ICG

Institut für Corporate Governance
in der deutschen Immobilienwirtschaft

Risikoübersicht DATENSCHUTZ und IT-SICHERHEIT

VORWORT

In einer digitalisierten Welt sind der Schutz und das Managen von elektronischen Daten von essentieller Bedeutung. Informationen sind der Schlüssel, um kundenspezifische Produkte anbieten und Markttrends antizipieren zu können. Um diese Informationen in einer Organisation nutzbar zu machen, müssen sie in Daten transformiert und durch spezielle Anwenderprogramme ausgewertet, transferiert und gespeichert werden. Dabei handelt es sich sowohl um Informationen mit Personenbezug als auch um spezifisches Wissen über den Markt. Es ist keine Übertreibung zu sagen, dass diese Informationen und die Möglichkeit sie zu verwenden, zu den wertvollsten Assets eines Unternehmens gehören. Diese Ressource ist durch die Digitalisierung unserer Geschäftswelt zunehmend gefährdet. Geraten sie in die falschen Hände, werden sie zu einer kaum einschätzbaren Bedrohung. Sind sie teilweise oder gänzlich nicht mehr verfügbar, kommt es zu einem „stand still" in der Organisation mit weitreichenden Folgen für das betroffene Unternehmen.

Die Regeln zum Umgang mit personenbezogenen Daten hat die EU mit der Datenschutz-Grundverordnung nun unionsweit vereinheitlicht und aktualisiert. Um ihrem Anliegen Nachdruck zu verleihen, wurde die DSGVO* mit einem drastischen Bußgeldrahmen ausgestattet, wie er vergleichbar bisher nur aus dem Kartellrecht bekannt war. Verstöße können mit einem Bußgeld in Höhe von bis zu 4% des globalen Jahresumsatzes bestraft werden. Nie zuvor spielte Datenschutz eine vergleichbar essentielle Rolle in den Risikoanalysen der Compliance-Profis.

Insgesamt ist es an der Zeit, dass auch die deutsche Immobilienwirtschaft den hohen Stellenwert dieser Themen erkennt und sich eingehend hiermit beschäftigt.

In der vorliegenden Risikoübersicht haben erfahrene Compliance-Verantwortliche aus den verschiedenen Marktsegmenten ihre Erfahrungen zusammengetragen, um der gesamten Immobilienbranche eine Hilfestellung bei der wichtigen Aufgabe der Datenschutz-Compliance anzubieten.

Dr. Ingo Seidner, JLL *Karin Barthelmes-Wehr, ICG*

* *Erläuterung der Fachbegriffe: siehe Glossar am Ende der Übersicht.*

Datenschutz BESTAND

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Bestandhalter	1	Verwendung eines betriebswirtschaftlichen Systems der Informationstechnik für die gesamte Verwaltung des Unternehmens – ERP – mit den Inhalten Kapital, Personal, Betriebsmittel, Informations- und Kommunikationstechnik	• Beschäftigte • Lieferanten • Kunden	• Offenlegung und Verlust von personenbezogenen Daten oder Geschäftsgeheimnissen • Verkettung • Datensammlung	■ **Berechtigungs- und Löschkonzept**
Bestandhalter	2	Bewertung im Bestand	Nutzer	Unbefugter Zugriff auf kritische Daten, z. B. zum Insolvenz- oder Mietausfallrisiko bei der **Due-Diligence**-Prüfung	■ **Pseudonymisierung** ■ **Anonymisierung** ■ **Kumulierung**
Bestandhalter	3	Speziell: Geltendmachung von Betroffenenrechten nach der EU-DSGVO	alle Berechtigten	Fristversäumnis	■ **Effiziente Geschäftsprozesse** ■ **Sicherstellung notwendiger Personalkapazitäten**

