immolex

NEUES MIET- UND WOHNRECHT
APRIL 2018

04

www.immolex.at

97 – 128

Rsp-Nr
35 – 44

Mietrecht

Der Unterbrechungsantrag als taktisches Element der Prozessführung

Erhöhter Mietzins und verbotene Ablöse

Wohnungseigentumsrecht

Erwachsenenschutz und Wohnungseigentum

Datenschutzrecht

Datenschutz im Wohnrecht

Forum Immobilientreuhänder

Zu den Grenzen der Vollmacht des Verwalters

MANZ

Datenschutz im Wohnrecht

Art 6 Abs 1 lit a, Art 13, 14 DSGVO

personenbezogene Daten; Einwilligung zur Verarbeitung von Daten; Erlaubnistatbestand; Auskunftspflichten; Videoüberwachung

Am Thema Datenschutz kommt dieser Tage wohl kaum jemand vorbei – ab 25. 5. 2018 ist die neue EU-Datenschutz-Grundverordnung[1] (im Folgenden kurz „DSGVO") unmittelbar anwendbar. Auch für die Immobilienbranche stellen sich iZm der DSGVO zahlreiche Fragen. Der folgende Artikel versteht sich als Versuch einer überblicksmäßigen Aufarbeitung ausgewählter Bestimmungen ohne Anspruch auf Vollständigkeit, da eine detaillierte Abhandlung im Rahmen des gegenständlichen Artikels aufgrund der Komplexität des Themas und der Vielzahl an Fragestellungen im Detail nicht möglich ist; schon gar nicht für alle unterschiedlichen Beteiligten der Immobilienbranche.

SIMONE MAIER-HÜLLE

A. Unter welchen Umständen sind Einwilligungen zu einer Datenverarbeitung einzuholen?

Ab 25. 5. 2018 unterliegt die Verarbeitung von personenbezogenen Daten,[2] wie bspw Personenstamm-, Kommunikations-, Vertragsstamm- und Abrechnungsdaten, den Grundsätzen und Anforderungen der DSGVO. Als Grundregel gilt, dass ein **Verantwortlicher**[3] personenbezogene Daten nur dann rechtmäßig verarbeitet, wenn die Datenverarbeitung auf einem **konkreten Erlaubnistatbestand** des **Art 6 DSGVO** beruht. Im Bereich des Wohnrechts kommen bspw die Erfüllung oder Vorbereitung von Miet- oder Verwaltungsverträgen, deren Vertragspartei die betroffene Person[4] ist, in Frage.

Ein in der Praxis äußerst relevanter Erlaubnistatbestand ist die **Einwilligung** der betroffenen Person in die Verarbeitung der sie betreffenden personenbezogenen Daten gem Art 6 Abs 1 lit a DSGVO. Um die informationelle Selbstbestimmung des Einzelnen sowie die Rechtssicherheit für die Verarbeitung durch den Verantwortlichen gleichermaßen zu schützen, normiert die DSGVO strenge Wirksamkeitsvoraussetzungen.[5]

Eine **wirksame Einwilligung** muss freiwillig und in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erfolgen. Die Einwilligung kann etwa durch eine schriftliche (auch elektronische) oder mündliche Erklärung, durch Anklicken eines Kästchens beim Besuch einer Internetseite oder durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft[6] erfolgen. **Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit** der betroffenen Person sind **keine DSGVO-konformen Einwilligungen.**

Als Bedingungen für die Einwilligung durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, normiert die DSGVO, dass das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen muss, sodass es von den anderen Sachverhalten klar zu unterscheiden ist.[7] Soweit der Verantwortliche daher vorformulierte Einwilligungserklärungen verwendet, sind diese entsprechend zu textieren und von anderen Vertragsklauseln unterscheidbar, etwa durch Hervorheben, zu gestalten.

