VERMÖGENSSCHADEN-HAFTPFLICHT

Datenschutz...

Foto: Ken Schluchtmann, diephotodesigner.de

...im digitalen Zeitalter

In einem digitalen Zeitaltern gehört die Erfassung und Speicherung von Kundendaten, die Versendung von E-Mails, die Nutzung digitaler Arbeitsmethoden wie Building-Informations-Modeling (BIM) und Drohnen, die Durchführung von Web-Meetings und Home-Office zum „new normal" unserer täglichen Arbeit. Damit sind zwangsläufig auch Haftungsrisiken wie Systemfehler, Fehlbedienung oder Virenverbreitung verbunden, die zu Datenveränderungen oder Datenbehinderungen bei Dritten führen.

Über allem schwebt ein Thema – die Einhaltung von Datenschutzbestimmungen. Seit dem 25.Mai 2018 gibt es die EU-Datenschutz-Grundverordnung (DSGVO), die auch für Kleinstunternehmen, kleinere und mittlere Unternehmen gilt. Die Beachtung der Vorschriften gilt daher auch für Architekten- und Ingenieurbüros, die Daten verarbeiten. Mit Einführung der DSGVO wurde das Thema Datenschutz jedoch nicht erstmalig aufgegriffen. 1970 verabschiedete Hessen bereits das erste Datenschutzgesetz. Das Bundesdatenschutzgesetz (BDSG) trat 1978 in Kraft. Datenschutz stammt also aus einer Zeit, in der noch die Schreibmaschine und Ablage in Aktenordner zum „ normal" gehörte (auch wenn sich die jüngere Generation nicht vorstellen kann, dass man jemals ohne digitale Welt und Handy überleben konnte). Seit 2018 ersetzt die DSGVO in großen Teilen das BDSG. Auch nach früherer Rechtslage musste man also schon technische und organisatorische Maßnahmen treffen, um Datenschutz zu gewährleisten. Mit Einführung der DSGVO, der zunehmenden Digitalisierung und auch bedingt durch die Corona Krise der letzten Jahren, hat das Thema Datensicherheit und Datenschutz noch einmal an Beachtung gewonnen.

Das Verhältnis zwischen DSGVO und BDSG

Das deutsche Bundesdatenschutzgesetz regelt zusammen mit den Datenschutzgesetzen der (Bundes)Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden.

Da der Datenschutz in einer vernetzten Welt nicht an den Ländergrenzen „stoppt" war ein zeitgemäßer Rechtsrahmen für den Umgang mit personenbezogenen Daten – auf nationaler, europäischer und internationaler Ebene erforderlich, der mit der DSGVO geschaffen wurde.

Die DSGVO ist das europarechtliche Regelwerk, welches für alle Mitgliedstaaten innerhalb der Europäischen Union gilt. Als Teil des Unionsrechts genießt die DSGVO Anwendungsvorrang vor Bundesrecht, d. h. im Fall einer Normenkollision zwischen der DSGVO und dem BDSG hat stets die DSGVO als ranghöheres Recht Anwendungsvorrang. Im Grunde ist das BDSG daher eine Ergänzung bzw. Konkretisierung der DSGVO.

DSGVO Anwendungsbereich

Die DSGVO regelt die Verarbeitung von personenbezogenen Daten natürlicher Personen durch natürliche Personen, Unternehmen oder Organisationen, soweit die Tätigkeit in der Europäischen Union erfolgt oder im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen in der Europäischen Union steht (sog. Marktortprinzip). Sie schützt personenbezogene Daten **unabhängig von der zur Datenverarbeitung verwendeten Technik** – sie ist technologieneutral und gilt für die automatisierte wie die manuelle Verarbeitung, sofern die Daten nach vorherbestimmten Kriterien (z. B. alphabetische Reihenfolge) geordnet sind.

Der Basisgedanke dabei ist, dass im Prinzip grundsätzlich die *Erhebung, Verarbeitung und Nutzung* von personenbezogenen Daten verboten ist. Sie ist nur dann erlaubt, wenn entweder eine klare Rechtsgrundlage gegeben ist (d. h., das *Gesetz erlaubt* die Datenverarbeitung) oder wenn die betroffene Person ausdrücklich ihre *Zustimmung erteilt*.

