Immobilienverband IVD

Das neue Datenschutzrecht

für die Praxis der Verwalter und Vermieter

Hier ist Immobilienkompetenz zu Hause

Impressum

Herausgeber
Immobilienverband Deutschland IVD
Bundesverband der Immobilienberater, Makler, Verwalter und Sachverständigen e.V.
Littenstraße 10, 10179 Berlin, Tel.: 0 30 – 27 57 26-0, Fax: 0 30 – 27 57 26-49
Mail: info@ivd.net
www.ivd.net

Layout
www.die-grafikagentur.de | Berlin; www.medienatelier.de

Die vorliegende Broschüre wurde mit inhaltlicher Unterstützung von ED Computer & Design erstellt.

8. März 2018

Inhalt

25. Mai 2018

I. Einleitung

Am 25. Mai 2018 tritt die Datenschutzgrundverordnung der EU (DSGVO) in Kraft. Die Verordnung| wird unmittelbar in sämtlichen Ländern der EU gelten. Gleichzeitig tritt die geänderte Fassung des Bundesdatenschutzgesetzes (BDSG) in Kraft, das ergänzend gilt.

Da schon das in Deutschland bisher geltende Datenschutzrecht sehr streng war, ergeben sich für deutsche Unternehmen keine schwerwiegenden Änderungen. Wichtig ist vor allem, dass die Anforderungen an das Verfahrensverzeichnis ausgeweitet worden sind (Art. 30 DSGVO).

Nach der DSGVO heißt dieses jetzt „Verzeichnis der Verarbeitungstätigkeit" und muss der Aufsichtsbehörde auf Verlangen vorgelegt werden. Neu sind auch die Transparenzpflichten in Gestalt einer Informationspflicht über die zu speichernden Daten gegenüber dem Betroffenen (Kunde, Mitarbeiter etc.). Wer sich bisher um das Datenschutzrecht nicht gekümmert hat, sollte dies jetzt tun, da die Prüfungen durch die Aufsichtsbehörden intensiver sein werden und auch höhere Bußgelder verhängt werden können.

Die nachfolgenden Informationen dienen insbesondere dem Verwalter und Vermieter von Wohnungen und sonstigen Flächen zur Umsetzung ihrer datenschutzrechtlichen Pflichten. Zahlreiche weitere Informationen, Orientierungshilfen finden sich im internen Bereich der Internetseite des IVD (www.ivd.net) und auf der Internetseite der Gesellschaft für Datenschutz und Datensicherheit e.V. (www.gdd.de).

1. Betroffene Unternehmen

Zur Einhaltung des Datenschutzrechts sind sämtliche Personen verpflichtet, die personenbezogene Daten verarbeiten. Hierzu gehören auch (private) Vermieter, Hausverwalter und Makler. Auf die Rechtsform oder die Größe des Unternehmens kommt es nicht an (Art. 4 Nr. 18 DSGVO). Auch kommt es nicht darauf an, ob der entsprechende Vertrag mit einem Verbraucher oder Unternehmer geschlossen wird. Lediglich die rein private Sammlung von Daten etwa in einem Fotoalbum oder privaten Telefonbuch ist nicht betroffen.

2. Zweck des Datenschutzes

Das Datenschutzrecht will erreichen, dass personenbezogene Daten nur in dem Umfang erhoben und gespeichert werden, in dem dies zur Erreichung des jeweiligen Zwecks (Vertragszweck oder zur Erfüllung gesetzlicher Verpflichtungen) erforderlich ist (Grundsatz der Datenminimierung, ehem. Datensparsamkeit, Art. 5 Abs. 1 c DSGVO). Entfällt dieser Grund später, etwa weil die gesetzliche Aufbewahrungspflicht abgelaufen oder der Vertragszweck erreicht ist, müssen die Daten wieder gelöscht werden.

Außerdem dürfen die Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben worden sind (Grundsatz der Zweckbindung).

3. Geschützte Daten

Dem Datenschutz unterliegen „personenbezogene Daten", die verarbeitet oder in einem Datensystem gespeichert werden. Als personenbezogene Daten gelten sämtliche Informationen, die einer Person zugeordnet werden können.

Dazu gehören insbesondere: Name, Anschrift, Telefonnummer, Steuernummer, Bankverbindung usw. Besonders strenge Regeln gelten für sensi-

ble Daten, wie beispielsweise über ethnische Zugehörigkeit, Sexualleben, Gesundheit etc. (Art. 9 DSGVO, §§ 22, 48 BDSG). Die Verarbeitung derartiger Daten ist grundsätzlich unzulässig.

Geschützt sind nur die Daten von natürlichen Personen. Daten juristischer Personen sind nicht geschützt. Allerdings sind die Daten derjenigen Personen geschützt, die für dieses Unternehmen handeln oder ihr Ansprechpartner sind.

Der Begriff der Verarbeitung von Daten ist sehr weitgehend und umfasst insbesondere das Erfassen, Organisieren, Ordnen, Speichern, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung und Offenlegung durch das Übermitteln von Daten.

Dies gilt nicht nur bei einer Verarbeitung mithilfe von Computern, sondern auch bei (analogen) Aufzeichnungen, die etwa handschriftlich erfolgen.

II. Verzeichnis der Verarbeitungstätigkeiten

Art. 30 DSGVO verlangt, dass jedes Unternehmen ein Verzeichnis seiner Verarbeitungstätigkeiten führt. Das Verzeichnis muss – anders als nach dem bisherigen Recht – nicht veröffentlicht werden. Auf Verlangen muss es jedoch der Aufsichtsbehörde vorgelegt werden. Das Verzeichnis muss bestimmte Mindestangaben enthalten, die in Art. 30 DSGVO genannt sind:

- Name und Kontaktdaten des Verantwortlichen (**Praxistipp:** An dieser Stelle müssen die Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten angegeben werden. Gemeinsam verantwortlich sind auch Auftragsverarbeiter.)

- Zweck der Verarbeitung (**Praxistipp:** Hier sollte aufgenommen, für welche Zwecke Daten von Betroffenen verarbeitet werden. Wobei hierunter vor allem das Kerngeschäft zu verstehen ist, wie etwa der Abschluss und die Durchführung von Mieterverträgen für die verwalteten Grundstücke sowie der Abschluss und die Durchführung von Verwalterverträgen. Hier können auch Beschäftigungsverhältnisse oder andere Verträge Erwähnung finden.)

- Beschreibung der Kategorien betroffener Personen und die Kategorie personenbezogener Daten (**Praxistipp:** Hier ist aufzunehmen, welche personenbezogenen Daten je Personengruppe wie Mietinteressent, Mieter, Handwerksunternehmen oder übrige Dienstleister erhoben werden, z.B. Name, Kontaktdaten. Das Geburtsdatum sollte nur erhoben werden, wenn dies unbedingt erforderlich.)

- Kategorie von Empfängern von Daten einschließlich Empfänger Drittstaaten inkl. Dokumentation geeigneter Garantien (**Praxistipp:** Hier sollte in- und externen Empfängern von Daten unterschieden werden.)

- Vorgesehene Fristen zur Löschung (**Praxistipp:** Grundsätzlich haben Personen, von den personenbezogene Daten erhoben wurden, ein Recht auf Vergessen, so dass ihre Daten auf Verlangen zu löschen sind. Dieser Löschung können jedoch gesetzliche Regelungen

wie die Abgabenordnung entgegenstehen. Von dieser sind beispielsweise alle Unterlagen und Angaben, die für die Besteuerung des Verantwortlichen relevant. In der Regel stehen einer Löschung vertragliche Interessen des Verantwortlichen entgegen. So darf er natürlich alle Unterlagen aufheben, mit denen er einen Anspruch begründen oder abwehren kann, wobei der Zugriff durch beispielsweise unbeteiligte Mitarbeiter einzuschränken ist. Dies sind beispielsweise Verträge, Geschäftsbriefe etc. Sobald etwaige Ansprüche verjährt sind, sind die Unterlagen zu löschen, es sei denn, spezialgesetzliche Regelungen stehen entgegen (z.B. Abgabenordnung).

