

Verwalterthema des Monats

Datenschutz in der Immobilienverwaltung

Reinhold Okon, München

Im Büro eines Immobilienverwalters werden regelmäßig personenbezogene Daten über Kunden, Mitarbeiter, Lieferanten und Geschäftspartner verarbeitet. Das Bundesdatenschutzgesetz steckt den zulässigen Umgang mit diesen Daten ab. Verstöße können teuer werden. Dieser Beitrag gibt einen Überblick, wo das Thema Datenschutz für Verwalter Fallstricke bereithält. Einzelne Aspekte werden dann in weiteren Beiträgen näher betrachtet.

1. Die Verantwortung des Verwalters

Immobilienverwalter verfügen über so viele persönliche Daten anderer Personen (z. B. Eigentümer- und Mieterlisten, oft mit Geburtsdaten, Familienstand, Anzahl der Kinder, wirtschaftliche Verhältnisse usw.) wie kaum ein anderes Berufsbild in der Dienstleistungsbranche. Dies bringt eine große Verantwortung und Pflichten nach dem Bundesdatenschutzgesetz (BDSG) mit sich. Letztere werden oft eher stiefmütterlich behandelt.

Aber allein schon aus Eigeninteresse können sich Verwalter hier keine Fehler leisten. So kann es – einmal abgesehen von finanziellen Einbußen durch Strafen oder Bußgelder – den Ruf eines Unternehmens nachhaltig schädigen, wenn sich herumspricht, dass mit den sensiblen Daten nicht sorgfältig umgegangen wird oder diese gar in falsche Hände geraten. Hinzu kommt, dass Verwalter künftig von den Behörden wohl genauer beobachtet werden dürften.

GRUNDLAGE: § 9 BDSG

Zentrale Norm ist § 9 BDSG. Dieser schreibt fest, dass zum Schutz der personenbezogenen Daten von den Daten verarbeitenden Stellen die notwendigen technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten.

Hier ist nicht die blanke Investition in neue Technik gemeint; dies umfasst auch Schulungen der Mitarbeiter, um die Umsetzung des BDSG sicherzustellen. Denn die häufigsten Datenschutzverstöße entstehen aufgrund von Unachtsamkeit und Unwissenheit der Mitarbeiter. Die Geschäftsführung ist daher dazu verpflichtet, die eigenen Mitarbeiter für den Umgang mit personenbezogenen Daten zu sensibilisieren.

Um ein gewisses Maß an Rechtssicherheit zu erlangen, ist es besonders wichtig, Verarbeitungsprozesse und Abläufe im eigenen Unternehmen genauestens zu analysieren.

PRAXIS-TIPP: KRITISCHE ANALYSE

Gehen Sie einmal aus der Sicht eines Kunden – wenn dieser denn jetzt hereinkäme – durch Ihr Büro. Was kann man hören und sehen? Wo und wie werden geschäftsinterne Informationen verarbeitet und weitergegeben? Wo werden Akten abgelegt? Schriftverkehr und Korrespondenz liegen nicht selten auf einem Tresen und können von Besuchern gelesen werden.

Wie werden schützenswerte Daten an andere übermittelt? Per E-Mail ist meist Standard. Werden die Mails verschlüsselt? Die E-Mail ist eigentlich einer Postkarte gleichzusetzen. Jeder könnte sie mit geringem Aufwand lesen.

Wird täglich eine Datensicherung aller Daten gemacht? Wenn ja, wo werden diese Daten gegen Verlust (Feuer, Wasser, Diebstahl, Manipulation) aufbewahrt? Sind meine Mitarbeiter in der Lage, datenschutzkonform zu arbeiten? Wissen meine Mitarbeiter überhaupt, wie mit personenbezogenen Daten umgegangen werden muss?

Erst wenn ein Verwalter/Unternehmer sich dieser Analyse selbst unterzieht, setzt er automatisch den Grundstein für Datenschutz in seinem Unternehmen.

2. Schwachstelle EDV

Aufgrund unserer multimedialen Vernetzung, also der Kommunikationswege, über die Daten weitergegeben werden können, ist das Arbeiten sehr schnell und komfortabel geworden, aber alles andere als sicher. Heute gibt es einfachste Programme, die anderen Personen ermöglichen, einen Datenverkehr (z. B. E-Mail) mitzulesen. Allein schon das ständige Online-Sein des Unternehmens – der Internet-Flatrate sei Dank – bietet nahezu unbegrenzte Möglichkeiten, in das Netzwerk bzw. System einzudringen.

