WILHELM

RECHTSANWÄLTE

Datenschutz

Die DSGVO – Schadenszenarien und Versicherungslösungen

www.wilhelm-rae.de

Januar 2019

WILHELM
RECHTSANWÄLTE

Von Frederic Neu

Datenschutz

Die DSGVO – Schadenszenarien und Versicherungslösungen

In Baden-Württemberg verhängte die Bußgeldstelle des Landesbeauftragten für den Datenschutz und die Informationssicherheit (LfDI) im November 2018 das erste Bußgeld in Deutschland nach der Datenschutz-Grundverordnung (DSGVO).

Ein Social-Media-Anbieter verstieß gegen die nach Artikel 32 DSGVO vorgeschriebene Datensicherheit, indem er notwendige Sicherheitsupdates zum Schutz seiner Nutzerdaten nicht rechtzeitig vornahm. Tausende Nutzerdaten wurden daraufhin von Hackern auf einer Filesharing-Plattform veröffentlicht. Daraufhin verhängte die Bußgeldstelle des LfDI ein Bußgeld in Höhe von EUR 20.000,00. Durch das Bußgeld und die aufgewendeten und avisierten Maßnahmen zur IT-Sicherheit erlitt das Unternehmen einen Gesamtschaden im sechsstelligen Bereich. Ob betroffene Nutzer zudem Schadensersatzansprüche gegen den Social-Media-Dienst geltend machen werden, ist noch nicht absehbar.

1. DIE DSGVO

Die DSGVO trat am 24. Mai 2016 in Kraft und ist seit dem 25. Mai 2018 anzuwenden. Mit gleichem Datum fasste der deutsche Gesetzgeber das Bundesdatenschutzgesetz (BDSG) zur Anpassung des Datenschutzrechts an die DSGVO und zur Umsetzung der Richtlinie (EU) 2016/680 der EU neu.

1.1 Was ist die DSGVO?

Die DSGVO ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Personenbezogene Daten sind hiernach Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen.

"Identifizierbar" ist eine Person dann, wenn sie direkt oder indirekt, vor allem mittels Zuordnung zu einer Kennung wie einem Namen, einer Telefonnummer, einer Emailadresse, Standortdaten oder anderen besonderen Merkmalen identifiziert werden kann.

Ziel der DSGVO ist neben dem Verbraucherschutz auch die Angleichung von Standards in der EU.

Die DSGVO enthält zahlreiche Regelungen, die den Verbraucherschutz stärken. Unternehmen haben inzwischen große Mengen an personenbezogenen Daten gespeichert, die sie immer besser und schneller auswerten, aber auch zueinander in Beziehung setzen können. Das wiederum ermöglicht es, umfassende Persönlichkeitsprofile zu erstellen und auf Vorlieben und Verhaltensweisen von Verbrauchern zurückzuschließen. Ein Thema, das sowohl Verbraucherschützer als auch die Gesetzgeber beschäftigt, weil hier unter Umständen auch Persönlichkeitsrechte verletzt werden.

1.2 Was ist das Ziel der DSGVO?

Mit der DSGVO gleicht die Europäische Union die Datenschutzregeln der Mitgliedsstaaten einander an. Unternehmen und Verbraucher können also in Zukunft darauf vertrauen, dass innerhalb der EU einheitliche Datenschutzstandards gelten. Die DSGVO gilt ebenfalls für Unternehmen mit Sitz außerhalb der EU, sofern diese Unternehmen Daten von Personen aus der EU verarbeiten oder eine Niederlassung in der EU haben (Artikel 3 DSGVO).

Neben der Angleichung der Standards ist das Ziel der DSGVO, den Bürgern die Hoheit über ihre persönlichen Daten soweit wie möglich zurück zu geben. Als Verbraucher, Kunden oder Nutzer sollen sie jederzeit über die Art und den Umfang ihrer bei Dritten gespeicherten personenbezogenen Daten Auskunft erlangen und eine Löschung dieser Daten verfügen können.