Im internen Bereich des IVD und www.ivd.net findet sich ein Musterverzeichnis im MS Word-Format zum Download sowie eins im Anhang dieser Publikation. Weitere Arbeitshilfen und Vorlagen finden sich im Internet auf der Seite der Gesellschaft für Datenschutz und Datensicherheit e.V.
https://www.gdd.de/

Praxistipp 1

Es empfiehlt sich das Verzeichnis in Gestalt einer Tabelle zu führen. Um eine Übersichtlichkeit und Lesbarkeit zu gewährleisten, empfiehlt es sich ggfls. sogar für jede Verarbeitungstätigkeit ein eigenes Dokument anzulegen, die Gesamtheit der Verarbeitungstätigkeiten bilden dann das Verzeichnis der Verarbeitungstätigkeiten.

III. Datenverarbeitung

Die Verarbeitung der Daten ist nur dann zulässig, wenn hierfür eine Rechtsgrundlage besteht (Verbot mit Erlaubnisvorbehalt, Art 6 Abs. 1 DSGVO). Als Rechtsgrundlage kommen nur in Betracht:

- Vertragserfüllung und Vertragsanbahnung
- Erfüllung einer rechtlichen Verpflichtung
- Wahrung der berechtigten Interessen
- Einwilligung des Betroffenen.

Die Daten von Mietinteressenten und Mietern dürfen erhoben und verarbeitet werden, um das Mietverhältnis anzubahnen und ggfls. den Mietvertrag erfüllen zu können (Art. 6 Abs. 1 b DGSVO).

Praxistipp 2

Auf eine Einwilligung des Mieterinteressenten kann man sich grundsätzlich nicht berufen, weil es insofern regelmäßig an der Freiwilligkeit des Betroffenen fehlen dürfte. Nach Art. 4 Nr. 11 DSGVO muss jede Einwilligung freiwillig sein und aufgrund ausreichender Information erfolgen (vgl. auch Art. 7 DSGVO). Die erforderliche Freiwilligkeit des Mietinteressenten fehlt jedoch, wenn ein erheblicher Nachfrageüberhang besteht und er sich dadurch gezwungen sieht, seine Daten etwa in einem Selbstauskunftsbogen anzugeben, um die Wohnung zu erhalten. Dies gilt auch dann, wenn die Felder in einem Selbstauskunftsbogen mit Hinweis „freiwillige Angabe" versehen ist. Außerdem setzt die Wirksamkeit einer Einwilligung die Einhaltung erheblicher Formalien voraus, die in der Praxis kaum gewährleistet werden können. Als Rechtsgrund sollte deshalb bei Verarbeitung der Daten von Vertragspartnern stets und ausschließlich der Rechtsgrund „Vertragserfüllung bzw. vorvertragliche Maßnahmen" angegeben werden.

IV. Informations- und Transparenzpflicht der Verwalter und Vermieter

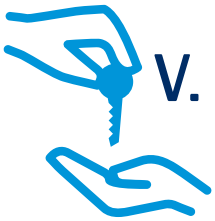
Werden personenbezogene Daten bei der betroffenen Person erhoben (z.B. Interessent oder Vermieter), so muss der Verwalter/Vermieter der betroffenen Person zum Zeitpunkt erstmaligender Erhebung dieser Daten informieren, welche erstmaligen Daten auf welche Art und Weise verarbeitet werden.

Über folgende Daten muss der Verwalter/Vermieter informieren:

- Namen und die Kontaktdaten des Verantwortlichen und ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Falls die Daten weitergegeben werden, die Kategorie der Empfänger (Vermieter, Ablesedienst, Handwerker)
- Verarbeitungszwecke und Rechtsgrundlage
- die Dauer der Speicherung
- die Rechte des Verbrauchers

Auf welche Art und Weise, die Information erfolgen muss, ist in Art. 12 DSGVO geregelt. Danach sind die Informationen der betroffenen Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Es empfiehlt sich eine übersichtliche Gestaltung in Form einer Tabelle (siehe Muster XIII., 2.). Im „Online-Bereich" kann auch auf eine Datenschutzerklärung verwiesen werden.

Allerdings ist davon auszugehen, dass ein bloßer Verweis auf eine im Internet bereitgestellte Datenschutzinformationen bei einer Direkterhebung von personenbezogenen Daten im „Offline-Bereich" nicht zulässig ist. Der Betroffene muss daher vor Ort informiert werden. Erfolgt die Erfassung von Kundendaten per Telefon, erscheint es zulässig, dass der Verwalter/Vermieter im Nachgang des Gespräches die Information per Email übersendet.



V. Verwalter- und vermieter-spezifische Besonderheiten

1. Vermietung einer Wohnung

Bevor es zum Mietvertrag kommt, werden verschiedene Daten zu unterschiedlichen Zeitpunkten erhoben. Dabei gilt der Grundsatz der Datenminimierung. Andererseits will der Verwalter im Auftrag des Vermieters schon möglichst viel über den Interessenten wisse, um abschätzen zu können, ob der Mietinteressent in Frage kommt.

Häufig werden von den Aufsichtsbehörden folgende Fragen und Sachverhalte beanstandet:

- **Kontaktdaten aus vorangegangenen Mietverhältnissen**

Diese Frage ist unzulässig. Sie ist zum einen für den Abschluss eines Mietvertrages nicht erforderlich und widerspricht zum anderen dem Grundsatz der Direkterhebung.

- **Bonitätsauskünfte**

Die undifferenzierte Forderung nach Vorlage einer „Schufa-Auskunft" oder „Schufa-Selbstauskunft" ist vor der Besichtigungunzulässig.

Diese Auskünfte enthalten deutlich mehr Datenktegorien als spezielle (häufig kostenpflichtige) zur Weiterleitung an Dritte geeignete Produkte undführen somit zu einer über das erforderliche Maß hinausgehenden Erhebung von Daten.

Erst wenn der Abschluss des Mietvertrags unmittebar bevorsteht, dürfen Bonitätsauskünfte bei Auskunfteien erfragt oder die Vorlage einer Bonitätauskunft durch (z. B. Schufa-Auskunft) die potentielle Mietpartei verlangt werden. Vor der Besichtigung darf lediglich gefragt werden, ob die Bonität ausreichend ist.

Praxistipp 3

Welche Daten von dem Mietinteressenten zu welchem Zeitpunkt erhoben werden dürfen, kann dem Ratgeber Nr. 10 des Berliner Beauftragten für den Datenschutz entnommen werden (www.datenschutz-berlin.de). Eine Orientierungshilfe und weitere Informationen hierzu finden sich auf der Internetseite der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten" und das Musterformular „Selbstauskunft zur Vorlage bei der Vermieterin oder dem Vermieter" sind abrufbar unter https://www.ldi.nrw.de/

Diese Hilfen sind zwar noch vor dem Inkrafttreten der DSGVO entstanden, sie haben aber noch uneingeschränkte Gültigkeit, da sich insoweit nichts geändert hat.

Praxistipp 4

Vor dem Besichtigungstermin darf der Vermieter grundsätzlich nur den Namen des Mietinteressenten und seine Kontaktdaten erfragen. Außerdem darf nach der Anzahl der Mitmieter, einem Wohnberechtigungsschein und etwaigen Haustieren gefragt werden. Ist die Wohnung noch bewohnt (ausgenommen Kleintiere), sind allerdings auch die schutzwürdigen Interessen des derzeitigen Mieters zu berücksichtigen. Um zu vermeiden, dass die Wohnung auch von Personen besichtigt wird, die als Mieter nicht in Betracht kommen, darf in diesem Fall bereits vor der Besichtigung gefragt werden, wie hoch das Einkommen ist, wobei auf die Vorlage von Nachweisen zu diesem Zeitpunkt verzichtet werden sollte.

• Angaben zum Familienstand
Wird lediglich die Mieterin oder der Mieter Vertragspartei, sind Angaben zum Familienstand für die Entscheidung über den Abschluss eines Mietvertrages nicht erforderlich und daher im Ergebnis unzulässig. Nahe Familienangehörige wie Ehegatten, Lebenspartner und Kinder dürfen nämlich auch ohne Erlaubnis in der Wohnung wohnen. Deshalb sind auch die Fragen zu Geburtstag sowie Verwandtschaftsverhältnis der zum Haushalt gehörenden Kinder und sonstigen Angehörigen nicht erforderlich und im Ergebnis unzulässig. Die Frage nach den Namen sowie dem Alter der einziehenden Personen ist dagegen zulässig.