Eine **Verarbeitung personenbezogener Daten** ist somit nur rechtmäßig mit **der Einwilligung** der betroffenen Person **oder** wenn die Verarbeitung **erforderlich ist**. Erforderlich heißt:

- **zur Erfüllung eines Vertrages oder Durchführung vorvertraglicher Maßnahmen**
- **zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritten, sofern nicht die Interessen oder Grundrechte/Grundfreiheiten der betroffenen Person überwiegen**
- **zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person,**
- **zur Wahrnehmung einer im öffentlichen Interesse liegenden oder in Ausübung hoheitlicher Gewalt erfolgenden Aufgabe des Verantwortlichen**
- **zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen**

Damit nicht vor allem in privaten Bereichen mit jeder WhatsApp oder E-Mail das Risiko einer Datenschutzverletzung einhergeht, macht das Gesetz Ausnahmen für

- natürliche Personen, die personenbezogene Daten zur **Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeiten** (privater Schriftverkehr, Adressbücher oder die Nutzung sozialer Netzwerke und Online-Tätigkeiten im Rahmen persönlicher oder familiärer Zwecke)
- **nicht automatisierten Verarbeitung** personenbezogener Daten, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Akten und Aktensammlungen, die nicht nach bestimmten Kriterien geordnet sind)

Was umfassen die Grundbegriffe **personenbezogene Verarbeitung:**

personenbezogene Daten	Verantwortlicher	Verarbeitung
■ Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.	■ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet Bsp.: in einem Konzern ist jede Tochtergesellschaft als separater Verantwortlicher zu betrachten	■ ist jedes mit oder ohne Hilfe automatisierte Verfahren, jeder ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten Bsp.: Erheben, Erfassen, Organisation, Ordnen, Speicherung

personenbezogene Daten sind z. B. Name und Vorname; eine Privatanschrift; eine E-Mail-Adresse wie vorname.nachname@unternehmen.com; eine Ausweisnummer; Standortdaten (z. B. die Standortfunktion bei Mobiltelefonen); eine IP-Adresse; eine Cookie-Kennung oder auch Daten, die in einem Krankenhaus oder bei einem Arzt vorliegen, die zur eindeutigen Identifizierung einer natürlichen Person führen könnten.

Keine personenbezogene Daten dagegen sind z. B. Handelsregisternummer; eine E-Mail-Adresse wie info@unternehmen.com oder anonymisierte Daten.

Verarbeitung kann bspw. Personalverwaltung; Zugang zu/Nutzung einer Kontaktdatenbank, die personenbezogene Daten enthält; Versand von Werbe-E-Mails; Vernichtung von Akten, die personenbezogene Daten enthalten; Veröffentlichung/Einstellung eines Fotos einer Person auf einer Website; Speicherung von IP- oder MAC-Adressen.

Besonderheiten in der DSGVO

Neben verschiedenen Rechten und Pflichten wurde mit der DSGVO erstmalig eine eigenständige Regelung zum „Recht auf Vergessen werden" geschaffen. Ein Anspruch darauf, dass personenbezogene Daten gelöscht oder gesperrt werden müssen. Dieser besteht dann,

- wenn für die Verwendung der Daten keine Berechtigung mehr vorliegt, die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt.
- wenn die betroffene Person gemäß Artikel 21 Absatz 1 DSGVO Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen, oder die
- wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

Zu berücksichtigen hierbei ist aber auch, dass der BGH in Urteilen entschieden hat, dass es kein generelles Recht auf Vergessen gibt, sondern die Abwägung wessen Rechte und Interessen im Einzelfall Vorrang haben. Das Recht auf Vergessen werden findet nach Art. 17 Abs. 3 DSGVO auch keine Anwendung, wenn z. B. die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information oder die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 DSGVO erforderlich ist.

Weitere Pflichten, Risiken und Rechte

Ein Großteil der mit der der DSGVO eingeführten Pflichten sind jedoch nicht neu. Bestimmte datenschutzrechtliche Vorgaben waren bereits vor deren Einführung von Architekten und Ingenieuren zu beachten und einzuhalten. Im Wesentlichen wurden die längst aus dem früheren Datenschutzrecht bekannten Grundsätze aufgenommen und konkretisiert. Bereits vor dem in Kraft treten der DSGVO musste eine Datenerfassung und deren Verarbeitung möglichst transparent und zweckgebunden erfolgen. Ebenso waren pauschale Datenverarbeitungen „auf Vorrat" sowie solche, die ohne eine entsprechende Rechtsgrundlage erfolgt sind, bereits damals schon nicht gestattet.

1. Rechenschafts- und Dokumentationspflicht

Neu hingegen ist beispielsweise die in Art. 5 Abs. 2 DSGVO normierte Rechenschaftspflicht, nach der der für die Datenverwertung Verantwortliche die Einhaltung der vorgenannten Grundsätze gewährleisten und nachzuweisen hat. Dabei sind die im Verhältnis zum BDSG deutlich strengeren Dokumentationspflichten zu beachten. Es genügt nicht mehr allein die Einhaltung der datenschutzrechtlichen Grundsätze,

vielmehr muss die verantwortliche Stelle auch aktiv in der Lage sein, die Einhaltung eben dieser Grundsätze nachzuweisen. Vereinfacht wird ein solcher Nachweis jedoch durch die in den Artikeln 42, 43 DSGVO eingeräumte Möglichkeit zur Zertifizierung des datenverarbeitenden Büros. Eine solche Zertifizierung kann sodann als Bestätigung zur Einhaltung sämtlicher in der DSGVO geregelten Grundsätze und Regelungen bei den Verarbeitungsvorgängen dienen.

