LEITFADEN ZUM SICHEREN UMGANG MIT DATEN

in der Immobilienbranche

ICG in Kooperation mit Freshfields Bruckhaus Deringer

Inhalt

IMPRESSUM

Herausgeber: Institut für Corporate Governance
in der deutschen Immobilienwirtschaft
Leipziger Platz 9 . 10117 Berlin
Tel.: +49 30 202 1585 55 . Fax: +49 30 202 1585 29
www.icg-institut.de

Bilder: Midjourney, KI
Ausgabe: 1 - 2024

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

VORWORT

Die europäische Datenschutz-Grundverordnung (DSGVO) und das deutsche Bundesdatenschutzgesetz (BDSG) haben zu einer Vereinheitlichung und Modernisierung des Datenschutzrechts geführt, aber zugleich sämtliche Unternehmen vor erhebliche Herausforderungen gestellt: Denn jedes Unternehmen verarbeitet personenbezogene Daten und ist damit unabhängig von der Branche zur Einhaltung des Datenschutzes verpflichtet. Der effektive Schutz personenbezogener Daten spielt in der Immobilienbranche für eine Vielzahl von Akteuren eine herausragende Rolle. Ob bei der Beauftragung von Maklern, der Abwicklung eines Kaufvertrags oder der Vermietung von Wohnobjekten: In all diesen Bereichen werden personenbezogene Daten verarbeitet. Der folgende Leitfaden soll aufzeigen, welche Risiken bei der Datenverarbeitung bestehen und durch welche Best Practices vertrauliche Daten geschützt werden können. Auf diese Weise können Unternehmen einen wichtigen Schritt hin zur Datenschutz-Compliance machen.

Der vorliegende Leitfaden stellt eine zusammenfassende Information über die DSGVO dar, die die Arbeit mit derselben im Immobilienkontext erleichtern und durch Praxisbeispiele Hilfestellungen zu bestimmten Fragen bieten soll.

Es handelt sich um **keine abschließende** und **keine verbindliche Information.** Eine Beratung im Einzelfall, bspw. durch eine spezialisierte Anwaltskanzlei, kann durch den Leitfaden nicht ersetzt werden.

Der Leitfaden wird regelmäßig einer Evaluierung und Aktualisierung unterzogen, um Neuerungen (vor allem auf europäischer Ebene) einbeziehen zu können.

Mitwirkende

Michael Schwaab, Principal Associate, Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB
Commercial litigation | Data, privacy and cybersecurity | Regulatory and compliance advisory

André Diedrich, betrieblicher Datenschutzbeauftragter, Becker & Kries Holding GmbH & Co. KG

Gregor Hoffmann, Datenschutzbeauftragter, OFB Projektentwicklung GmbH

Heiko Wegst, Datenschutzbeauftragter, GWG Gesellschaft für Wohnungs- und Gewerbebau Baden-Württemberg AG

LEKTORAT:
Katharina-Isabelle Prenzel, wissenschaftliche Mitarbeiterin, Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB

Datenschutzrechtliche Pflichten in allen Marktsegmenten

Die DSGVO regelt umfassend, was personenbezogene Daten sind, unter welchen Umständen sie verarbeitet werden dürfen, wer zu welchem Zeitpunkt, in welcher Weise und in welchem Umfang über die Verarbeitung informiert werden muss und welche Rechte den betroffenen Personen zustehen, deren Daten verarbeitet werden. Wer personenbezogene Daten verarbeitet, muss dies zumeist in einer bestimmten Weise dokumentieren. Die Erfüllung dieser und weiterer Pflichten ist für die Unternehmensführung besonders relevant, da Pflichtverstöße zu hohen Bußgeldern führen können.

A1

Datenschutzrechtliche Begriffe und ihre Bedeutung für die Immobilienwirtschaft

Die DSGVO verwendet spezielle Begriffe, die für die Einrodnung datenschutzrechtlicher Pflichten erforderlich sind.

1.1 Personenbezogene Daten

Unter dem Begriff "personenbezogene Daten" sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Der Begriff wird von den Gerichten und Datenschutzbehörden weit verstanden und kann nahezu jede Information umfassen, die in Verbindung mit einer natürlichen Person steht. Der Schutz der DSGVO ist damit nicht nur auf sensible oder private Informationen beschränkt, sondern umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, sofern es sich um Informationen über eine natürliche Person handelt (z. B. Name, Geburtsdatum, Anschrift, Telefonnummer, Bankdaten, Bonitätsauskünfte, Einkommensnachweise).

1.2 (Daten-) Verarbeitungen und Verarbeitungstätigkeiten

Die DSGVO unterteilt die „bunte Lebenswirklichkeit“ in Datenverarbeitungen. Dabei lässt sich jeglicher Umgang mit personenbezogenen Daten einer Verarbeitungstätigkeit zuordnen. Explizit benannt werden das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Eine Verarbeitungstätigkeit ist die Zusammensetzung mehrerer einzelner Verarbeitungen zu einer konkreten Tätigkeit (in einer gedanklichen Einheit). Hierzu zählt z. B.:

- die Abfrage von Informationen von Mietinteressenten;
- die Bonitätsprüfung von Mietinteressenten;
- die Organisation von Handwerkerterminen; oder
- das Management der Daten von Arbeitsplatzbewerbern.

Best Practice:

Alle Verarbeitungen, die personenbezogene Daten betreffen, sollten erfasst werden. Dies kann insbesondere durch ein sog. "Verzeichnis von Verarbeitungstätigkeiten" (VVT) nach Art. 30 DSGVO* erfolgen. Ein solches dient nicht nur der Dokumentation und Transparenz sondern hilft daneben auch dabei, auf Betroffenenanfragen schnell und präzise zu antworten.

* vgl. hierzu DSK, Kurzpapier Nr. 1

1.3 Verantwortlicher (Datenschutzrechtlich bzw. für die Datenverarbeitung)

Der Verantwortliche ist derjenige, dem eine Verarbeitungstätigkeit zugerechnet wird. Dies können Menschen im Sinne von Einzelunternehmen (z. B. Einzelkaufmann oder Freiberufler), Personen- oder Kapitalgesellschaften sein. Verantwortlicher ist (allgemein gesprochen), wer – entweder allein oder gemeinsam mit anderen – entscheidet, ob, wie und wozu eine Verarbeitungstätigkeit stattfindet. Schwierig kann die Zuordnung im Einzelfall sein, insbesondere wenn mehrere an der Verarbeitung beteiligt sind (z. B. Vermieter, Handwerker und Makler). Die Europäischen Datenschutzbehörden bieten zur Abgrenzung der Verantwortlichkeit spezielle Leitlinien.*

Risiko:

Werden die Verarbeitungstätigkeiten im Verhältnis zu Dienstleistern oder innerhalb eines Konzerns nicht klar zugeordnet, besteht die Gefahr, dass mehrere Rechtsträger als Verantwortliche für ein und dieselbe Verarbeitungstätigkeit gelten.

Best Practice:

Im Fall der (gleichberechtigten) Zusammenarbeit mehrerer Verantwortlicher sind die jeweiligen Datenschutzkonzepte, insbesondere die Bestimmung der Zwecke und Mittel der Verarbeitung, eng miteinander abzustimmen, um eine klare Abgrenzung der einzelnen Verantwortlichen festzulegen.