Viele verlassen sich auf ihren Systembetreuer, den „EDV-Menschen“. Dieser übernimmt sogar meist die Rolle des Datenschutzbeauftragten. Somit können schnell Probleme auf eine andere Person abgewälzt werden. Viele erforderliche Maßnahmen bleiben meist unausgesprochen oder werden dann nur spärlich umgesetzt. Dabei sind Immobilienverwalter gesetzlich verpflichtet, technische und organisatorische Maßnahmen zu treffen, um einen sicheren Betrieb der im Unternehmen eingesetzten EDV- und IT-Infrastruktur zu gewährleisten.

3. Grundgerüst des Datenschutzes

Die nachfolgenden Punkte stellen das primäre Gerüst in punkto Datenschutzkonformität für Immobilienverwalter dar:

Datenschutzbeauftragter

Wenn in einem Unternehmen mehr als neun Personen mit automatisierten oder mindestens 20 Personen die mit nichtautomatisierten Verfahren personenbezogene Daten erheben, bearbeiten oder nutzen, so muss ein Datenschutzbeauftragter bestellt werden. Dies kann ein Mitarbeiter (auch eine Aushilfe oder 400-Euro-Kraft) oder eine externe Person sein.

Auftragsdatenverarbeitung

Beauftragt der Verwalter ein anderes Dienstleistungsunternehmen, personenbezogene Daten für sich zu verarbeiten, so spricht man von einer Auftragsdatenverarbeitung. Hierunter fallen z. B. externe IT-Dienstleister, Steuerberater, Buchhaltungsservices und Unternehmen zur Akten- und Datenträgervernichtung. Ebenso können Dienstleistungsunternehmen im Bereich Gebäude- und Haustechnik betroffen sein, wenn sie Adressen, Telefonnummern und/oder E-Mail-Adressen bekommen, um sich mit den Mietern und Eigentümern abzustimmen.

Das Gesetz sieht den Dritten als ausführendes Organ („verlängerten Arm“) des Unternehmens an. Somit hat auch der Verwalter die Pflicht, sich vor der Auftragsvergabe selbst (u. U. sogar persönlich beim Auftragnehmer in dessen Büroräumen) davon zu überzeugen, dass der Auftragnehmer selbst datenschutzkonform aufgestellt ist, nach den Richtlinien zur Einhaltung des BDSG arbeitet und die nötige Sorgfalt im Umgang mit den zur Verfügung gestellten Daten einhält.

❗ WICHTIG:

Der Auftraggeber ist für die Einhaltung der Datenschutzvorschriften beim Auftragnehmer verantwortlich, nicht der Auftragnehmer!

Werden per Auftragsdatenverarbeitung erstmals Daten durch Dritte bearbeitet, müssen die betroffenen Personen benachrichtigt werden.

💡 PRAXIS-TIPP: GENERELLE INFORMATION

Eine Möglichkeit für eine solche Information ist, die Kunden pauschal darüber zu informieren, dass alle Partnerfirmen per Vereinbarung zur Auftragsdatenverarbeitung sich den Datenschutzbestimmungen unterwerfen und verpflichtet sind, alle Richtlinien und Gesetze gemäß BDSG anzuwenden und diese auch einzuhalten.

Mitarbeiterschulung und Verpflichtung

Alle Mitarbeiter, die personenbezogene Daten erheben, verarbeiten oder nutzen, sind nach § 5 BDSG auf die Einhaltung des Datengeheimnisses zu verpflichten und dementsprechend per Schulung zu unterweisen. In der Schulung werden im Allgemeinen Datenschutzgesetze etwas durchleuchtet und die Pflichten des Arbeitnehmers erhellte. Ebenso werden Praxisfälle von klassischen Verstößen angesprochen, um zu veranschaulichen, wo die häufigsten Defizite herrschen. Danach sollte eine Geheimhaltungsvereinbarung unterzeichnet werden.

Information und Auskunft an den Betroffenen

Betroffene können jederzeit Auskunft über die zu ihrer Person gespeicherten Daten verlangen. Von diesem Recht machen auch immer mehr Personen Gebrauch. Weiterhin haben sie das Recht, dass diese Daten wieder gelöscht, berichtigt oder verändert (z. B. nach einem Namenswechsel durch Heirat) werden. Daten für Vertrags-, Abrechnungs- und buchhalterische Zwecke sind hiervon i.d.R. nicht berührt.

Hier ist sicherzustellen, dass eine vollständige und richtige Auskunft über die Herkunft, die Verarbeitung, die Haltung und die Weitergabe der Daten gewährleistet ist. Der Verwalter muss also Auskunft darüber geben:

- Welche Daten wurden erhoben?
- Zu welchem Zweck wurden diese erhoben?
- Woher kommen diese Daten?
- Wer bekommt diese Daten noch?

