LOSCHELDER

Newsletter Datenschutzrecht
Dezember 2024

Sehr geehrte Damen und Herren,

der BGH hat zum Ende des Jahres noch einmal richtig Schwung in die datenschutzrechtliche Diskussion zum Schadensersatz nach Art. 82 DSGVO gebracht. Bereits in unserem November-Newsletter haben wir über die Leitentscheidung im sog. Scraping-Komplex (Urteil vom 18.11.2024 – VI ZR 10/24) berichtet, in dem es um immateriellen Schadensersatz wegen eines DSGVO-Verstoßes geht.

Nun liegen die vollständigen Urteilsgründe vor. Die Entscheidung hat weitreichende Auswirkungen, die wir mit Ihnen intensiv diskutieren möchten in unserem letzten Lunch@Loschelder Webinar in diesem Jahr:

BGH-Urteil zum Facebook-Datenleck - Tasche auf bei jeder Datenpanne?

Das Urteil des Bundesgerichtshofs vom 18.11.2024 zum sog. Scraping hat eine riesen Welle ausgelöst. Das mediale Echo zu dieser Entscheidung hallte unisono: Schadensersatzklagen von Verbrauchern sind nun ein Elfmeter ohne Torwart. Doch sind Unternehmen nun wirklich bei **jeder** Datenpanne zum Schadensersatz verpflichtet?! Wir meinen: So einfach ist das bei Weitem nicht!

Gemeinsam blicken wir genau auf die Voraussetzungen des immateriellen Schadensersatzes nach Art. 82 DSGVO und erläutern wie Unternehmen sich zeitlich vor und nach einem (potentiellen) Datenschutzverstoß aufstellen können.

Donnerstag, den 12. Dezember 2024 – 12:00 bis 12:45 Uhr
Ihre Referenten: Rebecca Moßner / Dennis Pethke, LL.M.

Alle Webinare bieten wir kostenfrei an und freuen uns über Ihre Anmeldung unter webinare@loschelder.de. Das Webinar findet über Teams statt, der Einladungslink wird rechtzeitig vor der Veranstaltung bereitgestellt.

Wir freuen uns über Ihr Interesse und Ihre Anmeldung!

Die Rechtsprechung zum Scraping-Urteil nehmen wir zum Anlass, auch eine Entscheidung des Bundessozialgerichts zu den Voraussetzungen des Schadensersatzanspruchs nach Art. 82 DSGVO näher zu beleuchten, die sich wunderbar in die aktuelle Diskussion einfügt.

Das Newsletter-Jahr schließen wir zudem mit einem weiteren Dauerbrenner der Datenschutz-Welt: dem „Recht auf Vergessenwerden“. Wir legen für Sie anhand zweier aktueller Entscheidungen des BGH und des EuGH dar, welche Voraussetzungen für den Löschungsanspruch gem. Art. 17 DSGVO vorliegen müssen. Selbst bei Vorliegen eines Rechtfertigungsgrunds für die Datenverarbeitung nach Art. 6 DSGVO kann dieser begründet sein – vielleicht müssen dafür aber auch erst 20 Jahre ins Land gehen.

Was passiert, wenn eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten nicht mehr besteht und diese dennoch gespeichert werden, musste ein Unternehmen in Hamburg nun auf sehr unangenehme Weise lernen: in Form eines Bußgelds in Höhe von 900.000 Euro. Auch hierüber berichten wir!

Spannend ist es zurzeit nicht nur beim Thema Datenschutz. Das deutsche Umsetzungsgesetz zur NIS-2-Richtlinie nimmt Formen an. Wir haben uns den Entwurf angeschaut und stellen Ihnen die wichtigsten Neuerungen und unsere Handlungsempfehlungen für Unternehmen vor. Dabei wird klar: In vielen Unternehmen besteht dringender Updatebedarf. Und: Dies gilt auch vor dem Hintergrund des frühzeitigen Endes der aktuellen Legislaturperiode. Die Umsetzung muss im kommenden Jahr erfolgen, die EU-Kommission hat wegen der verzögerten Umsetzung ins nationale Recht bereits ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet. Eigentlich hätte die NIS-2-Richtlinie bis zum 17.10.2024 umgesetzt werden müssen.

