeststandards dienen laut BSI nicht nur der Diskussion, sondern auch dem gemeinsamen Erstellen und Bearbeiten der Mindeststandards.

Es gehe darum Risiken im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität der übertragenen Daten zu vermeiden.

Die Mindeststandards sollen Sicherheitsanforderungen an Videokonferenzprogramme stellen. Es gehe dabei nicht nur um funktionale Anforderungen an das Programm selbst, sondern auch um die Konzeption, Planung, Beschaffung, den Betrieb sowie die Anforderungen an die Nutzer.

Der Entwurf beschreibt bisher die jeweilige Gefährdungslage und die Sicherheitsanforde-

rungen die beim Einsatz eines Videokonferenzprogramms beachtet werden müssen.

Konkret auf einzelne Anbieter wird nicht eingegangen. Dennoch kann damit gerechnet werden, dass die gängigen Videokonferenzprogramme, wenn die Mindeststandards einmal vom BSI festgelegt sind, an diesem Maßstab geprüft und dann auch bewertet werden.

Es dürfte dann um einiges einfacher sein Videokonferenzprogramme nach ihrer datenschutzrechtlichen Zulässigkeit bewerten zu können.

Das BSI hat Kommentierungen des Entwurfs bis zum 26. März 2021 zugelassen.

Abrufbar ist der Entwurf auf der Seite des BSI. https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Videokonferenzdienste/Videokonferenzdienste_node.html

LfD Mecklenburg-Vorpommern fordert Behörden zum Verzicht von Microsoft auf

Der Landesbeauftragte für den Datenschutz in Mecklenburg-Vorpommern und der dortige Rechnungshof haben von der Landesregierung gefordert ab sofort auf den Einsatz von Microsoft Produkten zu verzichten.

Da sich große Unternehmen, wozu auch Microsoft zählt, bei dem Problem der Übertragung personenbezogener Daten nicht zu bewegen scheinen, „bleibt letztlich nur der Rück-

griff auf Open-Source-Produkte, um den Datenschutz und auch die digitale Souveränität der Landesregierung zu wahren“, so der Landesdatenschutzbeauftragte Heinz Müller.

Müller fügt jedoch hinzu, dass ihm bewusst sei, dass nicht sofort auf Microsoft Produkte verzichtet werden könne. Dennoch gebe es schon länger Gespräche über das Thema, von denen er nun auch erwarte, dass Vorschläge für ei-

nen Übergang zu alternativer Software gemacht würden.

"Eine Vielzahl der in diesem Land genutzten Betriebssysteme, Büro-Anwendungen oder auch Videokonferenzlösungen lässt sich nicht betreiben, ohne dass personenbezogene Daten an Dritte abfließen", so Müller.

Der Europäische Gerichtshof (EuGH) hätte mit seinem Urteil zum Privacy Shield klargestellt, dass eine wirksame Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA derzeit nicht bestehe. Aufgrund der vom EuGH aufgestellten Grundsätze sei es nicht möglich Microsoft Produkte auf Basis von Standardvertragsklauseln zu nutzen.

Eine Nutzung von Microsoft ist daher momentan datenschutzkonform nicht möglich. Personenbezogene Daten würden ohne Rechtsgrundlage übertragen.

Sofern eine sichere Datenübermittlung nicht gewährleistet sei, müsste bei den Daten entweder der Personenbezug aufgelöst werden, die Daten verschlüsselt oder ein alternatives Produkt eingesetzt werden, so Müller.

Nicht nur für Behörden ist ein Einsatz von Microsoft datenschutzkonform momentan nicht

möglich. Die meisten Unternehmen verwenden Microsoft Produkte. Eine sichere Datenübertragung kann nicht gewährleistet werden.

Auch wenn es für viele Unternehmen bisher keine geeignete Alternative gibt sollten sich Unternehmen zumindest der Tatsache bewusst sein, dass eine Nutzung von Microsoft Produkten datenschutzrechtlich nicht zulässig ist.

Auch die DSK (Datenschutzkonferenz von Bund und Ländern) hatte bereits Ende letzten Jahres eine umstrittene Entscheidung dazu gefällt, dass Microsoft Office 365 derzeit nicht rechtskonform verwendet werden könne.

Innerhalb der Bundesländer sind die Ansichten jedoch sehr unterschiedlich. Die Annahme des Positionspapiers durch die DSK wurde nur von einer knappen Mehrheit getragen. Auch die DSK regte in einer Resolution aber an, verstärkt alternative Softwareprodukte sowie Open-Source-Programme einzusetzen.