Datenübermittlung

Das BDSG stellt an die Datenübermittlung besondere Anforderungen. Immer wieder ist festzustellen, dass in diesem Bereich die größten Datenschutzpannen und Verstöße stattfinden. Als Beispiel sei der Versand einer Liste mit Mieterdaten (Name, Adresse, Telefon, E-Mail, Geburtsdatum und Bankverbindung) per E-Mail genannt. Da es sich um personenbezogene Daten handelt, müssen Maßnahmen ergriffen werden, die die Sicherheit der Datenübermittlung gewährleisten. Der Verwalter sollte solche E-Mails entweder verschlüsseln oder einen anderen (sicheren) Übermittlungsweg, z. B. Einschreiben per Post, wählen.

Kontrollmaßnahmen nach § 9 BDSG

Bei den Kontrollmaßnahmen handelt es sich um Vorschriften und Voraussetzungen, die erfüllt werden müssen, um den Ansprüchen des BDSG gerecht zu werden – die sogenannten „8 Gebote des Datenschutzes“. Sie gehören zu den wichtigsten Fundamenten in punkto Datenschutz und Datensicherheit.

- Mit der **Zutrittskontrolle** werden Maßnahmen beschrieben, durch die unberechtigten Personen der körperliche Zutritt zu Datenverarbeitungsanlagen verwehrt werden soll. So sollten z. B. PCs möglichst nicht in Räumen mit Publikumsverkehr stehen.
- Mit der **Zugangskontrolle** werden Maßnahmen beschrieben, die das Eindringen unbefugter Personen in das EDV-System verhindern sollen. Beispiele sind die Vergabe von Passwörtern und das Sperren des PCs in der Pause oder bei längerer Abwesenheit vom Schreibtisch.
- Mit der **Eingabekontrolle** wird überprüft, welche Personen im Unternehmen zu welcher Zeit Veränderungen an personenbezogenen Daten vorgenommen oder diese gelöscht haben.
- Die **Zugriffskontrolle** soll sicherstellen, dass nur berechtigte Personen auf die benötigten Daten zugreifen können. Soll etwa eine Aushilfe oder der Hausmeister auf dieselben Daten zugreifen können wie die Buchhaltung? Dies muss im EDV-System per Rechtevergabe gesteuert werden.
- Im Rahmen der **Verfügbarkeitskontrolle** sollen sämtliche Maßnahmen ergriffen werden, die Daten vor Verlust durch Zerstörung und Beschädigung (z. B. durch Feuer, Wasserschaden, Stromausfall, Sturm) zu schützen. Maßnahmen sind hierbei z. B. der Einsatz einer unterbrechungsfreien Stromversorgung und die räumlich getrennte Aufbewahrung der Datensicherungsträger.
- Wenn zu unterschiedlichen Zwecken personenbezogene Daten erhoben werden, muss gewährleistet sein, dass diese Daten auf unterschiedlichen Datenträgern, Datenbanken etc. gespeichert werden. Eine Vermischung der Daten darf nicht stattfinden, besagt das **Trennungsgebot**.
- Die **Auftragskontrolle** stellt sicher, dass die im Auftrag verarbeiteten personenbezogenen Daten nur nach Weisung des Auftraggebers verarbeitet werden können. Hierbei ist es besonders wichtig, dass eine exakte Beschreibung zur Bearbeitung der personenbezogenen Daten vorliegt. Der Auftraggeber muss auch regelmäßig kontrollieren, dass der Auftragnehmer die geforderten Maßnahmen einhält. Hier sei nochmals erwähnt, dass die Auftragsdatenverarbeitung zu den größten Ursachen für Datenverlust zählt.
- Durch die **Weitergabekontrolle** soll schließlich sichergestellt werden, dass alle Datenträger, auf denen personenbezogene Daten gespeichert sind, von unbefugten Personen weder verändert, manipuliert, gelesen noch gelöscht werden können.

Betrachtet man diese 8 Gebote des Datenschutzes aus Sicht der Betroffenen (d. h. derjenigen, um deren Daten es geht), ist sehr gut nachvollziehbar, dass eine intensive Auseinandersetzung mit diesen Geboten unabdingbar ist. Hinzu kommt, dass Betroffene inzwischen häufig von ihrem Recht auf Schadensersatz Gebrauch machen, wenn aufgrund einer Missachtung der gesetzlichen Vorschriften ihr Persönlichkeitsrecht verletzt worden ist.