* vgl. hierzu EDPB Leitlinien 07/2020, zu den Begriffen "Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0

1.4 Betroffene Person

Die betroffene Person ist diejenige (identifizierte oder identifizierbare natürliche Person), deren personenbezogene Daten von einem Verantwortlichen verarbeitet werden. Für eine effizientere Dokumentation empfiehlt sich die Einteilung der betroffenen Personen in Kategorien. Als solche kommen speziell in der Immobilienwirtschaft die Folgenden infrage:

- **Mietinteressenten,** d.h. jeder, der Interesse an einer Anmietung ausdrückt und daher systematisch in eine Datensammlung jedweder Art aufgenommen wird.
- **Mieter** im Sinne des bürgerlichen Rechts, gleich ob von Wohn- oder Gewerberaum. Relevant für das Datenschutzrecht sind aber nur natürliche Personen oder Kleinstunternehmen, die eigentumsbasiert geführt werden (z. B. Einzelkaufmann oder Freiberufler).
- **Vermieter** im Sinne des bürgerlichen Rechts, gleich ob von Wohn- oder Gewerberaum. Als betroffene Personen sind Vermieter für das Datenschutzrecht nur relevant, wenn es sich bei ihnen um natürliche Personen handelt. So werden personenbezogene Daten von Vermietern (z. B. von Hausverwaltern) verarbeitet, die für eine WEG tätig sind.
- **Makler**, gleich ob vom Mieter oder Vermieter beauftragt.
- **Bewohner**, d.h. wer in einer Immobilie tatsächlich wohnt, gleich ob Mieter, deren Lebenspartner, Kinder oder Untermieter.
- **Immobilienverkäufer/-käufer**, soweit diese natürliche Personen sind.
- **Mitarbeiter** von in der Immobilienwirtschaft tätigen Arbeitgebern und entsprechende Bewerber.

1.5 Datenschutzrechtliche Grundsätze

Die DSGVO sieht in ihrem Art. 5 verschiedene Grundsätze bzw. wesentliche Grundprinzipien für die Verarbeitung von personenbezogenen Daten vor. Diese allgemein und als unmittelbare Pflichten für den Verantwortlichen geltenden Grundsätze ergeben sich darüber hinaus auch aus anderen Vorschriften der DSGVO und werden dort näher konkretisiert. Ihre Kenntnis hilft den Verantwortlichen dabei, das Datenschutzrecht als solches besser zu verstehen. Zu den datenschutzrechtlichen Grundprinzipien zählen:

- **Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a DSGVO):** Personenbezogene Daten dürfen nur auf der Grundlage einer rechtlichen Legitimation, nach Treu und Glauben sowie transparent, d.h. in einer für die betroffene Person nachvollziehbaren Weise, verarbeitet werden.
- **Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO):** Personenbezogene Daten dürfen nur für (zuvor) festgelegte, eindeutige und legitime Zwecke verarbeitet werden, wodurch insbesondere eine mit diesen Zwecken unvereinbare Weiterverarbeitung verhindert werden soll.
- **Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO):** Personenbezogene Daten dürfen nur verarbeitet werden, wenn sie dem Zweck angemessen und erheblich sowie auf das für die Verarbeitungszwecke notwendige Maß beschränkt sind.
- **Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO):** Personenbezogene Daten dürfen nur verarbeitet werden, wenn sie sachlich richtig und aktuell sind. In diesem Zusammenhang ist der Verantwortliche verpflichtet, alle angemessenen Maßnahmen zu treffen, um in Bezug auf die Verarbeitungszwecke unrichtige personenbezogene Daten unverzüglich zu löschen oder zu berichtigen.
- **Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO):** Personenbezogene Daten dürfen nur so lange aufbewahrt werden, wie es für die Verarbeitungszwecke erforderlich ist.
- **Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO):** Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Dazu gehören u.a. der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, der Schutz vor unbeabsichtigtem Verlust sowie der Schutz vor unbeabsichtigter Zerstörung oder Schädigung durch die Implementierung geeigneter technischer und organisatorischer Maßnahmen ("TOMs").
- **Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO):** Dem Verantwortlichen obliegt die Einhaltung der zuvor dargestellten Grundsätze des Art. 5 Abs. 1 DSGVO. Er muss geeignete Maßnahmen ergreifen, diese angemessen dokumentieren und entsprechende Nachweise erbringen.

1.6 Rechtsgrundlage

Die Verarbeitung personenbezogener Daten durch einen Verantwortlichen ist nur zulässig, wenn bestimmte Bedingungen vorliegen, die in der DSGVO als **«Rechtsgrundlagen»** bezeichnet werden. Als solche vorgesehen sind:

- die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO);
- die Vertragserfüllung und Durchführung vorvertraglicher Maßnahmen (Art. 6 Abs. 1 lit. b DSGVO);
- die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO);
- der Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 lit. d DSGVO);
- die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e DSGVO); und
- die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO).

Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, sind die zusätzlichen Anforderungen von Art. 9 DSGVO zu beachten.*

Risiko:

- Die Auswahl der richtigen Rechtsgrundlage kann sich im Einzelfall schwierig gestalten.
- Zur Einwilligung: Es besteht jederzeit die Möglichkeit, dass die betroffene Person ihre zuvor erteilte Einwilligung widerruft, womit die Pflicht der Löschung bzw. Anonymisierung der personenbezogenen Daten einhergeht.
- Zur Wahrung berechtigter Interessen: Neben dem Widerspruchsrecht der betroffenen Person besteht die Gefahr, dass die einzelnen Interessen im Einzelfall zu oberflächlich herausgearbeitet bzw. dargestellt werden und daraus die datenschutzrechtliche Angreifbarkeit der (Risiko-)Abwägung folgt.

Best Practice:

- Vor Beginn der Verarbeitung ist festzulegen, welche Rechtsgrundlage des Art. 6 Abs. 1 DSGVO für die konkrete Verarbeitung in Betracht kommt.
- Eine Einwilligung ist in der Regel erst dann in Betracht zu ziehen, wenn eine Datenverarbeitung aufgrund einer der anderen Rechtsgrundlagen nicht möglich ist (bspw. bei der Zusendung von Newslettern).**
- Insbesondere im Verhältnis gegenüber Mietern kann die Verarbeitung auf die Durchführung des (Miet-)Vertrages gemäß Art. 6 Abs. 1 lit. b DSGVO gestützt werden.
- In vielen Fällen kann auch Art. 6 Abs. 1 lit. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) einschlägig sein. Derartige Pflichten können sich insbesondere aus dem Geldwäschegesetz, der Abgabenordnung oder dem Handelsgesetzbuch ergeben.***
- Falls Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage herangezogen wird, ist eine dokumentierte (Risiko-)Abwägung der berechtigten Interessen des Verantwortlichen oder eines Dritten gegenüber den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person durchzuführen.

* vgl. hierzu vertiefend DSK, Kurzpapier Nr. 17 – Besondere Kategorien personenbezogener Daten

** vgl. ausführlich zur Einwilligung DSK, Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO sowie EDPB, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, 4.5.2020

*** vgl. hierzu ebenfalls das Beispiel von Rauchmeldern in Wohneinheiten auf der Internetseite des BlnDI

1.7 Auftragsverarbeiter (Dienstleister)

Der Verantwortliche kann unter bestimmten Bedingungen Datenverarbeitungen durch einen anderen durchführen lassen, ohne dass eine Weitergabe an einen weiteren Verantwortlichen vorliegt, für die eine eigene Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO erforderlich wäre. Das ist dann der Fall, wenn der andere als sog. Auftragsverarbeiter gemäß Art. 28 DSGVO tätig wird, wenn er also personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Eine Voraussetzung für die Rechtmäßigkeit dieser Konstellation ist, dass der Verantwortliche mit dem Auftragsverarbeiter eine Vereinbarung nach Art. 28 Abs. 3 S. 1 DSGVO abschließt, die Letzteren in Bezug auf den Verantwortlichen bindet. Sie muss unter anderem Gegenstand und Dauer, ebenso wie Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Rechte und Pflichten des Verantwortlichen festlegen und gemäß Art. 28 Abs. 3 S. 2 lit. a bis h DSGVO konkrete Verpflichtungen des Auftragsverarbeiters vorsehen.