2. Verzeichnis aller Verarbeitungstätigkeiten
Weiter hat die für die Datenerfassung und -verarbeitung verantwortliche Stelle zum Zwecke der Dokumentation ein Verzeichnis zu führen, in dem sämtliche Verarbeitungstätigkeiten aufgeführt sind. Welche Angaben genau in diesem Verzeichnis enthalten sein müssen, wird in Art. 30 DSGVO geregelt.

Von der Pflicht zur Führung eines solchen Verzeichnisses sind nur solche Betriebe befreit, die (1) weniger als 250 Mitarbeiter aufweisen und (2) bei denen eine entsprechende Datenverarbeitung nur **„gelegentlich"** erfolgt.

Insbesondere aufgrund der 2. Einschränkung ist jedoch davon auszugehen, dass die vorgenannte Ausnahmeregelung bei einem Großteil der Architekten- und Ingenieurbüros nicht greift und diese somit zur Führung eines solchen Verzeichnisses verpflichtet sind.

3. Datenschutzbeauftragter
Ebenso wird die Bereitstellung eines Datenschutzbeauftragten verlangt. Diese gilt allerdings nicht uneingeschränkt. Vielmehr sieht die DSGVO die Erforderlichkeit eines solchen lediglich in zwei Fällen vor, nämlich dann:

- wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen liegt und diese aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- wenn die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung besonderer Daten gemäß Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO besteht.

Dies mag zwar auf die meisten Architektur- und Ingenieurbüros nicht zutreffen, allerdings eröffnet Art. 37 Abs. 4 DSGVO die Möglichkeit, dass die Pflicht zur Bestellung eines Datenschutzbeauftragten durch nationale Gesetze ergänzt werden kann. Diese Möglichkeit hat der hiesige Gesetzgeber genutzt und mit § 38 BDSG einen dritten Fall geschaffen. Danach ist ein Datenschutzbeauftragter auch dann erforderlich,

- soweit in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Für eine entsprechende Einordnung ist folglich maßgeblich, was unter den Begriff der Verarbeitung fällt. Teilweise wird vertreten, dass eine *„automatisierte Verarbeitung personenbezogener Daten"* bereits dann vorliegt, wenn (digitale) Kundendateien schlicht genutzt oder verwendet werden, was zur Folge hat, dass wohl die meisten Architektur- und Ingenieurbüros ab 20 Mitarbeitern zur Bereitstellung eines geeigneten Datenschutzbeauftragten verpflichtet sind.

Wenn und soweit hiernach die Bestellung eines Datenschutzbeauftragten erforderlich ist, muss dieser Umstand sowohl der zuständigen Aufsichtsbehörde gemeldet sowie dessen Kontaktdaten sodann, beispielsweise durch die (frei zugängliche) Veröffentlichung auf der Internetseite des Betriebes, nach außen hin sichtbar gemacht werden.

4. Weitere Pflichten
Ferner lassen sich für den Datenverwerter noch zahlreiche weitere Pflichten, insbesondere aus den im 3. Kapitel der DSGVO (Art. 12–23) geregelten Rechten der betroffenen Person herleiten.

Darunter fällt insbesondere die in **Art. 13 DSGVO** festgelegte **Informationspflicht**, nach der der für die Datenerhebung Verantwortliche unter anderem über seine Person, über den ggf. erforderlichen Datenschutzbeauftragten, den Zweck und Dauer der Datenerhebung sowie über die der betroffenen Person zustehenden Rechte informieren muss.

Ferner steht der von der Datenverwertung betroffenen Person neben dem Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung unter anderem noch ein entsprechendes Auskunftsrecht zu (vgl. Art. 15 DSGVO). Dies verpflichtet die verantwortliche Stelle dazu, auf Anfrage, Auskunft darüber zu geben ob und, bejahendenfalls welche personenbezogenen Daten über die betroffene Person erhoben worden sind. Darüber hinaus umfasst das Recht auf Auskunft auch die Informationen zur Dauer der Speicherung eben dieser Daten.

Art. 12 Abs. 1 DSGVO gibt dabei grundsätzlich vor, dass all diese Auskünfte in präziser, transparenter, verständlicher und leicht zugänglicher Form erteilt werden müssen.