Zu guter Letzt, bedanken wir uns für Ihr Interesse auch in diesem Jahr, wünschen Ihnen eine fröhliche Weihnachtszeit im Kreis Ihrer Liebsten und einen fulminanten Start in ein 2025, das hoffentlich wieder mehr gute Nachrichten bringt!

Inhalt

BSG-Urteil: Nicht jeder Kontrollverlust ist ein nach der DSGVO ersatzfähiger Schaden

Im September durfte sich auch das Bundessozialgericht (BSG) mit den Voraussetzungen des datenschutzrechtlichen Schadensersatzes nach Art. 82 DSGVO beschäftigen. Dass auch der Verlust der Kontrolle über personenbezogene Daten einen Schaden darstellen kann, ist spätestens seit einer EuGH-Entscheidung aus Dezember 2023 kein Geheimnis mehr. Neu nach der Entscheidung des BSG ist aber, dass dieser Kontrollverlust nicht schon dann gegeben ist, wenn bloß verspätet Auskunft über eine Datenverarbeitung erteilt wird. In diesem Fall muss eine begründete Befürchtung für einen Datenmissbrauch bestehen.

Schadensersatzklagen nach Art. 82 DSGVO werden mehr und mehr zum „Daily Business" der deutschen Gerichte. Die Voraussetzungen, um hiermit Erfolg zu haben, wirken auf den ersten Blick eher gering. Die Vorschrift fordert ausdrücklich nur einen DSGVO-Verstoß und einen daraus resultierenden Schaden der betroffenen Person. Diese unkonkrete Formulierung macht es immer wieder erforderlich, dass sich Gerichte mit den Voraussetzungen des Art. 82 DSGVO im Detail auseinandersetzen.

Klage wegen verspäteter Auskunft

Ende September befasste sich das BSG mit einem Fall, in dem Schadensersatz wegen einer verspäteten Auskunftserteilung nach Art. 15 DSGVO verlangt wurde (Urteil vom 24.09.2024, Az. B 7 AS 15/23 R).

Der Kläger bezog mehrere Jahre lang Arbeitslosengeld vom Jobcenter. Im Juli 2019 forderte er dort Auskunft über seine verarbeiteten, personenbezogenen Daten. Diese Auskunft erhielt der Kläger erst nach mehreren Aufforderungen im Februar 2020. Die Frist für die Auskunftserteilung beträgt in der Regel maximal einen Monat. Das Jobcenter hatte diese hier deutlich überschritten. Der Kläger behauptete, während der Wartezeit auf seine Auskunft die Kontrolle über seine personenbezogenen Daten verloren zu haben. Diesen Kontrollverlust wolle er als immateriellen Schaden nach Art. 82 DSGVO ersetzt bekommen.

Kontrollverlust als Schaden

Dass ein Kontrollverlust über die eigenen personenbezogenen Daten einen Schaden begründen kann, wurde bereits mehrfach gerichtlich bestätigt (siehe dazu bereits unsere Beiträge aus Oktober 2024 und Dezember 2023). Im vorliegenden Fall lag die entscheidende Frage jedoch darin, ob hier überhaupt ein Kontrollverlust des Klägers vorlag. Das hat das BSG im Ergebnis verneint.

Um einen ersatzfähigen Schaden annehmen zu können, reicht ein bloßer Verstoß gegen eine Vorgabe aus der DSGVO noch nicht aus. Es muss irgendein – materieller oder immaterieller – Schaden tatsächlich eingetreten sein. Dabei gibt es keine Erheblichkeitsschwelle, die überschritten werden muss. Der Kläger muss den Schaden jedoch beweisen.

