



DATENSCHUTZGRUNDVERORDNUNG

Was Vermieter wissen müssen

Stand: 7. Juni 2018

Seit dem 25. Mai 2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Im Zuge dessen wurde das bisher in Deutschland geltende Bundesdatenschutzgesetz überarbeitet, welches neben den Regelungen der DSGVO auch für alle privaten Vermieter, Hausverwalter und Makler gilt.

Wer sich bisher noch nicht mit dem Datenschutzrecht beschäftigt hat, sollte sich nun mit den Anforderungen vertraut machen, um potenzielle Konflikte zu vermeiden. Denn im Falle datenschutzrechtlicher Pflichtverletzungen drohen Bußgelder sowie die Überprüfung der datenschutzrechtlich gebotenen Vorkehrungen durch die zuständige Landesdatenschutzbehörde.

Die sich aus der DSGVO ergebenden Pflichten sind vielfältig und können von privaten Vermietern nicht immer hundertprozentig erfüllt werden. Sich mit den neuen Regelungen auseinanderzusetzen ist für Vermieter erforderlich, um den Aufsichtsbehörden im Zweifelsfall Problembewusstsein und hinreichende datenschutzrechtliche Bemühungen aufzeigen zu können bzw. um einzelne Missstände und Lücken gegebenenfalls nach und nach zu schließen.

Da es sich bei der DSGVO um ein grundlegend neues Regelwerk handelt, sind viele darin enthaltenen Begriffe noch nicht näher definiert. Auch fehlt noch eine Judikatur zu strittigen Abgrenzungsfragen. Die folgenden datenschutzrechtlichen Ausführungen werden sich daher im Laufe der Zeit bestätigen oder werden durch anderslautende Rechtsprechung oder behördliche Entscheidungen dem jeweiligen Meinungsstand angepasst.

I. Persönlicher Anwendungsbereich

Natürliche Personen sind von dem Anwendungsbereich der DSGVO ausgenommen, wenn sie personenbezogene Daten ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten verarbeiten (Art. 1 Abs. 2 DSGVO). Alle geschäftlichen Prozesse eines privaten Vermieters unterfallen aber dem Anwendungsbereich, und zwar vollkommen unabhängig, ob er wenige oder viele Wohnungen vermietet.

Wenn der Zweck erreicht wurde und es keinen Grund für die weitere Datenaufbewahrung gibt (etwa wegen einzuhaltender Aufbewahrungsfristen nach der AO), müssen die Daten wieder gelöscht bzw. vernichtet werden.

II. Sachlicher Anwendungsbereich

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Dazu gehören unter anderem Namen und Adressdaten, Geburtsdaten, Bankdaten, Verbrauchsdaten. Werden personenbezogene Daten automatisiert, oder aber auch nicht automatisiert, verarbeitet und in einem Dateisystem gespeichert, müssen die Regelungen des Datenschutzrechts beachtet werden. Dabei liegt eine automatisierte Verarbeitung schon vor, wenn beispielsweise ein Kopierer oder ein Scanner benutzt wird. Auch handschriftliche Aufzeichnungen werden als nicht automatisierte Verarbeitung erfasst. Der Begriff der Datenverarbeitung ist dabei grundsätzlich weit auszulegen. Die Verarbeitung erfolgt u. a. durch das Erheben, Erfassen, Ordnen in Ablageordnern, Speichern, Verändern, Abfragen oder Verwenden (Art. 4 Nr. 2 DSGVO). Die

Offenlegung erfolgt durch das Übermitteln, Abgleichen, Verknüpfen sowie Löschen bzw. Vernichten personenbezogener Daten.

III. Grundsatz der Datenminimierung und Zweckbindung

Grundsätzlich gilt: Es ist unzulässig, so viele Daten wie möglich über Mieter und deren Familienangehörige zu sammeln (Grundsatz der Datensparsamkeit/Datenminimierung Art. 5 Abs. 1 lit. c DSGVO). Vielmehr dürfen nur die im Zusammenhang mit dem konkreten Zweck – zum Beispiel der Begründung eines Mietverhältnisses – erforderlichen Daten erhoben werden (Grundsatz der Zweckbindung Art. 5 Abs. 1 lit. b DSGVO). Vor jeder Datenerhebung ist daher ein konkreter Zweck zu ermitteln, nach welchem sich der Umfang der Datenverarbeitung bestimmt. Auch ist der Zweck für den zeitlichen Zusammenhang maßgeblich. Es geht also nicht darum, welche Daten der Vermieter möglicherweise zu einem späteren Zeitpunkt benötigt. Vielmehr muss er sich fragen, wozu er die Daten zum jetzigen Zeitpunkt konkret benötigt.