2. WESENTLICHE ÄNDERUNGEN IM DATENSCHUTZRECHT

Die DSGVO beinhaltet für Unternehmen wesentliche Änderungen des Datenschutzrechts. Sie müssen überprüfen, ob ihre bisherige Praxis der Erhebung und Verarbeitung personenbezogener Daten den strengen neuen Regelungen entspricht, also insbesondere betriebsintern ausreichende technisch-organisatorische Maßnahmen getroffen wurden und die Rechte der Betroffenen gewahrt sind.

2.1 Datensicherheit

Artikel 32 der DSGVO bestimmt nun den Grundsatz der Datensicherheit. Datenverarbeiter müssen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

2.2 Recht auf Vergessenwerden

Das Recht auf Vergessenwerden regelt Artikel 17 der DSGVO. Nutzer haben einen Anspruch auf die

Löschung oder Sperrung personenbezogener Daten, wenn für die Verwendung der Daten keine Berechtigung mehr vorliegt.

2.3 Einwilligung

Die Verarbeitung personenbezogener Daten ist generell verboten, so lange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder der Betroffene in die Verarbeitung eingewilligt hat.

Die grundsätzlichen Anforderungen an die Wirksamkeit einer rechtsgültigen Einwilligung regelt Artikel 7 der DSGVO. Die Einwilligung muss freiwillig, für einen konkreten Fall, nach ausreichender Information des Betroffenen und unmissverständlich abgegeben werden. Damit eine Einwilligung freiwillig ist, muss der Einwilligende eine echte Wahl haben. Zusätzlich gilt das sogenannte „Kopplungsverbot“. Hiernach darf ein Vertragsabschluss nicht von der Einwilligung zur Verarbeitung weiterer personenbezogener Daten abhängig gemacht werden, die für den Abschluss des Vertrags nicht erhoben werden müssen. Weiter muss die Einwilligung an einen oder mehrere bestimmte Zwecke gebunden sein. Diese Zwecke müssen dann ausreichend erläutert werden. Soll die Einwilligung die Verarbeitung von speziellen personenbezogenen Daten legitimieren, muss sie sich ausdrücklich auf diese beziehen. Der Einwilligende muss immer über die Möglichkeit zum Widerruf seiner Einwilligung aufgeklärt werden. Der Widerruf muss dabei genauso leicht möglich sein, wie die Abgabe der Einwilligungserklärung.

2.4 Bußgelder

Gemäß Artikel 83 DSGVO können Datenschutzaufsichtsbehörden Bußgelder bis zu einer Höhe von EUR 20 Mio. oder (bei Unternehmen) 4 Prozent des weltweiten Vorjahresumsatzes verhängen. Bislang lag die Obergrenze für Bußgelder bei EUR 300.000,00.

In der Vergangenheit reizten Datenschutzbehörden den Bußgeld-Rahmen nur sehr selten und bei dauerhaften Verstößen aus. Dies könnte sich jedoch mit der DSGVO ändern.

Die Obergrenze für Bußgelder erhöht die DSGVO deutlich.

2.5 Schadensersatz

Gemäß Art. 82 Abs. 1 DSGVO hat „jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, […] Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“ Auch immaterielle Schäden wie beispielsweise Reputationsverluste durch die Veröffentlichung kompromittierender Informationen sind demnach durch den Verantwortlichen zu ersetzen.

Die Pflichtverletzung des Verantwortlichen wird nach Artikel 82 DSGVO vermutet. Die Beweislastumkehr erleichtert die Geltendmachung der Ansprüche gegen Unternehmen auf Schadenersatz aufgrund Datenschutzverletzungen erheblich.

3. MÖGLICHE SCHADENSZENARIEN UND VERSICHERUNGSSCHUTZ

Verschiedene Szenarien können zu einem Verstoß gegen die DSGVO führen. Folgen dieser Verstöße können in Unternehmen signifikante Schäden verursachen. Denkbar sind hierbei insbesondere Bußgelder, Schadenersatzforderungen, Schadenminderungskosten und Rechtskosten.