• Fragen zum Beruf
Nach dem Beruf und Arbeitgeber/in darf zur Beurteilung der Bonität gefragt werden. Die Dauer einer Beschäftigung bietet jedoch in einer mobilen Gesellschaft keine Gewissheit für die Beständigkeit einer Beschäftigung. Diese Frage ist daher nicht geeignet, das Sicherungsbedürfnis einer Vermieterin oder eines Vermieters zu erfüllen und ist damit unzulässig.

• Personalausweiskopie
Kopien des Personalausweises sind bei Vermietungen in der Regel unzulässig. Gestattet ist allerdings, die Angaben zur Identität durch Vorlage des Personalausweises zu prüfen und das Ergebnis schriftlich festzuhalten. Notiert werden dürfen die zur Personenidentifikation notwendige Daten: Name und Vorname, Geburtsdatum und Anschrift. Eine weitergehende Notiz, zum Beispiel zur Seriennummer des Personalausweises, darf nicht erfolgen.

• Nutzung von Online-Kontaktformularen
Soweit es sich bei den Online-Formularen um ein allgemeines Kontaktformular handelt (HTTPS erforderlich), ist eine Antwort per E-Mail ausreichend. Die zusätzliche Angabe von Telefonnummer und/oder Anschrift als Pflichtfeldangabe ist damit nicht erforderlich und daher nicht gestattet.

(Quelle: Auszug aus Internetseite der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen)

Praxistipp 5

Kommt es nicht zu Abschluss eines Mietvertrages müssen die Daten des Mietinteressenten wieder gelöscht werden. Die Daten dürfen nur solange gespeichert bleiben, wie der Mietinteressent möglicherweise Ansprüche aus dem allgemeinen Gleichstellungsgesetz geltend machen kann (§ 19 AGG). Nach § 15 Abs. 4 AGG müssen solche Ansprüche innerhalb von zwei Monaten geltend gemacht werden. Wenn der Mietinteressent wünscht, dass seine Daten gespeichert bleiben, damit er informiert wird, „wenn wieder eine Wohnung frei wird", ist dies nur zulässig, wenn die formalen Voraussetzungen einer wirksamen und nachweisbaren Einwilligung (Art. 7 DSGVO) vorliegen.

2. Mieterhöhung bis zur ortsüblichen Vergleichsmiete (§ 558 Abs. 2 BGB)

Nach § 558 Abs. 2 BGB kann der Vermieter von dem Mieter verlangen, dass dieser einer Erhöhung der Miete auf die ortsübliche Vergleichsmiete zustimmt. Ein solches Mieterhöhungsverlangen ist nach § 558 a Abs. 1 BGB nur wirksam, wenn es begründet wird. Hierzu kann der Vermieter auf den Mietspiegel verweisen oder ein Sachverständigengutachten vorlegen.

Gem. § 558 a Abs. 2 Nr. 4 BGB kann der Vermieter sein Mieterhöhungsverlangen auch durch die Angabe von drei Vergleichswohnungen begründen. Nach der Rechtsprechung muss diese Vergleichswohnung so genau bezeichnet werden, dass der Mieter diese ohne weitere Nachforschungen aufsuchen kann, um die behauptete Vergleichbarkeit zu überprüfen.

Auch wenn der Vermieter den Namen des Mieters der Vergleichswohnung nicht angibt, kann der Mieter diesen anhand der angegebenen Adresse und Lage der Wohnung ausfindig machen. Damit handelt es sich bei der Miete der Vergleichswohnung um personenbezogene Daten des Mieters dieser Wohnung.

Dennoch ist die Mitteilung der Vergleichswohnung zulässig, weil der Vermieter dies tun muss, um seine Rechte aus dem Mietverhältnis zu wahren (Berechtigtes Interesse, Art. 6 Abs. 1 f DSGVO). Der Vermieter ist jedoch verpflichtet, dem Mieter der Vergleichswohnung mitzuteilen, dass und wem er die Höhe der Miete seiner Wohnung mitgeteilt hat.

3. Mietpreisbremse, Angabe der Vormiete

Nach der Mietpreisbremse darf die Anfangsmiete bei Neuvermietung einer Wohnung in der Regel höchstens 110 Prozent der ortsüblichen Vergleichsmiete betragen. War die Vormiete höher, kann stattdessen auch diese vereinbart werden.

Wenn der Mieter von dem Vermieter die Benennung der Vormieter verlangt, ist der Vermieter hierzu nach dem Mietrecht verpflichtet. In diesem Fall offenbart der Vermieter dem neuen Mieter personenbezogene Daten des Vormieters. Auch wenn er den Namen des Vormieters nicht nennt oder diesen in der Kopie des Vormietvertrages schwärzt, dürfte der Mieter ihn leicht ermitteln können. Dazu ist der Vermieter datenschutzrechtlich berechtigt, weil er hierzu zivilrechtlich verpflichtet ist (Art. 6 Abs. 1 lit. c) DSGVO). Allerdings muss er dem Vormieter mitteilen, dass er dem neuen Mieter seine Miete mitgeteilt hat.

4. Namen und Daten von Nachbarn

Vor Abschluss des Mietvertrages fragen Wohnungssuchende häufig, wer die neuen Nachbarn sind. Diese Frage darf nur pauschal beantwortet werden. Keinesfalls dürfen die Namen der Mitmieter, deren Berufe, Alter etc. mitgeteilt werden. Das Gleiche gilt gegenüber dem Käufer einer Eigentumswohnung.

Dem Käufer eines Mietwohnhauses muss vor dem Kauf die Mieterliste ausgehändigt werden, weil dieser hierauf einen zivilrechtlichen Anspruch hat. Natürlich sollte der Verwalter dies nur im Auftrag des Verkäufers machen. Weitere Daten über die Mieter, wie Telefonnummer, Beruf etc., dürfen jedoch nicht mitgeteilt werden.

5. Fotos der Wohnung

Bei Verkauf und Vermietung einer Wohnung werden in der Regel Fotos der Wohnung angefertigt. Ist die Wohnung noch bewohnt, bedarf es dazu der Zustimmung des Mieters. Der Eigentümer hat aber grundsätzlich einen Anspruch darauf, dass der Mieter derartige Fotos duldet.

Dem Mieter ist jedoch darzulegen, zu welchem Zweck die Fotos angefertigt werden. Nach Möglichkeit sollten die Fotos in Anwesenheit der Mieter gemacht werden. Der Mieter sollte jedoch keinesfalls auf dem Foto zu sehen sein. Wenn die Fotos keine Rückschlüsse auf die Person des Mieters zulassen, dürfen sie auch im Internet veröffentlicht werden. Im Zweifel sollten Verwalter oder Vermieter die Fotos gemeinsam mit dem Mieter sichten sich diese freigeben lassen.

6. Untervermietung

Möchte der Mieter einen Untermieter aufnehmen, benötigt er die Genehmigung des Vermieters.
Hierzu muss der Mieter dem Vermieter Namen und Anschrift des vorgesehenen Untermieters nennen. Weitere Angaben muss der Mieter nur in Ausnahmefällen machen.

7. Videoüberwachung durch Vermieter

Nach § 4 BDSG ist eine Videoüberwachung nur zulässig, wenn dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

a) öffentlich zugängliche Räume

Bei der Videoüberwachung von

- öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder

- Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse. Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

b) Innenbereich

Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses, etwa in den Kellerräumen oder den Aufgängen liegt ein berechtigtes Interesse nur vor, wenn die Situation typischerweise gefährlich ist, wie etwa in Selbstbedienungsläden oder Juweliergeschäften.

In üblichen Mehrfamilienhäusern dürfte dies nicht der Fall sein. Hier dürfte ein solches Interesse nur dann vorliegen, wenn konkrete Straftaten vorgekommen sind und deshalb ein besonderer Schutz vor Straftaten erforderlich ist oder zivilrechtliche Schadenersatzansprüche geltend werden müssen. Die abstrakte Abschreckung von Straftätern rechtfertigt eine dauerhafte Videoüberwachung dagegen nicht.

Gemäß § 4 Abs. 2 und 4 BDSG müssen jedenfalls der Umstand der Videoüberwachung sowie der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar gemacht werden.

Außerdem müssen der Zweck der Überwachung und die Dauer der Speicherung angegeben werden. Hierzu empfiehlt es sich, entsprechende Hinweisschilder anzubringen. Werden die Daten einer bestimmten Person zugeordnet, muss die betroffene Person gemäß Art. 13 und 14 DSGVO informiert werden.