IV. Besondere Kategorie personenbezogener Daten

Daten zum Sexualleben und sexueller Orientierung, rassischer oder ethnischer Herkunft, religiöser Weltanschauung oder politischer Einstellung sind sogenannte Daten der besonderen Kategorie (Art. 9 DSGVO). Solche Daten dürfen nur in sehr engen Ausnahmefällen erhoben werden. Im Mietverhältnis ist eine solche Datenerhebung grundsätzlich unzulässig. Ausnahmsweise können die Daten über ethnische Herkunft und/oder Religion abgefragt werden, wenn es für eine Stabilisierung der Bewohnerstrukturen und einer ausgewogenen Siedlungsstruktur sowie für ausgeglichene wirtschaftliche, soziale und kulturelle Verhältnisse notwendig ist (DSK, Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressentinnen, Version 0.6 vom 30.01.2018). Dies muss im Einzelfall gut begründet werden, beispielsweise auf der Grundlage eines wohnungspolitischen Konzepts. Vermietern können solche Daten auch aufgedrängt werden, beispielsweise indem der Mieter selbst solche Daten ungefragt übergibt oder sich Mitmieter schriftlich äußern. Solche Daten sind dann zu löschen bzw. zu vernichten.

V. Keine Datenverarbeitung ohne Rechtsgrundlagen

Die Datenerhebung, Ablage und Weitergabe ist nur zulässig, wenn eine Rechtsgrundlage die Verarbeitung erlaubt. Insbesondere folgende Rechtsgrundlagen (Art. 6 DSGVO) können für die Verarbeitung personenbezogener Daten herangezogen werden:

- **VERTRAGSERFÜLLUNG (Art. 6 Abs. 1 lit. b DSGVO):** Wenn die Verarbeitung für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist und die Person, dessen Daten verarbeitet werden, Vertragspartner ist oder werden soll
- **BERECHTIGTE INTERESSEN (Art. 6 Abs. 1 lit. f DSGVO):** Wenn die Verarbeitung zur Wahrung berechtigter Interessen des verantwortlichen Vermieters oder eines Dritten erforderlich ist, sofern nicht schutzwürdige Interessen der Person, dessen Daten verarbeitet werden, überwiegen
- **RECHTSPFLICHT (Art. 6 Abs. 1 lit. c DSGVO):** Wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung des verantwortlichen Vermieters erforderlich ist
- **EINWILLIGUNG (Art 6 Abs. 1 lit. a DSGVO):** Wenn die Person, dessen Daten verarbeitet werden soll, der Datenverarbeitung zugestimmt hat

VI. Einwilligung als Rechtsgrundlage

Die Einwilligung als Rechtsgrundlage ist an verschiedene Voraussetzungen geknüpft (Art. 7 DSGVO). So muss sie freiwillig, d. h. ohne Druck oder empfundenen Zwang, erteilt werden. Dies kann beispielsweise bei der Datenerhebung bei Mietinteressenten in einem angespannten Wohnungsmarkt problematisch sein. Darüber hinaus kann die Einwilligung auch jederzeit widerrufen werden (Art. 7 Abs. 3 DSGVO). Der Vermieter ist im Streitfall für den Nachweis der Rechtsgrundlage, auf der er die Daten erhoben und gespeichert hat, verantwortlich, mithin für die erteilte Einwilligung. Bei der Berufung auf eine Einwilligung als Rechtsgrundlage ist daher Vorsicht geboten.