Bei der **Erstellung von Einwilligungserklärungen** ist darüber hinaus das in der DSGVO normierte sog Koppelungsverbot zu beachten: **Eine Einwilligung gilt als nicht freiwillig erteilt,** wenn die Erfüllung eines Vertrags von ebendieser Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, obwohl diese Verarbeitung für die Vertragserfüllung nicht erforderlich ist.[8] Ebenso sind bei Verarbeitungen für mehrere Verarbeitungszwecke gesonderte Einwilligungen einzuholen.[9] Die betroffene Person ist vor Abgabe der Einwilligung zudem darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann.

Da die Einwilligung als Legitimationsgrundlage bereits vor der jeweiligen Datenverarbeitung vorliegen

Mag. *Simone Maier-Hülle* ist Rechtsanwältin in Wien.

1) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

2) Art 4 Nr 1 DSGVO definiert „personenbezogene Daten" wie folgt: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

3) Art 4 Nr 7 DSGVO definiert „Verantwortlicher" wie folgt: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

4) Art 4 Nr 1 DSGVO definiert eine „betroffene Person" als eine identifizierte oder identifizierbare Person; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insb mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem Merkmal oder zu mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

5) Art 4 Nr 11, Art 6 Abs 1 lit a und Art 7 iVm den Erwägungsgründen.

6) Darunter fallen insb der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern.

7) Art 7 DSGVO.

8) Art 7 Abs 4 DSGVO.

9) ErwGr 32.

und der für die Verarbeitung Verantwortliche die wirksame Erteilung der Einwilligung nachweisen muss, sind die vorliegenden Einwilligungen in Hinblick auf die Anforderungen der DSGVO zu prüfen und gegebenenfalls fehlende Einwilligungen einzuholen.

Bei Verstößen gegen den Grundsatz der Rechtmäßigkeit bzw die Bedingungen für die Einwilligung drohen **Geldbußen** von **bis zu 20 Mio Euro** oder im Fall eines Unternehmens von **bis zu 4%** des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist.

B. Wie kann den Informationspflichten entsprochen werden?

Zur Konkretisierung des Transparenzgebots[10] normieren **Art 13 und 14 DSGVO** Informationspflichten des Verantwortlichen gegenüber den von einer Datenverarbeitung betroffenen Personen. Dabei sind der betroffenen Person **datenschutzrelevante Informationen und Mitteilungen** präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst bereitzustellen. Verlangt wird, dass den betroffenen Personen ein aussagekräftiger Überblick über die Verarbeitung vermittelt wird. Dabei können zusätzlich auch standardisierte Bildsymbole als visuelle Elemente eingesetzt werden.[11]

Abhängig davon, ob der Verantwortliche die Daten bei der betroffenen Person selbst oder aus anderen Quellen erhebt, enthält die DSGVO konkrete Vorgaben, worüber und auch zu welchem Zeitpunkt zu informieren ist. In welcher **Form** der Betroffene zu informieren ist, ist hingegen weitgehend dem Verantwortlichen überlassen. Der Verantwortliche könnte die betroffene Person etwa schriftlich, per E-Mail oder mittels einer auf seiner Website veröffentlichten Datenschutzerklärung informieren. Auf Verlangen der betroffenen Person wäre sogar eine mündliche Information zulässig.

Erhebt der Verantwortliche die personenbezogenen Daten bei der betroffenen Person selbst, bspw durch Befragen oder Anfordern von Unterlagen, müssen dem Betroffenen Name und Kontaktdaten des für die Verarbeitung Verantwortlichen genannt werden. Soweit ein Datenschutzbeauftragter bestellt ist, sind auch dessen Kontaktdaten bekannt zu geben.

Weiters hat der Verantwortliche **Informationen zur Datenverarbeitung** bereitzustellen, und zwar

- den **Zweck,** für den die personenbezogenen Daten verarbeitet werden sollen,
- die **Rechtsgrundlage** für die Verarbeitung (zB Einwilligung, Vertragserfüllung),
- die **Empfänger bzw Kategorien** von Empfängern der personenbezogenen Daten,
- ggf die **Absicht zur Übermittlung an ein Drittland** oder eine internationale Organisation,
- über die **Dauer der Speicherung,**
- über **Strukturen automatisierter Entscheidungsfindung** („Profiling").

