TERCENUM AG
Datenschutz & Informationssicherheit

Die neue EU-Datenschutz-Grundverordnung - was gilt es jetzt als Verwalter zu beachten?

Sebastian Harrand, Vorstand Tercenum AG, Berlin

Agenda

TERCENUM AG
Datenschutz & Informationssicherheit

1. **Referent / Vorstellung**
2. **Ziel der Präsentation und Zielgruppe**
3. **Aktuelle Situation / Zeitliche Vorgaben**
4. **Änderungen der Anforderungen**
5. **Neue Anforderungen / Vorbereitung**

TERCENUM AG
Datenschutz & Informationssicherheit

Referent / Vorstellung

Referent

TERCENUM AG
Datenschutz & Informationssicherheit

Sebastian Harrand

- Senior Consultant
- Geprüfter Datenschutzauditor
- Geprüfter ISMS-Auditor / 27001
- ISIS 12 Auditor
- Auditleiter der DQS für ISO 27001
- Sicherheitsgutachter der TI der eGK

TERCENUM AG
Datenschutz & Informationssicherheit

Tätigkeiten: Beratung

- Datenschutzmanagement,
- externer Datenschutzbeauftragter,
- Durchführung von Datenschutzaudits;
- Informationssicherheitsmanagement,
- Implementierung
- Auditierung

Unternehmensvorstellung

TERCENUM AG
Datenschutz & Informationssicherheit

Die TERCENUM AG ist Ihr Partner für

- Datenschutz
- Informationssicherheit
- Auditierungen

Bundesweite und internationale Beratung mittelständischer Unternehmen und Konzerne zum Datenschutz- und Informationssicherheitsmanagement.

Kontakt:

www.tercenum.de

Dachverband Deutscher Immobilienverwalter e.V.

Wir sind Kooperationspartner des DDIV

TERCENUM AG
Datenschutz & Informationssicherheit

Ziel / Zielgruppen

Ziel / Zielgruppe

TERCENUM AG
Datenschutz & Informationssicherheit

- **Ziel**
  - Kurzübersicht über wesentliche Änderungen und Neuerungen in Bezug auf die Ablösung der EU-Datenschutz-Richtlinie durch die DSGVO.
  - **Welche Anforderungen kommen durch die neue EU-Datenschutzgrundverordnung auf Immobilienverwaltungen zu?**

- **Zielgruppe**
  - Unternehmensleitung
  - Datenschutzbeauftragte
  - Informationssicherheitsbeauftragte
  - Risikomanager

TERCENUM AG
Datenschutz & Informationssicherheit

Aktuelle Situation / Zeitliche Vorgaben

Aktuelle Situation / Zeitliche Vorgaben

TERCENUM AG
Datenschutz & Informationssicherheit

- Bisher und im Moment gilt das BDSG in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66) zuletzt geändert durch Gesetz vom 25.02.2015 (BGBl. I S. 162) m.W.v. 01.01.2016
- Dieses Gesetz dient der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31).

Aktuelle Situation / Zeitliche Vorgaben

TERCENUM AG
Datenschutz & Informationssicherheit

- Die DSGVO (679/2016) ist am 27. April 2016 veröffentlicht worden und am 20. Tag danach am 25. Mai 2016 in Kraft getreten. Sie löst die Richtlinie 95/46/EG ab.
- Die Umsetzung der erweiterten Regelungsmöglichkeiten (Öffnungsklauseln) erfolgt durch das BDSG-neu bzw. Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)

Aktuelle Situation / Zeitliche Vorgaben

TERCENUM AG
Datenschutz & Informationssicherheit

Übergangsregelungen

- **Übergangsregelung**
  - Zwei Jahre zwischen Inkrafttreten und Anwendung
  - Eingeschränkte Fortgeltung bestehender Grundlagen
- **Inkrafttreten und Anwendung Art. 99**
  - Inkrafttreten am 20. Tag nach ihrer Veröffentlichung im Amtsblatt der EU
- **Eingeschränkte Fortgeltung bestehender Gestaltungen unter DSGVO ErwGr 173**
  - Anpassung binnen 2 Jahren
  - Einwilligung
  - Entscheidungen/Beschlüsse der EU-Kommission

Aktuelle Situation / Zeitliche Vorgaben

TERCENUM AG
Datenschutz & Informationssicherheit

- Die DSGVO (679/2016) ist am 27. April 2016 veröffentlicht worden und am 20. Tag danach am 25. Mai 2016 in Kraft getreten.
- Sie gilt ab dem **25. Mai 2018**.

Die Übergangsfrist von 2 Jahren läuft bald ab!