VII. Datenerhebung anlässlich der Besichtigung einer Wohnung

Unter der Maßgabe einer Datenminimierung und Zweckbindung benötigt der Vermieter nur Namen und Kontaktdaten der Interessenten, wenn er eine Wohnung inseriert und zunächst eine allgemeine Wohnungsbesichtigung durchführen will, ohne zuvor eine Auswahl unter den Mietinteressenten zu treffen. Denn weitergehende Daten sind für die Durchführung einer Besichtigung grundsätzlich nicht notwendig. Ausnahmsweise kann der Vermieter anlässlich der Besichtigung weitergehende Daten erheben. Beispielsweise wenn der Vermieter nur zuvor ausgewählten Interessenten einen Besichtigungstermin anbietet, etwa weil die Böden der Wohnung besonders empfindlich sind oder die Wohnung noch vermietet ist und jeder einzelne Termin mit dem aktuellen Mieter abgestimmt werden muss. In diesem Fall geht es um die Auswahl des richtigen Mieters, bevor ihm die Wohnung gezeigt wird. Auf der Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO) kann der Vermieter dann weitere Daten, wie die Mieterselbstauskunft, erheben. Bei der Rechtsgrundlage „berechtigtes Interesse“ gilt immer der Maßstab der Verhältnismäßigkeit. Interessen von Vermieter und Mietinteressenten müssen abgewogen werden. So sind Kontodaten für die Auswahl nicht erforderlich. Diese können mit Abschluss des Mietvertrages erhoben werden.

VIII. Aufgedrängte Daten

Übergibt der Mietinteressent unaufgefordert Unterlagen mit persönlichen Daten, die etwa zur besonderen Kategorie gehören oder die für die Begründung des Mietverhältnisses keine Rolle spielen, sind diese Daten zu löschen. Dies gilt streng genommen auch für Bewerbungsunterlagen, die vor der Besichtigung eingereicht werden. Eine Löschung kann aber dann unterbleiben, wenn der Mietinteressent sein Einverständnis erteilt, dass die Unterlagen bis zur endgültigen Mieterauswahl beziehungsweise zur Begründung des Mietverhältnisses beibehalten werden.

IX. Mieterselbstauskunft

Nach der Wohnungsbesichtigung hat der Vermieter ein Interesse daran, die Zuverlässigkeit und Zahlungsfähigkeit der verbliebenen Interessenten zu prüfen, bevor er sich für einen Mieter entscheidet. Hierzu dient die Mieterselbstauskunft. Als Rechtsgrundlagen für die Datenerhebung im Rahmen einer Selbstauskunft kommen ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO) oder auch die Vertragsanbahnung (Art. 6 Abs. 1 lit. b DSGVO) in Betracht.

Dem Grundsatz der Datensparsamkeit folgend dürfen nur die für den Vertragsabschluss relevanten Daten erfasst werden. Das Verwandtschaftsverhältnis des potenziellen Mieters zu einer bestimmten Person kann zwar eine relevante Information sein, wenn dieser nach einem 20 Jahre andauernden Mietverhältnis stirbt und ein Abkömmling in den Vertrag eintreten will. Diese Personendaten sind aber für den Zweck der Begründung des Mietverhältnisses nicht erheblich.

X. Umgang mit einer Warteliste

Möchte ein nicht berücksichtigter Interessent gern benachrichtigt werden, wenn eine andere vergleichbare Wohnung frei wird, kann der Vermieter nicht ohne weiteres auf die zum Zeitpunkt der ersten Wohnungsbesichtigung übergebenen Daten zurückgreifen. Denn der Zweck der Anmietung einer bestimmten Wohnung entfällt, wenn die vorherige Wohnung anderweitig vergeben wurde. Name und Kontaktdaten können nur dann vorgehalten werden, wenn der Interessent eine Einwilligung erteilt. Dann muss er darüber aufgeklärt werden, dass er diese jederzeit widerrufen kann. Auch muss sichergestellt werden, dass die Daten nicht dauerhaft gespeichert werden.

XI. Abschluss des Mietvertrages

Bei Abschluss des Mietvertrages werden erneut Daten, beispielsweise Kontodaten, erhoben. Die Rechtsgrundlage hierfür bildet die Vertragserfüllung (Art. 6 Abs. 1 lit.b DSGVO).

XII. Weitergabe von Daten an Dritte und Auftragsdatenverarbeitung

Auch die Weitergabe von Daten an Dritte, wie Handwerker oder andere Mieter, ist eine Datenverarbeitung und darf, wenn keine Einwilligung der Person vorliegt, nur erfolgen, wenn eine Rechtsgrundlage dies gestattet. Der Dritte ist selbst verantwortlich für den ordnungsgemäßen Umgang mit den Daten. Vorsorglich sollte der Vermieter den Dritten aber verpflichten, die Daten seiner Mieter nur in dem Rahmen zu verarbeiten, zu dessen Zweck diese übermittelt wurden. Darüber hinaus muss der Vermieter auch seine Mieter darüber informieren, dass er Daten weitergegeben hat.