Datenschutz WOHNEN

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Wohnen	1	Vermietung über Internetportal (z. B. ImmoScout24)	• Interessenten • Mitarbeiter	Identitäts-Diebstahl durch **Passwort-Hack**	■ **Zweifaktor-Authentifizierung (z. B. Smartcard mit Pin)**
Wohnen	2	online Inserat/ bewohnte Wohnung	• Mitarbeiter • Mieter	Personenbezogene Daten im Bereich des Inserates: Bilder, Rufnummern etc.	■ **schriftliche Einwilligung zu Beweiszwecken (Art. 5 Abs. 1a, Art. 7 DSGVO)/Selbstauskunft des Betroffenen** ■ **Automatisierte Löschung (Art. 17 DSGVO) nach zwei Jahren**
Wohnen	3	Weitergabe von Adressdaten und Telefonnummern im Rahmen von Besichtigungsterminen	• Mieter	Personenbezogene Daten im Bereich des Inserates: Bilder, Rufnummern etc.	■ **schriftliche Einwilligung zu Beweiszwecken (Art. 5 Abs. 1a, Art. 7 DSGVO)/Selbstauskunft des Betroffenen** ■ **Automatisierte Löschung (Art. 17 DSGVO) nach zwei Jahren**
Wohnen	4	Mieterinteressentenbogen	• Interessenten	• Erhebung von personenbezogenen Daten gem. Art. 5 DSGVO • Beachtung des Grundsatzes der „Datenminimierung“ (Art. 5 Abs. 1c DSGVO)	■ **Muster-Interessentenbogen (keine Abfrage von Familienstand oder Religionszugehörigkeit)** ■ **keine Kopie des Personalausweises**
Wohnen	5	Bonitätsprüfung	• Interessenten	Der Vermieter muss ggf. beweisen, dass er zur Weitergabe von Daten anlässlich einer Bonitätsprüfung berechtigt war (Art. 7 DSGVO). Nach Erhalt der Bonitätsentscheidung darf kein Automatismus stattfinden, wonach eine Vermietung bei einer bestimmten Bonität automatisch abgelehnt wird. Trotz eventueller negativer Bonitätsauskunft muss danach eine Einzelfallentscheidung gefällt werden (Art. 22 DSGVO)	■ **schriftliche Einwilligung des Mietinteressenten zu Beweiszwecken** ■ **Einzelfallentscheidung nach Erhalt der Bonitätsdaten**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Wohnen	6	Weitergabe von Daten an Bonitätsauskunfteien/ Kautionsversicherer	• Interessenten • Mieter	wegen Art. 7 DSGVO nur mit schriftlicher Einwilligung (s.o.)	■ **schriftliche Einwilligung des Mietinteressenten zu Beweiszwecken** ■ **Einzelfallentscheidung nach Erhalt der Bonitätsdaten**
Wohnen	7	Weitergabe von Daten an Versorger (Strom/Gas)	• Mieter	Weitergabe von personenbezogenen Daten	■ **Datenweitergabe nur mit Einwilligung des Mietinteressenten (Art. 5 Abs. 1a DSGVO)**
Wohnen	8	Erhebung/Speicherung/ Löschung personenbezogener Daten bei Mietvertragsschluss	• Mieter	• Rechtsgrundlage für die Erhebung/ggf. Übermittlung (Art. 5 Abs. 1a DSGVO) • Pflicht zur Information des Betroffenen (Auskunftsrecht gem. Art. 15 DSVGO) • Löschpflicht (Recht auf Löschung, Art. 17 DSVGO)	■ **Einwilligung zur Datenerhebung** ■ **bei Anfrage Auskunft über die gespeicherten Daten** ■ **Löschung der Daten nach Mietvertragsende**
Wohnen	9	Werbung/Opt-in/Mieterkommunikation per Mail, App, Internet, Telefon	• Mieter	• Sichere Datentransfers in Mieterapp/Internet • Mailkommunikation/Telefon: Gewähr des richtigen Empfängers (Gewährleistung der Datensicherheit-Grundsatz der „Integrität und Vertraulichkeit“ gem. Art. 5 Abs. 1f DSGVO)	■ **Opt-In des Betroffenen bereits bei Vertragsschluss einholen** ■ **Sicherheitsabfrage bei telefonischer Kommunikation** ■ **Passwortschutz bei App/ Internet und gesicherte/ verschlüsselte Verbindung**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Wohnen	10	Weitergabe personenbezogener Daten bei: BK/Handwerker/Messdienstleister. Auftragsdatenverarbeitung	• Mieter	• Einwilligung des Betroffenen (Art. 5 Abs.1a DSGVO) • Datenspeicherung nur solange, wie es erforderlich ist; bei Wegfall der Erforderlichkeit sofortige Löschung (Art. 5 Abs. 1e DSGVO i.V.m. Art. 17 DSGVO)	■ **Einholung der Einwilligung des Betroffenen bei Schadenmeldung (Handwerker), sonst bei MV-Beginn**
Wohnen	11	Behördenkommunikation Weitergabe von Daten an Polizei, Jobcenter, Ordnungsbehörden, sonstige Leistungsträger	• Mieter	Auskunfterteilung und insbesondere Weitergabe personenbezogener Daten an die Behörde ohne ausreichende rechtliche Grundlage (Weitergabe an öffentl. Stellen in Ordnung, wenn eine rechtliche Verpflichtung (z. B. aus dem SGB) besteht (Art. 6 Abs. 1c DSGVO).	■ **Prüfung der rechtlichen Grundlage ggfs. Weigerung mit der Folge entsprechender Vorladung oder Beschlagnahme zur Herbeiführung der erforderlichen Rechtsgrundlage**
Wohnen	12	Datenverlust/ordnungsgemässe Datenerhebung und -verarbeitung	• Interessenten • Mitarbeiter	• Informationspflichten ggü. Betroffenen bei Datenverlust § 82 DSGVO • Auskunftspflichten ggü. Betroffenen zu Art und Weise der Datenerhebung/-verarbeitung § 13,14, 15 DSGVO	■ **Information des Mieters bei Datenverlust** ■ **Auskunft über die gespeicherten Daten auf Nachfrage des Mieters**