Natürlich unterliegen die Aufzeichnungen der Zweckbindung und müssen gelöscht werden, wenn ihre Speicherung nicht mehr erforderlich ist (§ 4 Abs. 5 BDSG). Außerdem gilt gemäß Art. 9 Abs. 1 DSGVO grundsätzlich ein Verbot der Verarbeitung biometrischer Daten zur Identifizierung einer natürlichen Person.

Zu bedenken ist außerdem, dass Mieter und deren Besucher sich mit zivilrechtlichen Unterlassungs- und Abwehransprüchen gegen einen etwaigen Eingriff in das Persönlichkeitsrecht wehren können. Denn eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses, zum Beispiel in Treppenaufgängen, im Fahrstuhlvorraum und im Fahrstuhl selbst, stellt einen schweren Eingriff in das Persönlichkeitsrecht der Betroffenen dar.

In der hierzu ergangenen zivilrechtlichen Rechtsprechung besteht Einigkeit darüber, dass eine Rundumüberwachung des sozialen Lebens nicht dadurch gerechtfertigt werden kann, dass der Vermieter mit der Überwachung Schmierereien, Verschmutzungen oder einmaligen Vandalismus verhindern möchte. In der Regel überwiegen daher die schutzwürdigen Interessen der Mieter und Besucher als Betroffene.

8. Weitergabe der Daten an Handwerksunternehmen

Die Weitergabe der Kontaktdaten des Mieters an Handwerksunternehmen zur Durchführung von Instandsetzungs- und Instandhaltungsmaßnahmen ist auch ohne Einwilligung des betroffenen Mieters zulässig, weil dies zur Erfüllung der mietvertraglichen Pflichten des Vermieters erforderlich ist. Selbstverständlich ist das Handwerksunternehmen

anzuhalten, den Datenschutz zu beachten und die erhaltenen Daten zu löschen, wenn sie nicht mehr benötigt werden.

9. Weitergabe der Daten an Dienstleister, Auftragsverarbeitung (Art. 88 DSGVO,)

Die Weitergabe der Daten des Mieters an Dienstleister wie z.B. Unternehmen zur Heizkostenabrechnung, ist auch ohne Einwilligung des betroffenen Mieters zulässig, weil es sich bei den Unternehmen um Auftragsverarbeiter handelt. Eine solche – privilegierte – Auftragverarbeitung liegt vor, wenn das Unternehmen, an das der (Verwalter/Vermieter) die Daten weitergibt, den Auftrag weisungsabhängig erfüllt und allein der Verwalter (Vermieter) über die Verwendung der Daten entscheidet.

Erforderlich ist, dass der Verwalter mit dem beauftragten Unternehmen einen speziellen Vertrag über die Auftragsverarbeitung abschließt, der das Weisungsrecht des Verwalters festlegt, die zu erledigenden Aufgaben genau beschreibt und das beauftragte Unternehmen zur Vertraulichkeit und zur Einhaltung der Datensicherheit verpflichtet.

Außerdem muss genau festgelegt werden, was mit den Daten nach Abschluss der Arbeiten geschieht (Art. 28 Abs. 3 DSGVO). Grundsätzlich hat der Verantwortliche das Recht, den Auftragsdatenverarbeiter zu überprüfen, ob er selbst die datenschutzrechtlichen Bestimmungen einhält. In der Praxis wird dies oftmals nicht berücksichtigt.

Praxistipp 6

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Verantwortlicher eine andere Stelle damit betraut, personenbezogene Daten zu verarbeiten, wobei entscheidend ist, dass der Beauftragte weisungsabhängig ist („verlängerte Werkbank"): externe Lohnbuchhaltung (auch durch Steuerberater), externe Buchhaltung, Ablesedienstleister, Werbeadressenverwaltung in einem Lettershop, Aktenvernichter. Keine Auftragsdatenverarbeitung liegt bei einer beratenden Tätigkeit durch einen Steuerberater oder Rechtsanwalt oder Bank vor, da es grundsätzlich an der Weisungsbefugnis mangelt.

Oftmals haben die Dienstleister entsprechende Musterverträge. Sollte dies nicht der Fall sein, findet sich ein Formulierungsvorschlag auf der Internetseite des IVD (www.ivd.net), der Aufsichtsbehörde des Landes Bayern https://www.lda.bayern.de/media/muster_adv.pdf oder der Gesellschaft für Datenschutz und Datensicherheit e.V. (www.gdd.de).

Praxistipp 7

Der Verwalter muss eine Liste der von ihm beschäftigten Auftragsverarbeiter führen. Außerdem sind die Auftragsverarbeiter im Verzeichnis der Verarbeitungstätigkeiten als „gemeinsame Verantwortliche" zu benennen.

10. Verbrauchsdaten

Verbrauchsdaten (Heizung, Wasser, Datenlogger) sind personenbezogene Daten. Ihr Verarbeitung Ist zur Vertragserfüllung erforderlich, weil der Verwalter sie benötigt, um die mietvertraglichen Abrechnungspflichten bzw. die Instandhaltungspflichten zu erfüllen.

Da die Erhebung der Daten nicht bei den betroffenen Personen erfolgt, sind diese gem. Art. 14 DSGVO über die Datenerhebung zu informieren.

Wollen Mieter zur Kontrolle der Abrechnung die Verbrauchswerte der übrigen Mieter erfahren,

haben Sie hierauf mietrechtlich grundsätzlich einen Anspruch und dürfen die Belege einsehen.

Die Weitergabe der Daten durch den Verwalter ist zulässig, weil er dazu mietrechtlich verpflichtet ist (Art. 6 Abs. 1 lit. c DSGVO) und er nur dadurch seine berechtigten Interessen wahren kann (Art. 6 Abs. 1 lit. f DSGVO).

11. Vermieterbescheinigung

In einigen Fällen erhält der Mieter von dem Jobcenter eine sog. „Vermieterbescheinigung", die der Vermieter ausfüllen soll, da sonst keine Leistungsbewilligung möglich sei. Die Weitergabe der Daten an das Jobcenter ist nicht zulässig, da der Vermieter hierzu rechtlich nicht verpflichtet ist. Nach § 67 a Abs. 2 SGB X sind Sozialdaten bei dem Betroffenen zu erheben (vgl. BSG, Urteil vom 25. Januar 2012, Az. B 14 AS 65/11 R 1).

12. Löschung der Daten

a) Daten des Mietinteressenten

Kommt es nicht zum Abschluss eines Mietvertrages müssen die Daten des Mietinteressenten wieder gelöscht werden. Die Daten dürfen nur solange gespeichert bleiben wie der Mietinteressent möglicherweise Ansprüche aus dem allgemeinen Gleichstellungsgesetz geltend machen kann (§ 19 AGG).

Derartige Ansprüche müssen innerhalb von zwei Monaten nach Absage geltend gemacht werden. Nach h.M. sollen die Daten aller Mietinteressenten deshalb grundsätzlich drei Monate aufbewahrt werden.

b) Daten des Mieters

Gemäß Art. 17 DSGVO sind die Daten des Mieters zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden.

c) Betriebskosten

Daten über die Betriebskosten sind mindestens so lange aufzubewahren bis die Frist für Einwendungen des Mieters abgelaufen ist. Dies sind gemäß § 556 Abs. 3 Satz 4 BGB 12 Monate nach Zustellung der Abrechnung.

d) Daten über Ansprüche des Vermieters

Daten über Ansprüche des Vermieters gegen den Mieter sind bis zum Ablauf der regelmäßigen Verjährungsfrist nach § 195 BGB gespeichert zulassen. Im Falle eines Rechtsstreits mit dem Mieter sind die Daten bis zum rechtskräftigen Abschluss des Gerichtsverfahrens aufzubewahren.

VI. Gesetzliche Aufbewahrungspflichten

Gesetzliche Aufbewahrungspflichten etwa nach dem Handelsgesetzbuch (HGB) oder der Abgabenordnung (AO) gehen der Löschungspflicht nach dem Datenschutzrecht vor. Nach dem Handels- und dem Steuerrecht müssen Bücher, Aufzeichnungen, Jahresabschlüsse und alle Verträge die Grundlage für Zahlungspflichten oder Zahlungsansprüche des Verwalters oder sonst für die Besteuerung des Verwalters relevant sind, 10 Jahre aufbewahrt werden.