Ein Vermieter kann auch Daten durch einen Dienstleister im Rahmen eines sogenannten Auftragsdatenverarbeitungsvertrages erheben und verarbeiten lassen (Art. 28 DSGVO). Der Auftragsdatenverarbeiter erhebt, speichert und bearbeitet Daten im Auftrag und nach Weisung des für den Datenschutz verantwortlichen Vermieters (Art. 4 Nr. 8 DSGVO). Als Abgrenzungskriterium für die Auftragsdatenverarbeitung gilt, dass allein der Vermieter entscheidet, welche Daten zu welchem Zweck und in welchem Umfang verarbeitet werden. Die Entscheidungen über die technisch-organisatorischen Fragen der Datenverarbeitung kann dann auf den Auftragsdatenverarbeiter übertragen werden (DSK, Kurzpapier Nr. 13, Auftragsdatenverarbeitung, Art 28 DSGVO vom 16.01.2018). Eine typische Auftragsdatenverarbeitung liegt beispielsweise bei der Beauftragung eines Unternehmens zur jährlichen Ablesung der Verbrauchsdaten und Erstellung der Heizkostenabrechnung vor.

Der Vermieter bleibt Verantwortlicher für den Datenschutz und muss mit dem Auftragsdatenverarbeiter zwingend einen schriftlichen oder elektronischen Vertrag mit dem Inhalt des Art. 28 DSGVO abschließen. Oftmals bieten die Dienstleister selbst die entsprechenden Verträge an. Ansonsten finden sich solche Verträge auch unter: https://www.lida.bayern.de/media/muster_adv.pdf.

XIII. Verbrauchsdatenerfassung durch Messdienstleister

Beim Ablesen der Verbrauchsdaten für Heizung und Warmwasser handelt es sich um eine Datenverarbeitung. Sie findet ihre Rechtsgrundlage in der Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO), weil die Datenerhebung zur Erfüllung der mietvertraglichen Abrechnungspflicht des Vermieters erforderlich ist. Die Mieter und möglichen Mitbewohner müssen über die Datenerhebung informiert werden (Art. 13 DSGVO). Dies kann entweder durch ein Informationsschreiben im Rahmen des Mietvertragsschlusses geschehen oder im Vorfeld der Ablesung durch ein entsprechendes Informationsschreiben. Da bei der Verbrauchserfassung durch einen Messdienstleister regelmäßig allein der Vermieter über die Verarbeitungszwecke und -mittel entscheidet, handelt es sich um eine Auftragsdatenverarbeitung (Art. 28 DSGVO), so dass ein Auftragsdatenverarbeitungsvertrag abzuschließen ist.

XIV. Einsichtsrecht eines Mieters in die Verbrauchsdaten der Mitmieter

Verlangt ein Mieter Einsicht in die Abrechnungsunterlagen zur Betriebskostenabrechnung, muss ihm der Vermieter auf Verlangen auch die Ablesbelege anderer Wohnungen im Haus vorlegen. Es handelt sich hierbei um eine Datenverarbeitung in Form der Weitergabe der Daten an Dritte. Eine Einwilligung der übrigen Mieter ist nicht erforderlich. Der Vermieter darf dem Mieter die Belege zur Verfügung stellen, denn er ist dazu mietrechtlich verpflichtet (zuletzt BGH, Urteil vom 7. Februar 2018, Az. VIII ZR 189/17). Der Vermieter kann sich gegenüber den betroffenen Mietern auf die Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 lit. f. DSGVO) berufen, da kein Grund zu der Annahme besteht, dass die übrigen Mietparteien ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Die übrigen Mieter und alle Mitbewohner müssen über die Datenweitergabe informiert werden (Art. 13 DSGVO).

XV. Weitergabe der Daten an Handwerker

Um seinen Instandhaltungspflichten nachzukommen, darf der Vermieter einen Handwerker beauftragen und ihm – sofern erforderlich – Namen und Kontaktdaten seiner Mieter benennen. Nach der hier vertretenen Auffassung handelt es sich um eine Weitergabe der Daten an Dritte, denn es werden fremde Fachleistungen bei einem eigenständigen verantwortlichen Dritten in Anspruch genommen, für die es einer Rechtsgrundlage bedarf. Als Rechtsgrundlage kommt bei Instandhaltungen und Modernisierungen die Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) sowie ein berechtigtes Interesse in Betracht (Art. 6 Abs. 1 lit. f DSGVO). Die Mieter sind über die Datenweitergabe zu informieren (Art. 13 DSGVO). Der Handwerker sollte verpflichtet werden, die Daten nach Erfüllung des Auftrages wieder zu löschen.