Praktische Tipps – auf was sollte ich achten
Ungeachtet der vorgenannten Pflichten ist zur Erfüllung eines Architekten- oder Ingenieurvertrages die Verarbeitung personenbezogener Daten grundsätzlich ohne Einwilligung des Bauherrn weiterhin möglich. Auch im vorvertraglichen Bereich ist eine solche ausdrückliche Einwilligung bislang nicht erforderlich. Weiter ist allerdings zu beachten:

- Werden diese Daten verarbeitet, hat der beauftragte Architekt oder Ingenieur seinem Auftraggeber unverzüglich umfassende Auskünfte unter anderem über den Namen und die eigenen Kontaktdaten, die des ggf. erforderlichen Datenschutzbeauftragten, über den Zweck, weswegen die personenbezogenen Daten erfasst und verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung zu geben.
- Wenn und soweit personenbezogene Daten gespeichert werden – wovon regelmäßig auszugehen ist – müssen hierfür geeignete technische und organisatorische Maßnahmen getroffen werden, um insbesondere die Rechte der betroffenen Personen zu schützen und lediglich hierzu berechtigten Personen den Zugriff auf die Daten zu ermöglichen. Gemäß § 62 Abs. 1 BDSG ist bei dem aufzuwendenden Schutz unter anderem der aktuelle Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung zu berücksichtigen. Grundsätzlich gilt: je mehr und je sensibler die Daten sind, die verarbeitet werden, desto höhere Anforderungen sind an das jeweilige Schutzniveau zu stellten.
- In dem Fall, in dem Drittunternehmer wie beispielsweise Copyshops zur Erstellung von Plänen o.Ä. hinzugezogen

und diesen personenbezogene Daten zur weiteren Verwendung weitergeleitet werden, sollte ein entsprechender Vertrag zur Auftragsverarbeitung abgeschlossen werden, um weiterhin die Sicherheit der übergebenen Daten gewährleisten zu können.
- Schließlich ist zu beachten, dass hinsichtlich der Einhaltung all dieser Pflichten grundsätzlich das Unternehmen selber nachweispflichtig ist. Jedem Architektur- oder Ingenieurbüro ist somit ungeachtet der ohnehin schon bestehenden Dokumentationspflichten zu raten, die zu verarbeitenden Daten auf das erforderliche Minimum zu reduzieren und sämtliche Schritte umfassend und letztlich nachweisbar festzuhalten.

Als ersten Anhaltspunkt für die sich aus der DSGVO sowie der BDSG ergebenen Rechte und Pflichten kann gut auf die von den jeweiligen Architektenkammern veröffentlichten Praxishinweise samt dazugehöriger Musterformulare oder entsprechende Broschüren zurückgegriffen werden. Dabei ist allerdings stets zu beachten, dass die darin enthaltenen Hinweise lediglich eine Erstinformation darstellen und die beigefügten Muster als Orientierungshilfe dienen sollen. Eine ggf. erforderliche individuelle Beratung kann und soll damit nicht ersetzt werden.

Foto: Ken Schluchtmann, diephotodesigner.de

Haftung und aktuelle Rechtsentwicklung

Gemäß Art. 33 DSGVO hat die für die Verarbeitung verantwortliche Stelle im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich eine entsprechende Meldung an die zuständige Aufsichtsbehörde abzugeben. Von einer solchen Meldung kann jedoch abgesehen werden, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Mit anderen Worten: Eine Meldung ist dann nicht erforderlich, wenn die Datenschutzverletzung im konkreten Fall gar keinen Schaden zur Folge haben kann oder wenn ein möglicher Schaden wahrscheinlich nicht eintreten wird und keine nachteiligen Auswirkungen für die betroffenen Personen absehbar sind.

Grundsätzlich stellt jedoch jeder Datenschutz-Verstoß erst einmal einen rechtswidrigen Zustand dar, der auszuräumen ist. Bei einem auf Unkenntnis beruhenden Erstverstoß ist allerdings davon auszugehen, dass dem kleinen Unternehmen keine oder nur kleinere Bußgelder drohen.

Dessen ungeachtet ist nach Maßgabe der DSGVO bei Verstößen gegen das Datenschutzrecht jedoch das Gesetz über Ordnungswidrigkeiten für die Verhängung von Geldbußen anwendbar (vgl. § 41 BDSG). Danach haben Datenschutzbehörden die Möglichkeit, Verstöße von Unternehmen bzw. juristischen Personen zu sanktionieren. Verstöße gegen Art. 13 DSGVO können beispielsweise mit einer Geldbuße von bis zu 20 Mio. EUR bzw. 4 % des weltweit erzielten Jahresumsatzes sanktioniert werden.

Darüber hinaus sieht **Art. 82 DSGVO** einen **Anspruch auf Schadensersatz** für (immaterielle) Schäden vor: Fällt dem Verarbeiter ein Datenschutzverstoß zur Last, können Betroffene Schadensersatz verlangen, wenn sich der Verarbeiter nicht exkulpieren kann (Abs. 3) und ein zurechenbarer Schaden entstanden ist.

