de Auslegungsfragen – etwa zur Reichweite des immateriellen Schadensbegriffs[48] – zur Vorabentscheidung vor.

Merke: 36

Gerichte in Deutschland sprechen Antragstellern zunehmend hohen immateriellen Schadensersatz nach Art. 82 DS-GVO zu.[49] Dieser Trend zeichnet sich auch bei der möglichen Haftung auf Schadensersatz nach bekannt gewordenen Datenschutzverletzungen ab. So sprach das LG München I einem von einer Datenschutzverletzung betroffenen Kunden immateriellen Schadensersatz in Höhe von 2.500 EUR zu. Der gegenständliche Vorfall hatte dazu geführt, dass unbekannte Dritte auf personenbezogene Daten des Klägers wie Namen, Kontaktdaten und steuerliche Informationen zugreifen konnten. Das Gericht wies bei der Bemessung der Höhe des immateriellen Schadensersatzanspruchs unter anderem auf die (vermeintliche) abschreckende Wirkung des DS-GVO-Schadensersatz hin. Es berücksichtigte zugunsten des beklagten Unternehmens, dass die Offenlegung der personenbezogenen Daten bislang zu keinen konkreten Nachteilen für den Kläger geführt hatte.[50] In einem Parallelverfahren hatte das LG Köln einem weiteren Kunden lediglich 1.200 EUR zugesprochen. Es begründete die geringere Schadensersatzsumme unter anderem damit, dass der Datenschutzverstoß allenfalls mitursächlich für den Schaden des Klägers geworden sei.[51]

IV. Mögliche Risiken für Unternehmen im Zusammenhang mit Massenverfahren

Unternehmen drohen infolge bekannt gewordener Datenschutzverletzungen gegebenenfalls auch Massenverfahren. Da solche Vorfälle oftmals eine Vielzahl von Personen in ähnlicher Weise betreffen, eignen sie sich in besonderem Maße für Massenklagen. Erste auf Datenschutz spezialisierte Verbraucheranwälte und -organisationen haben entsprechende Klageverfahren als neues, gewinnbringendes Geschäftsmodell identifiziert.[52] Teilweise werben diese gezielt betroffene Verbraucher an, um sie bei der Durchsetzung möglicher Ansprüche auf DS-GVO-Schadensersatz zu unterstützen. Sollten sich entsprechende Massenverfahren in der Praxis noch weiter etablieren, drohen Unternehmen weitreichende Haftungsrisiken. 37

V. Weitere Risiken

Neben den vorstehend dargestellten Schadensersatz- und Bußgeldrisiken drohen Unternehmen bei Datenschutzverletzungen auch erhebliche **Reputationsschäden.** Öffentlich bekannt gewordene Datenpannen können das Vertrauen von Kunden bzw. Nutzern in den sicheren und vertraulichen Umgang mit ihren personenbezogenen Daten negativ beeinträchtigen. Entsprechende Reputationsschäden können sich erheblich auf die weitere Geschäftsentwicklung des Unternehmens auswirken.[53] 38

[48] So etwa LG Saarbrücken v. 22.11.2021 – 5 O 151/19, GRUR-RS 2021, 39544; Vorabentscheidungsersuchen vom 1.12.2021 – C-741/21.
[49] ZB: OLG Dresden v. 30.11.2021 – 4 U 1158/21, ZD 2022, 159: 5.000 EUR; LAG Berlin-Brandenburg v. 18.11.2021 – 10 Sa 443/21, ZD 2022, 341: 2.000 EUR; OLG Düsseldorf v. 28.10.2021 – 16 U 275/20, ZD 2022, 337: 2.000 EUR; LG München I v. 9.12.2021 – 31 O 16606/20, ZD 2022, 242: 2.500 EUR; AG Pforzheim v. 25.03.2020 – 13 C 160/19, BeckRS 2020, 27380: 4.000 EUR.
[50] LG München I v. 9.12.2021 – 31 O 16606/20, ZD 2022, 242.
[51] LG Köln v. 18.5.2022 – 28 O 328/21, ZD 2022, 506 (507).
[52] Wybitul NJW 2021, 1190; instruktiv dazu Paal/Kritzer NJW 2022, 2433; Wybitul/Leibold ZD 2022, 207.
[53] Wenzel/Wybitul ZD 2019, 290 (294).

