
REAL ESTATE PRIVACY COMPLIANCE 2018 IN A NUTSHELL

Dieses Dokument richtet sich an Unternehmen der Immobilienwirtschaft und enthält eine Orientierung zu neuen Datenschutzerfordernungen nach der Europäischen Datenschutz-Grundverordnung (DS-GVO oder Verordnung genannt) ab dem 25. Mai 2018. Die nachfolgenden Hinweise sind nicht dazu gedacht, eine Beratung im Einzelfall zu ersetzen.

Worum geht es?

Die Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung¹ personenbezogener Daten². Jede Stelle, die allein oder gemeinsam mit anderen personenbezogene Daten verarbeitet, steht als sog. Verantwortlicher oder als sog. Auftragsverarbeiter in der Pflicht. Das trifft auch auf Management- oder Dienstleistungsunternehmen der Immobilienwirtschaft zu. Gleich, ob Eigentümer oder Verwalter (Asset-, Property- oder Facility-Manager), aber auch das Maklerunternehmen und sonstige Dienstleister - jedes dieser Unternehmen ist dafür verantwortlich, dass es die Anforderungen der DS-GVO einhält. Entweder Ihr Unternehmen verarbeitet selbst personenbezogene Daten – dann ist Ihr Unternehmen ein „Verantwortlicher“ – oder Ihr Unternehmen lässt solche Daten von Dritten, meist externen Dienstleistern, verarbeiten – dann spricht man von „Auftragsverarbeitung“.

Ihr Unternehmen verarbeitet beispielsweise personenbezogene Daten, wenn Namen und Vornamen von Personen, beispielsweise in Mieterlisten, in digitalen Dokumenten auf Datenträgern, auf Servern oder in der Cloud gespeichert werden. Es geht um Informationen aller Art, die die Identität einer Person bestätigen - unter anderem Name, E-Mail-Adresse, Kennnummer, Wohnort, Beruf, Einkommen, Bankverbindung, IP-Adresse etc. Aber nicht nur digitale Daten sind geschützt. Auch die analoge Sammlung strukturierter Daten, die sich auf Personen beziehen – etwa die in Papierform geführte Mieterkartei – muss den Anforderungen der DS-GVO entsprechen. Natürlich bezieht sich die Verordnung unter anderem auch auf Daten der Beschäftigten Ihres Unternehmens und auf Daten, die von der Website Ihres Unternehmens oder der Website Ihrer Immobilie gesammelt werden. Die Zusammenstellung, die Speicherung und das Zugänglichmachen von transaktionsbezogenen Daten müssen ebenfalls neu bedacht werden. In der Regel finden sich bei Due Diligence-Unterlagen personenbezogene Daten. Haben Sie kürzlich solche Daten in einen virtuellen Datenraum hochgeladen? Speichert der Datenraumbetreiber die Daten im außereuropäischen Ausland? Geht der Datenraumbetreiber und gehen die Beteiligten der Transaktion sorgfältig mit den Daten um? Protokolliert der Datenraumbetreiber den Zugriff von identifizierbaren Personen auf bestimmte

¹ „**Verarbeitung**“ meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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.

² „**Personenbezogene Daten**“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Unterlagen? Vielleicht wissen Sie es gar nicht. Dann sollten Sie darüber nachdenken, die Compliance-Anforderungen zu überprüfen.

Bewährtes und Neues

Auch wenn die DS-GVO den Datenschutz nicht neu erfindet und sich auf die seit Jahrzehnten geltenden Grundsätze des Datenschutzes stützt, so enthält sie auch einige neue Prinzipien. So erstreckt sich der Anwendungsbereich auch auf außereuropäische Unternehmen, die aber auf dem europäischen Markt tätig sind (Marktortprinzip). Zum anderen soll eine möglichst einheitliche Anwendung der Regelungen der DS-GVO in den EU-Mitgliedstaaten gewährleistet werden. Die Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“, der „Datensicherheit“ und der „Transparenz“ prägen die Verordnung. Ferner erfährt die Datenübermittlung ins EU-Ausland eine detaillierte Regelung.

Verbot mit Erlaubnisvorbehalt

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine Einwilligung oder eine andere in der Verordnung normierte Ausnahme vorliegt (Verbot mit Erlaubnisvorbehalt). Erlaubt ist die Verarbeitung nur, wenn

- die Verarbeitung für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- wenn sie im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist oder
- sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Häufig geben ein „Vertrag“ oder „berechtigtes Interesse“ eine ausreichende Grundlage für die Verarbeitung. Die Verarbeitung von Daten ist erlaubt, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist. Ein berechtigtes Interesse könnte vorliegen, wenn eine Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde ist oder ein Dienstleistungsverhältnis besteht. Aber Achtung! So mag die temporäre Speicherung von Daten für die Vertragserfüllung oder aufgrund eines berechtigten Interesses gerechtfertigt sein. Die Verwendung der Daten für Werbezwecke, beispielsweise für die Übermittlung von Newslettern, ist davon in der Regel nicht gedeckt.

Datenvermeidung und Datensparsamkeit

Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und sachlich relevant sowie auf das für den Zweck der Datenverarbeitung notwendige Maß beschränkt sein.

Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden.