4. Gefährliche Sammelwut

In der letzten Zeit ist immer wieder festzustellen, dass viele Verwalter mehr Daten sammeln als nötig bzw. zulässig ist, z. B. im Bewerbungsbogen für eine Wohnung. Viele Verwalter versuchen schon während der ersten Wohnungsbesichtigung, so viele Informationen wie möglich über

den etwaigen zukünftigen Mieter abzufragen. Das Fragerecht des Vermieters bezüglich persönlicher Verhältnisse des Interessenten wird teilweise so ausschweifend angewandt, dass so mancher Mietinteressent so weit geht, sämtliche Daten von sich preiszugeben, in der Hoffnung, eine Zusage für die beworbene Wohnung zu bekommen.

Häufig findet man im letzten Abschnitt des Bewerbungsbogens die Klausel, dass ein Mietvertrag nur unter der Bedingung zustande kommt, dass die Angaben des Mieters vollständig und wahrheitsgemäß sind und Falschangaben zu einer Anfechtung des Mietvertrags oder einer Kündigung berechtigen sollen. Dies widerspricht nicht nur den Datenschutzvorschriften, sondern hilft im Einzelfall auch nicht weiter, da Mieter nur auf zulässige Fragen wahrheitsgemäß antworten müssen.

Übersicht: Zulässige und unzulässige Fragen an Mietinteressenten

Zulässige Fragen im Sinne des BDSG sind:

- Fragen nach dem Einkommen
- Fragen nach dem Familienstand
- Fragen über und Dauer des Beschäftigungsverhältnisses
- Fragen über Verbraucherinsolvenz oder Restschuldbefreiung
- Fragen zum Bezug von Arbeitslosengeld II
- Fragen zu Anzahl und Alter der Personen, die im Haushalt leben werden

Unzulässige Fragen im Sinne des BDSG sind:

- Fragen nach Zugehörigkeit zu einer Gewerkschaft
- Fragen nach laufenden Ermittlungsverfahren
- Fragen nach politischer Ausrichtung und/oder Parteizugehörigkeit
- Fragen nach Schwangerschaft und Kinderwünschen
- Fragen nach Vorstrafen
- Fragen nach der Mitgliedschaft in einem Mieterverein
- Fragen zur Dauer des vorigen Mietverhältnisses
- Fragen dazu, warum das vorherige Mietverhältnis beendet worden ist

5. Kontrollen durch die Behörden

Die Einhaltung der datenschutzrechtlichen Bestimmungen unterliegt der Kontrolle durch Aufsichtsbehörden. Hierbei müssen die Unternehmen mitwirken. Nach § 38 Abs. 3 BDSG haben Unternehmen die Pflicht, der Aufsichtsbehörde auf Verlangen alle erforderlichen Auskünfte unverzüglich zu erteilen.

Derzeit haben die Aufsichtsbehörden aufgrund mangelnden Personals zur Durchführung der Kontrollen in den Unternehmen noch wenig Aktionsmöglichkeiten. Allerdings dürften die Aufsichtsbehörden ein Unternehmen jedenfalls dann unter die Lupe nehmen, wenn ihnen ein Verstoß gemeldet wird, etwa ein Betroffener von seinem Auskunftspflicht Gebrauch macht, das Unternehmen diese Informationen aber nicht vollständig, rechtzeitig oder richtig erteilt hat. Stellt die Behörde den Tatbestand einer Ordnungswidrigkeit fest, droht ein Bußgeld von bis zu 50.000 Euro.

6. Fazit

Das BDSG verlangt ein Umdenken bezüglich der Prioritäten im Umgang mit Daten anderer Personen. Hier tun sich viele Immobilien- und Hausverwalter noch sehr schwer. Das BDSG ist zwar nicht sehr lang (knapp 50 Paragraphen), jedoch für viele so unübersichtlich, dass sie es schlichtweg unter den Tisch fallen lassen.

Dabei sollten Sie sich nicht auf das Argument „das haben wir schon immer so gemacht und es ist nie etwas passiert“ verlassen, denn diese Sicherheit trügt. Tatsache ist, dass bei Verfehlungen drastische Strafen drohen. Wenn man bedenkt, dass schon eine Übersendung einer simplen Excel-Liste mit Eigentümer- oder Mieterdaten per E-Mail in nicht verschlüsselter Form ein Verstoß gegen die technischen und organisatorischen Maßnahmen darstellt, ist es nur eine Frage der Zeit, dass hierbei etwas schiefgeht. Dann ist es zu spät und die Existenz des Unternehmens kann auf dem Spiel stehen. Lassen Sie es nicht darauf ankommen.



Weiterführende Informationen:

Datenschutz (WEG) → **636379**

DER AUTOR

Reinhold Okon ist Datenschutzbeauftragter des Bundesfachverbandes der Immobilienverwalter e.V. (BVI).