XVI. Weitergabe der Daten an den Steuer- oder Rechtsberater

Der Vermieter darf die Daten seiner Mieter – soweit erforderlich – auch im Rahmen einer Rechtsberatung bzw. zum Zwecke der Steuerberatung und -erklärung einem Anwalt bzw. Steuerberater übermitteln. Es handelt nicht um eine Auftragsdatenverarbeitung. Vielmehr wird eine fremde Fachleistung bei eigenständiger Verantwortung des Beraters in Anspruch genommen (DSK Kurzpapier Nr. 13, Auftragsdatenverarbeitung, Art. 28 DSGVO vom 16.01.2018). Bei einer Weitergabe von personenbezogenen Daten an Berufsgeheimnisträger – wie hier –, muss der verantwortliche Vermieter die Mieter hierüber nicht informieren (§ 29 Abs. 2 BDSG).

XVII. Mietverwaltung

Beauftragt der Vermieter eine Verwaltung mit der Mietverwaltung, ist dies kein Fall der Auftragsdatenverarbeitung. Die Verwaltung wird regelmäßig bevollmächtigt, selbstständig alle Entscheidungen bezüglich des Mietverhältnisses zu treffen. Es kommt auf den konkreten Verwaltervertrag an, denn häufig lässt sich in der Mietverwaltung eine gemeinsame Verantwortlichkeit konstruieren (Art 26 DSGVO.) Im Falle der gemeinsamen Verantwortung entscheiden mehrere über die Verarbeitungszwecke und -mittel, so dass gemeinsam festzulegen ist, wer von ihnen welche Verpflichtung der DSGVO erfüllt.

XVIII. Betroffenenrechte

1. Informationspflichten

Jeder Betroffene hat das Recht zu erfahren, welche Daten von ihm zu welchem Zweck gespeichert wurden (Art. 13 und Art. 14 DSGVO). Sofern die Person, deren Daten verarbeitet werden, die Daten selbst nicht übermittelt oder auch von der Verarbeitung, beispielsweise durch die Weitergabe an Dritte,

nichts weiß, muss sie über die Verarbeitung informiert werden. Dabei muss der Vermieter dem Betroffenen zum Zeitpunkt der Datenverarbeitung Folgendes mitteilen:

- Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten
- Zweck der Datenverarbeitung und Rechtsgrundlage sowie Dauer der Speicherung
- Gegebenenfalls Empfänger der personenbezogenen Daten
- Hinweis auf Auskunftsrecht, Beschwerderecht bei der zuständigen Aufsichtsbehörde, Widerspruchsrecht, Recht auf Löschung usw.
- Zusätzlich auch die Kategorien personenbezogener Daten, die verarbeitet werden, wenn die Datenerhebung nicht bei der betroffenen Person erfolgt

2. Auskunftsrecht

Das Auskunftsrecht (Art. 15 DSGVO) gibt dem Betroffenen zunächst nur einen Anspruch auf Bestätigung, ob der verantwortliche Vermieter überhaupt Daten der betroffenen Person verarbeitet. (Abs. 1 S. 1). Nur wenn personenbezogene Daten verarbeitet werden, steht dem Betroffenen ein weitergehendes Auskunftsrecht unter anderem auf folgende Informationen zu:

- die Verarbeitungszwecke
- die Kategorien der personenbezogenen Daten
- deren Empfänger im Falle der Offenlegung
- die geplante Dauer der Speicherung (Art. 15 Abs. 1 S. 2 lit. a bis c DSGVO).

Diesbezüglich hat der datenschutzrechtlich verantwortliche Vermieter eine Kopie der personenbezogenen Daten, die verarbeitet werden, dem Mieter auszuhändigen (Art. 15 Abs. 3 S. 1 DSGVO). Kopie bedeutet in diesem Zusammenhang lediglich, dass der Vermieter dem Auskunftsberechtigten eine Abschrift der verarbeiteten Daten zur Verfügung stellen muss (Kamlah in Plath, Kommentar zum BDSG und zur DSGVO, 2. Auflage, Köln, 2016 Art. 15 Rn. 16) Grundsätzlich ist die Auskunft kostenlos zu erteilen. „Für alle weiteren Kopien“ ist dem Vermieter zugebilligt, ein angemessenes Entgelt auf der Grundlage seiner Verwaltungskosten zu verlangen (Art. 15 Abs. 3 S. 2 DSGVO). Dies gilt insbesondere für Auskunftsverlangen, die unbegründet bzw. in unangemessen kurzen Abständen wiederholt gemacht werden.