Auftragsverarbeiter in der Immobilienbranche sind z. B.:

- Wärmedienstleister;
- Sicherheitsunternehmen, die eine Videoüberwachung auswerten;
- nicht aber Hausverwalter.*

Risiko:

- Risiken bestehen u.a. im Falle eines fehlenden und/oder fehlerhaften Auftragsverarbeitungsvertrags.
- Denkbar ist ein Datenschutzverstoß bei Nichtbeachtung hinreichender technischer und organisatorischer Maßnahmen („TOMs“) durch den Auftragsverarbeiter.

Best Practice:

- Es empfiehlt sich, einen Standard-Auftragsverarbeitungsvertrag abzuschließen, wenn von einer Auftragsverarbeitung ausgegangen wird. Zu beachten ist hierbei, dass dieser Vertrag den Anforderungen des Art. 28 Abs. 3 DSGVO genügt.**
- Die Aspekte Datenschutz sowie IT-Sicherheit sind bei der Auswahl des Dienstleisters bzw. Auftragsverarbeiters frühzeitig einzubinden und eine Konformitätsprüfung ist zu dokumentieren.

* vgl. AG Mannheim, Urt. v. 11.9.2019 – 5 C 1733/19 WEG, NZM 2020, 70 (72 f., Rn. 23)

** vgl. hierzu ausführlich DSK, Kurzpapier Nr. 13 – Auftragsverarbeitung, Art. 28 DS-GVO sowie EDPB, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, 7.7.2021

A2

Umsetzung der Betroffenenrechte

Die DSGVO gibt betroffenen Personen, deren personenbezogene Daten verarbeitet werden oder wurden, eine Reihe von Rechten (sog. Betroffenenrechte) an die Hand, mit deren Hilfe sie in die Lage versetzt werden, auf unterschiedliche Weise Informationen über die genaue Verarbeitung ihrer Daten zu erhalten und diese ggf. zu beenden.

Die Wahrung der Betroffenenrechte ist von zentraler Bedeutung und kann bei Nichteinhaltung zu Schadensersatzansprüchen von betroffenen Personen (bspw. im Fall einer verspäteten Auskunft), aber auch zu Bußgeldern führen.

Risiko:

Die Wahrung der Betroffenenrechte innerhalb der gesetzlichen Fristen (in der Regel ein Monat nach Eingang, was u.U. um zwei Monate verlängert werden kann) stellt Unternehmen häufig vor große Herausforderungen und kann bei der Nichteinhaltung zu Bußgeldern führen.

Best Practice:

Jeder Verantwortliche sollte nach Möglichkeit sämtliche Verarbeitungen identifizieren können. Dies ist eine Grundvoraussetzung, um die Betroffenenrechte einzuhalten.

* vgl. hierzu ausführlich DSK, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO

2.1 Informationspflichten (Art. 13 und 14 DSGVO)

Nach Art. 13 bzw. 14 DSGVO sind die betroffenen Personen in leicht verständlicher Weise über die geplante Verarbeitung zu informieren. Dabei sieht die DSGVO einen gewissen Mindestinhalt vor, der einer betroffenen Person grundsätzlich vor Beginn der geplanten Datenverarbeitungstätigkeit mitgeteilt werden muss.

Best Practice:

- Jeder Verantwortliche muss die betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten informieren. Es bietet sich an, Standarddatenschutzinformationen (bspw. für die Verarbeitung im Miet- oder Arbeitsverhältnis) zu erarbeiten.
- Die betroffenen Personen müssen diesen Informationen zwar nicht zustimmen; es sollte aber angemessen dokumentiert werden, dass sie die Informationen erhalten haben.*

*vgl. ausführlich zu den Informationspflichten gemäß Art. 13 und 14 DSGVO bereits Art. 29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 01, 11.4.2018 sowie DSK, Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung

2.2 Auskunftsanspruch (Art. 15 DSGVO)

Nach Art. 15 DSGVO haben die betroffenen Personen das Recht, vom Verantwortlichen zu erfahren, welche Daten über sie verarbeitet werden.

Best Practice:**

- Zur Beantwortung dieser Auskünfte sollte ein Prozess definiert werden. Dieser muss u.a. eine Verifizierung der Identität der anfragenden Person enthalten.
- Nach Art. 12 Abs. 3 DSGVO ist der anfragenden Person unverzüglich (spätestens innerhalb eines Monats) eine Statusmeldung bzgl. ihrer Anfrage zu erteilen.
- Zu berücksichtigen ist auch die jeweils aktuelle EuGH-Rechtsprechung zum Auskunftsanspruch (siehe zuletzt Urt. v. 26.10.2023 – C-307/22; Urt. v. 22.6.2023 – C-579/21; Urt. v. 4.5.2023 – C-487/21 (Österreichische Datenschutzbehörde); Urt. v. 12.1.2023 – C-154/21 (Österreichische Post)).

** vgl. ausführlich zum Auskunftsanspruch DSK, Kurzpapier Nr. 6 – Auskunftsrecht der betroffenen Person, Art. 15 DSGVO sowie EDPB, Guidelines 01/2022 on data subject rights – Right of access, Version 2.0, 28.3.2023

2.3 Recht auf Vergessenwerden (Art. 17 DSGVO)

Nach Art. 17 DSGVO ist das Recht auf Vergessenwerden das Recht der betroffenen Personen, dass über sie gespeicherte Daten unter bestimmten Umständen gelöscht werden.

Best Practice:*

- Es sind Daten-Lifecycles zu erstellen und revisionssichere Archive zu nutzen; insbesondere sind sog. Schattenarchive möglichst zu vermeiden.
- Es sollte ein (abgestuftes) Löschkonzept bzgl. sämtlicher personenbezogenen Daten erstellt und die Löschung dokumentiert werden.

* vgl. ausführlich zum Recht auf Vergessenwerden DSK, Kurzpapier Nr. 11 – Recht auf Löschung /„Recht auf Vergessenwerden“

2.4 Recht auf Widerspruch (Art. 21 DSGVO)

Art. 21 DSGVO gewährt das Recht einer betroffenen Person, gegen eine Verarbeitung von Daten Widerspruch einzulegen. Dies ist jedoch nur dann gegeben, wenn die Verarbeitung auf der Rechtsgrundlage von Art. 6 Abs. 1 lit. e oder f DSGVO erfolgt.

Die Verarbeitung muss dann vom Verantwortlichen nochmals dahingehend geprüft werden, ob seine Interessen an der (weiteren) Verarbeitung die schutzwürdigen Interessen der betroffenen Person überwiegen. Dies kann bspw. bei Videoaufzeichnungen oder der Weitergabe von Daten an Kreditauskunfteien relevant sein.