Zudem muss sich der Verpflichtete dazu rechtfertigen, warum er diese Daten verarbeitet, ob der Betroffene verpflichtet ist, an der Datenerhebung mitzuwirken, und welche Folgen eine Verweigerung der Mitwirkung hätte. Der Verantwortliche muss ebenso auf die **Rechte der betroffenen Person** hinweisen. Stehen der Verantwortliche und die betroffene Person in einem ständigen geschäftlichen Kontakt und verfügt die betroffene Person daher (zumindest teilweise) über mitzuteilende Informationen, so ist der Verantwortliche im Hinblick auf diese vorhandenen Informationen von seiner Informationsverpflichtung befreit. Weitere **Ausnahmen** sind das Vorliegen von speziellen gesetzlichen Verpflichtungen zur Speicherung/Offenlegung der personenbezogenen Daten oder bei Unmöglichkeit oder bei unverhältnismäßigem Aufwand für den Verantwortlichen.

Werden **personenbezogene Daten auf andere Weise als bei der betroffenen Person** erhoben, zB bei Datenerhebung ohne deren Kenntnis oder **aus Datenbeständen Dritter,** muss der Verantwortliche zusätzlich auch über die Kategorien der verarbeiteten personenbezogenen Daten sowie die konkrete Quelle der personenbezogenen Daten informieren. Der Verantwortliche muss die betroffene Person regelmäßig innerhalb angemessener Frist, jedoch maximal einen Monat nach Erlangung der personenbezogenen Daten informieren. Verfügt der Verantwortliche auch über **Post- oder E-Mail-Adressen sowie Telefonnummern,** muss er seine Informationspflicht spätestens zum Zeitpunkt der ersten Mitteilung erfüllen.

Je nachdem, welche Personen von einer Datenverarbeitungen betroffen sind, haben Unternehmen ihre vorhandenen **Datenschutzerklärungen anzupassen** und **Datenschutzfolder oder Informationsschreiben** zu erstellen, um ihre Informationspflichten nach DSGVO fristgerecht erfüllen zu können.

Bei Verstößen **gegen den Transparenzgrundsatz,** die **Transparenzvorschrift** und die **Informationspflichten nach der DSGVO** drohen Geldbußen von **bis zu 20 Mio Euro** oder im Fall eines Unternehmens von **bis zu 4%** des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, wiederum je nachdem, welcher der Beträge höher ist.

C. Wie ist die Tätigkeit der Hausverwaltung aus dem Blickwinkel der DSGVO zu beurteilen?

Was nun zB die Verwaltung von Mietverhältnissen oder von Wohnungseigentum und alle damit zusammenhängenden einschlägigen Tätigkeiten mit sich bringen, kann für die Verarbeitung von personenbezogenen Daten idR vom Vorliegen eines **Erlaubnistatbestands ausgegangen werden,** da die Verarbeitung der Daten für die Erfüllung eines Vertrags, dessen Vertragspartei der Betroffene ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage des Betroffenen erfolgen, wie zB Vorbereitungsmaßnahmen zum Abschluss eines Mietvertrags. Das Einholen einer gesonderten **Einwilligung des Betroffenen** zur Verarbeitung seiner Daten ist daher **nicht erforderlich.**

10) Art 5 Abs 1 lit a DSGVO.

11) Art 12 DSGO; ErwGr 58.

D. Wie haben Hausverwaltungen auf Auskunftsbegehren von Mietern/ Eigentümern zu reagieren?

Dem Auskunftsbegehren eines Mieters / Eigentümers ist gem **Art 15 DSGVO** zu entsprechen; dies ehestmöglich, jedoch längstens binnen eines Monats.