Dies bedeutet jedoch nicht, dass sämtliche Verstöße gegen den Datenschutz eine solche Schadensersatzklage zur Folge haben. Maßgeblich kommt es vielmehr auf die Frage nach der Bemessung des vermeintlich entstandenen Schadens an.

In bislang knapp einem Dutzend veröffentlichten Urteilen wurde ein immaterieller Schadensersatz zugesprochen. Dabei variieren die zugesprochenen Beträge zwischen 300 Euro und 5.000 Euro.[1)] Auch das Landgericht Dresden beispielsweise hat einen solchen Schaden aufgrund einer versehentlichen Weitergabe von personenbezogenen Daten an einen Dritten bejaht und die Beklagte zur Zahlung eines Betrages in Höhe von EUR 1.000 verurteilt. Trotz der geringen persönlichen Beeinträchtigung, die das Opfer erlitten habe, habe nach Ansicht des erkennenden Gerichts jedenfalls ein hohes Risiko für die persönlichen Rechte und Freiheiten bestanden.[2)]

Diesen Entscheidungen stehen allerdings mindestens ebenso viele Urteile gegenüber, die einen Schadensersatzanspruch aufgrund des fehlenden immateriellen Schadens verneint haben. Beispielsweise hat das Oberlandesgericht Dresden die Berufung eines Klägers mit dem Hinweis zurückgewiesen, dass das Datenschutzrecht nicht dazu diene, Bagatellverstöße zu verhindern. Ein entsprechender Schadensersatzanspruch

[1] Schadensersatz für Datenschutzverstöße, Dr. Stefan Korch, NJW 2021, 978 Rn. 6
[2] LG Dresden, Urt. v. 26.05.2020 – 13 O 244/19

sei nicht bereits bei jeder individuell empfundenen Unannehmlichkeit oder bei Bagatellverstößen ohne ernsthafte Beeinträchtigungen für das Selbstbild oder Ansehen der betroffenen Person begründet. Vielmehr sei ein schwerwiegender Eingriff in das allgemeine Persönlichkeitsrecht erforderlich, dessen Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann.[3)]

Vermutlich aufgrund der vorgenannten Unstimmigkeiten bzw. der unterschiedlichen Schadensbeurteilung sah sich das Bundesverfassungsgericht jüngst dazu veranlasst, einer Verfassungsbeschwerde gegen eine weitere ablehnende Entscheidung recht zu geben. Nach Ansicht des BVerfG sei es unzulässig, eine wegen der Verletzung des Datenschutzes eingereichte Klage auf Zahlung eines Schmerzensgeldes wegen Fehlens eines erheblichen Schadens abzuweisen, ohne zuvor eine Entscheidung des EuGH zur Auslegung des Schadensbegriffs in Art. 82 DSGVO einzuholen.[4)]

Der pauschalen, mit Verweis auf Bagatellschäden gestützten Ablehnung entsprechender Schadensersatzklagen scheint damit (jedenfalls vorerst) ein Riegel vorgeschoben zu sein. Vielmehr muss sich die Rechtspraxis nun intensiver als bisher mit dem europäischen Charakter des datenschutzrechtlichen Schadensersatzanspruchs auseinandersetzt. Entsprechende Entscheidungen stehen bislang allerdings noch aus.

Versicherungsschutz

Nach den Allgemeinen GDV Muster Versicherungsbedingungen für die Berufshaftpflichtversicherung von Architekten, Bauingenieuren und Beratenden Ingenieuren (AVB Arch./Ing.) Stand Mai 2020 sind Schäden im Zusammenhang mit der Übertragung elektronischer Daten im folgendem Umfang mitversichert.[5)]

Gemäß Ziff. A1-6.11 ist die gesetzliche Haftpflicht des Versicherungsnehmers wegen Schäden aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten (z. B. im Internet, per E-Mail oder mittels Datenträger) versichert. Dies gilt jedoch nicht uneingeschränkt. Versicherungsschutz besteht für Schäden aus

a) der **Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung** von Daten (Datenveränderung) bei Dritten durch Computer-Viren und/oder andere Schadprogramme;
b) der Datenveränderung aus sonstigen Gründen sowie der Nichterfassung und fehlerhaften Speicherung von Daten bei Dritten und zwar wegen
- sich daraus ergebender **Personen- und Sachschäden,** nicht jedoch weiterer Datenveränderungen sowie
- der Kosten zur Wiederherstellung der veränderten Daten bzw. Erfassung/korrekten Speicherung nicht oder fehlerhaft erfasster Daten;

Erfasst werden sollen damit alle Fälle der Datenveränderung, unabhängig davon, ob diese durch einen Virus oder aus an-

