Datenschutz für den Verwalter

Deutscher Immobilientag 2018
Tor zur Zukunft
14. Und 15. Juni 2018

Referent Eric Drissler

EU Datenschutzgrundverordnung

- EU Datenschutzgrundverordnung (DSGVO), ist eine Verordnung damit verbindlich in allen Mitgliedsstaaten der EU und muss nicht in nationales Recht umgesetzt werden
- es gibt 99 Artikel, die Hintergründe werden in 173 Erwägungsgründen beschrieben
- Teilweise sind sogenannte „Öffnungsklauseln“ enthalten, so dass die nationalen Staaten dies eigenständig regeln bzw. ergänzen können – in Deutschland ist das BDSG n. F.
- BDSG n.F. mit weiteren 84 Paragraphen → Teil 2 + Teil 3 für nicht öffentliche Stellen
- 24. Mai 2016 beschlossen, aktiv seit 25. Mai 2018

Räumliche Anwendung

- Sitzlandprinzip
- Marktortprinzip → Unternehmen müssen nicht mehr in der EU einen Sitz haben, damit die Verordnung greift
- Beobachten des Verhaltens innerhalb der EU bzw. betroffene der EU
- ob entgeltlich oder unentgeltlich ist unerheblich

Grundsätze:

Grundsätze für die Verarbeitung personenbezogener Daten - Art. 5 DSGVO

- **rechtmäßige Weise**, nach **Treu und Glauben** und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden → Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und **dürfen nicht** in einer mit diesen Zwecken **nicht zu vereinbarenden Weise weiterverarbeitet werden** ....
- dem **Zweck angemessen** und erheblich sowie auf das für die Zwecke der Verarbeitung **notwendige Maß beschränkt** → Datenminimierung bspw. Mieterselbstauskunft mit Zug um Zug Erhebung
- **sachlich richtig** und erforderlichenfalls auf dem **neuesten Stand** sein... → Richtigkeit
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen **nur so lange ermöglicht**, wie es **für** die Zwecke, für die sie **verarbeitet werden, erforderlich ist**... → Speicherbegrenzung
- in einer Weise verarbeitet werden, die eine **angemessene Sicherheit**... gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und **vor unbeabsichtigtem Verlust**, **unbeabsichtigter Zerstörung** oder **unbeabsichtigter Schädigung** ... → Integrität und Vertraulichkeit

Grundsätze:

Rechtmäßigkeit der Datenverarbeitung - Art. 6 DSGVO

„Die **Verarbeitung** ist **nur rechtmäßig**, wenn **mindestens eine** der nachstehenden **Bedingungen erfüllt** ist:“

- Art. 6 (1) a - die betroffene Person hat ihre Einwilligung zu der Verarbeitung … gegeben → bspw. Suchprofil, Newsletter, kritisch! Auskunfteien wegen Freiwilligkeit im knappen Wohnmarkt & Kopplung
- Art. 6 (1) b - die Verarbeitung ist für die Erfüllung eines Vertrags, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen → bspw. Mietvertrag
- Art. 6 (1) c - die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt → bspw. steuerrechtliches, Geldwäschegesetz
- Art. 6 (1) f - die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt → bspw. Kameraüberwachung nach Anlass (Beschilderung nicht vergessen, Löschfristen festlegen und Verarbeitungsvorgang dokumentieren), ggf. Auskunfteien
- .....

Rechte der betroffenen Person:

Transparenz und Informationspflichten - Art. 13 DSGVO

„Werden **personenbezogene Daten** bei der betroffenen Person erhoben, so **teilt der Verantwortliche** der betroffenen Person **zum Zeitpunkt der Erhebung** dieser Daten Folgendes **mit**: “

- Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters
- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission .....

und weitere .... **bei Dritterhebung entsprechend die Pflichten nach Art. 14 DSGVO beachten!**

Rechte der betroffenen Person:

Betroffenenrechte - Art. 15ff DSGVO

Die Rechte der Betroffenen sind auch in der EU DSGVO enthalten und wurden zusätzlich gestärkt und ergänzt, konkret sind das u.A.:

- Auskunftsrechte
- Rechte zur Berichtigung
- Rechte auf Vergessenwerden = Löschen
- Rechte auf Datenübertragbarkeit

Verantwortlicher & Auftragsverarbeiter:

Privacy by Design & Default - Art. 25 DSGVO

„Unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere** der mit der Verarbeitung **verbundenen Risiken** für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl **zum Zeitpunkt der Festlegung** der Mittel für die Verarbeitung als auch zum **Zeitpunkt der eigentlichen Verarbeitung** geeignete **technische und organisatorische Maßnahmen**....“

Beispiele:

- HTTPS Verschlüsslung auf Webseite
- minimale Pflichtfelder; Selbstauskunft reduziert

„Der Verantwortliche trifft **geeignete technische und organisatorische Maßnahmen**, die sicherstellen, dass **durch Voreinstellung** grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck **erforderlich ist**, verarbeitet werden....“

Beispiele:

- Haken muss bewusst gesetzt werden

Verantwortlicher & Auftragsverarbeiter:

Auftragsverarbeiter - Art. 28 DSGVO

- Grundsatz der Privilegierung bleibt erhalten, **Auftragsverarbeiter ist kein Dritter**
- ersetzt die Auftragsdatenverarbeitung
- „legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**. Sie legen in einer Vereinbarung in **transparenter Form** fest, **wer** von ihnen **welche Verpflichtung** gemäß dieser Verordnung erfüllt, insbesondere was **die Wahrnehmung der Rechte** der betroffenen Person angeht, und **wer welchen Informationspflichten** **...**nachkommt..“
- Haftung endlich beidseitig – bisher nur Auftraggeber!

Bspw. IT-Dienstleister, Webhoster & Clouddienstleister, Heizkostenabrechner, Wartungsunternehmen, Aktenvernichter, Lohn- & Gehaltsabrechner; nicht Auftragsverarbeitung sind Handwerker – hier muss aber der Datenschutz eingehalten werden und eine Rechtsgrundlage muss vorliegen

Verantwortlicher & Auftragsverarbeiter:

Verzeichnis der Verarbeitungstätigkeiten - Art. 30 DSGVO

„Jeder **Verantwortliche** und gegebenenfalls sein Vertreter führen ein **Verzeichnis aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben..:“

- Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation und Vorhandensein oder fehlen eines Angemessenheitsbeschlusses
- vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Verantwortlicher & Auftragsverarbeiter:

Meldepflicht bei Datenschutzverletzungen - Art. 33 DSGVO

„im Falle einer **Verletzung des Schutzes personenbezogener Daten** meldet der Verantwortliche **unverzüglich und möglichst binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, **es sei denn**, dass die **Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten** natürlicher Personen führt…“

- Beschreibung der Art der Verletzung
- Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen bzw. Datensätze
- Namen und die Kontaktdaten des Datenschutzbeauftragten
- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten ….

Verantwortlicher & Auftragsverarbeiter:

Datenschutz-Folgeabschätzung - Art. 35 DSGVO

„hat eine **Form der Verarbeitung**, insbesondere bei **Verwendung neuer Technologien**, aufgrund der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche **vorab eine Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden. … erforderlich für“

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen…
- …Verarbeitung besonderer Kategorien von personenbezogenen Daten…
- …Verarbeitung personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten…
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche → bspw. Kameraüberwachung

Verantwortlicher & Auftragsverarbeiter:

Datenschutzbeauftragter - Art. 37 - 39 DSGVO, § 38 BDSG n. F.

- Bestellpflicht nach BDSG n.F.: „soweit sie in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“ → Personen, nicht mehr Beschäftigte!
- Sonderfälle direkte Bestellung: öffentliche Stellen / Behörden, bei Kerntätigkeit Überwachungsmaßnahmen, bei Kerntätigkeit besondere Kategorien von Daten oder pbD über strafrechtliche Verurteilungen und Straftaten
- **interner DSB und externer DSB weiterhin zulässig**
- **seit 25.05.2018** muss der **DSB der zuständigen Aufsichtsbehörde gemeldet werden** mit Kontaktdaten und **transparent gemacht werden bspw. in der Datenschutzerklärung der Webseite**
- nach wie vor darf es **keine Interessenskonflikte** geben

Hinweis: bei internem Kündigungsschutz und Fortbildungsanspruch-/Verpflichtung beachten!