39 **Praxistipp:**

Unternehmen sollten auch berücksichtigen, dass Geschäftspartner oder Kunden im Falle eines bekannt gewordenen Datenschutzvorfalls gegebenenfalls auch von vertraglichen oder gesetzlichen **Sonderkündigungsrechten,** etwa nach § 314 BGB, Gebrauch machen könnten. Dieses Risiko ist in der Praxis insbesondere für IT-Provider oder Cloud-Anbieter relevant. Als mögliche Anknüpfungspunkte für entsprechende Sonderkündigungsrechte kommen beispielsweise Verstöße gegen vertragliche Nebenpflichten (§ 241 Abs. 2 BGB) oder vertragliche Vereinbarungen zur Datensicherheit in Betracht. So können Datenschutzverstöße beispielsweise vorhandene Defizite bei der Umsetzung vertraglich vereinbarter TOMs offenlegen. In diesem Zusammenhang sollten Unternehmen auch mögliche vertragliche Informationspflichten gegenüber Kunden im Falle von bekannt gewordenen Datenschutzvorfällen berücksichtigen.

D. Empfehlungen zum Umgang mit Datenschutzvorfällen

40 Um die in den vorstehenden Abschnitten des Beitrags dargestellten Risiken möglichst weitergehend zu verringern, ist es wichtig, effektive Strategien zum Umgang mit möglichen Datenschutzvorfällen zu entwickeln und umzusetzen. Der nachstehende Abschnitt dieses Beitrags gibt einen Überblick über mögliche präventive Maßnahmen, um das Risiko für Datenschutzvorfälle zu minimieren. Zudem zeigt er mögliche Notfall-Maßnahmen auf, die Unternehmen im Falle eines bekannt gewordenen Vorfalls ergreifen können, um dessen Auswirkungen zu begrenzen.

41 Wie bereits vorstehend[54] dargestellt, ist dabei eine umfassende und gerichtsfeste Dokumentation der ergriffenen Maßnahmen für die Verteidigung in möglichen Schadens- und Bußgeldverfahren sehr wichtig.

42 **Praxistipp:**

Die europäischen Datenschutzbehörden haben zahlreiche Handlungsempfehlungen zum Umgang mit Datenschutzverletzungen veröffentlicht. Die entsprechenden Leitlinien beschreiben unter anderem typische Beispielfälle für Datenschutzvorfälle und die jeweils vom Verantwortlichen zu treffenden Maßnahmen.[55]

I. Vorbereitung auf mögliche Datenschutzvorfälle

43 Da die Anzahl der Datenschutzvorfälle – etwa in Form von Hacker-Angriffen – in der Praxis stark zunimmt, ist es wichtig, die eigenen IT- und Datensicherheitsstrukturen auf dem aktuellen Stand der Technik zu halten und ihre Wirksamkeit laufend zu überprüfen. Die folgende Übersicht gibt hierzu und zu möglichen weiteren präventiven Maßnahmen einen ersten Überblick.

1. Maßnahmen zur Datensicherheit

44 Unternehmen sollten sicherstellen, dass sie den Anforderungen von Art. 32 DS-GVO entsprechende **Maßnahmen zur IT- und Datensicherheit** umsetzen.[56] Die nach Art. 32 DS-GVO erforderlichen Maßnahmen richten sich dabei nach den Umständen des Einzel-

[54] Vgl. hierzu → Rn. 24f.

[55] Beispielsfälle enthalten die „Guidelines 1/2021 on examples regarding Personal Data Breach Notification" des Europäischen Datenschutzausschusses (EDSA) vom 03 Januar 2021 Die Guidelines sind abrufbar unter: https://edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf, abgerufen am 7.3.2023; Vgl. auch EDSA-Guidelines 9/2022 (siehe Fn. 845),

[56] Taeger/Gabel/Schultze-Melling DS-GVO Art. 32 Rn. 12f.

falls. Im Rahmen dieser Einzelfallabwägung sind insbesondere mögliche Risiken für die von der Datenverarbeitung betroffenen Personen zu berücksichtigen. Darauf aufbauend sollten Unternehmen risikoorientierte Maßnahmen ergreifen. Hierzu können beispielsweise Maßnahmen zur Pseudonymisierung und Verschlüsselung von personenbezogenen Daten, effektive Firewalls und Antiviren-Programme sowie Maßnahmen zur Begrenzung und Kontrolle von Zugriffsrechten und -möglichkeiten zählen.[57] Bei der Auswahl und Umsetzung der entsprechenden Maßnahmen sollte man eng mit den zuständigen IT- und Datenschutzabteilungen zusammenarbeiten. Zudem ist es wichtig, die umgesetzten Maßnahmen regelmäßig auf ihre Wirksamkeit zu kontrollieren.