Die Daten des Hauseigentümers muss der Verwalter daher nach Beendigung des Verwaltungsvertrages aus steuer- und handelsrechtlichen Gründen noch 10 Jahre aufbewahren. Auch die Daten von Auftragnehmer, an die der Hausverwalter Zahlungen geleistet hat, muss er 10 Jahre aufbewahren.

Fristbeginn ist in der Regel der 31. Dezember des Jahres, in dem die jeweilige Erhebung erfolgt.

VII. Datenschutzbeauftragter

Ein Datenschutzbeauftragter muss bestellt werden, wenn in dem Unternehmen mindestens 10 Personen beschäftigt sind, die personenbezogene Daten verarbeiten (Art. 37 Abs. 1 DSGVO und § 38 BDSG). Maßgeblich ist die Anzahl der beschäftigten Personen, auch wenn diese nur in Teilzeit arbeiten oder sich in der Berufsausbildung befinden. Auch wenn keine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, kann dieser freiwillig bestellt werden (Art. 37 Abs. 4 Satz 1 Halbsatz 1 DSGVO).

Als Datenschutzbeauftragter kann ein eigener Mitarbeiter oder ein externer Dienstleister beauftragt werden (Art. 37 Abs. 6 DSGVO). Ein eigener Mitarbeiter darf die Funktion allerdings nur ausüben, wenn es dabei nicht zu einem Interessenkonflikt kommt (Art. 38 Abs. 6 Satz 2 DSGVO). Der EDV-Verantwortliche dürfte daher in aller Regel nicht als Datenschutzbeauftragter geeignet sein. Die Kontaktdaten des Datenschutzbeauftragten müssen der Aufsichtsbehörde mitgeteilt werden (Art. 37 Abs. 7 DSGVO).

Die Form der Benennung muss nicht mehr zwingend schriftlich erfolgen. Dies ist jedoch empfehlenswert, um die Nachweispflichten aus Art. 24 Abs. 1 DSGVO und Art. 5 Abs. 2 DGSVO erfüllen zu können. Eine schriftliche Benennung dient ferner der Rechtssicherheit.

Bereits nach dem BDSG erfolgte Bestellungen behalten grundsätzlich ihre Gültigkeit. Anderenfalls müssen sie angepasst werden.

Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen (bspw. auf der Webseite) und der Aufsichtsbehörde mitzuteilen.

Praxistipp 8

Ein Datenschutzbeauftragter ist gesetzlich vorgeschrieben, wenn mehr als neun Personen ständig mit der Verarbeitung von personenbezogenen Daten befasst sind. Dabei gilt das Kopfprinzip. Ist ein Datenschutzbeauftragter nicht erforderlich, befreit dies nicht von den übrigen Pflichten.

VIII. Auskunftsrecht

Der Betroffene hat das Recht (Art. 15 DSGVO), zu erfahren, welche seiner Daten zu welchem Zweck gespeichert sind und wie sie genutzt werden. Auf Antrag des Betroffenen muss der Verwalter ihm daher kostenlos mitteilen, welche Daten von ihm gespeichert sind, wozu die Speicherung erfolgt und wann die Daten gelöscht werden. Außerdem muss der Betroffene auf sein Beschwerderecht bei der Aufsichtsbehörde hingewiesen werden.

IX. Verpflichtung von Beschäftigten auf das Datengeheimnis

Das neue Datenschutzrecht sind im Gegensatz zur alten Regelung keine schriftliche Belehrung und Verpflichtung der Beschäftigten auf den Datenschutz vor. Dennoch sollte jedes Unternehmen seine Mitarbeiter, die für die Verarbeitung personenbezogener Daten verantwortlich sind, vor der Aufnahme der Tätigkeit schriftlich auf die Vertraulichkeit der Daten verpflichten (vgl. Art. 32 Abs. 4 DSGVO).

Praxistipp 9

Eine Verpflichtung von Beschäftigten auf das Datengeheimnis kann auch im Arbeitsvertrag aufgenommen werden.

X. Technische und organisatorische Maßnahmen zum Schutz der Daten (TOM), (Art. 32 Abs. 1 DSGVO)

Das Unternehmen muss gemäß Art. 32 Abs. 1 DSGVO technische und organisatorische Maßnahmen treffen, um die Daten wirksam zu schützen. Dabei sollen die Eintrittswahrscheinlichkeit und die Schwere des Risikos einer Verletzung des Datenschutzes berücksichtigt werden. Die Einhaltung dieser Maßnahmen unterfällt der Rechenschaftspflicht (Art. 5 Abs. 5 DSGVO).

Die DSGVO fordert:

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste,
- die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten soweit möglich,

- eine rasche Wiederherstellung der Daten und Zugänge nach einem physischen oder technischen Zwischenfall

- sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Zu berücksichtigen sind dabei:

- der Stand der Technik,

- der Implementierungskosten,

- Art, Umfang, Umstände und Zwecke der Verarbeitung

- sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere von Datenschutz-Risiken.

Welche Maßnahmen dies sein können, können Sie unserer Ausfüllhilfe für die technischen und organisatorischen Maßnahmen für die einzelnen Kontrollziele entnehmen. Wichtig ist hierbei die erforderliche Risikoanalyse, da die Eintrittswahrscheinlichkeit und Risiken eine entscheidende Rolle spielen.

Wie die Bezeichnung schon aussagt, sind nicht alle Maßnahmen technischer Natur – natürlich ist die Sicherstellung und Überprüfung damit häufig einfacher. Es gibt jedoch auch viele Punkte die organisatorisch geregelt werden müssen. Das heißt es ist eine ganze Reihe an Arbeitsrichtlinien zu definieren und sicherzustellen bspw.:

- Arbeitsplatz/IT-Policy beinhaltet bspw. CleanDesk Regelung inkl. Bildschirmsprerre, Passwort-Regelungen, Umgang mit Wechseldatenträgern, Nutzung und Installation von Software/Diensten, Vernichtung von Papier/Datenträgern

- Mobile Device Policy beinhaltet bspw. Verschlüsslung, erforderlichen Passwortschutz, Meldepflicht bei Verlust, keine Weitergabe an Dritte, keine sensiblen Telefonate/Datennutzung in der Öffentlichkeit

- E-Mail Policy – dienstlicher E-Mail Account, nur dienstlich!

- Internet-Policy

- Meldepflicht bei Datenpannen Policy

- HomeOffice Policy

XI. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung

Gemäß Art. 25 DSGVO soll bereits bei der Einführung technischer Verfahren die Grundsätze des Datenschutzes berücksichtigt werden. Beispielsweise soll die eigene Webseite ausschließlich unter HTTPS aufrufbar sein, wenn dort Kontaktformulare vorhanden sind (Privacy by design). Außerdem sollen sämtliche Voreinstellungen datenschutzfreundlich gestaltet sein (Privacy by default). Daher sollten Formulare nur Felder für Daten enthalten, deren Angabe zur Vertragserfüllung erforderlich ist (keine freiwillig auszufüllenden Felder).

Praxistipp 10

Kontaktformulare erfreuen sich enormer Beliebtheit. Bei der Gestaltung sind jedoch die Grundsätze des Datenschutzes zu beachten, insbesondere die sog. Datenminimierung (bisher Datensparsamkeit). Zudem ist darauf zu achten, dass keine Felder vorausgefüllt oder Häkchen bereits gesetzt sind (opt-out). Diese müssen stets vom Betroffenen gesetzt werden (opt-in).

XII. Behördliche Aufsicht

Die Einhaltung des BDSG wird durch Aufsichtsbehörden der Länder überwacht (Art. 51 ff DSGVO). Die Aufsichtsbehörden sind befugt, die Geschäftsräume des Unternehmens während der Geschäftszeiten zu betreten und dort die Unterlagen einzusehen. Bei Verstößen gegen die DSGVO kann die Behörde ein Bußgeld von bis zu 20 Mio. Euro oder 4% des Vorjahresumsatzes (je nachdem was höher ist) verhängen. Hierbei können verbundene Unternehmen als Unternehmensgruppe mitbetrachtet werden.