Änderungen / Anforderungen

Änderungen / Anforderungen

TERCENUM AG
Datenschutz & Informationssicherheit

Vorrang einer EU-Verordnung vor nationalem Recht

- **Richtlinie muss durch Mitgliedsstaaten umgesetzt werden**
  RL 95/46 EG › BDSG
- **Verordnung gilt unmittelbar**
  - Kein weiterer Rechtsakt erforderlich
  - Aber: generelle erweiterte Regelungsmöglichkeiten für öffentlichen Bereich (Art. 6 Abs. 2 DSGVO)
  - ePrivacy-RL 2002/58/EG
  - Keine weiteren Pflichten durch DSGVO hinsichtlich öffentlicher Kommunikation, zu denen aus der RL 2002/58/EG, soweit, diese dasselbe Ziel verfolgen (Art. 95 DSGVO)
- **Erweiterte Regelungsmöglichkeiten**
  - Für bestimmte Anforderungen können Mitgliedsstaaten Ausnahmen und Sonderregelungen treffen

Änderungen / Anforderungen

TERCENUM AG
Datenschutz & Informationssicherheit

Vorrang einer EU-Verordnung vor nationalem Recht

- Aufbau: 11 Kapitel, 173 Erwägungsgründe, 99 Artikel
- Kapitelstruktur

I. Allgemeine Bestimmungen

II. Grundsätze

III. Rechte der betroffenen Person

IV. Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter

V. Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen

VI. Unabhängigkeit der Aufsichtsbehörden

VII. Zusammenarbeit und Kohärenz

VIII. Rechtsbehelfe, Haftung und Sanktionen

IX. Vorschriften für besondere Verarbeitungs-situationen

X. Delegierte Rechtsakte und Durchführungsakte

XI. Schlussbestimmungen

Änderungen / Anforderungen

TERCENUM AG
Datenschutz & Informationssicherheit

Betriebliche/r Datenschutzbeauftragte/r

Europaweite Regelung, Benennungsvoraussetzung

- Die bestehenden Bestellvoraussetzungen aus dem BDSG-alt wurden in das BDSG-neu (Datenschutz-Anpassungs- und Umsetzungsgesetz – DSAnpUG) übernommen

Art. 37 Abs. 4 DSGVO
§ 38 DSAnpUG

Änderungen / Anforderungen

TERCENUM AG
Datenschutz & Informationssicherheit

Grundsätze in Bezug auf Verarbeitung personenbezogener Daten

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Art. 5 Abs. 1 EU-DSGVO

TERCENUM AG
Datenschutz & Informationssicherheit

Neue Anforderungen / Vorbereitung

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

- Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden

Art. 13 und 14 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

(1) 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 ggf. seines Vertreters
- Ggf. die Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung sowie die Rechtsgrundlage für die Verarbeitung
- Das berechtigte Interesse sofern die Verarbeitung auf Art. 6 Abs. 1 lit. f beruht
- Ggf. die Empfänger oder Kategorien von Empfängern
- Ggf. die Absicht einer Übermittlung in ein Drittland (mit fehlendem anerkannten Datenschutzniveau)

Art. 13 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

(2) Zusätzlich zu den Informationen gemäß Absatz1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- Dauer der Speicherung
- Bestehen des Rechts auf Auskunft und Widerspruch
- Widerrufsrecht bei Einwilligungen
- Bestehen des Rechts auf Beschwerde bei einer Aufsichtsbehörde
- Notwendigkeit der Bereitstellung der pbDaten (j/n) und Information über die Folgen bei Nichtbereitstellung
- Ggf. Bestehen einer autom. Entscheidungsfindung

Art. 13 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

Bedeutung für Immobilienverwalter

- Information des Betroffenen bei Begründung und vor (Mieterselbstauskunft) bei Abschluss eines Mietvertrages (abgestuftes Verfahren berücksichtigen)
- Information des Betroffenen vor der Nutzung digitaler Medien (Website etc.)
- Gilt auch gegenüber Mitarbeitern (vor Begründung eines Arbeitsrechtsverhältnisses sowie vor Änderung von Verarbeitungstätigkeiten)
- Im Rahmen einer Videoüberwachung sind die Informationspflichten ebenfalls zu beachten

Art. 13 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

(1) Werden personenbezogene Daten **nicht** bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Folgendes mit:

- Namen und die Kontaktdaten des verantwortlichen sowie ggf. seines Vertreters
- Ggf. die Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung sowie die Rechtsgrundlage für die Verarbeitung
- Kategorien personenbezogener Daten
- Ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
- Ggf. die Absicht einer Übermittlung in ein Drittland (mit fehlendem anerkannten Datenschutzniveau)

Art. 14 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

(2) Zusätzlich zu den Informationen gemäß Absatz1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person eine faire und transparente Verarbeitung zu gewährleisten:

- Dauer der Speicherung
- Wenn Verarbeitung auf Artikel 6 Abs. 1 lit. f beruht, die berechtigten Interessen
- Bestehen des Rechts auf Auskunft und Widerspruch
- Widerrufsrecht bei Einwilligungen
- Bestehen des Rechts auf Beschwerde bei einer Aufsichtsbehörde
- **Quelle der pbDaten**
- Ggf. Bestehen einer autom. Entscheidungsfindung