Macht ein Mieter seine Rechte geltend, muss der verantwortliche Vermieter reagieren. Verlangt der Mieter beispielsweise Auskunft, hat der Vermieter die Daten des auskunftsverlangenden Mieters zusammenzustellen und ihm unverzüglich, regelmäßig, aber innerhalb eines Monats nach Eingang des Antrags, zur Verfügung zu stellen (Art. 12 Abs. 3 DSGVO.) Die Identität des Auskunftsverlangenden muss vor der Erteilung der Auskunft gesichert sein (vgl. Art. 12 Abs. 1 S. 3 letzter Halbsatz, Abs. 6 DSGVO), z. B. durch Vorlage eines Ausweisdokuments. Der Vermieter muss keine Abschrift der verarbeiteten Daten aushändigen, wenn er die Rechte und Freiheiten anderer Personen dadurch gefährdet (Art. 15 Abs. 4 DSGVO). Dies schließt auch seine eigenen Interessen ein. Übermittelt der Vermieter Daten seines Mieters an einen Rechtsanwalt oder Steuerberater, muss er darüber weder informieren (§ 29 Abs. 2 BDSG) noch Auskunft erteilen (§ 34 Abs. 1 BDSG). Die Ablehnung des Auskunftsverlangens ist aber zu dokumentieren.

3. Weitere Rechte

Daneben stehen dem Betroffenen auch noch folgende weitere Rechte zu:

- Berichtigung (Art. 16 DSGVO, Löschung § 35 BDSG-neu, Art. 18 DSGVO)
- Widerspruch gegen die Verarbeitung (§ 36 BDSG)
- Recht, keiner automatisierten Entscheidung unterworfen zu sein (§ 37 BDSG, Art. 22 DSGVO)

XIX. Löschfristen

Alle personenbezogenen Daten sind zu löschen, wenn diese für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (§ 17 DSGVO). Der Zeitpunkt des Wegfalls hängt also vom jeweiligen Zweck der Datenbearbeitung ab:

- Daten zu den Betriebskosten sind mindestens bis zum Ablauf der Mieter-Einwendungsfrist aufzubewahren (gemäß § 556 Abs. 3 S. 4 BGB zwölf Monate nach Zustellung der Abrechnung).
- Daten, die Vermieteransprüche betreffen, sind mindestens bis zum Ablauf der regelmäßigen Verjährungsfrist gem. § 195 BGB (drei Jahre) aufzubewahren.
- Im Falle eines Rechtsstreits sind die Daten nicht vor rechtskräftigem Abschluss des Rechtsstreits zu löschen.
- Mietverträge und Betriebskostenabrechnungsunterlagen sind gemäß § 147 AO zehn Jahre aufzubewahren.

XX. Verzeichnis der Datenverarbeitungstätigkeit

Ob auch private Vermieter als Verantwortliche ein sogenanntes Verzeichnis der Datenverarbeitungstätigkeiten (Art. 30 DSGVO) führen müssen, ist bisher nicht abschließend geklärt. Haus & Grund empfiehlt, ein solches Verzeichnisse zu erstellen. Ein Verzeichnisse ist immer dann zu führen, wenn die Verarbeitung von Daten nicht nur gelegentlich erfolgt (Art. 30 Abs. 5 DSGVO). Nach den Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO der DSK (Datenschutzkonferenz) liegt eine gelegentliche Datenverarbeitung bereits dann nicht mehr vor, wenn z. B. regelmäßig Lohnabrechnungen getätigt werden. Dieses Beispiel ist wohl gleichzusetzen mit der Abrechnung monatlicher Mieteinnahmen.

Das Verzeichnis der Datenverarbeitungstätigkeiten kann jederzeit bearbeitet und ergänzt werden. Auch hier gibt es kein verbindliches Muster. Erst die Praxis wird in den kommenden Jahren zeigen, wie die Anforderungen konkret auszusehen haben.