Um mögliche Risiken im Hinblick auf die IT- und Datensicherheit weitgehend zu reduzieren, sollte man die vorstehend genannten Maßnahmen und Vorgaben möglichst bereits bei der Entwicklung und Einführung neuer technischer Systeme, Software und Prozesse berücksichtigen und umsetzen.[58] 45

2. Kontrolle von Auftragsverarbeitern

Viele Unternehmen binden in der Praxis IT-Provider und sonstige Dienstleister in das Hosting und die Verwaltung von personenbezogenen Daten ein. Entsprechende Beauftragungen erfolgen in der Regel im Wege der Auftragsverarbeitung nach Art. 28 DS-GVO. Die DS-GVO verpflichtet Auftraggeber, dh die datenschutzrechtlich Verantwortlichen, durch geeignete Auswahlkriterien und Kontrollen sicherzustellen, dass die beauftragten Auftragsverarbeiter die Vorgaben zum Datenschutz und zur Datensicherheit einhalten, vgl. Art. 28 Abs. 1 DS-GVO. Daher sollte man nur mit Dienstleistern zusammenarbeiten, die über ein dem Stand der Technik entsprechendes IT- und Datensicherheitskonzept verfügen. Zusätzlich müssen sich Verarbeiter kontinuierlich vergewissern, dass Auftragsverarbeiter die Anforderungen zum Datenschutz und Datensicherheit auch tatsächlich einhalten.[59] 46

Praxistipp: 47

Eine umfangreiche Kontrolle der eingesetzten Auftragsverarbeiter ist auch im Hinblick auf mögliche Verteidigungsszenarien in etwaigen Schadensersatzverfahren nach Art. 82 DS-GVO wichtig. Ist ein möglicher Datenschutzvorfall auf unzureichende IT- und Datensicherheitsstrukturen des Auftragsverarbeiters zurückzuführen, muss sich der Verantwortliche die entsprechenden Verstöße gegebenenfalls zurechnen lassen.[60] Verantwortliche und von ihnen eingesetzte Auftragsverarbeiter haften insofern als Gesamtschuldner, vgl. Art. 82 Abs. 2 DS-GVO.[61] Nach Art. 82 Abs. 3 DS-GVO wird der Verantwortliche nur dann von der Pflicht zur Zahlung von Schadensersatz befreit, wenn er nachweisen kann, „dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist." Eine solche Exkulpation setzt voraus, dass der Verantwortliche nachweisen kann, dass er den Auftragsverarbeiter sorgfältig ausgewählt und kontrolliert hat.[62] Um entsprechenden Nachweispflichten nachkommen zu können, kann es hilfreich sein, mit den Auftragsverarbeitern möglichst konkrete TOMs und sonstige Vorgaben zur Datensicherheit zu vereinbaren."

---

[57] Weitere Beispiele für organisatorische Maßnahmen zur Vorbeugung/Milderung der Auswirkungen von Angriffen finden sich in den EDSA-Guidelines 1/2021 (siehe Fn. 845), Rn. 70.

[58] Siehe hierzu die Vorgabe zu Privacy by Design und Privacy by Default, Art. 25 DS-GVO.

[59] BeckOK DatenschutzR/Spoerr DS-GVO Art. 28 Rn. 35; Kühling/Buchner/Hartung DS-GVO Art. 28 Rn. 60; Paal/Pauly/Martini DS-GVO Art. 28 Rn. 20.

[60] Ehmann/Selmayr/Nemitz DS-GVO Art. 82 Rn. 24; Moos Datenschutz/Moos § 8 Rn. 163; Taeger/Gabel/Moos/Schefzig DS-GVO Art. 82 Rn. 66; Wybitul/Haß/Albrecht NJW 2018, 113 (114); Wybitul/Neu/Strauch ZD 2018, 202 (204).

