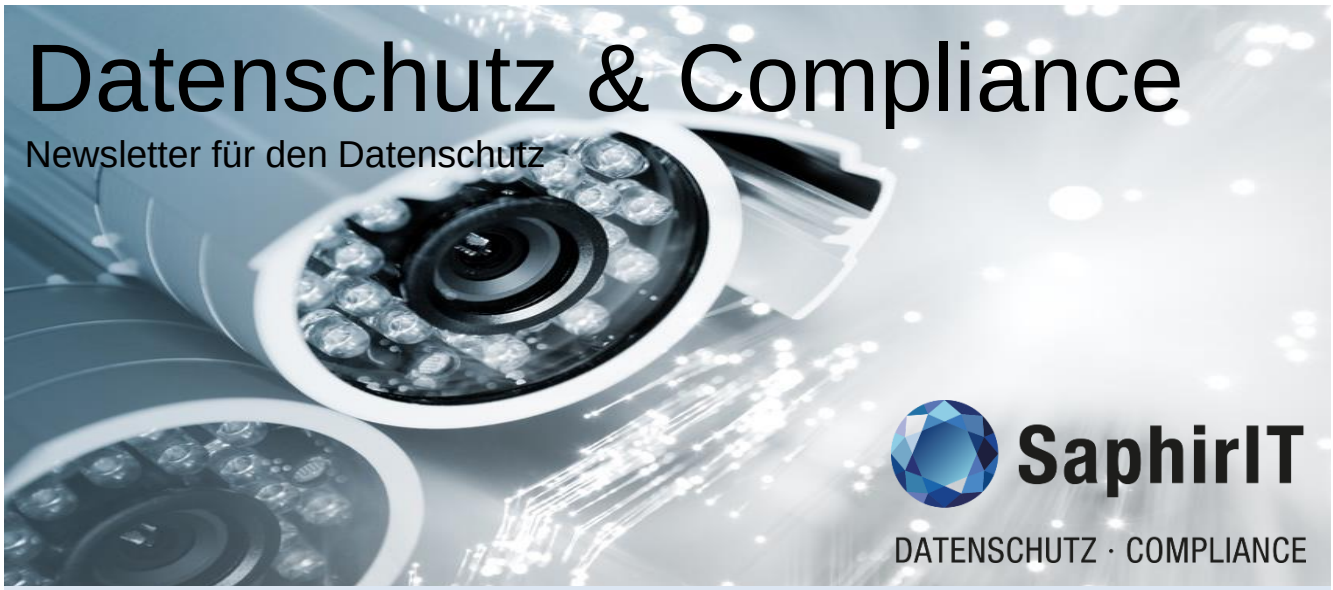

Ausgabe Januar 2021 | Seite 200 - 204

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Januar 2021.

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

Wir wünschen Ihnen ein gesundes und erfolgreiches neues Jahr!

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Brexit – Auswirkungen auf den Datenschutz

Seit dem 01.01.2021 ist das Vereinigte Königreich endgültig nicht mehr Mitglied der Europäischen Union. Das wird in allen Bereichen Auswirkungen haben, auch im Bereich der Datenübermittlung ist dies der Fall.

Eine gute Nachricht ist erst einmal, dass vorerst eine Schonfrist für Unternehmen, die personenbezogene Daten im Vereinigten Königreich verarbeiten, speichern bzw. dort mit Unternehmen zusammenarbeiten, vereinbart wurde.

Für erst einmal vier Monate gilt das Vereinigte Königreich diesbezüglich nicht als Drittland. Auch die Möglichkeit einer Verlängerung um weitere zwei Monate ist vorgesehen. Allerdings können beide Seiten der automatischen Verlängerung widersprechen, sodass man sich hierauf besser nicht verlassen sollte.

Bis mindestens zum **30.04.2021** (evtl. sogar bis zum 30.06.2021) ist ein Datentransfer aber unter unveränderten Bedingungen möglich.

Dennoch, der Tag wird kommen, an dem auch die letzte gewährte Schonfrist ablaufen wird und allerspätestens dann sollten alle Unternehmen in der Lage sein ihren Datentransfer in das Vereinigte Königreich auch anderweitig rechtmäßig zu gestalten.

Theoretisch ist es möglich, dass die EU-Kommission bis Ende April 2021 einen Angemessenheitsbeschluss erlässt und das Vereinigte Königreich damit zwar Drittland bliebe, ein sicherer Datentransfer dann aber trotzdem weiterhin möglich wäre. Angesichts der kurzen Zeit scheint dies aber eher hypothetisch.

Hinzukommt, dass im Vereinigten Königreich, ähnlich wie in den Vereinigten Staaten, die Sicherheitsbehörden weitreichende Befugnisse haben. Bisher war dies nicht wirklich von Bedeutung, da das Vereinigte Königreich trotz dieser Befugnisse dem europäischen Datenschutzstandard und den europäischen Datenschutzvorschriften nach der Datenschutzgrundverordnung (DSGVO) unterlag. Dies ist nun nicht mehr der Fall.