2.5 Weitere Rechte

Nach Art. 16 DSGVO besteht das Recht auf Berichtigung von Daten. Dies kann etwa die Löschung unberechtigter Beschwerden von anderen über einen Mieter oder die Berichtigung der personenbezogenen Daten (z. B. des Namens) im Mietvertrag beinhalten, falls diese nicht (mehr) richtig oder unvollständig sind.

Nach Art. 18 DSGVO besteht ein – in der Praxis bisher wenig relevantes – Recht auf Einschränkung der Verarbeitung. Dieses ist regelmäßig als eine Art „Zwischenlösung" zu verstehen und soll in dem Zeitraum, in dem über eine endgültige Löschung der Daten entschieden wird, dergestalt für Sicherheit sorgen, dass die Daten lediglich gespeichert, aber nicht mehr auf andere Weise verarbeitet werden dürfen.*

Art. 20 DSGVO verpflichtet den Verantwortlichen, den betroffenen Personen die über sie gespeicherten Daten zur Verfügung zu stellen bzw. auf Verlangen an andere Verantwortliche weiterzuleiten. Das Recht kann bei solchen Daten relevant werden, die eine betroffene Person auf einer Plattform gespeichert hat, wenn sie nunmehr zu einem anderen Plattformanbieter wechseln möchte. In Zukunft sind neben den diesbezüglichen Vorgaben der DSGVO auch noch diejenigen des Data Acts und anderer Rechtsakten der EU zu berücksichtigen. Im Immobilienkontext ist dieses Recht allerdings bisher (noch) nicht relevant geworden.**

Nach Art. 77 DSGVO hat die betroffene Person ein Recht darauf, Beschwerde bei einer Datenschutzbehörde einzulegen.

* vgl. hierzu BfDI, Das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
** vgl. ausführlich zum Recht auf Datenübertragbarkeit bereits Art. 29-Datenschutzgruppe, Guidelines on the right to data portability, WP 242 rev. 01, 5.4.2017

A3

Anfragen nach personenbezogenen Daten durch Behörden und andere Dritte

Anfragen nach personenbezogenen Daten können von Behörden (z. B. der Staatsanwaltschaft, Polizei, Sozialbehörde, dem Gesundheitsamt, Finanzamt, etc.) oder von anderen Dritten (z. B. Verwandten, (Ex-)Lebenspartnern, Gläubigern, Inkassobüros, etc.) gestellt werden. Sie können bspw. die Fragen zum Inhalt haben, ob mit einer bestimmten Person ein Mietverhältnis besteht, wo die Person wohnt, ob die Person ihre Mietschuld bedient, etc.

Manche dieser Anfragen dürfen nicht beantwortet werden, andere müssen sogar beantwortet werden. Daher müssen sich die Verantwortlichen darauf vorbereiten, im Ernstfall (datenschutzrechtlich) angemessen mit solchen Anfragen umzugehen.

Risiko:

- Die ungeprüfte Beantwortung einer Anfrage birgt die Gefahr, dass personenbezogene Daten herausgegeben werden, ohne dass eine Pflicht hierzu besteht. In solchen Fällen handelt es sich um eine rechtswidrige Verarbeitung.
- Die Verweigerung der Beantwortung einer Anfrage birgt - insbesondere im Fall der Nichtbeantwortung trotz entsprechender Legitimation der anfragenden Stelle - die Gefahr der Verletzung einer bestehenden Kooperationspflicht des Verantwortlichen (z.B. auf dem Gebiet des Ordnungsrechts, Steuerrechts, etc.).
- Ferner besteht das Risiko der Verhängung von Sanktionen.

Best Practice:

- Sofern Rechtsgrundlage und Zweck der Anfrage nicht bereits im Rahmen der Belehrungen vonseiten der anfragenden Behörde genannt werden, sind diese stets zu erfragen und sodann zu dokumentieren, um insbesondere bei etwaigen späteren Anfragen einer Datenschutzbehörde möglichst detailliert und umfassend antworten zu können.
- Für die Offenlegung von Informationen gegenüber Privaten besteht meist keine Rechtsgrundlage. Selbst wenn der Anfragende behaupten sollte, die betroffene Person befände sich in Gefahr, sollte der Notruf verständigt, auf eine Herausgabe der angefragten personenbezogenen Daten aber dennoch verzichtet werden.
- Besondere Vorsicht ist geboten bei Individualanfragen per E-Mail.*
- Niemals sollten Auskünfte am Telefon erteilt werden. Es hat sich bewährt, die anfragende Person darum zu bitten, ihre Anfrage schriftlich einzureichen.

* vgl. hierzu ausführlich DSK, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, 16.6.2021

A4

Kontaktaufnahme durch Datenschutzaufsichtsbehörden

Vor allem bei größeren Unternehmen der Immobilienbranche besteht die Möglichkeit, dass Datenschutzaufsichtsbehörden durch die Beschwerde einer betroffenen Person oder auf andere Weise auf das Unternehmen aufmerksam werden. Die Landesdatenschutzbehörden haben nach Art. 58 DSGVO in Verbindung mit dem jeweiligen Datenschutzgesetz des einzelnen Bundeslandes die Befugnis, die Einhaltung der datenschutzrechtlichen Pflichten durch den Verantwortlichen zu überprüfen und ggf. Sanktionen zu verhängen.*

Risiko:

- Im Fall einer mangelhaften Datenschutzumsetzung droht die Verhängung eines Bußgeldes durch die zuständige Datenschutzaufsichtsbehörde.

Best Practice:

- Es empfiehlt sich im Regelfall, auf Anfragen von Datenschutzaufsichtsbehörden mit kooperativem Verhalten zu reagieren.
- Es sind ggf. die Geschäftsführung, der Datenschutzbeauftragte, die IT-Leitung oder ähnliche Stellen zu konsultieren.
- Es ist sorgsam zu prüfen, wie und in welchem Umfang angeforderte Datenschutzdokumentationen (wie z.B. Datenschutzkonzepte, IT-Datensicherheitskonzepte, etc.), die regelmäßig über den gesetzlichen Mindestinhalt hinausgehen, herausgegeben werden.
- Je nach Einzelfall sollte eine externe Rechtsberatung hinzugezogen werden.

*vgl. hierzu ausführlich DSK, Kurzpapier Nr. 2 – Aufsichtsbefugnisse/Sanktionen

A5

Datenschutz für Mitarbeiter

Datenschutzstandards gelten nicht nur im Umgang mit Daten Dritter, sondern auch hinsichtlich der Verarbeitung von Mitarbeiterdaten. Zu solchen gehören z. B. die Personalakte oder der Inhalt des betrieblichen E-Mail-Postfachs. Ein Unternehmen der Immobilienbranche steht hier vor der gleichen Aufgabe wie jedes andere Unternehmen, das in der EU tätig ist und Mitarbeiter beschäftigt. Rechtsgrundlage für die meisten Verarbeitungstätigkeiten im Unternehmen ist der Arbeitsvertrag, folglich Art. 6 Abs. 1 lit. b DSGVO.