[61] Vgl. ErwGr 146 DS-GVO; Wybitul/Haß/Albrecht NJW 2018, 113 (114).

[62] In diese Richtung Schantz/Wolff Neues DatenschutzR/Schantz Kap. F. Rn. 1251; Taeger/Gabel/Moos/Schefzig DS-GVO Art. 82 Rn. 86.

3. Trainings und Awareness

48 Datenschutzvorfälle beruhen in der Praxis oft auf versehentlichem Fehlverhalten einzelner Mitarbeiter. Ein anschauliches Beispiel hierfür ist das unbedachte Öffnen einer Phishing-Mail durch einen Mitarbeiter. Für eine effektive Prävention von Datenschutzvorfällen sind daher auch regelmäßige Schulungen und Trainings zum Datenschutz wichtig. Im Rahmen entsprechender Awareness-Maßnahmen sollte man die Mitarbeiter nicht nur auf die Risiken hinweisen, die Datenschutzvorfälle für das Unternehmen, dessen Kunden sowie die Belegschaft haben können.

49 **Praxistipp:**

In der Praxis hat es sich zudem als hilfreich erwiesen, die Mitarbeiter auch auf mögliche eigene Haftungsrisiken bei Datenschutzvorfällen hinzuweisen. Eine solche Haftung kann beispielsweise im Rahmen eines sogenannten Mitarbeiterexzesses bestehen. Zudem haften Mitarbeiter gegebenenfalls nach den Grundsätzen des innerbetrieblichen Schadensausgleichs. Danach besteht eine Haftung des Mitarbeiters im Innenverhältnis gegenüber dem Arbeitgeber gegebenenfalls bereits bei mittlerer Fahrlässigkeit.[63].

4. Einführung von Reaktionsplänen

50 Als Vorbereitung auf mögliche Datenschutzvorfälle sollte man auch die Einführung eines Reaktionsplans für den Ernstfall (sogenannte **„Data Breach Procedures"**) erwägen. Dies umfasst gegebenenfalls einen Ablaufplan, der konkrete Vorgaben und Prozesse zum Umgang mit bekannt gewordenen Datenschutzvorfällen vorsieht. Entsprechende Richtlinien regeln zudem typischerweise die einschlägigen internen Zuständigkeiten sowie konkrete Vorgaben für die Einbindung der relevanten Unternehmensfunktionen und etwaiger Rechtsberater und sonstiger Dienstleister.[64]

51 Die Entwicklung solcher Notfallpläne hat sich in der Praxis als sehr hilfreich erwiesen. Da Datenschutzvorfälle – aufgrund der knapp bemessenen Zeitfenster zur Meldung – oftmals mit hohem zeitlichen Druck verbunden sind, ist es für Unternehmen wichtig, im Einzelfall schnell und abgestimmt reagieren zu können.

52 **Praxistipp:**

Unternehmen schließen in der Praxis immer häufiger sogenannte Cyberversicherungen ab, die im Rahmen von Datenschutzvorfällen entstandene Schäden abdecken sollen. Vor dem Abschluss eines entsprechenden Vertrages sollte man die Vertragsbedingungen genau prüfen. Dies gilt insbesondere für die Voraussetzungen für eine Kosten- bzw. Schadensübernahme im Versicherungsfall. Die Versicherungsbedingungen vieler Cyberversicherungen sehen insofern umfassende Informationspflichten gegenüber der Versicherung im Falle eines bekannt gewordenen Datenschutzvorfalls vor.

II. Reaktion auf mögliche Datenschutzvorfälle

53 Wird ein Datenschutzvorfall beim eigenen Unternehmen bekannt, sollte man zeitnah und effektiv reagieren, um mögliche Risiken für das Unternehmen und die von dem Vorfall betroffenen Personen zu minimieren. Der nachstehende Abschnitt dieses Beitrags gibt einen Überblick über mögliche Handlungsstrategien im Falle eines bekannt gewordenen Datenschutzvorfalls.

---

[63] Vgl. zu den entsprechenden Aspekten Taeger/Gabel/Moos/Schefzig DS-GVO Art. 82 Rn. 132; MAH ArbR/Reichold Band 1 § 57 Rn. 40.