XIII. Datenschutzerklärung nach § 13 TMG

Nach § 13 Telemediengesetz (TMG) muss der Betreiber einer Webseite den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in allgemein verständlicher Form unterrichten. Außerdem muss der Nutzer darüber aufgeklärt werden, dass er die Möglichkeit hat, die Einwilligungen zur Nutzung seiner Daten jederzeit zu widerrufen. Es muss gewährleistet sein, dass der Nutzer bereits zu Beginn des Nutzungsvorgangs, d. h. bei Aufruf der Startseite des Internetangebots, einen eindeutigen Hinweis auf die Unterrichtung erhält und dieser Hinweis sofort erkennbar ist.

Diese Voraussetzungen sind nach Auffassung der Aufsichtsbehörden bei der Aufnahme von Ausführungen zum Datenschutz unter einem Link auf das „Impressum" für nicht gegeben. In der Praxis sind die datenschutzrechtlichen Ausführungen daher häufig unter einem eigenen Link mit Bezeichnungen wie „Datenschutzerklärung", „Datenschutzhinweis" und ähnliche zu finden.

Praxistipp 11

Die Datenschutzerklärung kann eine idealer Weg sein, um den Transparenzpflichten (Art. 13 DSGVO) zu genügen, wenn hier die entsprechenden Angaben enthalten sind und bei Kontaktformularen ein entsprechender Verweis vorhanden ist, idealerweise mit einem zu setzenden Häkchen.

Beim Einsatz der Reichweitenmessung durch Google Analytics muss der Webseitenbetreiber den Webseitennutzer in seiner Datenschutzerklärung über den Einsatz von Google Analytics informieren und ihn auf seine Möglichkeiten des Widerspruchs durch den Einsatz des Browser-Plugins hinweisen.

Die entsprechende Seite muss hinsichtlich der Widerspruchsmöglichkeit verlinkt sein. Hinweise zum datenschutzkonformen Einsatz von Google Analytics finden sich auf der Seite des Landesamtes für Datenschutz Bayern unter:

http://lda.bayern.del

Da IP Adressen als personenbezogene Daten gelten, ist hier die anonymisierte Erfassung zu aktivieren. Zusätzlich ist mit Google eine entsprechende vertragliche Vereinbarung zu schließen. Zuvor erfasste Daten sind zu löschen.

Verletzungen der Vorgaben für die Datenschutzerklärung aus § 13 TMG können nach Auffassung einiger Gerichte gemäß §§ 3, 4 Nr. 11 UWG wie eine Verletzung von § 5 TMG kostenpflichtig abgemahnt werden.

XIV. E-Mail-Marketing/Newsletter

Im Online-Marketing spielt der Newsletter eine große Rolle. Möchte der Unternehmer bestehenden Newsletter-Empfängern weiterhin den Newsletter zustellen, müssen folgende Voraussetzungen erfüllt sein (vgl. § 7 Abs. 3 UWG):

- Unternehmer hat E-Mail-Adresse im Zusammenhang mit einem Vertrag erhalten (in Betracht kommt hier nur der Verwaltervertrag).
- Unternehmer will Adresse für eigene Zwecke verwenden (nicht Angebote Dritter)
- Kunde hat Verwendung der E-Mail-Adresse nicht widersprochen.
- Kunde wurde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann (Button: Newsletter abbestellen)

Neuabonnenten dürfen grundsätzlich nur aufgenommen werden, wenn sie hierzu ihre Einwilligung geben. Eine bestimmte Form ist für diesen Fall nicht vorgeschrieben.

Ausreichend ist eine eindeutig bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Dies kann das Anklicken eines Kästchens beim Besuch einer Internetseite sein. Das Opt-Out-Verfahren ist nach der DSGVO unzulässig.

Bietet ein Unternehmer einen Newsletter auf seiner Webseite an, sollte er diesen in der Datenschutzerklärung berücksichtigen, die ebenfalls auf der Webseite zur Verfügung gestellt wird.

XV. Anlagen/Muster

Die nachfolgenden Muster können verwendet werden, wobei eine Verwendung auf eigene Gefahr erfolgt. Die Muster erheben keinen Anspruch auf Richtigkeit und Vollständigkeit. Sie wurden seitens der ED Computer & Design GmbH Co. KG nach bestem Wissen erstellt. Hilfestellung beim Ausfüllen können der Systemadministrator des Verpflichteten oder ein auf Datenschutz spezialisiertes Unternehmen wie ED Computer & Design GmbH Co. KG bieten.

1. Verzeichnis über Verarbeitungstätigkeiten

Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	**Verantwortlicher:** <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> **gemeinsam Verantwortliche:** (Partnerunternehmen, z.B. IT Dienstleister, Aktenvernichter (Auftragsverarbeiter)) <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> <Beschreibung der Teilleistung> **Datenschutzbeauftragter:** <Name> <Geschäftsadresse> <Telefonnummer> <E-Mail>
Zweck der Datenverarbeitung	<Zweck z.B. Abschluss und Durchführung von Mieterverträgen für die verwalteten Grundstücke>
Kategorien der betroffenen Personen	<Auflistung: welche Personengruppen sind betroffen z.B. Mietinteressenten, Mieter, Handwerksunternehmen, Dienstleister, Versorger, Mitarbeiter>
Kategorien der Daten	<pro Personengruppe: welche personenbezogenen Daten werden erhoben? z.B. Mieter: Name, Kontaktdaten, Bankverbindung, Geburtsdatum, Mietvertrag>
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen	<Auflistung: wer erhält personenbezogene Daten? z.B. Handwerksunternehmen, Versorger> <pro Empfänger: welche personenbezogenen Daten von wem erhält er? z. B. Handwerksunternehmen: Name und Kontaktdaten> <Empfänger in Dittländern und geeignete Garantien>
Vorgesehene Fristen zur Löschung der verschiedenen Datenkategorien	<Fristen der Löschung z. B. Unterlagen, die für die Besteuerung relevant sind, werden nach zehn Jahren vernichtet, Vertragsdaten werden für die Dauer des Vertrages selbst und für die Dauer der regelmäßigen Verjährung (drei Jahre) von Ansprüchen gespeichert und im Anschluss gelöscht.>
Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs. 1 DSGVO	In separater Anlage aufgeführt.

2. Informationspflicht/Transparenzpflicht gemäß Art. 13 DSGVO (Direkterhebung)

Hinweis an Verpflichteten: Angaben in roter Schriftfarbe sind zu berücksichtigen, wenn Daten durch einen Dritten (z.B. Online-Marktplatz/Portal) erhoben werden (Dritterhebung, Artikel 14 DSGVO).

Hiermit informieren wir Sie, wie wir mit Ihren personenbezogenen Daten verfahren, die wir im Rahmen des Vertragsverhältnisses erheben und speichern. Personenbezogenen Daten sind Informationen, die sich auf Ihre Person beziehen und zu Ihrer Identifizierung führen können:

Namen und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	**Verantwortlicher:** <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> **Datenschutzbeauftragter:** (immer eine natürliche Person) <Name> <Geschäftsadresse> <Telefonnummer> <E-Mail>
Zweck der Verarbeitung und Rechtsgrundlage	Die Erhebung der Daten erfolgt zum Zwecke <Wieso soll dieser Verarbeitungsvorgang eingeführt werden? Z. B. vorvertragliche Maßnahme, Vertrag> Verwaltervertrag (Geschäftsbesorgungsvertrag nach §§ 611, 635, 675 BGB) oder Maklervertrag (§ 652 BGB)
Kategorie der Daten	Folgende personenbezogene Daten werden erhoben und verarbeitet: <Welche Daten sollen verarbeitet werden?>
Empfänger der Daten	Die Daten werden ganz oder teilweise übermittelt an: < Identität der Empfänger, z. B. Vermieter, Eigentümer, Notar, Messdienstleister, etc.>
Dauer der Speicherung	Die Daten werden so lange gespeichert, ergänzt und fortgeschrieben, wie es der Zweck erfordert, für den die personenbezogenen Daten erhoben werden und der von Ihnen gewünscht ist, sofern keine anderslautenden gesetzlichen Verpflichtungen, wie zum Beispiel Aufbewahrungspflichten nach Geldwäschegesetz (5 Jahre), Handelsrecht (6 Jahre), Steuerrecht (10 Jahre) oder Makler- Bauträgerverordnung (5 Jahre), entgegenstehen.
Recht auf Auskunft	Sie haben das Recht, jederzeit Auskunft über Ihre von uns gespeicherten Daten zu verlangen.
Recht auf Berichtigung oder Löschung der Daten	Für den Fall, dass diese Daten unrichtig oder unvollständig gespeichert wurden, haben Sie das Recht, eine Berichtigung oder Löschung zu verlangen.
Recht auf Einschränkung der Verarbeitung	Sie dürfen die Einschränkung der Verarbeitung verlangen, wenn Sie die Richtigkeit der erhobenen Daten bestreiten, die Verarbeitung unrechtmäßig oder der Zweck der Verarbeitung erfüllt ist.
Recht auf Widerruf der Einwilligung	Soweit die Verarbeitung Ihrer personenbezogenen Daten zu einem bestimmten Zweck aufgrund Ihrer Einwilligung erfolgt, können Sie diese jederzeit widerrufen; bis zum Zeitpunkt Ihres Widerrufes bleibt die Datenverarbeitung jedoch rechtmäßig.
Recht auf Widerspruch gegen die Verarbeitung	Der Verarbeitung Ihrer personenbezogenen Daten können Sie jederzeit widersprechen; eine Verarbeitung erfolgt dann nicht mehr.
Recht auf Übertragung der Daten	Sie haben das Recht, Ihre dem Verantwortlichen zur Verfügung gestellten Daten auf einen Dritten übertragen zu lassen.
Beschwerderecht	Sie haben das Recht auf Beschwerde bei der Aufsichtsbehörde, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden Daten rechtswidrig ist.
Datenquelle	<Woher stammen die Daten, z. B. Immobilienportal, Tippgeber? Stammen sie ggfls. aus öffentlich zugänglichen Quellen?>
Automatisierte Entscheidungsfindung (inkl. Profiling)	<Welche Logik wird verwendet? Welche Tragweite und Auswirkungen hat die Verarbeitung für den Betroffenen?>