Die Konsequenzen die sich aus einer Datenweitergabe an Sicherheitsbehörden ergeben sind weitreichend bekannt. Sowohl das Safe Harbor Abkommen, als auch das EU-US-Privacy-Shield mit den Vereinigten Staaten wurden vom Europäischen Gerichtshof (EuGH) gekippt, mit der Folge, dass ein datenschutzkonformer Datentransfer in die USA momentan kaum möglich ist.

Das gleiche dürfte nun auch mit dem Vereinigten Königreich zu erwarten sein.

Auch in dieser Hinsicht dürfte der Erlass eines Angemessenheitsbeschlusses daher fraglich sein. Selbst wenn ein solcher erlassen werden würde, würde der EuGH dagegen vermutlich aus denselben Gründen wie bei den Vereinigten Staaten Einwände erheben.

Für den Fall, dass ein Angemessenheitsbeschluss doch käme, so wäre dieser erst einmal geeignet, um einen Datentransfer wie bisher zu rechtfertigen. Es müsste dann vermutlich erst viele Monate gewartet werden, bis der EuGH sich dazu äußern würde.

Sind Sie betroffen?

Betroffen vom Brexit sind alle Unternehmen, die personenbezogene Daten in das Vereinigte Königreich übermitteln. Darunter fallen zum Beispiel Name, Anschrift, Geburtsdatum, Bankdaten, etc. sowohl von Kunden, Beschäftigten, Vertragspartnern, etc. Auch die Inanspruchnahme von IT-Dienstleistungen durch Britische Unternehmen (z.B. Microsoft Europe mit diversen Cloud-Lösungen) oder die Durchführung einer Auftragsverarbeitung durch ein europäisches Unternehmen für einen Verantwortlichen im Vereinigten Königreich stellen eine Datenübermittlung dar, die nach den Standards der Datenschutzgrundverordnung durchgeführt werden muss.

Warum müssen Sie tätig werden?

Im Falle der Nichteinhaltung datenschutzrechtlicher Vorschriften hat die zuständige Aufsichtsbehörde umfassende Befugnisse. Sie hat gemäß Art. 58 Abs. 2 lit. j DSGVO die Möglichkeit die Datenübermittlung auszusetzen. Zudem steht ihr gemäß Art. 83 Abs. 5 lit. c die Möglichkeit zu, eine Geldbuße zu verhängen.

Was müssen Sie tun?

Immer wenn es um eine Datenübermittlung in ein Drittland geht, ist dies mit einem mal mehr, mal weniger großen Umsetzungsaufwand verbunden.

1. Informationsblatt zur Datenverarbeitung

In Ihrem Informationsblatt zur Datenverarbeitung sowie in der Datenschutzerklärung auf Ihrer Website muss über die Datenübermittlung in ein Drittland informiert werden.

2. Auskunftsrecht

Macht eine betroffene Person von ihrem Auskunftsrecht Gebrauch, so ist sie darauf hinzuweisen, dass eine Datenübermittlung in ein Drittland stattfindet.

3. Verzeichnis von Verarbeitungstätigkeiten

Auch das Verzeichnis von Verarbeitungstätigkeiten ist dahingehend zu ergänzen, dass eine Datenübermittlung in ein Drittland stattfindet. Im Übrigen sind die erforderlichen Abgaben zu machen.

4. Datenschutz-Folgenabschätzung

Sofern die übermittelten Daten einer Datenschutz-Folgenabschätzung unterliegen muss diese durchgeführt werden, oder sofern dies bereits geschehen ist, muss diese noch einmal überprüft werden.

5. Rechtsgrundlage für die Datenverarbeitung

Der wichtigste Punkt, sollte es nicht zu einem Angemessenheitsbeschluss kommen, dürfte die Rechtsgrundlage sein auf die die Datenverarbeitung gestützt werden kann.

Die Datenübermittlung in ein Drittland muss neben den übrigen Anforderungen der DSGVO auch den Art. 44 ff. DSGVO, welcher die Übermittlung personenbezogener Daten in ein Drittland regelt genügen.

Die verantwortlichen Stellen müssen geeignete Garantien im Sinne von Art. 46 ff. DSGVO schaffen, um die Datenübermittlung datenschutzkonform durchführen zu können.

In Art. 46 Abs. 2 und 3 DSGVO ist aufgezählt welche Garantien geschaffen werden müssen. Diese sind häufig nicht einfach umzusetzen und bereiten in der Praxis erhebliche Probleme. Unter anderem gibt es die Möglichkeit sog. Standardvertragsklauseln mit dem jeweiligen Unternehmen abzuschließen, die garantieren, dass ein angemessenes Datenschutzniveau vorliegt. Auch bestimmte Zertifizierungsmechanismen sind denkbar.

Pauschal kann nicht gesagt werden was bei Ihnen im Unternehmen die „beste“ Möglichkeit ist. Es muss im Einzelfall geschaut werden wo die Vor- und Nachteile liegen, bzw. welche Garantien sich überhaupt praktisch umsetzen lassen.