[64] Hierzu auch Wybitul NJW 2020, 2577 (2581).

1. Erste Maßnahmen

Zunächst sollte man sich einen ersten Überblick über die möglichen Ursachen und Auswirkungen des Datenschutzvorfalls verschaffen. Eine belastbare Aufklärung des Sachverhalts ist insbesondere für die Bewertung einer möglichen Meldepflicht nach Art. 33 DS-GVO wichtig.[65] Handelt es sich um einen komplexen Sachverhalt, sollte man gegebenenfalls die Einschaltung spezialisierter Dienstleister, wie IT-Forensiker und Rechtsanwaltskanzleien, prüfen. Zudem sollten die für die Sachverhaltsaufklärung maßgeblichen Unternehmensfunktionen (wie IT und gegebenenfalls die Personalabteilung) zeitnah in die Sachverhaltsaufklärung eingebunden werden. 54

Praxistipp: 55

In Einzelfällen kann es sinnvoll sein, eine aus externen und internen Spezialisten zusammengesetzte Arbeitsgruppe („**Task Force**") zu bilden. Die Anzahl der beteiligten Personen sollte dabei möglichst gering gehalten werden, um eine zeitnahe und effektive Abstimmung zu ermöglichen.

2. Erfüllung von möglichen Meldepflichten

Um nicht gegen die Meldepflichten nach Art. 33, 34 DS-GVO zu verstoßen, ist es wichtig, zeitnah zu prüfen und zu entschieden, ob ein nach der DS-GVO meldepflichtiger Vorfall vorliegt. Man sollte die Entscheidung sowie die dafür relevanten Aspekte umfassend dokumentieren. Dies gilt insbesondere in Fällen, in denen man von einer Mitteilung an die Aufsichtsbehörde mangels Risiken absieht. 56

Zudem gilt es, zeitnah mögliche **ad-hoc-Meldepflichten** zu prüfen, die insbesondere für börsennotierte Unternehmen relevant sind (etwa Pflichten nach dem WpHG). Hierfür wird regelmäßig die Einbindung der Rechtsabteilung oder spezialisierter Rechtanwaltskanzleien notwendig sein. 57

3. Kooperation mit Aufsichtsbehörden?

Liegen die Voraussetzungen für eine Meldepflicht nach Art. 33 DS-GVO vor, sollte man die entsprechende Meldung zeitnah vorbereiten und einreichen, um die 72-Stunden-Frist einhalten zu können. Nach Einreichung einer entsprechenden Meldung stellen Aufsichtsbehörden oftmals spezifische Nachfragen. In der Praxis hat sich eine kontinuierliche und enge **Kooperation** mit Aufsichtsbehörden oftmals als hilfreich erwiesen. Dies gilt etwa im Hinblick auf die mögliche Information der vom Vorgang betroffenen Personen und die Umsetzung zusätzlicher Abhilfemaßnahmen.[66] Ob eine solche Kooperation sinnvoll ist, hängt von den Umständen des Einzelfalls und den möglichen Auswirkungen des Vorfalls ab. 58

4. Kommunikationsstrategie

Besteht das Risiko, dass der Datenschutzvorfall publik werden könnte, sollte man zeitnah die zuständige Kommunikationsabteilung im Unternehmen einbinden. Dies gilt insbesondere dann, wenn – etwa aufgrund des großen Umfangs des Vorfalls – substanzielle Reputationsrisiken drohen. Negative Pressemitteilungen können insofern auch zu Umsatzeinbußen führen. Durch eine effektive und abgestimmte Kommunikationsstrategie lassen sich entsprechende Risiken oftmals erheblich reduzieren. 59

[65] Siehe hierzu sogleich unter D.II.2 → Rn. 56.

[66] Zu den Vor- und Nachteilen einer engen Kooperation mit Aufsichtsbehörden Wenzel/Wybitul ZD 2019, 290 (294).

5. Behebung möglicher Schwachstellen

60 Drohen infolge des Vorfalls weitergehende Auswirkungen, wie etwa ein zusätzlicher Datenverlust, sollten umgehend Maßnahmen getroffen werden, um die maßgeblichen Schwachstellen belastbar zu identifizieren und zeitnah und nachhaltig zu beheben.