Datensicherheit

Daten müssen sicher sein. Es sind geeignete technische und organisatorische Maßnahmen zu ergreifen. Das Sicherheitslevel muss im Verhältnis zum Risiko angemessen sein. Danach kann unter anderem eine Pseudonymisierung oder Verschlüsselung von Daten geboten sein. Fähigkeit, Vertraulichkeit, Integrität und Verfügbarkeit und Belastbarkeit der IT-Systeme sind zu gewährleisten.

Transparenz

Die Rechte der betroffenen Person werden gestärkt. Grundlage der Betroffenenrechte sind die Anforderungen an die Transparenz der Informationen, an die Kommunikation und die Modalitäten für die Ausübung der Rechte der betroffenen Person. Es gibt einen umfangreichen Katalog obligatorischer Benachrichtigungen an den Betroffenen. Dies betrifft unter anderem Kontaktdaten des Verantwortlichen, die Verarbeitungszwecke sowie die Rechtsgrundlage, gegebenenfalls die Empfänger sowie die Absicht der Übermittlung in ein Drittland, aber auch die Dauer der Speicherung, beziehungsweise die Kriterien für die Festlegung dieser Dauer. Der Betroffene ist schließlich über seine Rechte zu informieren.

Betroffenenrechte

Die betroffene Person hat unter anderem das Recht,

- eine Bestätigung zu verlangen, ob personenbezogene Daten verarbeitet werden;
- auf Auskunft über diese Daten sowie über Informationen unter anderem über die Verarbeitungszwecke, deren Herkunft, Empfänger, über die Dauer der Speicherung sowie über ihre Rechte;
- die Berichtigung sowie im Hinblick auf den Zweck die Vervollständigung sie betreffender unzutreffender personenbezogener Daten zu verlangen;
- die Löschung ihrer Daten zu verlangen – zum Beispiel, wenn diese zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind oder die dazu erteilte Einwilligung widerrufen wurde. Eine Ausnahme besteht zum Beispiel, soweit die Verarbeitung zur Ausübung der freien Meinungsäußerung erforderlich ist;
- auf „Vergessenwerden“, wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat. Dann muss sie vertretbare Schritte unternehmen, um die Stellen, die diese Daten verarbeiten, zu informieren, dass die betroffene Person von ihnen die Löschung aller Daten oder von Kopien oder Replikationen verlangt;
- in bestimmten Fällen die Einschränkung der Verarbeitung zu verlangen, zum Beispiel, wenn der Verantwortliche die Daten nicht mehr länger, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt oder die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen;
- auf Mitteilung jeder Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen; und
- unter bestimmten Voraussetzungen eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten.

Datenübermittlung in Drittstaaten

Eine Übermittlung von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die einschlägigen Bedingungen erfüllen und auch die sonstigen Bestimmungen der Verordnung beachtet werden. Als Daumenregel gilt: Drittländer sind Länder außerhalb der EU oder des Europäischen Wirtschaftsraums.

Meldungen von Datenschutzverletzungen

Verletzungen des Schutzes personenbezogener Daten müssen unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Aufsichtsbehörde gemeldet werden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt.

Datenschutz-Folgenabschätzung

Birgt die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten, muss der Verantwortliche bereits vorab eine Abschätzung der Folgen für den Schutz personenbezogener Daten durchführen. Dies ist insbesondere der Fall bei neuen Technologien,

aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. Klingt in Ihrem Arbeitsbereich abwegig? Was ist mit der Videoüberwachung in Ihren Immobilien?

Pflicht zur Bestellung eines Datenschutzbeauftragten

Unternehmen in Deutschland müssen – wie bisher – einen Datenschutzbeauftragten bestellen, wenn mehr als 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Verarbeitung besonders sensibler Daten

Die Verarbeitung besonders sensibler Daten unterliegt besonderen Bedingungen. So ist die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung grundsätzlich untersagt, es sei denn, es liegen bestimmte ausdrücklich geregelte Ausnahmen vor.

Drastische Sanktionen

Die Einhaltung der Datenschutzanforderungen werden durch unabhängige Datenschutzbehörden überwacht. Die Sanktionsmöglichkeiten werden deutlich ausgedehnt. So sind für bestimmte Rechtsverstöße Bußgelder bis zu 4 % des Jahresumsatzes eines Unternehmens, beziehungsweise EUR 20 Mio., zulässig, wobei der jeweils höhere Wert gilt. Dabei ist auf den gesamten weltweiten Jahresumsatz des betreffenden Unternehmens abzustellen.

Fazit

Alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind auf einen Anpassungsbedarf im Hinblick auf die Umsetzung der Verordnung zu überprüfen. Dies betrifft insbesondere die rechtlichen, technischen und organisatorischen Bereiche in Ihrem Unternehmen. Die Kernaufgabe wird sein, herauszufinden, welche Prozesse im Unternehmen anzupassen sind.

Weitergehende Orientierung

Wir empfehlen für eine weitergehende Orientierung die Kurzpapiere der Datenschutzkonferenz zum neuen Datenschutzrecht. Diese Kurzpapiere sind auf der Website des Bundesbeauftragten für den Datenschutz abrufbar:

https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html

Als Einstieg eignet sich das Kurzpapier „Maßnahmenplan DS-GVO für Unternehmen“.

Um besser abschätzen zu können, wie gut Ihr Unternehmen auf die neuen Datenschutzanforderungen vorbereitet ist, empfehlen wir das Online-Tool des Bayerischen Landesamtes für Datenschutzaufsicht:

<https://www.lida.bayern.de/tool/start.html>

Stand: Mai 2018

KUCERA Rechtsanwälte