Verantwortlicher & Auftragsverarbeiter:

Sicherheit der Verarbeitung - Art. 32 DSGVO

„unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der Art, des **Umfangs**, der **Umstände** und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Das heißt Sie müssen die Maßnahmen nicht nur dokumentieren, sondern Eintrittswahrscheinlichkeit und Schwere des Risikos bewerten vgl. Risikoanalyse

Rechtsbehelfe, Haftung und Sanktionen:

Haftung und Recht auf Schadenersatz - Art. 82 DSGVO

Jede Person, der wegen eines **Verstoßes gegen diese Verordnung** ein **materieller** oder **immaterieller Schaden** entstanden ist, hat **Anspruch auf Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Rechtsbehelfe, Haftung und Sanktionen:

Sanktionen - Art. 83 & 84 DSGVO

Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen ... in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Beachtet werden:

- **Art, Schwere und Dauer** des Verstoßes sowie **Ausmaß**;
- **Vorsätzlichkeit oder Fahrlässigkeit** des Verstoßes
- jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter **getroffenen Maßnahmen** zur Minderung des den betroffenen Personen entstandenen Schadens;
- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen ... **getroffenen technischen und organisatorischen Maßnahmen**;
- etwaige einschlägige **frühere Verstöße** des Verantwortlichen oder des Auftragsverarbeiters;
- Umfang der **Zusammenarbeit mit der Aufsichtsbehörde**, ...
- **Kategorien personenbezogener Daten**, die von dem Verstoß betroffen sind;
- **Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde**, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
- .....

Rechtsbehelfe, Haftung und Sanktionen:

Sanktionen - Art. 83 & 84 DSGVO

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **10 Mio. EUR** oder im Fall eines Unternehmens von bis **zu 2** % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
- ...

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **20 Mio. EUR** oder im Fall eines Unternehmens von bis zu **4** % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

- die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
- die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
- die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
- ...

22 Tage DSGVO geltend – erste Erfahrungen

Pünktlich mit dem Start des EU-DSGVO am 25.05.2018 hat es die ersten Abmahnungen, sämtlich initiiert von Mitbewerbern, gegeben. Bekannt sind bislang Rügen folgender Mängel:

- Fehlende Datenschutzerklärung auf der Website
- Einbindung von Google Fonts auf der Website
- fehlerhafte Einbindung von Google Analytics
- Facebook like und share Buttons
- fehlende Verschlüsselung von Kontaktformularen (https)

Am 05.06.2018 kam das EuGH Urteil wegen Facebook Fanpages - künftig Fanpageinhaber und Facebook gemeinsam verantwortlich → konkrete erforderliche Maßnahmen noch unbekannt

IVD Datenschutzhotline musste leider Datenschutzhotline einstellen
→ 325 beantworte Anfragen (Ende 2018 bis Anfang Mai 2018), fast 80 Stunden Hotlinezeit
→ 341 Neuanfragen im Mai 2018

Zusammenfassung?

- prüfen Sie gerade Ihre Webseite auf https (bei Formularen), Datenschutzerklärung, Cookie Hinweise usw.
- denken Sie an die Informationspflichten
- Bestellen Sie Ihren DSB wenn erforderlich und melden diesen der zuständigen Datenschutzaufsichts-behörde und machen diesen transparent
- Kümmern Sie sich um Ihre Verpflichtungserklärungen mit den Mitarbeitern
- Überprüfen Sie Ihre bestehenden Auftragsdatenverarbeitungsverträge und überführen Sie diese zu Auftragsverarbeitungsverträge; schließen Sie neue Auftragsverarbeitungsverträge ab
- Erstellen Sie Policies und Richtlinien
- Sorgen Sie für ausreichende Sicherheit der Verarbeitung und dokumentieren diese
- Erstellen Sie das Verzeichnis der Verarbeitungstätigkeiten
- Führen Sie Datenschutzfolgeabschätzung wo erforderlich durch
- Beachten Sie Privacy by Design und Default
- Beachten Sie die Meldepflicht bei Datenpannen

Hilfe und Unterstützung? Kontaktdaten?

Broschüren, Vorlagen und Informationen:
als Download im IVD Mitgliederbereich

Workshops, Seminare, Webinare
Webinar: EU Datenschutzgrundverordnung (EU DSGVO) - was bedeutet das für mich als Immobilienprofi?
Veranstalter: Sprengnetter Akademie, 19.06.2018 10:00 – 12:00 Uhr

Umsetzungsworkshop zur EU DSGVO
Veranstalter IVD Mitte, 26.07.2018 10:00 – 18:00 Uhr, Bad Vilbel

Übersicht unter https://www.edcud.de/EDdatenschutz-Schulungen

Beratung, Datenschutz-Audit, Mitarbeiter Schulungen, externer DSB:
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 datenschutz@edcud.de Internet www.edcud.de