6. Dokumentation

61 Unternehmen sollten die im Zuge des Datenschutzvorfalls ergriffenen und geplanten Maßnahmen sowie die Ergebnisse der Sachverhaltsaufklärung umfassend dokumentieren. Eine umfassende und gerichtsfeste Dokumentation ist für eine Verteidigung in möglichen Behördenverfahren oder Schadensersatzprozessen betroffener Personen von zentraler Bedeutung.[67]

7. Vorbereitung auf die effektive Verteidigung gegen Schadensersatzforderungen und Geldbußen

62 Neben der Dokumentation des Sachverhalts und der getroffenen Abhilfemaßnahmen können Unternehmen noch weitere Maßnahmen ergreifen, um sich effektiv auf mögliche Behörden- oder Schadensersatzverfahren vorzubereiten. Hierzu zählt die Vorbereitung auf mögliche Auskunftsanträge betroffener Personen nach Art. 15 DS-GVO. Betroffene machen in der Praxis immer häufiger von ihrem Auskunftsrecht Gebrauch, um sich weitere Kenntnisse über den Datenschutzvorfall zu verschaffen. Oftmals nutzen sie entsprechende Informationen in möglichen Schadensersatzprozessen. In Einzelfällen kann es sich daher anbieten, bereits proaktiv mögliche Antwortschreiben auf Auskunftsersuchen vorzubereiten.

8. Exkurs: Reaktion auf Ransomeware-Attacken

63 In der Praxis werden Unternehmen immer häufiger Opfer von sogenannten Ransomware-Attacken. Hierbei greifen Hacker die IT-Systeme von Unternehmen an, indem sie Schadprogramm in die Systeme einschleusen (etwa durch Phishing-Mails). Mithilfe dieser Schadprogramme können die Angreifer den Zugriff des Unternehmens auf die auf den Systemen gespeicherten Daten ganz oder teilweise dauerhaft blockieren. Hierzu werden die Daten mithilfe der Schadsoftware verschlüsselt. In der Praxis kann dies zu einer kompletten Stilllegung des Geschäftsbetriebs des angegriffenen Unternehmens führen.[68] Die Angreifer stellen den Unternehmen den für die Entschlüsselung notwendigen Code oftmals nur gegen Zahlung einer hohen „Lösegeldsumme" zur Verfügung.[69]

64 In der Praxis hat es sich als hilfreich erwiesen, bei Ransomware-Angriffen umgehend Kontakt mit dem für Cybercrime zuständigen Landeskriminalamt aufzunehmen, um das weitere Vorgehen abzustimmen. Soweit von dem Angriff auch personenbezogene Daten umfasst sind, sollte man parallel auch die zuständige Datenschutzaufsichtsbehörde informieren.

65 **Praxistipp:**

In der Praxis verfügen Unternehmen oftmals nicht über hinreichende Backups, die ihnen eine zeitnahe Wiederherstellung der verschlüsselten Daten ermöglichen könnten. In diesen Fällen stellt sich die drängende Frage, ob man der „Lösegeldforderung" der Angreifer nachkommen sollte. Es hat sich als hilfreich erwiesen, diese Frage eng mit den beteiligten Behörden abzustimmen.

---

[67] Vgl. Wybitul/Venn ZD 2021, 343 (347); Wybitul NJW 2020, 2577 (2582).
[68] Siehe dazu den Bericht des BSI zu „Ransomware – Bedrohungslage 2022".
[69] Vgl. auch Meyer/Biermann MMR 2022, 940 (940).

Hierbei ist zu berücksichtigen, dass die Zahlung eines „Lösegeldes" gegebenenfalls eine negative Vorbildwirkung für zukünftige Fälle haben kann – oder dass eine Entschlüsselung trotz gezahltem Lösegeld nicht erfolgt. Die schwerwiegenden Auswirkungen des Angriffs und der damit verbundene hohe Zeitdruck können aber im Einzelfall auch für die Zahlung eines „Lösegeldes" sprechen. Die handelnden Personen auf Unternehmensseite sollten sich hierbei aber bewusst sein, dass entsprechende Zahlungen ein eigenständiges – gegebenenfalls persönliches – Sanktionsrisiko beinhalten können. Lösegeldzahlungen könnten gegebenenfalls als Unterstützung einer terroristischen Vereinigung[70] oder als Zahlung an eine „Denied Party" im Sinne des internationalen Sanktionsrechts gewertet werden. Die von den Erpressern angegebene Empfänger-Wallet sollte daher insbesondere mit den Sanktionslisten der U.S. Office of Foreign Assests Control („**OFAC**")[71] abgeglichen werden.