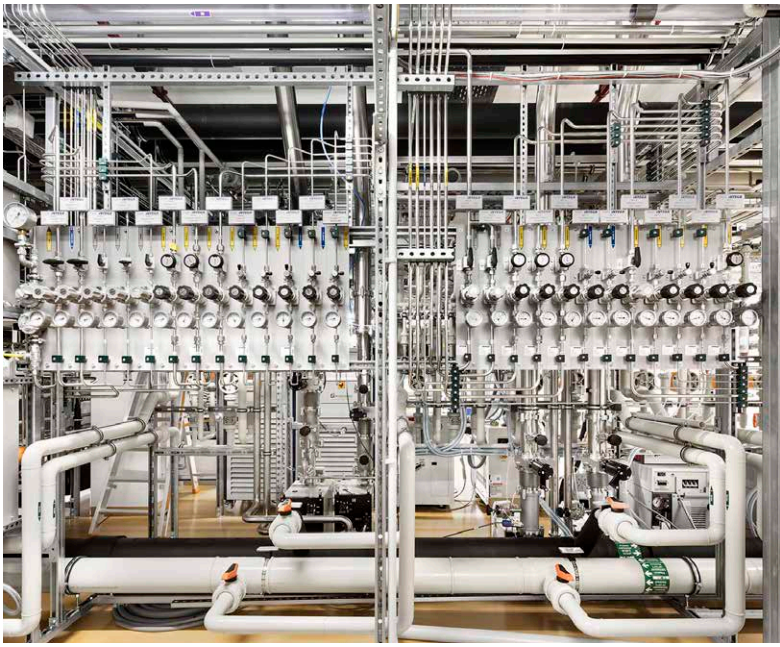


Foto: Ken Schluchtmann, diephotodesigner.de

deren Gründen entstanden sind. **Löschung** umfasst die Fälle, in denen eine Speicherung aufgehoben oder unwiederbringlich unkenntlich gemacht wurde. Der Begriff **Unterdrückung** von Daten beinhaltet, dass die Nutzung der Daten dem Berechtigten gegenüber dauerhaft oder zumindest für einen nicht unerheblichen Zeitraum entzogen wurden. **Unbrauchbar** sind Daten, wenn diese nicht mehr bestimmungsgemäß verwendet werden können. Veränderung erfasst jede inhaltliche Umgestaltung gespeicherter Daten[6)]. Darüber hinaus sind auch Fälle erfasst, in denen ohne physisches Einwirken auf den Datenträgers an sich – also z. B. durch Überschreibung – Schäden erfasst werden. Der Begriff Datenveränderung orientiert sich an § 303a des Strafgesetzbuch, nach dem die unbefugte Löschung, Unterdrückung, Unbrauchmachung oder Veränderung der Daten strafbar ist. Der Versicherungsschutz bezieht sich auf den Ersatz von Personen- und Sachschäden und der Kosten der Datenwiederherstellung. Ein Betriebsunterbrechungsschaden z. B. wäre damit nicht erfasst.

Versichert sind außerdem Schäden

c) der Störung des Zugangs Dritter zum elektronischen Datenaustausch

Da im elektronischem Datenverkehr auch Fälle denkbar sind, bei denen – ohne Datenveränderung – z. B. ein System vom Zugang zum Datenaustausch Ursache des Schadens ist, werden auch diese Fälle erfasst.

Voraussetzung bei den vorgenannten Punkten ist jedoch, dass die Daten mit ausreichenden Sicherheitsmaßnahmen und/oder Techniken wie z. B. eine Virenscanner gesichert waren, die dem Stand der Technik entsprechen.

Darüber beinhaltet der Versicherungsschutz auch – abweichend zu der sonstigen Deckung der Musterbedingungen –

d) **Schäden aus der Verletzung von Persönlichkeits- und Namensrechten.**

3 OLG Dresden, Urt. v. 11.06.2019 – 4 U 760/19
4 BVerfG, Beschl. v. 14.01.2021 – 1 BvR 2853/19
5 Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV)
6 Haftpflichtversicherung, Kommentar zu den AHB, Späte/Schimikowski, 2015, Ziff 7 AHB, Rdnr.420,

Hierfür besteht auch Versicherungsschutz für immaterielle Schäden.