Nur bei begründeter Befürchtung des Datenmissbrauchs

Zwar ist der Kontrollverlust über personenbezogene Daten grundsätzlich geeignet, einen ersatzfähigen Schaden zu begründen. Für das Vorliegen des Kontrollverlusts genügt jedoch nicht schon jede Ungewissheit über den Verbleib der eigenen personenbezogenen Daten für einen bestimmten Zeitraum. Das BSG hat klargestellt, dass ein Kontrollverlust nur dann anzunehmen ist, wenn „die betroffene Person die begründete Befürchtung hegt, dass einige ihrer personenbezogenen Daten künftig von Dritten weiterverbreitet oder missbräuchlich verwendet werden“ (Rn. 31). Das rein hypothetische Risiko für einen Datenmissbrauch kann nicht als ausreichend angesehen werden. Mehr als dieses hypothetische Risiko konnte hier allerdings nicht festgestellt werden und wurde auch nicht vom Kläger vorgebracht. Zwar hatte der Kläger über mehrere Monate keine Auskunft über seine Daten erhalten. In dieser Zeit befanden sich die Daten jedoch beim Jobcenter und es gab kein konkretes Risiko einer missbräuchlichen Verwendung. Die bloße verspätete Auskunft führt für sich genommen noch nicht zu einem Kontrollverlust.

Das Urteil verdeutlicht also: Es bedarf im Einzelfall konkreter Anhaltspunkte für einen tatsächlichen Kontrollverlust. Andernfalls wäre der Schadensersatzanspruch bei jeglicher Ungewissheit über den aktuellen Verbleib der eigenen personenbezogenen Daten oder in jedem Fall verspäteter Auskunftserteilung begründet. Dies würde selbst angesichts des hohen Schutzniveaus in Bezug auf

personenbezogene Daten in der EU über das Ziel hinausschießen. Und dieses Ergebnis hat auch nach der BGH-Entscheidung im Scraping-Komplex noch Bestand, denn dort sind die Anforderungen an den Schadensnachweis nur für den Fall gesenkt, in dem es tatsächlich zu einem Kontrollverlust gekommen ist. Mehr dazu besprechen wir in unserem Webinar am 12.12.2024, zu dem Sie hier weitere Informationen finden!

Aktuelle Entwicklungen zum „Recht auf Vergessenwerden“: BGH und EuGH konkretisieren Löschungsanspruch

Der Löschungsanspruch gem. Art. 17 DSGVO ist ein wichtiges, wenn nicht sogar das zentrale Betroffenenrecht in der DSGVO. Es soll dem Betroffenen das Bestimmungsrecht über seine personenbezogenen Daten erhalten. Wie weit dieses sog. „Recht auf Vergessenwerden“ in der Praxis reicht, zeigen zwei aktuelle Entscheidungen des BGH und des EuGH.

Art. 17 Abs. 1 DSGVO regelt sowohl das subjektive Recht der betroffenen Person auf unverzügliche Löschung ihrer personenbezogenen Daten als auch die objektive Pflicht des Verantwortlichen zur Löschung, sofern ein entsprechender Löschungsgrund vorliegt: Zweckerreichung, Widerruf der Einwilligung, Widerspruch, unrechtmäßige Verarbeitung, rechtliche Verpflichtung, Minderjährigkeit. Wenn der Verantwortliche personenbezogene Daten öffentlich gemacht hat, trifft ihn im Falle

eines begründeten Löschungsverlangens zudem eine Informationspflicht gegenüber anderen Verantwortlichen, die Daten des Betroffenen verarbeiten (Art. 17 Abs. 2 DSGVO). Auch diese müssen zur effektiven Durchsetzung des „Rechts auf Vergessenwerden“ über das Löschungsbegehren informiert werden. Diese Pflicht wird vor allem mit Blick auf den uferlosen Adressatenkreis im Internet relevant. Bei Online-Veröffentlichungen muss der Verantwortliche etwa auch die Anbieter der wichtigsten Suchmaschinen von dem Löschungsverlangen in Kenntnis setzen. Unter bestimmten Voraussetzungen können Löschungs- und Informationspflicht ausgeschlossen sein. Hierbei läuft es regelmäßig auf eine Abwägungsentscheidung hinaus: Überwiegt das Interesse des Verantwortlichen bzw. das öffentliche Interesse an der weiteren Datenverarbeitung das Interesse des Betroffenen an seiner Privatsphäre?