XXI. Technische und organisatorische Maßnahmen (TOM) ergreifen

Die Datenverarbeitungsgeräte (wie PC, Tablets, Smartphones etc.) müssen überprüft werden, um den Datenschutz zu gewährleisten. Denn die jeweils datenschutzrechtlich Verantwortlichen sind verpflichtet, geeignete technische und organisatorische Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Daten sicherzustellen (Art. 32 DSGVO, § 64 BDSG). Es gibt hierfür keinen standardisierten Katalog. Die Maßnahmen müssen unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignet und angemessen sein, um das Schutzniveau zu gewährleisten. Das bedeutet, dass bei einer privaten Vermietung weniger Wohnungen ohne Einsatz von eigenen Servern, Personal etc. andere technische Maßnahmen zu erwarten sind als von einer großen Hausverwaltung, die dutzende Datensätze, wechselndes Personal und Dienstleister beschäftigt.

Gemäß Art. 32 Abs. 1 DSGVO, werden folgende Maßnahmenbereiche für die nach Art. 30 DSGVO vorzunehmenden technischen und organisatorischen Maßnahmen vorgegeben:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen und technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen.

Darüber hinaus werden weitere Maßnahmenbereiche durch die Anforderung des § 64 BDSG ergänzt:

- **ZUGANGSKONTROLLE:** Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte
- **DATENTRÄGERKONTROLLE:** Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
- **SPEICHERKONTROLLE:** Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
- **BENUTZERKONTROLLE:** Verhinderung der Nutzung automatisierter Verarbeitungssysteme mithilfe von Einrichtungen zur Datenübertragung durch Unbefugte
- **ZUGRIFFSKONTROLLE:** Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben
- **ÜBERTRAGUNGSKONTROLLE:** Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
- **EINGABEKONTROLLE:** Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind
- **TRANSPORTKONTROLLE:** Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden
- **WIEDERHERSTELLBARKEIT:** Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können
- **ZUVERLÄSSIGKEIT:** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden
- **DATENINTEGRITÄT:** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können
- **AUFTRAGSKONTROLLE:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können
- **VERFÜGBARKEITSKONTROLLE:** Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind
- **TRENNBARKEIT:** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Folgende technische Schutzmaßnahmen können unter Beachtung des Verhältnismäßigkeitsgrundsatzes von privaten Vermietern, die selbst wenige Wohnungen vermieten und über kein Personal und Dienstleister verfügen, im Allgemeinen erwartet werden:

- Die Geräte müssen über einen aktuellen Anti-Viren-Schutz und eine aktuelle Firewall verfügen.
- Die Geräte müssen passwortgesichert sein. Das Passwort sollte Zahlen sowie eine Kombination aus Groß- und Kleinbuchstaben enthalten. Es sollte auch nicht zu kurz sein.
- Sofern Dritte – wie Familienangehörige – ebenfalls das Gerät benutzen, müssen Ordner mit personenbezogenen Daten passwortgesichert sein, sodass sie für Dritte nicht zugänglich sind.
- Die Weitergabe von Daten sollte verschlüsselt erfolgen. Sofern personenbezogene Daten per E-Mail versendet werden, ist eine Transportverschlüsselung (TLS- oder SSL-Verschlüsselung) erforderlich. Sofern Dienstleister Dokumentenmanagementsysteme zum Hochladen von Dateien und zur Kommunikation anbieten, die mit Benutzerkonto und individuellem Passwort gesichert sind, sollten diese genutzt werden. Sofern möglich, sollten Daten in anonymisierter oder pseudonymisierter Form weitergegeben werden.
- Von den Dateien sind regelmäßig Sicherheitskopien zu erstellen. Dabei sind die Löschpflichten zu beachten. Daher sollten die Datenträger regelmäßig überschrieben werden.
- Akten mit personenbezogenen Daten sind so aufzubewahren, dass Dritte keinen ungehinderten Zugang erhalten. Dies kann durch verschließbare Aktenschränke oder durch Abschließen des Raumes geschehen. Auch ausgedruckte E-Mails und Briefe dürfen nicht offen herumliegen.
- Bei der Benutzung von Mailverteiltern gilt: E-Mail-Adressen der anderen Empfänger dürfen nicht sichtbar sein (bcc-Einstellungen); nur verschlüsselte W-LANs sollten genutzt werden.
- Akten sind bei Ablauf der Löschfristen ordnungsgemäß durch den Einsatz von Aktenvernichtern oder durch Dienstleister zu vernichten. Auch Datenträger und Computer sind, nachdem sie aussortiert wurden, ordnungsgemäß zu löschen, beispielsweise durch Einsatz von professioneller Überschreibungssoftware.
- Etwaiges Reinigungspersonal ist sorgfältig auszuwählen.
- **Achtung:** Clouddienste sind regelmäßig Auftragsdatenverarbeiter, so dass Auftragsdatenverarbeitungsverträge abzuschließen sind. Dies ist bei E-Mail-Konten nicht der Fall.