Risiko:

- Zu lange Aufbewahrungsfristen und fehlende oder unzureichend durchdachte bzw. differenzierte Löschkonzepte bergen datenschutzrechtliche Risiken, insbesondere in Bezug auf Daten von abgelehnten Bewerbern oder ausgeschiedenen Mitarbeitern.
- Die Datenweitergabe sollte auch innerhalb des Unternehmens stets sorgsam durchdacht werden und niemals unüberlegt erfolgen. Es ist zu beachten, dass auch innerhalb eines Konzerns bzw. einer Unternehmensgruppe oftmals jeder Rechtsträger (sprich die Muttergesellschaft sowie etwaige Tochtergesellschaften) selbst Verantwortlicher ist (es also kein sog. Konzernprivileg gibt). In solchen Fällen bedarf die Weitergabe von Daten von einer Gesellschaft an eine andere Gesellschaft innerhalb desselben Konzerns bzw. derselben Unternehmensgruppe ebenfalls einer Rechtsgrundlage im Sinne des Art. 6 Abs. 1 DSGVO. Ggf. sind entsprechende Auftragsverarbeitungsverträge oder Vereinbarungen über eine gemeinsame Verantwortlichkeit zwischen den einzelnen Gesellschaften des Konzerns bzw. der Unternehmensgruppe zu schließen.

Best Practice:*

- Es ist zu prüfen, ob für alle unternehmensinternen Datenverarbeitungstätigkeiten eine Rechtsgrundlage besteht. Dies geschieht typischerweise in einem Abschnitt des Verzeichnisses von Verarbeitungstätigkeiten.
- Vorsicht ist geboten bei Datenverarbeitungstätigkeiten, die gerade nicht zur Durchführung des Beschäftigungsverhältnisses notwendig sind und für die ggf. die Rechtsgrundlage der Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO herangezogen werden muss. Dies kann bspw. der Fall sein bei der Veröffentlichung von Bildern der Mitarbeiter auf der Internetseite des Verantwortlichen.
- Wenn Mitarbeiter überwacht werden (etwa bzgl. ihrer IT-Aktivitäten, per Videoüberwachung, etc.), ist der Sicherheitsvorteil sorgfältig gegen den Eingriff in das Persönlichkeitsrecht abzuwägen. Diese Überlegungen sollten dokumentiert werden.
- Ein System zum Bewerberunterlagenmanagement, das auch die – idealerweise automatisierte – Löschung der Bewerbungsunterlagen um-

Best Practice:*

fasst, sollte eingeführt werden. Es kann aus einer speziellen IT-Plattform oder einer Arbeitsanweisung an die Personalabteilung bestehen.

- Es muss festgelegt werden, was im Falle eines Ausscheidens mit den Mitarbeiterdaten geschieht und nach welchen Fristen diese zu löschen sind (Löschkonzept).
- Sollte ein Betriebsrat existieren, so sind seine Mitbestimmungsrechte zu berücksichtigen. Da jedoch auch ein Betriebsrat personenbezogene Daten verarbeitet, obliegt er den gleichen datenschutzrechtlichen Pflichten wie der Verantwortliche.

* vgl. ausführlich zu den Mitarbeiterdaten DSK, Kurzpapier Nr. 14 – Beschäftigtendatenschutz

Best Practices im Marktsegment **«Wohnen»**

B1

Mietanbahnung sowie Mietinteressentenbögen

Bei der Anbahnung von Mietverhältnissen bzw. der Ausgabe von Mietinteressentenbögen werden personenbezogene Daten des Mietinteressenten verarbeitet. Dies löst die Pflicht des Vermieters aus, die oben beschriebenen Betroffenenrechte zu achten. Die Rechtsgrundlage für die Datenverarbeitung ist Art. 6 Abs. 1 lit. b DSGVO, also die Erforderlichkeit im Rahmen eines vorvertraglichen Schuldverhältnisses.

Risiko:

- Denkbar sind etwa Datenschutzverstöße durch unzureichende Information oder exzessive Auskunftsverlangen, die den Datenschutzaufsichtsbehörden insbesondere von abgelehnten Mietinteressenten gemeldet werden.

Best Practice:

- Mietinteressenten sind gemäß Art. 13 DSGVO über die Datenverarbeitung zu informieren. Dazu sollte ein Formblatt „Datenschutzinformationen für Mietinteressenten“ erstellt und verwendet werden.
- Das Stufenmodell gemäß der „Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen“ der DSK* ist zwingend zu beachten. Danach ist bspw. eine Kopie des Personalausweises nicht erforderlich, vielmehr genügt die Einsichtnahme des Ausweises und die Dokumentation, dass die Identität durch Vorlage bestätigt wurde (siehe ebd. S. 2).
- Unterlagen von abgelehnten Bewerbern sind spätestens nach sechs Monaten zu löschen.

* DSK (Version 1.0, 24.1.2024)

B2

Bonitätsprüfung

Für die Bonitätsprüfung können Vermieter – vor allem Wohnungsgesellschaften – Informationen über den Schuldner direkt bei Auskunfteien (wie bspw. der Schufa Holding AG) anfragen. Die Verarbeitung personenbezogener Daten zu Zwecken der Bonitätsprüfung war zuletzt Gegenstand verschiedener Entscheidungen des EuGH (bspw. C-634/21*, C-26/22 und C-64/22**) und wird verstärkt von europäischen Datenschutzaufsichtsbehörden unter die Lupe genommen. In vielen Fällen liegen berechtigte Interessen vor, sodass die Verarbeitung auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann.

Risiko:

- Denkbar sind etwa Datenschutzverstöße durch fehlende Aufklärung des Mieters oder fehlende Dokumentation der Abwägung der berechtigten Interessen.
- Wird eine Bonitätsauskunft unzulässigerweise gespeichert, besteht die Gefahr der Rechtswidrigkeit der Datenverarbeitung.

* EuGH, Urt. v. 7.12.2023, C-634/21

** EuGH, Urt. v. 7.12.2023, C-26/22 und C-64/22 (verbundene Rechtssachen)

Best Practice:

- Die Bonitätsauskunft sollte erst eingeholt werden, wenn der Abschluss des Mietvertrags nur noch von ihr abhängt. Bei der Selbstauskunft von Mietinteressenten ist darauf zu achten, um welche Art von Auskunft es sich handelt, da manche Auskünfte zusätzliche, ggf. nicht benötigte Angaben enthalten können und dann wegen dem Datenminimierungsgrundsatz nicht verarbeitet werden dürfen.
- Sofern ein Vermieter die Bonität eines Mietinteressenten vor der Vermietung bei der Auskunftei abfragen will, muss der Vermieter den Mietinteressenten in der Regel darauf hinweisen (bspw. durch einen entsprechenden Datenschutzhinweis).
- Der Vermieter muss nachweisen, dass der Mietinteressent diese Informationen erhalten hat. Dies kann bspw. umgesetzt werden durch eine Unterschrift des Mietinteressenten auf dem Kenntnisnahme-Formular bzw. digital durch die Verwendung einer Checkbox. Das unterschriebene Kenntnisnahme-Formular ist für zwölf Monate aufzubewahren.
- Der Vermieter darf die Auskunft bei der Einzelfallentscheidung heranziehen und nicht dauerhaft speichern.

B3

Mietvertragsschluss und Durchführung des Mietvertrags

Mit dem Abschluss und während der Durchführung des Mietvertrags werden weitere personenbezogene Daten verarbeitet.