E. Was sollte aus datenschutzrechtlicher Sicht noch beachtet werden?

Datenschutzrechtlich spannend ist auch die Frage nach der Zulässigkeit von **Bonitätsauskünften und Einkommensnachweisen,** die mittlerweile bei Mietvertragsabschlüssen regelmäßig abverlangt werden. Strittig ist hier zunächst, ob und in welchem Umfang ein Vermieter (Verwaltung) im Vorfeld eines Vertragsabschlusses Daten über Mietinteressenten einholen darf. Der Umfang einer zulässigen Datenverarbeitung hängt hier insb davon ab, wie weit die Vertragsverhandlungen schon fortgeschritten sind. Grundsätzlich gilt – je konkreter die Vertragsverhandlungen sind, desto mehr Daten dürfen erhoben werden. Eine konkrete Bonitätsanfrage – zB bei einschlägigen Auskunftsbüros – darf erst dann eingeholt werden, wenn das Zustandekommen eines Mietvertrags nur noch von einer positiven Bonitätsauskunft abhängt. Sehr wohl zulässig ist aber eine Abfrage von Daten aus sog **Warndateien,** die dem Schutz vor Mietnomaden dienen; dies auch schon im Vorfeld zur Vorauswahl von bestimmten Mietinteressenten.

Jedenfalls wird man durch geeignete **Zugriffskontrollen** auch gewährleisten müssen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, um zu vermeiden, dass personenbezogene Daten bei der Verarbeitung und Nutzung nicht unbefugt gelesen, kopiert, verändert und gelöscht werden können. Es ist demgemäß sicherzustellen, dass jeder Mitarbeiter im Rahmen seiner Tätigkeit nur auf solche Daten zugreifen kann, die er zur Erfüllung seiner Aufgabe tatsächlich benötigt, sog **„need to know-Prinzip".**

Dass darüber hinaus der zuständige Verwalter oder der Buchhalter Kenntnis über das konkrete Mieterkonto haben muss, versteht sich von selbst. Ob darüber hinaus aber auch für jeden anderen Mitarbeiter im Unternehmen eine Notwendigkeit dazu besteht, darf bezweifelt werden. Die **internen Organisationsabläufe** müssen daher auch in diese Richtung abgeklärt und angepasst werden. In Bezug auf die unternehmensinterne Verwendung und Weitergabe von Daten sind daher entsprechende **technische und organisatorische Maßnahmen** im Hinblick auf die Datensicherheit zu setzen.

Die DSGVO selbst sieht folgende Maßnahmen vor:

- **Pseudonymisierung und Verschlüsselung** personenbezogener Daten, zB durch Passwortsicherungen von Dateien?
- **Sicherstellung der Vertraulichkeit der Systeme** iZm der Verarbeitung auf Dauer, zB Zutritts-/ Zugangskontrollen, Zugriffsbeschränkungen?
- **Wiederherstellung der Verfügbarkeit** personenbezogener Daten bei einem technischen Zwischenfall, zB durch Backup-Programme?
- **Verfahren zur regelmäßigen Überprüfung,** Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, zB Selbstevaluierungsprozesse.

Generell gilt das Prinzip des sog **„risikobasierten Ansatzes"** – dh Risiken, die mit der Verarbeitung verbunden sind, insb bei unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu personenbezogenen Daten, sind zu beachten. Wie dies konkret organsiert wird, hängt von den jeweiligen Unternehmensstukturen im Einzelfall ab und kann daher nicht pauschal festgelegt werden.

SCHLUSSSTRICH

Wie anhand vieler Neuerungen – man denke an die Einführung der Immobilienertragsteuer oder der Umsetzung der 4. GeldwäscheRL – wird sich auch im Anwendungsbereich der DSGVO erst in der Praxis zeigen, welche Maßnahmen sich als effizient und tauglich erweisen. Auch wenn die Umsetzung der DSGVO vermutlich eher die richtig großen Datenbetreiber wie Facebook, Google etc und einen diesbezüglich sensibleren Umgang mit Daten im Auge gehabt haben dürfte, ist es dringend geboten, sich rechtzeitig mit dem Thema und den nunmehrigen gesetzlichen Vorgaben auseinanderzusetzen. Die Höhe der Strafen wurde vielfach als überzogen kritisiert. Freilich wird davon ausgegangen werden dürfen, dass die Behörde hier auch mit dem entsprechenden Augenmaß vorgehen wird müssen. Gerade für Einzelunternehmen oder KMU könnte sich ein Verstoß gegen datenschutzrechtliche Bestimmungen ansonsten mitunter existenzvernichtend auswirken.