XXII. Datenschutzbeauftragter

Ein Datenschutzbeauftragter muss nur dann bestellt werden, wenn in einem Unternehmen mindestens zehn Personen mit der automatisierten Datenverarbeitung von personenbezogenen Daten beschäftigt sind (Art. 37 Abs. 1 DSGVO, § 38 BDSG). Dies ist bei der privaten Vermietung regelmäßig nicht der Fall.

XXIII. Rechtsfolgen etwaiger Pflichtverletzungen

Die DSGVO sieht im Falle einer Verletzung ihrer datenschutzrechtlichen Pflichten eine diesbezügliche Meldung des Vorfalls an die zuständige Aufsichtsbehörde (Art. 33 DSGVO), eine dahingehende Benachrichtigung des Betroffenen (Art. 34 DSGVO) sowie als flankierende Sanktionen einen Schadensersatzanspruch der betroffenen Person (Art. 82 DSGVO) und die Verhängung von Bußgeldern (Art. 83 DSGVO) vor.

1. Melde- bzw. Benachrichtigungspflicht

Für den Fall einer Verletzung datenschutzrechtlicher Pflichten nach der DSGVO hat der datenschutzrechtlich verantwortliche Vermieter dies binnen 72 Stunden nach Bekanntwerden gegenüber der zuständigen Aufsichtsbehörde zu melden, wenn nicht ein Risiko für den Schutz der personenbezogenen Daten des Mieters der Voraussicht nach auszuschließen ist (Art. 33 Abs. 1 DSGVO). Plastische Beispiele für entsprechende Datenpannen können u. a. gehackte E-Mail oder Bankkonten sein.

Neben dem datenschutzrechtlich verantwortlichen Vermieter unterliegt auch der Auftragsdatenverarbeiter einer Meldepflicht: so ist dieser dem Vermieter zur unverzüglichen Meldung etwaiger Verletzungen verpflichtet (Art. 33 Abs. 2 DSGVO). Des Weiteren bestehen im Zuge einer Datenpanne besondere Dokumentationspflichten. Denn die im Zusammenhang mit der Verletzung stehenden Fakten, die konkreten Auswirkungen sowie von dem Vermieter ergriffene Abhilfemaßnahmen sind zu dokumentieren (Art. 33 Abs. 5 DSGVO).

Grundsätzlich ist auch der betroffene Mieter von einer Verletzung unverzüglich, d. h. ohne schuldhaftes Zögern (§ 121 BGB), zu benachrichtigen, soweit der Voraussicht nach ein „hohes Risiko“ für den Schutz seiner personenbezogenen Daten besteht (Art. 34 Abs. 1 DSGVO). Die DSGVO lässt aber die Benachrichtigungspflicht auch entfallen, und zwar insbesondere,

- wenn vorab geeignete Sicherheitsvorkehrungen getroffen wurden, die einen Drittzugriff ausschließen (Art. 34 Abs. 3 lit. a DSGVO) oder
- durch nachträgliche Maßnahmen dafür gesorgt ist, dass das Risiko für den betroffenen Mieter aller Wahrscheinlichkeit nach nicht mehr besteht (Art. 34 Abs. 3 lit. b DSGVO).

2. Schadensersatz und Bußgeld

Im Falle der Verletzung datenschutzrechtlicher Pflichten aus der DSGVO kann der Betroffene Ansprüche gegen den Verantwortlichen sowie den jeweiligen Auftragsverarbeiter geltend machen (Art. 82 Abs. 1 und 2 DSGVO).

Neben dem Schadensersatz ist auch die Verhängung von Bußgeldern durch die Aufsichtsbehörde als Sanktion für einen Pflichtverstoß möglich. Die Höhe des Bußgeldes steht im Ermessen der jeweiligen Behörde, wobei die DSGVO Kriterien (z. B. Vorsatz, Grad der Verantwortung, Art und Schwere des Verstoßes) zur Festsetzung enthält (Art. 83 Abs. 2 DSGVO) und diese in Abhängigkeit von dem konkreten Regelverstoß hinsichtlich der Bestimmungen der DSGVO bestimmt (Art. 83 Abs. 4 und 5 DSGVO).