- Der Vermieter verarbeitet den Namen, die Kontakt- und Bankdaten, etc. des Mieters zur Durchführung des Mietvertrags gemäß Art. 6 Abs. 1 lit. b DSGVO.
- Die Weitergabe der Mieterdaten an den Grundversorger beruht oftmals auf der Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.
- Bzgl. der Rechtsgrundlage für die Datenübermittlung an Handwerker werden unterschiedliche Auffassungen vertreten, wobei die wohl überzeugendsten Argumente dafürsprechen dürften, dass die Rechtsgrundlage der berechtigten Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO oftmals einschlägig ist, da die berechtigten Interessen des Vermieters an der ordnungsgemäßen Instandhaltung seiner Mietsache regelmäßig überwiegen.
- Die Datenweitergabe an den Wärmedienstleister erfolgt in der Regel im Wege der Auftragsverarbeitung (für weitere Informationen siehe Art. 28 und die obigen Ausführungen zu Art. 28 DSGVO).
- Die Datenweitergabe an potenzielle Nachmieter (zum Zweck einer Terminvereinbarung) erfolgt im Regelfall auf der Grundlage der Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO.
- Die Weitergabe an Behörden/öffentliche Stellen beruht meistens auf der Rechtsgrundlage der rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO.

Risiko:

- Datenschutzrechtliche Risiken drohen etwa bei fehlenden oder widerrufenen Einwilligungen sowie bei fehlenden Informationen zur oder einem (drohenden) Widerspruch gegen die Datenverarbeitung, insbesondere aufgrund eines berechtigten Interesses (Art. 13 Abs. 1 lit. d, Art. 21 Abs. 1 DSGVO).
- Fehlende Aktualisierungen der Datenschutzinformationen bei Änderungen.

Best Practice:

- Der Vermieter sollte ein Formblatt „Datenschutzinformationen für Mieter“ erstellen und spätestens bei Vertragsschluss aushändigen, um seiner Informationspflicht nach Art. 13 DSGVO nachzukommen. Ändern sich Umstände oder Prozesse beim Vermieter, müssen die Mieter neue bzw. entsprechend aktualisierte Datenschutzinformationen erhalten. Zwingend enthalten sein müssen die Pflichtinformationen gemäß Art. 13 DSGVO, die u.a. Folgendes beinhalten:
  - Informationen zur möglichen Weitergabe der Daten an Handwerker;
  - Informationen zum Einsatz von Wärmedienstleistern; sowie

Best Practice:

- sonstige Informationen zur Weitergabe der Daten.
- Der Mieter sollte im Idealfall bestätigen, dass er die Datenschutzinformationen erhalten hat. Eine Einwilligung wird jedoch nicht abgefragt.
- Für die Weitergabe der Daten an den Grundversorger ist eine gesonderte Einwilligung der betroffenen Person einzuholen, die der Mieter auch verweigern können muss, ohne etwaige Nachteile zu erleiden. Vor der entsprechenden Datenweitergabe ist der Mieter gemäß Art. 13 DSGVO zu informieren.
- Die Weitergabe der Daten an Dritte erfordert eine Einzelfallbetrachtung (siehe oben, B.III.). Die betroffene Person ist vorher ebenfalls nach Art. 13 DSGVO zu informieren.
- Auch während des Mietverhältnisses gilt, dass personenbezogene Daten zu löschen sind, die für keine Zwecke mehr benötigt werden, sofern keine (bspw. gesetzliche) Aufbewahrungspflicht besteht.

B4

Beendigung des Mietverhältnisses

Auch nach Beendigung des Mietverhältnisses können datenschutzrechtliche Pflichten weiterbestehen. So können einerseits bspw. personenbezogene Daten des Mieters für die Zwecke der Endabrechnung auch noch Monate nach Auszug benötigt werden; andererseits dürfen personenbezogene Daten nur so lange gespeichert werden, wie sie benötigt werden (vgl. Grundsatz der Datenminimierung). Daher ist auch in der Zeit nach der Beendigung des Mietverhältnisses sicherzustellen, dass nur die Daten weiterhin verarbeitet werden, die noch für bestimmte Zwecke benötigt werden.

Risiko:

- Eine unbeschränkte und unbefristete Speicherung personenbezogener Daten nach Beendigung des Mietverhältnisses würde dem Grundsatz der Datenminimierung und der Speicherbegrenzung widersprechen.

Best Practice:

- Sollten Daten an potenzielle Nachmieter (zum Zweck einer Terminvereinbarung) weitergegeben werden, ist u.U. sogar die Einwilligung der betroffenen Person einzuholen und sie ist vorher gemäß Art. 13 DSGVO zu informieren.
- Durch ein zeitlich abgestuftes Löschkonzept kann sichergestellt werden, dass nur die personenbezogenen Daten gespeichert werden, die tatsächlich für konkrete Verarbeitungszwecke benötigt werden. Hierbei bietet es sich an, spezifische Datencluster zu bilden. Für bestimmte Datencluster können Aufbewahrungsfristen zu beachten sein (bspw. aufgrund von Pflichten gemäß dem HGB/der AO). Die Daten eines Datenclusters müssen dann nach dem Ablauf der jeweiligen Frist gelöscht werden, im Idealfall automatisch, ansonsten jedenfalls manuell nach einer entsprechenden Arbeitsanweisung.

B5

Einsatz von Videoüberwachung an bzw. in Mietgebäuden

Der Einsatz von Videoüberwachung an Mietgebäuden ist besonders datensensibel und daher nur unter strengen Voraussetzungen zulässig. Betroffen sind nicht nur die Mieter, sondern alle Bewohner und deren Besucher. Die Rechtmäßigkeit einer Videoüberwachung ist auf der Grundlage des Art. 6 Abs. 1 lit. f DSGVO im Einzelfall genau zu prüfen. Das hierfür erforderliche berechtigte Interesse kann insbesondere in der Wahrung des Hausrechts, der Aufdeckung und Verfolgung von Straftaten sowie der Durchsetzung zivilrechtlicher Ansprüche zu sehen sein, wobei die konkreten Anforderungen an die Rechtmäßigkeit sehr einzelfallabhängig sind.*

Risiko:

- Eine unzureichende oder zu späte Informationsbereitstellung sowie eine pauschale Abwägung zugunsten der Sicherheitsinteressen kann zur Unzulässigkeit der Videoüberwachung führen.

Best Practice:

- Die nach Art. 6 Abs. 1 lit. f DSGVO durchzuführende Risikoabwägung ist zwingend zu dokumentieren.
- Die Informationspflichten nach Art. 13 DSGVO könnten mithilfe eines zweistufigen Informationssystems erfüllt werden:
  - **Stufe 1:** vorgelagerte komprimierte Informationen über die Datenverarbeitung (bspw. durch ein Hinweisschild an den Eingängen zu den überwachten Bereichen).
  - **Stufe 2:** detaillierte Informationen im Nachgang (bspw. durch einen Link oder QR-Code auf dem Hinweisschild).
- Bei der Entwicklung eines Überwachungssystems sind stets die Grundsätze „Privacy by Design“ sowie „Privacy by Default“ umsetzen (siehe hierzu Art. 25 DSGVO).

*vgl. ausführlich zur Videoüberwachung im privaten Bereich BVerwG, Urt. v. 27.3.2019 – 6 C 2.18; BayLDA, Videoüberwachung (mit zahlreichen zusätzlichen Informations-Links); DSK, Kurzpapier Nr. 15 – Videoüberwachung nach der Datenschutz-Grundverordnung; DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 17.7.2020; EDPB, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0

Betroffenenrechte von Mietern

Den Mietern stehen die allgemeinen datenschutzrechtlichen Betroffenenrechte zu. Relevant ist insbesondere der Auskunftsanspruch nach Art. 15 DSGVO. Wie oben dargestellt (B.II.), muss der Vermieter sich auf die Geltendmachung dieses Anspruchs vorbereiten und Prozesse implementieren, die eine zügige Bearbeitung sicherstellen.