Nicht immer sind Schäden aus DSGVO-Verstößen versicherbar.

Teilweise gewähren die bisher bereits bestehenden Versicherungspolicen Schutz für die durch Verstöße gegen die DSGVO eingetretenen Schäden. Teilweise haben Anbieter Versicherungsprodukte entwickelt um den neuen Haftungsrisiken zu begegnen. Aber nicht immer sind Schäden versicherbar.

Schadenszenario 1:

Ein mittelständisches Unternehmen betreibt eine Website. Die Datenschutzhinweise auf der Website entsprechen nicht den Vorgaben der DSGVO. Zudem ist die Verschlüsselung des Kontaktformulars nicht korrekt eingerichtet. Personenbezogene Daten werden dadurch nicht sicher an das Unternehmen übertragen. Ein Wettbewerber mahnt das Unternehmen erfolgreich ab.

Die Abmahnkosten sind nicht versichert. Gegebenenfalls anfallende Rechtsanwaltskosten können unter einer Rechtsschutzversicherung versichert sein. Das Unternehmen kann zudem prüfen, ob Dritte für den entstandenen Schaden haftbar zu machen sind. Sofern beispielsweise die Datenschutzhinweise von einem externen Datenschutzbeauftragten erstellt wurden oder die Programmierung der Verschlüsselung durch einen externen Programmierer erfolgte, so kann das Unternehmen Regress gegen diese nehmen. Die Dienstleister wiederum schützt ggf. ihre Berufs- bzw. Betriebshaftpflichtversicherung eingeschränkt (z.B. über die BBR-IT).

Schadenszenario 2:

Ein privater Krankenversicherer wird Ziel eines Hackerangriffs. Die vollständigen Gesundheitsdaten von rund 200.000 Versicherten gelangen in die Hände von Kriminellen. Das Unternehmen reagiert umgehend und kooperiert mit den Behörden. Ein externes IT-Spezialistenteam schließt die Sicherheitslücke innerhalb kurzer Zeit und verhindert den Abfluss weiterer Daten.

Aufgrund der umfassenden Kooperation und schnellen Reaktion des Krankenversicherers verhängt die zuständige Datenschutzbehörde ein Bußgeld in Höhe von nur EUR 50.000,00 und bleibt damit weit unter dem möglichen Höchstsatz. Die IT-Spezialisten rechnen einen vergleichbaren Betrag ab. Mehrere tausend Versicherte verlangen zudem Schadensersatz im jeweils vierstelligen Bereich von ihrem Krankenversicherer. Sie begründen dies mit der hohen Sensibilität der verlorenen Daten. Das Unternehmen sieht sich in

der Summe einem hohen Millionenschaden ausgesetzt.

Das verhängte Bußgeld ist in Deutschland nach überwiegender Auffassung nicht versicherbar. Die Kosten für die IT-Dienstleister können als Schadenminderungskosten unter einer bestehenden Cyberversicherung gedeckt sein. Auch die Haftungsansprüche der geschädigten Dritten sowie die Anwalts- und Gerichtskosten für die Verteidigung wären ggf. unter der Cyberversicherung oder einer angepassten Betriebshaftpflichtversicherung gedeckt (eine rein AHB-basierte Betriebshaftpflichtversicherung bietet nur unzureichenden Versicherungsschutz, vgl. den Ausschluss von IT-Risiken gemäß Ziff. 7.15 AHB 2008/2016).