Sowohl der BGH als auch der EuGH haben die Voraussetzungen und den Umfang des „Rechts auf Vergessenwerden“ in zwei aktuellen Entscheidungen weiter konkretisiert.

BGH: Unbeschränkter Abruf von Daten im Internet nach 20 Jahren nicht mehr verhältnismäßig

Im Juni 2024 hat der BGH (Beschluss vom 04.06.2024, Az. II ZB 10/23) entschieden, dass ein Vereinsvorstandsmitglied fast 20 Jahre nach seinem Ausscheiden aus dem Amt gegen das Registergericht einen Anspruch auf Löschung seiner im Vereinsregister eingetragenen personenbezogenen Daten hat. Diese waren bis dahin im Registerportal im Internet für jeden einsehbar.

Der BGH stützte den Löschungsanspruch in diesem Fall auf Art. 17 Abs. 1 lit. d DSGVO. Danach besteht ein Löschungsanspruch, wenn personenbezogene Daten unrechtmäßig verarbeitet werden. Unrechtmäßig ist eine Verarbeitung nicht nur, wenn überhaupt keine Rechtsgrundlage für die Datenverarbeitung vorliegt, sondern auch dann, wenn ihre Grenzen oder Vorgaben im Einzelfall nicht eingehalten werden. Letzteres sah der BGH im Fall des ehemaligen Vereinsvorstandsmitglieds gegeben: Grundsätzlich greife zwar der Rechtfertigungsgrund des Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO ein, da u. a. aus §§ 55a, 79 Abs. 1–4 BGB die rechtliche Verpflichtung folge, die im Vereinsregister gespeicherten Daten ehemaliger Vorstandsmitglieder im Internet über das Registerportal zu veröffentlichen. Allerdings greife vorliegend die Grenze des Art. 6

Abs. 3 S. 4 DSGVO ein. Die Verpflichtung zur unbeschränkten Abrufbarkeit der Daten im Internet über das Registerportal steht *nicht mehr* in einem angemessenen Verhältnis zu dem mit der Veröffentlichungspflicht verfolgten Ziel, die Rechtssicherheit und den Schutz der Lauterkeit und Leichtigkeit im Rechtsverkehr mit eingetragenen Vereinen zu gewährleisten.

Der BGH begründet dies vor allem mit der zeitlichen Komponente. Er führt aus, dass das Informationsinteresse der Öffentlichkeit an den im Vereinsregister gespeicherten Daten nicht ohne Weiteres mit dem Ausscheiden eines Vorstandsmitglieds aus dem Amt entfalle. Maßgeblich sei der Einzelfall und insbesondere die Länge des seitdem verstrichenen Zeitraums. Jedenfalls nach 20 Jahren überwiegen laut BGH die Rechte des ehemaligen Vorstandsmitglieds auf Schutz seiner personenbezogenen Daten (Art. 8 GRCh) und auf Achtung des Privat- und Familienlebens (Art. 7 GRCh) das öffentliche Informationsinteresse an unbeschränkter Einsicht in die personenbezogenen Daten des ehemaligen Vorstandsmitglieds. Zulässig bleibt laut BGH jedoch auch nach 20 Jahren ein Bereitstellen der Daten im Einzelfall bei Darlegung eines berechtigten Interesses.