Einsatz von Internetportalen bzw. Maklern

Die Vermietung über Internetportale und/oder beauftragte externe Makler ist in der Regel keine Auftragsverarbeitung im Sinne des Art. 28 DSGVO. Das bedeutet: Das Internetportal bzw. der Makler muss die Informationspflichten, d.h. die Informationen zu seiner eigenen Datenverarbeitung, nach Art. 13 DSGVO selbst erfüllen.

Risiko:

- Eine im Einzelfall unklare Verantwortungsverteilung kann zur Rechtswidrigkeit der Datenverarbeitung bzw. zu einem Verstoß gegen datenschutzrechtliche Vorgaben führen.

Best Practice:

- Die Informationspflichten nach Art. 13 bzw. 14 DSGVO sind vom Verantwortlichen (Vermieter/Eigentümer) erst dann zu erfüllen, wenn die Interessentendaten vom Internetportal bzw. Makler in seinen Verfügungsbereich gelangen, also beim Verantwortlichen verarbeitet werden.
- Daher sollte ein beauftragter externer Makler ausdrücklich dazu verpflichtet werden, seine datenschutzrechtlichen Pflichten gemäß Art. 13 DSGVO selbst zu erfüllen.

Best Practices im Marktsegment **«Gewerbe»**

Analoge Anforderungen zum Wohnbereich bei Standardprozessen

Eine Vielzahl von Standardprozessen im Rahmen der Vertragsabwicklung unterliegt denselben Anforderungen wie die aufgezeigten Vorgänge im Wohnbereich, wenn personenbezogene Daten verarbeitet werden. Dies ist der Fall bei der Vermietung an gewerbetreibende Einzelpersonen oder Kleinstunternehmen, die eigentümerbezogen geführt werden (z. B. Einzelkaufmann oder Freiberufler).

Sanktionslistenabgleich

In besonderen Einzelfällen kann es erforderlich sein zu überprüfen, ob die am Vertragsverhältnis beteiligten Personen ggf. auf (inter-)nationalen Sanktionslisten stehen, die den Vertragsschluss mit ihnen untersagen. Zudem können sich aus dem Geldwäschegesetz besondere Anforderungen ergeben.

Best Practices im Marktsegment **«Investment»**

Vertraulichkeit

Schutz der Daten von Käufern und Verkäufern

Bei der Beauftragung von Maklern für den An-/Verkauf einer Immobilie oder bei einer Projektentwicklung können für alle Parteien Verschwiegenheitspflichten außerhalb des Datenschutzrechts bestehen.

Risiko:

- Fehlende Regelungen zur Vertraulichkeit können zu einer unberechtigten Weitergabe personenbezogener Daten an Dritte und einer unangemessenen Sicherheit der Daten führen.

Best Practice:

- Es sollten Vertraulichkeitsvereinbarungen mit allen Beteiligten geschlossen werden.
- Die erlangten Daten sollten nicht für alle Parteien sichtbar abgespeichert, sondern getrennt voneinander aufbewahrt werden.
- Die Parteien sind stets auf die Vertraulichkeit der Daten hinzuweisen.

Eine Verpflichtung als Verantwortlicher besteht auch dann, wenn ein Unternehmen Immobilien in größerer Zahl von Verkäufern kauft oder an Käufer verkauft, bei denen es sich um natürliche Personen handelt und deren personenbezogene Daten in irgendeiner Form in einem Dateisystem gespeichert sind. Hinsichtlich der Daten von Kauf-/Verkaufsinteressenten gelten im Wesentlichen die gleichen Anforderungen wie hinsichtlich der Mietinteressenten.

D3

Übernahme und Übergabe von Mieterdaten

Wenn vermietete Immobilien ge- oder verkauft werden, entsteht im Moment der Wirksamkeit des Grundstücksübergangs (Eintragung im Grundbuch) ein Mietverhältnis gleichen Inhalts zwischen Mieter und Erwerber. Die Rechtsgrundlage für die Weitergabe der Mieterdaten an den Erwerber dürften die berechtigten Interessen nach Art. 6 Abs. 1 lit. f DSGVO des Veräußerers sein.* Der Erwerber verarbeitet seinerseits die Daten zur Erfüllung des neu entstandenen Mietvertrags nach Art. 6 Abs. 1 lit. b DSGVO.

Best Practice:

- Veräußerer und Erwerber informieren vor der Weitergabe der Daten gemeinsam den Mieter und erfüllen so ihre jeweiligen Pflichten nach der DSGVO.
- Dies dürfte auch gelten, wenn der schuldrechtlich festgelegte Übergang der Nutzen und Lasten mit der Wirkung des Verfügungsgeschäfts auseinanderfällt. Zwischen Erwerber und Mieter besteht dann ein vorvertragliches Verhältnis.

* vgl. hierzu das Gutachten des Deutschen Notarinstituts vom 3. September 2021 (Abruf-Nr.: 183895), Datenschutzrechtliche Beurteilung der Weitergabe von Unterlagen des Verkäufers an den Käufer im Rahmen eines Grundstückskaufvertrags, S. 2 f.

Best Practices in der **IT-Sicherheit**

Besonderen Anforderungen unterliegt die Einhaltung von IT-Sicherheitsstandards. Diese bilden die Grundlage eines effektiven Datenschutzkonzepts.

E1

IT-Notfallkonzept – Backupkonzept

Es sind hinreichende Notfall- sowie Backupkonzepte zu errichten, sowohl aus regulatorischen Gründen als auch im Eigeninteresse zur Sicherung wertvoller Informationen.

Risiko:

- Fehlt es an einem hinreichenden Backupkonzept, kann eine bedarfsabhängige Wiederherstellung von gesicherten Daten im Einzelfall eine unrechtmäßige Datenverarbeitung darstellen.

Best Practice:

- Es bietet sich bspw. an, das Notfallkonzept an den Anforderungen des Con.3 Datensicherungskonzepts (Stand: 2023)* des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu orientieren.
- Weiterhin ist eine Zertifizierung nach ISO 27001 in Betracht zu ziehen, insbesondere wenn ein Unternehmen international tätig ist. Analog ist auch eine BSI-Zertifizierung für in Deutschland tätige Unternehmen anzuraten.

* CON.3 Datensicherungskonzepts (Stand: 2023)

E2

Verschlüsselte Übertragung der Internetseite bei Aufrufen sowie verschlüsselte Übermittlung von E-Mails

Sowohl die auf einer Internetseite bereitgestellten Informationen als auch etwaige E-Mails sollten stets über einen Verschlüsselungsmechanismus (Transport Layer Security-Verschlüsselung) übertragen bzw. übermittelt werden, um das Mitlesen der Daten durch Dritte zu verhindern. Dabei muss das Unternehmen nach der Empfehlung des BSI die Transportverschlüsselung TLS in der Version TLS 1.2 oder TLS 1.3 einsetzen.*

Risiko:

- Es besteht die Gefahr etwaiger Zugriffsmöglichkeiten auf die Daten durch Dritte während der Verarbeitung (z. B. bei der Datenerfassung in Formularen oder bei der Übermittlung von E-Mails).

Best Practice:

- Sowohl Internetseiten, auf denen personenbezogene Daten erhoben werden, als auch etwaige E-Mails müssen grundsätzlich verschlüsselt sein.
- Dies gilt in Bezug auf Internetseiten in jedem Fall dort, wo es um Kontaktformulare oder Newsletter-Anmeldungen geht.
- HTTPS** sollte auf Internetseiten als Voreinstellung Standard sein. Zusätzlich könnte die Sicherheit gesteigert werden durch den Einsatz des HSTS-Mechanismus („HTTP Strict Transport Security“).