Ausnahmsweise darf eine Datenübermittlung in ein Drittland auch ohne das Vorliegen geeigneter Garantien durchgeführt werden.

Die **Ausnahmetatbestände** regelt Art. 49 DSGVO:

- wirksame Einwilligung der betroffenen Person
- Erforderlichkeit zur Vertragserfüllung
- wichtige Gründe des öffentlichen Interesses
- Verfolgung von Rechtsansprüchen
- Schutz lebenswichtiger Interessen
- Wahrung zwingender berechtigter Interessen

Sollten Sie bisher Daten in das Vereinigte Königreich übermittelt haben und haben dies auch weiterhin vor, so müssen Sie ausreichende Vorkehrungen treffen. Es bedarf einer genauen Auseinandersetzung mit Ihren Interessen und wie diese datenschutzkonform (weiterhin) gewährleistet werden können.

Sollten Sie diesbezüglich Fragen haben sprechen Sie uns gerne an. Wir helfen Ihnen eine Lösung zu finden.

Unrechtmäßige Videoüberwachung

10,4 Mio. Euro Bußgeld

Am 08.01.2021 veröffentlichte die Landesbeauftragte für den Datenschutz in Niedersachsen eine Pressemitteilung, wonach sie gegenüber der *notebooksbilliger.de AG* ein Bußgeld in Höhe von 10,4 Millionen Euro verhängt hat. Das Bußgeld ist das mit Abstand höchste von der Behörde bisher verhängte.

Anlass für das Bußgeld war eine in vielerlei Hinsicht unrechtmäßige Videoüberwachung.

Die Überwachung erfasste unter anderem Arbeitsplätze, Verkaufsräume, Lager und Aufenthaltsbereiche. Die Aufnahmen waren weder auf einen bestimmten Zeitraum, noch auf konkrete Beschäftigte beschränkt. Auch Kundinnen und Kunden waren von der unzulässigen Videoüberwachung betroffen.

Die Aufnahmen wurden bis zu 60 Tage lang gespeichert, was unzweifelhaft unverhältnismäßig ist. Mildere Mittel, um den beabsichtigten Zweck, die Aufdeckung von Straftaten zu erreichen, wurden nicht ausgeschöpft.

Das verantwortliche Unternehmen trug vor, das Vorgehen sei in der Branche so Standard. In erster Linie werde der Warenfluss im Unternehmen kontrolliert, um Beschädigungen oder Diebstähle aufzuklären. Eine Auswertung des Materials erfolge ausschließlich zu diesem Zweck.

Hinsichtlich einer von der Aufsichtsbehörde monierten Verhaltensüberwachung trug das Unternehmen lediglich vor, dass die Überwachung „technisch überhaupt nicht dafür ausgestattet“ sei.

Das Unternehmen sei jedoch kooperativ gewesen und die Überwachung erfolge inzwischen rechtmäßig.
Die Aufsichtsbehörde entschied sich dennoch ein erhebliches Bußgeld zu verhängen. Es verwies dabei auf die Rechtsprechung des Bundesarbeitsgerichts, wonach aus einer Überwachung ein Überwachungsdruck für die Mitarbeiter entstehe. Im Einzelfall seien hohe Hürden zu überwinden, um eine Überwachung der Mitarbeiter zu legitimieren.

Der Bußgeldbescheid ist noch nicht rechtskräftig. Das Unternehmen hat bereits angekündigt insbesondere ganz grundlegende Aspekte nach dem Maßstab des Verschuldens sowie zum Ablauf des Verfahrens diskutieren zu wollen. Das Bußgeld stehe in keinem Verhältnis zur Größe und Finanzkraft des Unternehmens sowie zur Schwere des vermeintlichen Verstoßes, so das Unternehmen.

Dennoch sollte man beachten, dass die DSGVO durchaus gerade vorschreibt, dass Bußgelder eine abschreckende Wirkung haben sollen.

In Anbetracht der Höhe des Bußgeldes kann damit gerechnet werden, dass es eine gerichtliche Auseinandersetzung geben wird.

Es ist davon auszugehen, dass die Entscheidung dann weitere hilfreiche Informationen hinsichtlich der Möglichkeiten und Grenzen von Videoüberwachung enthalten wird.

Auch hinsichtlich der Bemessung vom Bußgeldern herrschen noch immer Unklarheiten, die durch weitere Urteile beseitigt werden könnten.

Sollten Sie bei sich im Unternehmen eine Videoüberwachung haben so sollten Sie ganz besonders darauf achten, dass diese rechtmäßig ist. Gerade in öffentlich zugänglichen Bereichen bietet die Videoüberwachung häufig eine beliebte Angriffsfläche, da für jeden sichtbar ist wo Kameras möglicherweise aufzeichnen. Sollten Sie Fragen hinsichtlich der rechtmäßigen Installation einer Videoüberwachungsanlage haben sprechen Sie uns gerne an.

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