Hackerangriff: Haftung des Verantwortlichen entfällt nur im Ausnahmefall

Kommt es zu einem Datenleck oder Hackerangriff, können millionenfach personenbezogene Daten in die Hände Unbefugter gelangen, wie es im Juli 2019 bei der bulgarischen Nationalen Agentur für Einnahmen (NAP) erfolgte. Fraglich ist dann, ob und wie weit der datenschutzrechtlich Verantwortliche für einen entstandenen Schaden haftet. Der Generalanwalt beim EuGH legt einen weiten Maßstab an.

Wenn es zu einem unbefugten Zugang zu personenbezogenen Daten durch Dritte kommt, so haftet der Verantwortliche geschädigten Betroffenen nach den Maßstäben des Art. 82 DSGVO, auch für einen immateriellen Schaden in Form von Angst und Sorge wegen eines möglichen Datenmissbrauchs. Erforderlich ist, dass dieser Schaden tatsächlich nachgewiesen ist. An das Verschulden des Verantwortlichen will der Generalanwalt dabei keine hohen Anforderungen stellen und spricht gar von einem womöglich „vermuteten Verschulden", wobei unklar bleibt, ob dies tatsächlich der Fall sein soll (Rn. 73). Wir sehen für ein vermutetes Verschulden jedenfalls keinen Anhaltspunkt in Art. 82 DSGVO und auch der Generalanwalt äußert sich hier nicht klar (Generalanwalt Pitruzzella, Schlussanträge vom 27.04.2023 zur Rs. C-340/21).

Den Schlussanträgen zugrunde liegt der folgende Fall: Im Juli 2019 wurde in bulgarischen Medien bekannt gegeben, dass im Internet Steuer- und Sozialversicherungsdaten von Millionen bulgarischen Bürgern und Bürgerinnen im Internet veröffentlicht wurden. Diese hatte sich ein Unbefugter mittels eines Hackerangriffs auf das Informationssystem der Nationalen Agentur beschafft. In einer Klage gegen die Agentur verlangte die Klägerin Schadensersatz aufgrund der Angst und Befürchtung, zukünftig einen Datenmissbrauch zu erleiden. Im Rahmen dieser Klage legte das Gericht dem EuGH einige Vorlagefragen zur Klärung vor. Darunter fand sich auch die Frage, ob eine Befürchtung, in Zukunft einen Missbrauch von personenbezogenen Daten zu erleiden, einen immaterieller Schaden

i.S.d. Art. 82 DSGVO darstellt und wer die Beweislast dafür trägt, dass geeignete Maßnahmen zum Schutz der personenbezogenen Daten getroffen wurden.

Schaden: Die Befürchtung, dass ein Missbrauch von personenbezogenen Daten erfolgen wird, kann dann einen immateriellen Schaden nach Art. 82 Abs. 1 DSGVO darstellen, wenn die betroffene Person nachweisen kann, dass sie tatsächlich einen realen und sicheren emotionalen Schaden erlitten hat. Es reiche demnach nicht aus, wenn die betroffene Person lediglich verärgert ist.

Mit dem Verlust der Daten und der damit vorliegenden Datenpanne lag auch ein tatbestandlicher DSGVO-Verstoß vor. Fraglich war allerdings, ob der Verantwortliche diesen auch zu verschulden hatte.

Zur Frage, ob ein **Haftungsausschluss** in Betracht kommt, wenn der Datenverstoß von einem Dritten ausging, führt der Generalanwalt aus, dass dies für sich genommen keinen solchen Ausschluss begründen kann. Hierzu muss der Verantwortliche vielmehr nachweisen, dass er in keinerlei Hinsicht für den Verstoß verantwortlich ist. Im Kern kommt es damit darauf an, ob der Verantwortliche die Daten angemessen gesichert hat:

Bei angemessener Datensicherheit i.S.d. Art. 24, 32 DSGVO hat der Verantwortliche Schäden eines Hackerangriffs nicht zu verschulden und muss keinen DSGVO-Schadensersatz zahlen.