Es bleibt abzuwarten wie sich die Diskussion um Microsoft weiter entwickeln wird. Bisher sieht es nicht danach aus, dass eine datenschutzkonforme Nutzung möglich ist bzw. sein wird. Es wird abzuwarten bleiben inwiefern sich die Datenschutzbehörden zu eventuellen Alternativen äußern werden.

Schmerzensgeldanspruch nach der DSGVO – Europäischer Gerichtshof muss entscheiden

Bereits seit in Kraft treten der Datenschutzgrundverordnung (DSGVO) herrscht unter den Gerichten Uneinigkeit darüber unter welchen Umständen einem Betroffenen neben einem möglicherweise entstandenen Schadenersatzanspruch, ein Anspruch auf Schmerzensgeld wegen einer Verletzung nach der DSGVO zustehen kann.

Insbesondere die Frage, ob erst ein erheblicher Schaden eintreten muss um einen Schmerzensgeldanspruch begründen zu können wird viel diskutiert.

Nun könnte das Bundesverfassungsgericht dabei helfen.

Hintergrund war eine ursprüngliche Entscheidung des Amtsgerichts Goslar.

Ein Rechtsanwalt hatte ohne seine Einwilligung Werbeemails von einem Unternehmen erhalten und forderte neben der Unterlassung der weiteren Zusendung von E-Mails auch ein Schmerzensgeld von mindestens 500,00 EUR.

Der Rechtsanwalt stützte seinen Anspruch auf Art. 82 DSGVO. Wegen seiner fehlenden Einwilligung liege ein Datenschutzverstoß vor. Art. 82 DSGVO sehe für diesen Fall ein angemessenes Schmerzensgeld vor.

Das Amtsgericht bestätigte einen Datenschutzverstoß, einen Anspruch auf Schmerzensgeld habe der klagende Anwalt jedoch nicht, da ein Schaden nicht ersichtlich sei.

Da Berufung und Revision nicht zugelassen wurden wäre die Entscheidung eigentlich endgültig gewesen.

Der Kläger erhob jedoch Verfassungsbeschwerde vor dem Bundesverfassungsgericht. Das Bundesverfassungsgericht entschied dabei aber nicht ob ein Schmerzensgeldanspruch besteht oder nicht, sondern welches Gericht mit der Frage noch hätte befasst werden müssen.

Gemäß Art. 101 Grundgesetz (GG) darf niemand seinem gesetzlichen Richter entzogen werden.

Das Bundesverfassungsgericht bemängelte, dass das Amtsgericht den Fall nicht dem Europäischen Gerichtshof (EuGH) im Wege des sog. Vorabentscheidungsverfahrens vorgelegt habe. Der EuGH sei ebenfalls ein gesetzlicher Richter im Sinne des Art. 101 GG, da er zuständig sei für die Auslegung von europäischen Rechtsakten, wie der DSGVO, die in Deutschland Wirkung entfalte.

Die Frage des Geldentschädigungsanspruchs nach der DSGVO sei in der Rechtsprechung

des EuGHs bisher weder erschöpfend geklärt, noch könnten die Voraussetzungen der DSGVO entnommen werden.

Das Amtsgericht hat zwar eine eigene Auslegung vorgenommen, diese hätte jedoch, so das Bundesverfassungsgericht, der EuGH vornehmen müssen.

Folge ist nun, dass das Urteil des Amtsgerichts durch das Bundesverfassungsgericht aufgehoben

wurde und das Amtsgericht nun erneut entscheiden muss.

Es wird somit bald dazu kommen, dass es die erste höchstrichterliche Rechtsprechung zur Auslegung des Art. 82 DSGVO geben wird. Sobald der EuGH die Frage beantwortet hat muss das Amtsgericht sein Urteil erneut fällen (BVerfG, Beschluss der 2. Kammer des Ersten Senats vom 14. Januar 2021, Az. 1 BvR 2853/19).

Falls Sie unseren Newsletter in Zukunft nicht mehr erhalten möchten, schicken Sie bitte eine kurze E-Mail an info@saphirit.de

SaphirIT GmbH
Sutthausen 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



Unsere jeweils aktuellen Datenschutzinformationen finden Sie unter
<https://www.saphirit.de/datenschutz.html>