Nicht versicherte Tatbestände:

Kein Versicherungsschutz besteht für folgende Tätigkeiten oder Leistungen:

- IT-Beratung, -Analyse, -Organisation, -Einweisung, -Schulung;
- Software-Erstellung, -Handel, -Implementierung, -Pflege;
- Netzwerkplanung, -installation, -integration, -betrieb, -wartung, -pflege;
- Bereithalten fremder Inhalte, z. B. Access-, Host-, Full-Service-Providing;
- Betrieb von Rechenzentren und Datenbanken;
- Betrieb von Telekommunikationsnetzen;
- Tätigkeiten, für die eine gesetzliche Pflicht zum Abschluss einer Vermögensschadenhaftpflichtversicherung, z. B. nach SigG/SigV, De-Mail-G, besteht

Vom Versicherungsschutz ausgeschlossen sind darüber hinaus Ansprüche, die im Zusammenhang stehen mit

- massenhaft versandten, vom Empfänger ungewollten elektronisch übertragenen Informationen (z. B. Spamming),
- Dateien (z. B. Cookies), mit denen widerrechtlich bestimmte Informationen über Internet-Nutzer gesammelt werden können;

Außerdem ausgeschlossen sind Ansprüche wegen Schäden, die von Unternehmen, die mit dem Versicherungsnehmer oder seinen Gesellschaftern durch Kapital mehrheitlich verbunden sind oder unter einer einheitlichen Leitung stehen, geltend gemacht werden und Versicherungsansprüche aller Personen, die den Schaden durch bewusstes Abweichen von gesetzlichen oder behördlichen Vorschriften sowie von schriftlichen Anweisungen oder Bedingungen des Auftraggebers oder durch sonstige bewusste Pflichtverletzungen herbeigeführt haben.

Darüber hinaus sehen Versicherungskonzepte am Markt zusätzlich die **Mitversicherung von Datenschutzverletzungen** vor, nach der Schäden – auch immaterielle – aus der Verletzung von Datenschutzgesetzen durch Verarbeitung personenbezogener Daten mitversichert sind. Damit sind z. B. auch die zuvor dargestellten Schadenersatzansprüche gemäß Art. 82 DSGVO vom Versicherungsschutz gedeckt. Bußgelder sind davon jedoch nicht erfasst, da es sich hierbei nicht um privatrechtliche Ansprüche handelt.

Aus dem bisher dargestellten ergibt sich ein bereits recht umfassender Versicherungsschutz im Zusammenhang mit der Verwendung oder Übertragung von Daten. Dieser Schutz hat aber natürlich auch Grenzen, die z. B. darin bestehen, dass nur bestimmte Schäden und nur Schäden, die bei Dritten eingetreten sind umfasst sind. Inwiefern eine Cyberdeckung hier eine sinnvolle Ergänzung sein kann erklärt Peter Bertram aus dem Bereich Cyberversicherung der HDI Versicherung AG.

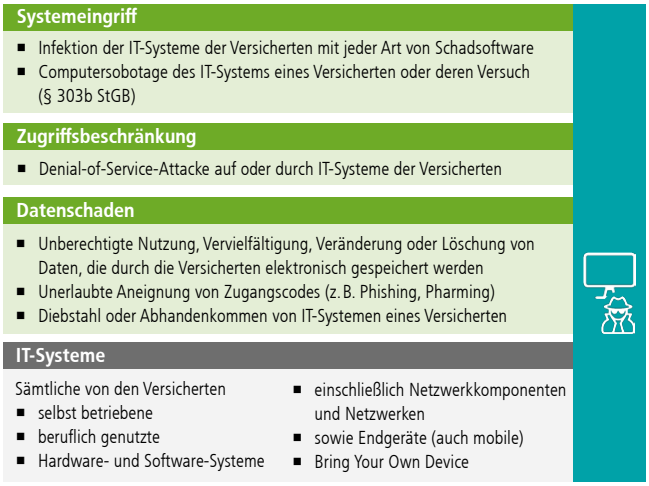
Berufshaftpflichtversicherung für Architekten und Ingenieure und Cyberversicherung

Um die Abgrenzung zu einer Cyberversicherung zu verdeutlichen, muss man sich im ersten Schritt die grundsätzliche Zusammensetzung der Cyberversicherung ansehen. Als wesentliches auslösendes Ereignis der Cyberversicherung steht hier die Informationssicherheitsverletzung. Diese setzt sich aus drei Bereichen zusammen: **Der Datenschutzverletzung**, der **Datenvertraulichkeitsverletzung** und der **Netzwerksicherheitsverletzung**.

Die **Datenschutzverletzung** umfasst die Verletzung von anwendbaren gesetzlichen Regelungen zum Datenschutz. Dies kann somit unter anderem auch die DSGVO bzw. das Bundesdatenschutzgesetzt sein, aber auch andere gesetzliche Regelungen.

Auch die **Datenvertraulichkeitsverletzung** umfasst elektronische wie physische Daten Dritter. Wo die Datenschutzverletzung vor allem personenbezogene Daten im Fokus hat, berücksichtigt die Datenvertraulichkeitsverletzung jegliche Art von Daten, also auch nicht personenbezogene Daten und schließt somit die Lücke. Inhaltlich geht es um die Datenvertraulichkeit (nur für bestimmten Personenkreis z. B. einsehbar), die Datenintegrität (nicht veränderbar) und die Datenverfügbarkeit (Verarbeitung/Verfügbarkeit muss gewährleistet werden).