3. Verpflichtung auf die Vertraulichkeit personenbezogener Daten

**Verpflichtung auf die Vertraulichkeit personenbezogener Daten,
des Fernmeldegeheimnisses gemäß § 88 Telekommunikationsgesetz (TKG)
und zur Wahrung von Geschäftsgeheimnissen**

Verpflichtung auf die Vertraulichkeit personenbezogener Daten
Es ist mir untersagt, personenbezogene Daten, zu denen ich dienstlich Zugang habe, unbefugt zu erheben, zu verarbeiten oder zu nutzen. Dies gilt sowohl für die dienstliche Tätigkeit innerhalb wie auch außerhalb (z.B. bei Kunden und Interessenten) des Unternehmens. Dieses Verbot besteht auch nach der Beendigung meiner Tätigkeit fort.

Verpflichtung auf das Fernmeldegeheimnis nach § 88 TKG
Ich bin zur Wahrung des Fernmeldegeheimnisses verpflichtet, soweit ich im Rahmen meiner Tätigkeit bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirke.

Verpflichtung auf Wahrung von Geschäftsgeheimnissen
Über alle Angelegenheiten des Unternehmens, beispielsweise Einzelheiten der Organisation, Geschäftsvorgänge und Zahlen des internen Rechnungswesens, ist von mir Verschwiegenheit zu wahren, sofern sie nicht allgemein öffentlich bekannt geworden sind. Hierunter fallen auch Vorgänge von Drittunternehmen, mit denen ich befasst bin. Auf die gesetzlichen Bestimmungen über den unlauteren Wettbewerb wurde ich besonders hingewiesen.

Alle Aufzeichnungen, Abschriften, Geschäftsunterlagen, Ablichtungen dienstlicher oder geschäftlicher Vorgänge, die mir dienstlich überlassen oder von mir angefertigt werden, sind vor der Einsichtnahme durch Unbefugte zu schützen.

Von diesen Verpflichtungen habe ich Kenntnis genommen. Die Pflicht zur Wahrung Vertraulichkeit personenbezogener Daten und der genannten Geheimnisse gilt zeitlich unbegrenzt auch über die Beendigung des Arbeitsverhältnisses hinaus. Ich bin mir bewusst, dass die Verletzung der Vertraulichkeit personenbezogener Daten, des Fernmeldegeheimnisses oder von Geschäftsgeheimnissen strafbar sein kann, insbesondere nach §§ 41 bis 43 BDSG (neu), § 206 StGB und nach § 17 UWG. Das Merkblatt zur Verpflichtungserklärung mit den Abschriften aller genannten Vorschriften habe ich erhalten.

Ggfls. Datenschutzbeauftragte/r
Der/Die Datenschutzbeauftragte für dieses Unternehmen ist Name, Kontaktdaten. Er/Sie steht mir für Fragen/Beratung mit datenschutzrechtlichem Bezug zur Verfügung.

Ort, Datum	Ort, Datum
Vorname Name Arbeitgeber/in	Name Arbeitnehmer/in

Quelle: ED Computer

4. Technische und organisatorische Maßnahmen als Teil der Sicherheit der Verarbeitung gemäß Art. 32 EU DSGVO

Verantwortlicher:
<Firmenname>
vertreten durch <die/die Geschäftsführer/Inhaber/Vorstand>:
<Namen der vertretungsberechtigten Personen>
<Geschäftsadresse>

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle Kein unbefugter Zutritt zu Datenverarbeitungsanlagen.	☐ Sicherheitsschlösser ☐ Manuelles Schließsystem ☐ Chipkarten-/Transponder-Schließsystem ☐ Schließsystem mit Codesperre ☐ Biometrische Zutrittssperren ☐ Automatisches Zutrittskontrollsystem ☐ Schlüsselregelung (Schlüsselausgabe etc.) ☐ Alarmanlage ☐ Lichtschranken / Bewegungsmelder ☐ Videoüberwachung der Zugänge ☐ Personenkontrolle beim Pförtner / Empfang ☐ Protokollierung der Besucher ☐ Tragepflicht von Berechtigungsausweisen ☐ Sorgfältige Auswahl von Wachpersonal ☐ Sorgfältige Auswahl von Reinigungspersonal
Zugangskontrolle Keine unbefugte Systembenutzung.	☐ Zuordnung von Benutzerrechten ☐ Passwortvergabe sicherer Kennwörtern ☐ regelmäßige Passwortänderungen ☐ Authentifikation mit Benutzername / Passwort ☐ Authentifikation mit biometrischen Verfahren ☐ Zuordnung von Benutzerprofilen zu IT-Systemen ☐ Schlüsselregelung (Bereichsabhängig etc.) ☐ automatische Sperrmechanismen ☐ Sperren von externen Schnittstellen (USB etc.) ☐ Verschlüsselung von mobilen Datenträgern ☐ Verschlüsselung von Datenträgern in Notebooks ☐ Verschlüsselung von Smartphone-Inhalten / Tablets ☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) ☐ Einsatz einer Software-Firewall ☐ Einsatz einer Hardware-Firewall ☐ Einsatz von Intrusion-Detection-Systemen ☐ Einsatz von Virtual Private Networks (VPN) Technologie ☐ Einsatz von Anti-Viren-Software ☐ Patchmanagement für Betriebssystem und Anwendungen
Zugriffskontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems.	☐ Rechtvergabe nach dem „need to know" Prinzip ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel ☐ Verwaltung der Rechte durch Systemadministrator ☐ Anzahl der Administratoren auf das „Notwendigste" reduziert ☐ automatische Sperrmechanismen ☐ Verschlüsselung von mobilen Datenträgern ☐ Verschlüsselung von Datenträgern in Notebooks ☐ Verschlüsselung von Smartphone-Inhalten/ Tablets ☐ physische Löschung von Datenträgern vor Wiederverwendung ☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern ☐ Protokollierung der Vernichtung ☐ Sichere Aufbewahrung von Datenträgern