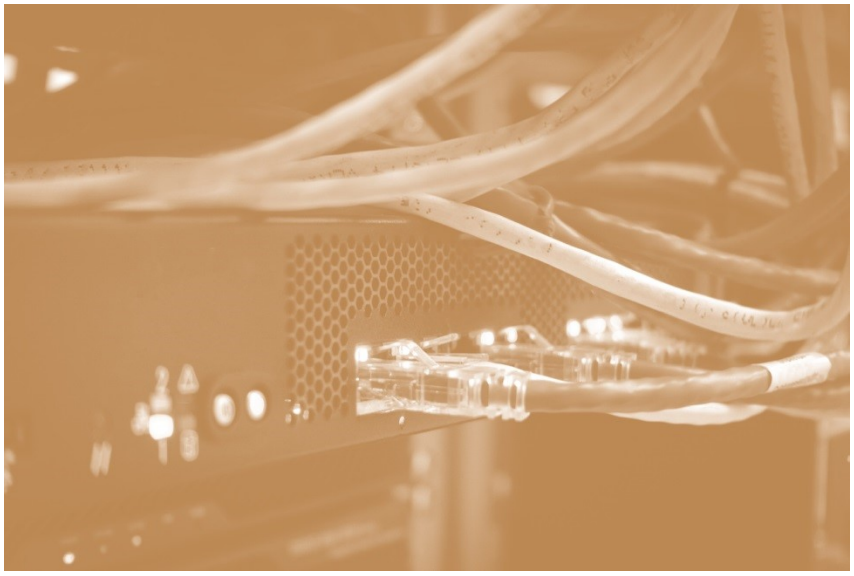
EuGH: Umfang des Löschungsanspruchs richtet sich nach Erforderlichkeit der Daten

Der EuGH hatte in einem Vorabentscheidungsverfahren (C-200/23) die Frage zu beantworten, ob personenbezogene Daten, die im Internet veröffentlicht wurden und nach gesetzlichen Offenlegungspflichten nicht erforderlich sind, gem. Art. 17 DSGVO gelöscht werden müssen. Dies bejahte der EuGH im Falle einer bulgarischen Gesellschafterin, die gegen eine Handelsregister-veröffentlichung im Internet durch die zuständige Behörde klagte. Veröffentlicht wurde dort unter anderem eine ungeschwärzte Version des Gesellschaftsvertrages. Diese Version enthielt Namen, Vornamen, die Identifikationsnummer, die Nummer des Personalausweises, das Datum und den Ort der Ausstellung dieses Ausweises sowie die Anschrift der Gesellschafterin und ihre Unterschrift. Das bulgarische Handelsrecht schreibt eine Veröffentlichung des Gesellschaftsvertrages vor. Diese muss aber nur den Namen und die Identifikationsnummer der Gesellschafter enthalten. Die Veröffentlichung weiterer Daten ist gesetzlich nicht erforderlich.

Der EuGH entschied nun: Soweit die Veröffentlichung personenbezogener Daten nach dem Gesetz nicht zwingend vorgeschrieben ist, stehe dem Betroffenen ein Löschungsanspruch aus Art. 17 DSGVO in Bezug auf eine für jedermann zugängliche Internetveröffentlichung zu. Nicht erforderliche personenbezogene Daten seien im Zweifel zu schwärzen. In seiner Antwort bestätigt der EuGH seine **Prüfreihenfolge** für einen Löschungsanspruch gem. Art. 17 DSGVO:

In einem ersten Schritt sei festzustellen, auf welcher Rechtsgrundlage gem. Art. 6 DSGVO die Verarbeitung der personenbezogenen Daten des Betroffenen erfolgt sei. Davon hinge in einem zweiten Schritt der Umfang des Löschungsanspruchs ab: Fehle es an einer Rechtsgrundlage, so habe der Betroffene einen Löschungsanspruch aus Art. 17 Abs. 1 lit. d DSGVO. Für den Fall, dass ein Rechtfertigungsgrund vorliege, seien die übrigen Löschungstatbestände des Art. 17 DSGVO zu prüfen. Bei diesen komme es laut EuGH im Endeffekt immer auf eine Abwägung an: Die Interessen des Verantwortlichen bzw. die öffentlichen Interessen seien stets mit den Grundrechten des Betroffenen auf Achtung des Privatlebens (Art. 7 GRCh) und auf Schutz personenbezogener Daten abzuwägen (Art. 8 GRCh).