Leitungspersonen auf Unternehmensseite treffen im Falle von Ransomware-Attacken 66
weitreichende Sorgfalts- und Aufsichtspflichten[72], bei deren Verletzung gegebenenfalls eine Strafbarkeit wegen Untreue[73] in Betracht kommen kann. Dies setzt im Einzelfalle eine Schädigung des Bestands bzw. Vermögens des Unternehmens voraus. Eine solche Schädigung kann beispielsweise in der Freigabe von Lösegeld liegen, obwohl eine eigenständige Entschlüsselung der verschlüsselten Datensätze möglich ist oder der Empfänger auf einer behördlichen Sanktionsliste gelistet ist. Lösegeldzahlungen sollten daher nur auf Basis einer hinreichenden und angemessenen Informationsgrundlage und nach sorgfältiger Abwägung freigegeben werden, um mögliche Strafbarkeitsrisiken zu verringern.[74] Zudem sollte man sich hierbei eng mit den Strafverfolgungsbehörden abstimmen.

E. Ausblick

Angesichts der fortschreitenden Digitalisierung ist damit zu rechnen, dass die Zahl der Da- 67
tenschutzvorfälle zunehmen wird. Statistiken zeigen bereits einen deutlichen Anstieg von Datenschutzverletzungen im Jahr 2021 im Vergleich zum Vorjahr. Insbesondere Ransomware-Angriffe betreffen Unternehmen immer häufiger.[75] Der Branchenverband bitkom kam im Rahmen einer Studie zu dem Ergebnis, dass der deutschen Wirtschaft jährlich ein Schaden von 203 Milliarden EUR durch Angriffe auf deutsche Unternehmen entsteht.[76] Es wird daher für Unternehmen immer wichtiger, sich auf mögliche Datenschutzvorfälle effektiv vorzubereiten. Verstöße gegen die Vorgaben zum Datenschutz und der Datensicherheit können für Unternehmen weitreichende rechtliche und finanzielle Folgen haben. Diese können im Einzelfall auch den künftigen Geschäftserfolg erheblich beeinträchtigen.

Gerichte und Aufsichtsbehörden in der EU legen die entsprechenden rechtlichen Vor- 68
gaben zunehmend streng aus. Der Europäische Gerichtshof hat sich zwar noch nicht abschließend zu den Voraussetzungen für die Verhängung von Geldbußen und Schadensersatz nach der DS-GVO geäußert. Angesichts der verbraucher- und datenschutzfreundli-

[70] § 129a Abs. 5 StGB iVm § 129a Abs. 2 Nr. 2 StGB.
[71] Verstöße gegen die entsprechenden Vorgaben können zu weitreichenden Sanktionen durch die OFAC führen.
[72] Entsprechende Pflichten finden sich beispielsweise in §§ 91 Abs. 2, 93 Abs. 1 AktG und in § 43 Abs. 1 GmbHG.
[73] § 266 Abs. 1 StGB.
[74] Vgl. Heinrichs/Neumeier CB 2022, 14 (15).
[75] Der Annual Data Breach Report 2021 des Identity Theft Centers hat festgestellt, dass in den Vereinigten Staaten im Jahre 2021 ca. 68 Prozent mehr Datenschutzverletzungen als im Vorjahr gemeldet wurden. Dies gilt insbesondere auch für Ransomware-Angriffe, abrufbar unter https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf, abgerufen am 7.3.2023.
[76] Bitkom e. V., Presseinformation vom 31.8.2022, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022, abgerufen am 7.3.2023.

chen Auslegungspraxis des EuGH in der Vergangenheit ist jedoch nicht damit zu rechnen, dass der Gerichtshof die Vorschriften eng auslegen wird. Es ist wahrscheinlich, dass der EuGH die strenge Sanktionierungspraxis der Aufsichtsbehörden fortführen bzw. bekräftigen wird.