

Datenschutz & Compliance

Newsletter für den Datenschutz



SaphirIT

DATENSCHUTZ · COMPLIANCE

Ausgabe März 2020 | Seite 152 - 155

INHALT

SEITE 152

Home-Office – Datenschutzkonformes Arbeiten von zu Hause aus im Unternehmen gewährleisten

SEITE 154

OLG Stuttgart zur Abmahnfähigkeit von Datenschutzverstößen

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter März 2020.

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

...und ja, es gibt Wichtigeres als Datenschutz... bleiben Sie gesund!

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Datenschutzkonformes Arbeiten von zu Hause aus im Unternehmen gewährleisten

Das Thema Corona ist allgegenwärtig. In diesem Artikel wollen wir Ihnen veranschaulichen wie die Verwendung von Home-Office im Unternehmen datenschutzkonform gestaltet werden kann. Diese Anmerkungen sollten unabhängig von der aktuellen Situation beachtet werden und sind essentiell um bei einer möglichen Überprüfung durch die Datenschutzaufsichtsbehörde nicht negativ aufzufallen.

Grundsätzlich muss ein Arbeitnehmer im Home-Office dieselben datenschutzrechtlichen

Vorschriften einhalten wie im Unternehmen vor Ort.

Am besten gelingt das Ganze, wenn die Arbeit im Home-Office in einer eigenen Betriebsanweisung (Richtlinie) geregelt wird, die von allen Arbeitnehmern eingesehen werden kann.

Primär ist es erst einmal Aufgabe des Arbeitgebers die notwendigen Vorkehrungen zu treffen.

Neben dem Bereitstellen einer IT-Ausstattung muss auf die notwendige Verschlüsselung der Geräte geachtet werden. Zur Verfügung gestellte Zugriffe auf Betriebssysteme des Unternehmens sollten kennwortgesichert sein.

Auch der Versand von E-Mails sollte verschlüsselt erfolgen. Ein Zugriff in das Unternehmensnetzwerk über eine VPN-Verbindung sollte, bevor Beschäftigte in großer Zahl darauf zugreifen, ausreichend getestet werden.

Für den Fall, dass Arbeitnehmer Unterlagen mit personenbezogenen Daten auch zu Hause ausdrucken, muss gewährleistet werden, dass diese auch ordnungsgemäß vernichtet werden können. Arbeitnehmern sollte bestenfalls auch im Home-Office ein Shredder oder eine Datentonne zur Verfügung gestellt werden.

Sollte vom Arbeitgeber keine Datentonne oder Shredder zur Verfügung gestellt werden, so sollten zu vernichtende Unterlagen zumindest kleinteilig zerrissen werden.

Der Arbeitnehmer muss dagegen darauf achten, dass Daten mit denen er im Home-Office arbeitet nicht von Dritten eingesehen werden können.

Bestenfalls sollten Unterlagen mit personenbezogenen Daten in einem separaten abschließbaren Raum aufbewahrt werden. Sollte dies nicht möglich sein, sollten Unterlagen zumindest in einem abschließbaren Schrank aufbewahrt werden.

Hinsichtlich der vom Arbeitgeber zur Verfügung gestellten IT-Geräte sollte darauf geachtet werden, dass diese nur für die Tätigkeit im Home-Office und nicht privat genutzt werden.

Umgekehrt dürfen private IT Geräte nicht für betriebliche Angelegenheiten genutzt werden. Dies betrifft auch den Telefonanschluss, den Kopierer, das Faxgerät oder den Drucker.

Des Weiteren sollte der PC/ das Notebook auch bei kurzzeitigem Verlassen des Arbeitsplatzes, wie auch im Unternehmen, immer gesperrt werden.

Sollten Sie Fragen zu der Erstellung einer Home-Office Richtlinie haben sprechen Sie uns gerne an. Bei einer solchen Richtlinie handelt es sich außerdem um ein Verfahren mit personenbezogenen Daten, welches in das Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden muss.

Hinweis: Grundsätzlich ist es so, dass Arbeitgeber nicht einseitig festlegen dürfen wann und ob Arbeitnehmer im Home-Office arbeiten. Eine Verpflichtung der Arbeitnehmer unter bestimmten Umständen im Home-Office zu arbeiten ist daher nur möglich, wenn dies vorab im Arbeitsvertrag vereinbart wurde. Ist dies nicht geschehen kann selbstverständlich aber auch durch Vereinbarung mit den jeweiligen Arbeitnehmern eine Home-Office Regelung getroffen werden. Betriebsverfassungsrechtliche Mitbestimmungsrechte wären ebenfalls zu prüfen.

Oberlandesgericht Stuttgart

zur Abmahnfähigkeit von Datenschutzverstößen

Noch immer herrscht Uneinigkeit darüber wann und unter welchen Voraussetzungen Datenschutzverstöße nach der Datenschutzgrundverordnung (DSGVO) abgemahnt werden können.

Durch ein Urteil des OLG Stuttgarts (OLG) erlangt das Thema einmal mehr Aufmerksamkeit. Kläger im betreffenden Fall war ein Interessenverband von Online-Unternehmen. Der Beklagte vertreibt Kfz-Zubehör über die Plattform eBay.

Der Kläger trägt vor, der Beklagte habe es versäumt Betroffene über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten zu informieren. Der Beklagte verstoße daher gegen § 13 Telemediengesetz (TMG) sowie Art. 13 DSGVO.

Im erstinstanzlichen Urteil hatte das Landgericht Stuttgart (LG) entschieden, dass die Klage zwar zulässig, aber unbegründet sei.

Der Kläger könne keinen Anspruch aus dem TMG geltend machen, da diese gesetzliche Regelung seit Inkrafttreten der DSGVO keinen Anwendungsbereich mehr habe. Ein Verstoß gegen Art. 13 DSGVO läge möglicherweise vor, allerdings seien die Sanktionsmöglichkeiten der DSGVO abschließend in den Art. 77 – 84 DSGVO geregelt.

Das OLG Stuttgart schloss sich in vielen Punkten den Entscheidungsgründen des Landgerichts Stuttgart an. Hinsichtlich eines Datenschutzverstoßes führte es aus, dass ein Verstoß gegen Art. 13 DSGVO deshalb vorlag, weil von dem Beklagten keinerlei Informationen zur Verarbeitung personenbezogener Daten bereitgestellt worden seien.

Bezüglich der Abmahnfähigkeit von Datenschutzverstößen widersprach das OLG dem LG. Die Regelungen der DSGVO seien nicht generell abschließend. Vielmehr könne eine europäische Verordnung durch nationale Normen ergänzt werden, sofern diese nicht die unmittelbare Anwendbarkeit der Verordnung vereitelten.

Ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb (UWG) könne somit vorliegen, da es sich bei Art. 13 DSGVO um eine Marktverhaltensregelung im Sinne des § 3a UWG handele.

Einen abmahnfähigen Datenschutzverstoß nahm das OLG daher an.

Hinweis:

Bisher gibt es jedoch noch kein höchstrichterliches Urteil zu der Frage, ob Datenschutzverstöße wettbewerbsrechtlich abgemahnt werden können. Solange dieses nicht vorliegt, ist nicht

abschließend geklärt wie es sich in solchen Fällen verhält. Bis dahin sollten Unternehmen jedenfalls darauf achten, dass sie die außenwirksamen Vorgaben der DSGVO gewissenhaft umsetzen um überhaupt schon der Gefahr einer kostenträchtigen Abmahnung aus dem Weg zu gehen.

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>