Daraus folge – wie der EuGH bereits in der Vergangenheit entschieden hat –, dass es im Einzelfall aus überwiegenden und schutzwürdigen Gründen, die sich aus dem konkreten Fall der betroffenen Person ergeben, gerechtfertigt sein könne, den Zugang zu personenbezogenen Daten, die nach dem Unionsrecht offenlegungspflichtig sind, auf Dritte zu beschränken, die ein besonderes Interesse nachweisen. Erst recht müsse dies in Fällen gelten, in denen die Veröffentlichung der personenbezogenen Daten, wie hier in Bulgarien, weder nach Unionsrecht noch nach dem nationalem Recht erforderlich ist.



Verstoß gegen die Löschpflicht: Unternehmen muss Bußgeld in Höhe von 900.000 Euro zahlen

Es genügt nicht, das fein ausgetüftelte Löschkonzept bloß in der Schublade aufzubewahren. Es muss auch umgesetzt werden, sonst drohen im Zweifel hohe Bußgelder. Diese Lektion musste im vergangenen Monat ein Hamburger Dienstleister aus dem Forderungsmanagement lernen. Er bewahrte personenbezogene Daten trotz abgelaufener Löschfrist bis zu fünf weitere Jahre auf. Die hamburgische Datenschutzaufsichtsbehörde verhängte aufgrund dessen gegen ihn ein Bußgeld in Höhe von 900.000 Euro.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) prüfte im Rahmen einer Schwerpunktprüfung marktstarke Unternehmen aus dem Forderungsmanagement. Bei den personenbezogenen Daten, die in dieser Branche verarbeitet werden, handelt es sich um kritische Daten, die oft auch an Auskunfteien und Adressermittlungsdienste weitergegeben werden. Insofern ist es von besonderer Bedeutung, dass die betreffenden Daten so auch verarbeitet werden dürfen und richtig sind. Diesen Umstand nahm der HmbBfDI zum Anlass, ganz unabhängig von individuellen Beschwerdefällen im Rahmen einer Schwerpunktprüfung zu kontrollieren, wie die Daten der Schuldnerinnen und Schuldner bei den jeweiligen Dienstleistern aufbewahrt und verarbeitet werden. Und er wurde fündig…

Wie fiel der Verstoß auf?

Ausführliche Fragebögen gaben der Aufsichtsbehörde ein umfassendes Bild der Datenhaltung in den jeweiligen Unternehmen. Unterlagen aus dem Bereich der Datenschutz-Dokumentation, wie Verzeichnisse von Verarbeitungstätigkeiten, Auflistungen der Sicherheitsmaßnahmen und Musterschreiben brachten noch mehr Licht ins Dunkel. In vielen Fällen werden derartige Fragebögen in einer Form verschickt, die nicht zwingend beantwortet werden müssen. Es sollte aber stets abgewogen werden, ob eine Beantwortung nicht sinnvoll ist, da Auskunftsrechte der Behörden bestehen und diese die Fragen daher auch in anderer, zwangsweise durchsetzbarer Form adressieren könnten.

In einigen Fällen entschied der HmbBfDI sich in der vorliegenden Schwerpunktprüfung, über die Auswertung der Antworten hinaus für Vor-Ort-Prüfungen in den Geschäftsräumen der Unternehmen.

Just bei einem solchen Besuch stellten die Hamburger-Datenschützer fest, dass Datensätze trotz der abgelaufenen Löschfrist bis Mitte November 2023 und damit bis zu fünf Jahre über die Löschfrist hinaus weiter aufbewahrt wurden.

Ergebnis der Prüfung

Für die Speicherung personenbezogener Daten bedarf es nach Art. 6 Abs. 1 DSGVO stets einer Rechtsgrundlage. Außerdem gelten für Datenverarbeitungen die Grundsätze der „**Rechtmäßigkeit**“ und der „**Zweckbindung**“: Die Daten dürfen nur auf rechtmäßige Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DSGVO) und insbesondere nur für einen festgelegten, eindeutigen und legitimen Zweck (Art. 5 Abs. 1 lit. b DSGVO). Der Zweck für die Speicherung war im vorliegenden Fall entfallen, die Aufbewahrungsfrist war abgelaufen und damit auch eine Rechtsgrundlage für die Speicherung nicht mehr vorhanden.