Schadenszenario 3:

Ein Handelsunternehmen, das einen großen Online-Shop betreibt, wird Ziel eines Cyberangriffs. Rund eine Million Kundendaten, darunter Kreditkarteninformationen, gehen verloren. Das Bußgeld, Schadensersatzansprüche von Geschädigten und IT-Kosten belaufen sich auf rund EUR 2 Mio. In der Schadenregulierung stellt sich heraus, dass die Sicherheitsmaßnahmen des Unternehmens unzureichend waren. Auf die Notwendigkeit weiterer Maßnahmen hatte die IT-Abteilung gegenüber der Geschäftsführung zuvor hingewiesen. Der zuständige Geschäftsführer hatte die erforderliche Investition jedoch hinausgezögert. Der Cyberversicherer kürzt seine Leistung aufgrund der fahrlässigen Herbeiführung des Versicherungsfalls um 80%.

Der Vermögensschaden des Unternehmens infolge der Leistungskürzung des Cyberversicherers sowie infolge des (nicht versicherbaren) Bußgelds kann aufgrund der Pflichtverletzung des Geschäftsführers einen Schadensersatzanspruch des Unternehmens gegen den Manager begründen. Ggf. wären Ansprüche des Unternehmens gegen den Geschäftsführer unter einer D&O-Versicherung gedeckt.

4. FAZIT

In Deutschland bestand bereits vor Inkrafttreten der DSGVO mit dem BDSG a.F. ein umfangreiches Datenschutzgesetz. Trotzdem führt die DSGVO nochmals zu erhöhten Risiken für Unternehmen. Diese umfassen die nun signifikant erhöhten Bußgelder, aber auch die höhere Exponierung gegenüber Schadenersatzansprüchen. Darüber hinaus können Unternehmen weitere Kosten im Rahmen der Schließung von Datenlecks und durch Rechtsverfolgungskosten entstehen.

Im Licht der DSGVO sollten Unternehmen bestehende Versicherungsprogramme überprüfen.

Unternehmen sollten daher ihre bestehenden Versicherungsprogramme an diese neuen Risiken anpassen. Oftmals gewähren die Betriebshaftpflicht- und D&O-Versicherungen Erweiterungen und Anpassungen an Datenschutz-Risiken. Darüber hinaus können Unternehmen speziell konzi-

pierte Cyber-Versicherungen abschließen, welche ausdrücklichen Schutz bei Verstößen gegen die DSGVO bieten sollten.

Diesen Beitrag veröffentlichte die Zeitschrift *Die Versicherungspraxis* in ihrer Ausgabe 01/2019.

Für Rückfragen steht Ihnen der Autor gern zur Verfügung:

Frederic Neu
Rechtsanwalt

WILHELM Partnerschaft von Rechtsanwälten mbB

Tel: +49 30 8172732-10
frederic.neu@wilhelm-rae.de

WILHELM

RECHTSANWÄLTE

Über uns:

Die Sozietät Wilhelm ist spezialisiert auf die Beratung von Unternehmen und deren Entscheidungsträgern in kritischen Situationen – vom Großschaden über die persönliche Inanspruchnahme bis hin zum Compliance-Verstoß im Unternehmen. Sechzehn Berufsträger an zwei Standorten (Düsseldorf und Berlin) vereinen hierfür Expertise aus den Bereichen Versicherung, Haftung, Wirtschaftsstrafrecht und Gesellschaftsrecht. Weltweit kooperiert die Sozietät mit Kanzleien unter anderem in Chicago, New York, London, Paris, Rom, Warschau und Brüssel. Mit seinen internationalen Kooperationspartnern bietet Wilhelm die Expertise zur Lösung grenzüberschreitender Haftungs- und Deckungsstreitigkeiten, M&A-Transaktionen sowie internationaler Großprojekte.

WILHELM Partnerschaft von Rechtsanwälten mbB

Düsseldorf:

Reichsstraße 43
40217 Düsseldorf

Telefon: + 49 (0)211.68 77 46-0
Telefax: + 49 (0)211.68 77 46-20

info@wilhelm-rae.de

Berlin:

Mommsenstraße 45
10629 Berlin

+ 49 (0)30.81 72 732-0
+ 49 (0)30.81 72 732-0

berlin@wilhelm-rae.de

JUVE 2017 AWARDS
Kanzlei des Jahres für Versicherungsrecht