Wann aber liegt eine angemessene Datensicherheit vor?

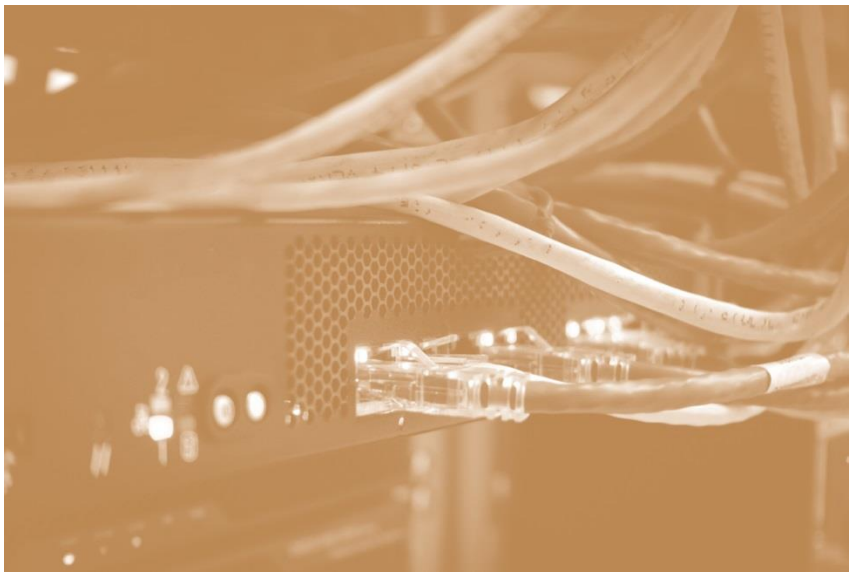
Der Generalanwalt stellt diesbezüglich fest, dass allein das Vorliegen einer Verletzung des Schutzes von personenbezogenen Daten nicht ausreicht, um festzustellen, ob die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten ungeeignet waren. Hierzu muss vielmehr eine Prüfung des Einzelfalles stattfinden, in der die konkreten Maßnahmen, deren Umsetzung unter Berücksichtigung der technischen Möglichkeiten und die Interessen der Betroffenen zu beachten sind.

Weiter stellt der Generalanwalt fest, dass die Beweislast, ob die ergriffenen Maßnahmen geeignet waren, beim Verantwortlichen liegt. Dies folgt vor allem aus dem Umstand, dass es dem Betroffenen aufgrund des Informationsdefizits nicht möglich sei, die

Ungeeignetheit nachzuweisen. Die zulässigen Beweismittel und deren Beweiskraft sind von den nationalen Gerichten zu bestimmen. Im deutschen Recht wird hier das Institut der sekundären Beweislast zur Anwendung kommen können: Der Betroffene weist die Anknüpfungstatsachen nach – der Verantwortliche und potentielle Anspruchsgegner muss sich dann entlasten.

Es ist offen, ob der EuGH der Entscheidung folgt. Sie hat das Potential zur erheblichen Sicherheit für die Unternehmen, die Opfer von Hackerangriffen geworden sind. Allerdings bringt sie auch klare Lasten mit sich: Der Verantwortliche muss letztlich darlegen, dass er angemessene technische und organisatorische Maßnahmen implementiert hatte und es dennoch zu dem Angriff kam. Das erfordert eine umfassende Dokumentation (und natürlich entsprechende Vorarbeit in puncto Datensicherheit).

Letztere, die IT-Sicherheit, wird ohnehin zunehmend wichtig und zur Managementaufgabe: Der Cyber-Vorstand muss seiner neuen Rolle gerecht werden. Mehr dazu lesen Sie, unabhängig von der vorstehenden EuGH-Rechtsprechung, unter https://www.deutscheranwaltspiegel.de/anwaltspiegel/cybersecurity/cybersecurity-ist-c-level-aufgabe-31306/ und https://www.boersen-zeitung.de/recht-kapitalmarkt/was-der-cyber-vorstand-leisten-sollte



Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de