Das besondere Ausmaß der unerlaubten Datenspeicherung führte sodann zu dem hohen Bußgeldbetrag von 900.000 Euro: Das Unternehmen speicherte eine sechsstellige Zahl von Datensätzen ohne Rechtsgrundlage und dies teilweise noch fünf Jahre nach Ablauf der gesetzlichen Aufbewahrungsfrist.

So schlecht fiel das Ergebnis übrigens nicht bei allen geprüften Unternehmen der Branche aus: In den überwiegenden Fällen konnte

ein hohes Maß an Professionalität und Sensibilität festgestellt werden, insbesondere im Hinblick auf aussagekräftige Auskünfte nach Art. 15 DSGVO und Prozesse zur fristgerechten Auskunftserteilung. Auch das betroffene Unternehmen zeigte sich einsichtig und ließ sich auf eine Kooperation mit der Behörde ein. Das Lehrgeld muss es dennoch zahlen: Der Bußgeldbescheid ist mittlerweile rechtskräftig.

Neues IT-Sicherheitsrecht – Updates in vielen Unternehmen dringend notwendig

Die CrowdStrike-Panne hat gezeigt: In Sachen Cybersicherheit in Unternehmen ist an vielen Stellen noch Luft nach oben. Die durch die Panne eingetretenen Betriebsstörungen haben bereits nach kurzer Zeit wirtschaftliche Schäden verursacht. Um solche Vorfälle möglichst zu verhindern bzw. ein effektives Vorgehen im Falle eines Cyber-Incidents sicherzustellen, wurde auf EU-Ebene Ende 2022 eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) beschlossen. Der Entwurf eines deutschen Umsetzungsgesetzes enthält weitreichende Pflichten für einen großen Kreis von Unternehmen. Ob dieser Entwurf vor dem Hintergrund des Ampel-Aus noch vor den Neuwahlen im Frühjahr 2025 beschlossen wird oder ob uns in der neuen Legislaturperiode ein neuer Entwurf erwartet, bleibt abzuwarten. Fest steht jedoch: Der Schutz vor Cybersicherheitsvorfällen ist auch schon jetzt wichtiger denn je. Mit einer Umsetzung der NIS-2-Richtlinie ist auch zeitnah zu rechnen, zumal die EU-Kommission wegen der verzögerten Umsetzung bereits ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet hat. Mit der Vorbereitung auf neue Pflichten kann nicht früh genug begonnen werden.

Am 19. Juli 2024 führte ein fehlerhaftes Update beim Cybersicherheitsdienstleister CrowdStrike zu weltweiten Ausfällen von IT in Unternehmen. Fast 50 % der betroffenen Unternehmen mussten in der Folge ihren Betrieb zeitweise einstellen. Server sind ausgefallen, Flüge wurden gestrichen und Beschäftigte nach Hause geschickt. Die Störungen wurden teilweise als „gravierend für die deutsche Wirtschaft“ bezeichnet. Das geht aus einer Befragung einiger der betroffenen Unternehmen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Digitalverband Bitkom hervor.

Als Reaktion auf diesen Cybersicherheitsvorfall ergriffen die befragten Unternehmen verschiedene Maßnahmen. Darunter die Erstellung bzw. Verbesserung ihres IT-Notfallplans, die Durchführung von Schulungen aber auch technische Maßnahmen wie Updates und Backups. 20 % der Unternehmen gaben an, in Zukunft ihre Kriterien bei der Auswahl von IT-Sicherheitsanbietern zu verändern. Einzelne Unternehmen wechselten ihre IT-Sicherheitsanbieter bereits.