Netzwerksicherheitsverletzung



Unter eine **Netzwerksicherheitsverletzung** fällt auch die Weitergabe von Schadsoftware an andere Unternehmen und umfasst daraus resultierende Schadensersatzansprüche oder auch das Ausspähen von Passwörtern – also das ganze Feld der „Hackerangriffe". Dabei ist es unerheblich, ob der Angriff gezielt auf ein Unternehmen stattgefunden hat, oder ob es sich um breit gestreute Angriffe, z. B. via schadhafter E-Mails, handelt.

Foto: Ken Schluchtmann, diephotodesigner.de

Ergänzt wird die Informationssicherheitsverletzung mit den auslösenden Ereignissen des Bedienfehlers (die unsachgemäße Nutzung oder Bedienung von IT-Systemen) sowie einer Cyber-Erpressung.

Im Gegensatz zu dem zuvor dargestelltem Versicherungsschutz der Berufshaftpflichtversicherung leistet die Cyberversicherung nicht nur im Bereich der Drittschäden, also von Haftpflichtansprüchen, sondern auch im Bereich der Eigenschäden oder auch der Betriebsunterbrechung. Somit sind z. B. Kosten Leistungsbestandteil, die auf die Wiederherstellung der eigenen IT-Systeme oder der eigenen Datenwiederherstellung abzielen.

Kosten für forensische Untersuchungen zur Feststellung des Schadenfalls, aber auch Kosten für rechtliche Beratung und PR-Maßnahmen z. B. wären ebenfalls gedeckt. Gerade durch das hohe Potenzial einer möglichen Betriebsunterbrechung können Cyberschäden eine existenzbedrohende Wirkung haben. Eine Betriebsunterbrechung kann nicht nur durch einen Hackerangriff entstehen, sondern auch aufgrund einer Stilllegung durch eine Datenschutzbehörde als Folge eines Datenschutzverstoßes. Auch hier bieten die meisten Deckungskonzepte entsprechende finanzielle Absicherung.

Oftmals wird unterschätzt, dass grundsätzlich jede Netzwerksicherheitsverletzung als Datenschutzverstoß zu sehen ist. Dieses ist vielen Unternehmen so nicht bewusst, daher sind Kosten für die Bewertung durch ein Krisenmanagement in der Cyberversicherung enthalten. Dieses gibt auch Empfehlung zu weiteren Schritten und bietet Unterstützung bei der Kommunikation mit Behörden. Die Cyberdeckung geht oftmals noch weiter, sodass auch Kosten für Callcenter Leistungen oder spezielle Websites umfasst sind, falls entsprechende Informationspflichten verhängt werden. Eines der wichtigsten Leistungsmerkmale einer Cyberversicherung ist das Managen des Dienstleisternetzwerkes, also der Experten im Schadenfall, je nach Bedarf und Schwere der Informationssicherheitsverletzung. Es ist vergleichbar mit einem Bauleiter, der den Überblick auf das Gesamtbauwerk hat und die einzelnen Gewerke steuert.

Zusammenfassung und Fazit

Datenschutz umfasst eine Fülle von Pflichten und kann unterschiedliche Risikosituationen mit sich bringen. Wichtig ist daher, dass Pflichten und Risiken bekannt sind, um sich entsprechend aufzustellen und abzusichern. Ein umfassender Versicherungsschutz ist in jedem Fall sinnvoll und empfehlenswert. Die Berufshaftpflichtversicherung der Architekten und Ingenieure bietet im Bereich Datenschutz eine gute Basis. Eine Ergänzung durch eine zusätzliche Absicherung mit einer Cyberversicherung bietet sich an, da vor allem Leistungen aus dem Bereich der Eigenschadendeckung – der von der Berufshaftpflichtdeckung nicht umfasst ist – den Versicherungsschutz abrunden. Eine Cyberversicherung bietet ein umfassend spezialisiertes Netzwerk an Dienstleistern und übernimmt im Schadenfall die Rolle des Krisenmanagers, um diese bestmöglich im Sinne der Kunden einsetzen zu können.

Autor

Mona Rizkallah
Syndikusrechtsanwältin
Produktmanagement Planungshaftpflicht
HDI Versicherung AG
Hannover
mona.rizkallah@hdi.de

Autor

Richard Koenn
Rechtsanwalt
Leinemann & Partner Rechtsanwälte mbB
Köln
Richard.Koenn@leinemann-partner.de

Autor

Peter Bertram
Produktmanagement Cyber
HDI Versicherung AG
Hannover
peter.bertram@hdi.de