* siehe hierzu ausführlich BSI, Mindeststandard des BSI zur Verwendung von Transport Layer Security nach § 8 Absatz 1 Satz 1 BSIG, Version 2.4, 25.5.2023 (S. 7 f.) und vgl. für weitere Hinweise explizit in Bezug auf die Übermittlung von E-Mails DSK, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, 16.6.2021

** siehe hierzu BSI, Mindeststandard des BSI zur Verwendung von Transport Layer Security nach § 8 Absatz 1 Satz 1 BSIG, Version 2.4, 25.5.2023 (S. 5))

E3

Einsatz von Künstlicher Intelligenz («KI»)

Der Einsatz von Künstlicher Intelligenz (KI) birgt neben umfassenden Chancen auch Risiken, insbesondere in Bezug auf die datenschutzrechtliche Compliance. So können bspw. beim Einsatz von generativer KI (z.B. ChatGPT) große Mengen personenbezogener Daten verarbeitet werden, wobei die Umstände der Datenverarbeitung nicht immer transparent sind und im Einzelfall vor dem Einsatz geprüft werden müssen.

Risiko:*

- Externe KI-Dienste könnten Daten für eigene Zwecke, wie Training oder Analyse, speichern und es besteht das Risiko, dass sensible Informationen unbeabsichtigt veröffentlicht oder geteilt werden.
- Die unbeabsichtigte/unerwünschte Datenübermittlung in Drittländer, inklusive des Abflusses von personenbezogenen Daten in großem Umfang, birgt ein datenschutzrechtliches Risiko.
- Wird eine Entscheidung ausschließlich durch die KI getroffen (bspw. über den Abschluss des Mietvertrags) kann es sich in Einzelfällen um eine automatisierte Entscheidung gemäß Art. 22 DSGVO handeln, für die weitere strenge Anforderungen zu beachten sind.

Best Practice:**

- Die Mitarbeiter sollten beim Umgang mit KI geschult und sensibilisiert werden. Wenn die KI nicht nachweisbar DSGVO-konform ausgestaltet ist, dürfen keine personenbezogenen Daten an sie übergeben werden.
- Werden personenbezogene Daten durch die KI verarbeitet, sollten auch ein Auftragsverarbeitungsvertrag und, sofern erforderlich, die anwendbaren EU-Standardvertragsklauseln (SCC) mit dem KI-Unternehmen als Auftragsverarbeiter abgeschlossen werden.
- Mit dem Inkrafttreten der KI-Verordnung sind für den Einsatz von sog. Hochrisiko-KI-Systemen, aber auch für den Einsatz von KI-Systemen mit begrenztem oder minimalem Risiko zusätzliche Anforderungen einzuhalten (diese Anforderungen werden im vorliegenden Leitfaden allerdings nicht behandelt).

* Risiken (siehe hierzu ausführlich VIS-Dokumentvorlage: Vortrag (bund.de) und VIS-Dokumentvorlage: Vortrag (bund.de)

** (vgl. zu den Maßnahmen bei KI-Systemen das Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 6.11.2019):

Umgang mit Datenschutzverletzungen («Data Breaches»)

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn die personenbezogenen Daten von einem sicherheitsrelevanten Ereignis betroffen sind, das zu einer Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität führt. Wenn dies geschieht und die Verletzung womöglich ein Risiko für die Rechte und Freiheiten einer betroffenen Person darstellt, ist die zuständige Datenschutzaufsichtsbehörde unverzüglich und spätestens binnen 72 Stunden, nachdem die Verletzung bekannt wurde, darüber zu unterrichten. Hat die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die betroffene(n) Person(en) zur Folge, muss/müssen u.U. auch die betroffene(n) Person(en) darüber informiert werden.

Eine solche Verletzung kann bspw. dann vorliegen, wenn sich Dritte unberechtigt Zugang zu IT-Systemen verschaffen und dabei auf personenbezogene Daten von Mietern, Mietinteressenten und/oder Mitarbeitern zugreifen, diese auslesen oder sperren.

Risiko:

- Ein Verstoß gegen die Melde- und Benachrichtigungspflichten innerhalb der engen Fristen kann zu empfindlichen Sanktionen (u.a. Bußgelder) führen.

Best Practice:*

- Es sollten Notfallpläne/Prozesse geschaffen werden, um im Fall einer Datenschutzverletzung die sehr kurzen Fristen von 72 Stunden für die Meldung an die zuständige Datenschutzaufsichtsbehörde und die Benachrichtigung der betroffenen Personen einhalten zu können.
- Datenschutzvorfälle sollten - unabhängig von einer Meldung an die Datenschutzbehörde oder einer Benachrichtigung der Betroffenen - dokumentiert werden, um gegenüber einer Datenschutzbehörde (aber auch gegenüber den Betroffenen) die getroffenen Erwägungen nachweisen zu können.
- Sollten Datenabflüsse an unbefugte Dritte nicht ausgeschlossen werden können, könnten diese im Darknet auftauchen. Eine Darknetrecherche (über IT-Security-Unternehmen) kann hier wertvolle Kenntnisse über einen möglichen Abfluss liefern.

* vgl. hierzu ausführlich EDPB, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, 28.3.2023

Berechtigungs- bzw. Zugriffskonzept auf Mieterdaten

Personenbezogene Daten sind so zu verarbeiten, dass ihre Integrität und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben. Hierzu zählen nicht nur Dritte, sondern auch Personen innerhalb des eigenen Unternehmens. Denn nicht jeder Beschäftigte im Unternehmen benötigt bspw. Einsicht in Personaldaten, Kundendaten oder Daten sonstiger Personen.

Daher sollte der Zugriff auf personenbezogene Daten nur auf solche Personen beschränkt werden, die diesen Zugriff zur Wahrnehmung ihrer Aufgaben zwingend benötigen. Diese Vorgehensweise wird auch "Need-to-know-Prinzip" genannt.

Risiko:

- Keine angemessene Beschränkung des Zugriffs und der damit verbundenen Berechtigungen im Fall der Verarbeitung personenbezogener Daten kann im Einzelfall gegen den Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f und Art. 32 Abs. 1 lit. b DSGVO verstoßen.

Best Practice:

- Das "Need-to-know-Prinzip" sollte konsequent etabliert werden, d.h. Mitarbeiter und sonstige Personen sollten im Rahmen ihrer Tätigkeit nur auf solche personenbezogenen Daten Zugriff haben, die für die Erledigung der konkreten Tätigkeiten notwendig sind.
- Bei der Umsetzung des Need-to-know-Prinzips sind insbesondere folgende Punkte zu berücksichtigen:
  - Zugriffsrechte mit differenzierten Rechten für Lesen, Veränderung oder Löschung von Daten,
  - Definition von Rollenkonzepten für die Zugriffsrechte,
  - Etablierung eines administrativen Prozesses zur Einrichtung, Vergabe, Anpassung und zum Entzug von Zugriffrechten und
  - Einführung eines Prozesses zur regelmäßigen Kontrolle der Zugriffrechte. Außerdem kann ein Change- bzw. Veränderungsmanagement dabei helfen, die Umsetzung neuer Datenschutzpraktiken zu gewährleisten.

Institut für Corporate Governance
in der deutschen Immobilienwirtschaft
www.icg-institut.de