Nicht nur diese Crowdstrike-Panne zeigt, wie dringend in vielen Unternehmen Anpassungsbedarf beim Thema Cybersicherheit besteht. Auch der aktuelle BSI-Lagebericht 2024 hat erneut deutlich gemacht, dass die Sicherheitslage besorgniserregend ist. Aus gutem Grund werden daher bald für viele Unternehmen IT-Sicherheitsmaßnahmen gesetzlich verpflichtend. Die Umsetzung der NIS-2-Richtlinie befindet sich in Deutschland derzeit in Arbeit. Im Entwurf eines Umsetzungsgesetzes, das im Wesentlichen eine Neufassung des Gesetzes über das Bundesamt für Informationssicherheit (BSIG) ist, finden sich zahlreiche neue Sicherheitspflichten. Wesentlich ist die Sicherstellung angemessener Risikomanagementmaßnahmen, mit denen Systemstörungen vermieden und Auswirkungen von Sicherheitsvorfällen möglichst gering gehalten werden. Diese sind von der Geschäftsleitung zu überwachen. Dazu kommen Registrierungspflichten und Meldepflichten bei Sicherheitsvorfällen. Bei Verstößen drohen hohe Bußgelder.

Adressiert werden zudem insgesamt deutlich mehr Unternehmen, denn bisher richtete sich das BSIG nur an Betreiber kritischer Infrastrukturen, sog. KRITIS. In Zukunft können auch mittlere bis große Unternehmen von den Regelungen betroffen sein, sofern sie in den einschlägigen Sektoren tätig sind. Sie werden in „besonders wichtige“ und „wichtige Einrichtungen“ aufgeteilt. Neben den Sektoren spielen auch Mitarbeiterzahl sowie Jahresumsatz eine Rolle bei der Bestimmung, welche Pflichten genau gelten. Beispielsweise gelten nach dem BSIG-Entwurf Unternehmen, die in bestimmten Sektoren tätig sind, schon ab 50 Mitarbeitern oder einem Jahresumsatz von über zehn Mio. Euro als „wichtige Einrichtungen“. An dem deutlich weiteren Anwendungsbereich wird sich auch durch einen neuen Entwurf in einer neuen Legislaturperiode nichts ändern, denn diesen schreibt die NIS-2-Richtlinie verpflichtend vor. Die vielen Betroffenheitsanalysen, die wir für unsere Mandanten durchführen, zeigen eines deutlich: Es sind nicht nur Unternehmen betroffen, deren Ausfall vom Durchschnittsbürger als „gesellschaftlich kritisch“ angesehen wird. Durch die weiten Definitionen, die auf die statistische Klassifizierung der Wirtschaftszweige abstellen, sind auch etliche in der allgemeinen Wahrnehmung als weniger kritische Bereiche eingeschätzte Sektoren erfasst, etwa alle Bereiche des Maschinenbaus oder jegliche Verwalter von IT-Systemen („Managed Service Providers“).

Sicherheitspflichten beziehen sich nun insbesondere auch auf die Lieferkette. Die Risikomanagementmaßnahmen eines von der NIS-2-Richtlinie erfassten Unternehmens müssen auch die „Sicherheit der Lieferkette“ umfassen (Art. 21 Abs. 2 lit. d) NIS-2-Richtlinie). Daher sollte sichergestellt werden, dass auch für beliefernde Unternehmen Sicherheitsanforderungen (vertraglich) geregelt werden, sog. „Cyber-Supply Chain Risk Management“.

Doch wie ist das in der Praxis umsetzbar? Primär bedarf es einer Bedarfsanalyse und der Verteilung von Zuständigkeiten im Unternehmen. Gegebenenfalls müssen vorhandene Sicherheitssysteme überarbeitet werden. Vor allem aber muss zukunftsorientiert gedacht werden: langfristige Cybersecurity-Strategien und regelmäßige Sicherheitsaudits sind unerlässlich, um die sich ständig entwickelnden rechtlichen Rahmenbedingungen einhalten zu können. Je nach Größe des Unternehmens können dabei Arbeitsgruppen erstellt, externe Berater hinzugezogen oder Rechts- und IT-Abteilungen erweitert werden. Es muss klar sein, wie im Falle von Cyberangriffen zu reagieren ist, bevor es zu einem Angriff kommt, damit schnell die notwenigen Abhilfemaßnahmen wirksam getroffen und größere Schäden verhindert werden können.

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

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

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

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-337
rebecca.mossner@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