Art. 14 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Transparenz gegenüber dem Betroffenen

Bedeutung für Immobilienverwalter

- Information des Betroffenen bei Übernahme von Beständen

Art. 14 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) *„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…“*

Art. 25 Abs. 1 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(2) *„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. Diese Verpflichtung **gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Sperrfrist und ihre Zugänglichkeit.** Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl natürlicher Personen zugänglich gemacht werden…“*

Art. 25 Abs. 2 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bedeutung für Immobilienverwalter

- Der **Verantwortliche ist** der Betreiber des Systems (**Verwalter**) nicht der Entwickler!
- Ggf. Anpassung von digitalen Anwendungen (Software, Applikationen..) und Datenbanksystemen, z.B. elektronische Mieterakte
- Berücksichtigung der Anforderungen bei Neuanschaffungen von digitalen Anwendungen

Art. 25 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Auftragsverarbeiter

*(1) „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die **hinreichend Garantien** dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“*

*(3) “Die Verarbeitung durch einen Auftragsverarbeiter erfolgt **auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments** nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.“*

Art. 28 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Verzeichnis von Verarbeitungstätigkeiten

*„(1) **Jeder** Verantwortliche und ggf. sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.*

…

*(5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von Ihnen vorgenommene Verarbeitung nicht ein **Risiko für die Rechte und Freiheiten** der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die **Verarbeitung besonderer Datenkategorien** gemäß Artikel 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.“*

Art. 30 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Verzeichnis von Verarbeitungstätigkeiten

Bedeutung für Immobilienverwalter

- Aufgrund der regelmäßigen Verarbeitung personenbezogener Daten (Informationen über wirtschaftliche Verhältnisse, Abrechnungsdaten – Finanzdaten, Sozialdaten bei Leistungsempfängern) ist davon auszugehen, dass die Verarbeitungstätigkeiten zu dokumentieren sind.

Art. 30 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Sicherheit der Verarbeitung

*„(1) 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 der natürlichen Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignet technische und organisatorische Maßnahmen, um ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten…“*

Art. 32 Abs. 1 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Sicherheit der Verarbeitung

*„(1) 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 der natürlichen Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignet technische und organisatorische Maßnahmen, um ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten…“*

„…d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“ = Betrieb eines Managementsystems

Art. 32 Abs. 1 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Sicherheit der Verarbeitung

Bedeutung für Immobilienverwalter

- Einführung eines Datenschutz-Managementsystems
- Technische und organisatorische Maßnahmen sind zu definieren und **regelmäßig zu überprüfen.**
- Dokumentation der Prüfungen

Art. 32 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Meldung von Verletzungen des Schutzes pbDaten an die Aufsichtsbehörde

(3) "Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

- *eine **Beschreibung der Art der Verletzung** des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;*
- *den **Namen und die Kontaktdaten des Datenschutzbeauftragten** oder einer sonstigen Anlaufstelle für weitere Informationen;*
- *eine **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten;*
- *eine **Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls **Maßnahmen zur Abmilderung** ihrer möglichen nachteiligen Auswirkungen."*

Art. 33 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Benachrichtigung der von einer Verletzung des Schutzes pbDaten betroffenen Person

(1) *"Hat die Verletzung des Schutzes personenbezogener Daten **voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen** zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung."*

Art. 34 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Datenschutz-Folgenabschätzung

*„(1) 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…“*

Art. 35 Abs. 1 DSGVO

Neue Anforderungen / Vorbereitung

TERCENUM AG
Datenschutz & Informationssicherheit

Datenschutz-Folgenabschätzung

Bedeutung für Immobilienverwalter

- Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde ein.
- Die Aufsichtsbehörden werden eine Liste der Verarbeitungsvorgänge erstellen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist.

Art. 35 DSGVO

Zusammenfassung

Zusammenfassung

TERCENUM AG
Datenschutz & Informationssicherheit

- Die Übergangsfrist läuft bereits
- Bestellverpflichtung bzgl. des Datenschutzbeauftragten erfüllt?
- Ggf. Meldung der Kontaktdaten des Datenschutzbeauftragten bis 25. Mai 2018
- Transparenz gegenüber dem Betroffenen – Informationspflichten
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Anpassung der Regelungen zur Auftragsverarbeitung
- Verzeichnis von Verarbeitungstätigkeiten
- Datenschutz-Folgenabschätzung
- Sicherheit der Verarbeitung
- Löschkonzept
- Beweislastumkehr
- Dokumentation der Aktivitäten zum Datenschutz

TERCENUM AG
Datenschutz & Informationssicherheit

Danke für Ihre Aufmerksamkeit

TERCENUM AG

Unter den Linden 16, 10117 Berlin, www.tercenum.de