Trennungskontrolle Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.	☐ physikalische Trennung ☐ logische Mandantentrennung (softwareseitig) ☐ Versehen der Datensätze mit Zweckattributen/ Datenfeldern ☐ Erstellung eines Berechtigungskonzepts ☐ Sandboxing ☐ Trennung von Produktiv- und Testsystem
Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.	☐ Nutzung von Pseudonymisierung wo möglich (u.a. bei Weitergabe) ☐ geeignete Wahl der Pseudonymisierungsschlüssel ☐ Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)	
Weitergabekontrolle Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport.	☐ E-Mail TLS Verschlüsslung ☐ E-Mail TLS Verschlüsslung mit pfs ☐ E-Mail End2End Verschlüsslung (u.a. pgp, S/MIME) ☐ elektronische Signatur ☐ Verschlüsselung von mobilen Datenträgern ☐ Verschlüsselung von Datenträgern in Notebooks ☐ Verschlüsselung von Smartphone-Inhalten / Tablets ☐ Weitergabe von Daten in anonymisierter oder mindestens pseudonymisierter Form ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen ☐ Erstellen einer Übersicht der Abruf- und Übermittlungsvorgänge ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen ☐ Beim physischen Transport: sichere Transportbehälter/ -verpackungen
Eingabekontrolle Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	☐ Dokumentenmanagement ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)	
Verfügbarkeitskontrolle Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust.	☐ gespiegelte Festplatten (RAID) ☐ gespiegelte Systeme / Cluster ☐ Unterbrechungsfreie Stromversorgung (USV) ☐ Schutzsteckdosenleisten in Serverräumen / Überspannungsschutz ☐ Einsatz einer Software-Firewall ☐ Einsatz einer Hardware-Firewall ☐ Einsatz von Intrusion-Detection-Systemen ☐ Einsatz von Anti-Viren-Software ☐ Erstellen eines Backup- & Recoverykonzepts, u.a. (online/offline; on-site/off-site) ☐ regelmäßige Datenwiederherstellungtests

	☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort ☐ Klimaanlage in Serverräumen ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen ☐ Feuer- und Rauchmeldeanlagen ☐ Feuerlöschgeräte in Serverräumen (CO2) ☐ Serverräume nicht unter sanitären Anlagen, wasserführenden Leitungen ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen ☐ Serverräume über der Wassergrenze (Hochwasser) ☐ Wartungsverträge mit geeigneter Reaktionszeit ☐ Patchmanagement für Betriebssystem und Anwendungen
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)	☐ Erstellen eines Notfallplans ☐ Nutzung virtueller Maschinen mit Offsitesicherung ☐ passender Hardware-Service-Vertrag ☐ eigene Ersatzteilbevorratung ☐ Wartungsverträge mit geeigneter Reaktionszeit
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 DSGVO)	
Datenschutz-Management	☐ Bestellung eines Datenschutzbeauftragter ☐ Einsatz vom Datenschutzkoordinatoren ☐ Verzeichnis von Verarbeitungstätigkeiten ☐ Datenschutzfolgeabschätzungen ☐ Schulungsmaßnahmen/ Sensibilisierungsmaßnamen mit Nachweis ☐ Verpflichtung auf Vertraulichkeit der Mitarbeiter ☐ definierte und dokumentierte Prozesse ☐ Arbeitsanweisungen/ Polices mit Datenschutzhintergrund ☐ Review Prozesse
Incident-Response-Management	☐ Definition von Zuständigkeiten und Verantwortlichkeiten für Vorfälle (z.B. Vorfallteam) ☐ definierter Meldeprozess ☐ definierte Maßnahmen für relevante und denkbare Vorfälle ☐ definierte Eskalationswege ☐ aktuelle Melde- und Kontaktlisten ☐ Prüfungsprozess für gemeldete Vorfälle und anschließender Risiko-klassifizierung wenn zutreffend ☐ vorbereitete Reaktionen auf den Vorfall (Kommunikation wie auch technische Maßnahmen) ☐ Reflexion und Nachbereitungsprozess um aus Vorfällen zu lernen
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)	☐ Prozess zur Sicherstellung von Privacy by Design bei Änderungen ☐ Prozess zur Sicherstellung von Privacy by Default bei Änderungen
Auftragskontrolle Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten ☐ vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen ☐ Sicherstellung der Verpflichtung auf die Vertraulichkeit durch den Auftragnehmer ☐ Auftragnehmer hat Datenschutzbeauftragten bestellt ☐ vertraglich festgelegte Verpflichtungen und Zuständigkeiten ☐ Auftragsverarbeitungsverträge ☐ wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart ☐ Vertragsstrafen bei Verstößen / klare Haftungsregelungen ☐ schriftliche Weisungen an den Auftragnehmer ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ☐ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

5. Datenschutzfolgeabschätzung gemäß Art. 35 DSGVO

Name der Folgeabschätzung: <Name des geplanten Verarbeitungsvorgangs> erstellt am: <Datum der Erstellung> betrachtet am: <Datum des letzten jährlichen Reviews – zur Fortschreibung>	
Namen und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten	**Verantwortlicher:** <Firmenname> Vertreten durch die Geschäftsführer: <Namen der vertretungsberechtigten Organe (Geschäftsführer)> <Geschäftsadresse> <Telefonnummer> <E-Mail> **Datenschutzbeauftragter:** (immer eine natürliche Person) <Name> <Geschäftsadresse> <Telefonnummer> <E-Mail>
Beteiligte an dieser Datenschutzfolgeabschätzung	<Vor- und Nachname> <Position>
systematische Beschreibung des geplanten Verarbeitungsvorgangs inkl. der Datenflüsse<Beschreibung>	Kategorien betroffener Personengruppen <Wer ist von diesem Verarbeitungsvorgang betroffen?>
Kategorien von Daten<Welche Daten sollen verarbeitet werden?>	Zweck der Verarbeitung<Wieso soll dieser Verarbeitungsvorgang eingeführt werden?>
berechtigtes Interesse des Verantwortlichen einschließlich der Rechtsgrundlage	<Beschreibung des berechtigten Interesses inkl. der Rechtsgrundlage>
Bewertung der Notwendigkeit und Verhältnismäßigkeit	<objektive Bewertung mit Begründung, ob diese Verarbeitung wirklich notwendig und verhältnismäßig ist>
Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (ohne Abhilfemaßnahmen) – Risikobewertung unter Berücksichtigung a) möglicher physischer, materieller und immaterieller Schäden, b) deren Schwere sowie c) Eintrittswahrscheinlichkeit	<Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen in Bezug auf Schutzklasse, Eintrittswahrscheinlichkeit, Schwere und Folgen, Vertraulichkeit, Integrität, Verfügbarkeit inkl. Begründung ohne Abhilfemaßnahmen>
geplanten Abhilfemaßnahmen zur Bewältigung der Risiken einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren – dies sind u.a. technische und organisatorische Maßnahmen; Wirksamkeitsprüfungen benennen; Restrisiken sind ebenfalls zu benennen	<alle konkrete geplanten Maßnahmen, Sicherheitsmaßnahmen, Garantien und Verfahren zur Reduzierung der Risiken für die Rechte und Freiheiten betroffener Personen inkl. der Wirksamkeitsprüfungen sowie evtl. Restrisiken>
Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (mit Abhilfemaßnahmen) – Risikobewertung unter Berücksichtigung a) möglicher physischer, materieller und immaterieller Schäden, b) deren Schwere sowie c) Eintrittswahrscheinlichkeit	<Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen in Bezug auf Schutzklasse, Eintrittswahrscheinlichkeit, Schwere und Folgen, Vertraulichkeit, Integrität, Verfügbarkeit inkl. Begründung unter Beachtung der getroffenen Maßnahmen>
Freigabe des Verarbeitungsvorgang	<Kann die Freigabe erfolgen? Sind Auflagen vorhanden die zuerst erledigt sein müssen vor einer Erneutbewertung? Freigabe der Aufsichtsbehörde erforderlich?>

Hinweis: Aus Gründen verbesserter Lesbarkeit wurde in der Regel die männliche Schreibweise verwendet. Wir weisen an dieser Stelle ausdrücklich darauf hin, dass sowohl die männliche, als auch die weibliche Schreibweise gemeint sind.

ED Computer & Design GmbH & Co. KG ist ein bundesweit tätiger Full Service IT-Dienstleister mit Sitz in Köln. Zum Leistungsportfolio gehört neben dem Webdesign, Webhosting, EDV-Support auch der Datenschutz. Das Unternehmen ist ein langjähriger Kooperationspartner des IVD.

ED Computer & Design GmbH & Co. KG
Lina-Bommer-Weg 4
51149 Köln

Telefon +49 (0) 221 28 88 77 66
Telefax +49 (0) 221 28 88 77 67

E-Mail: info@edcud.de
Internet: www.edcud.de

Immobilienverband Deutschland IVD
Bundesverband der Immobilienberater, Makler,
Verwalter und Sachverständigen e.V.
Littenstraße 10
10179 Berlin

Tel.: (030) 27 57 26-0
E-Mail: info@ivd.net
Internet: www.ivd.net