Datenschutz GEWERBE

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Gewerbe	1	z. B. Bonitätsprüfung von potenziellen Vertragspartnern	• Interessenten • Kunden • Lieferanten/ Dienstleister	• Rechtsgrundlage für die Erhebung/ggf. Übermittlung • Pflicht zur Information des Betroffenen • Löschpflicht	■ **Einwilligung/Selbstauskunft des Betroffenen** ■ **Automatisierte Löschung nach zwei Jahren**
Gewerbe	2	Erfassung nicht relevanter Personenmerkmale über „Entscheider“ auf Kundenseite und Speicherung in der Kundendatenbank. **Beispiel:** *Herr Müller, verantwortlich für den Bereich Real Estate, sagte im Telefonat, dass er aufgrund der schweren Krebserkrankung seiner Ehefrau die Verantwortung an die Kollegin Schmidt übergeben hat.*	Ansprechpartner auf Kundenseite	• Keine Rechtsgrundlage für die Erhebung/Speicherung • Teilweise sensible Daten • Mangel an Sensibilität bei Mitarbeitern	■ **Datenbanken müssen regelmäßig bereinigt werden** ■ **Mitarbeiter müssen sensibilisiert werden**
Gewerbe	3	Erlangung von Informationen über sog. Tippgeber	• Investoren • Eigentümer • Vermieter	• Zum Teil Erlangung von personenbezogenen Daten über potenzielle Geschäftspartner von Tippgebern • Rechtsgrundlage zu Erhebung zweifelhaft • Informationspflicht nach DSGVO	■ **zu erarbeiten**
Gewerbe	4	Versendung eines Mailings	Potentielle Kunden	• Versendung Mailing ohne vorherige Zustimmung Kunde • Generierung der E-Mail-Adresse ggf. ohne Zustimmung Adressat	■ **Double-opt-In Verfahren nutzen**

Datenschutz SHOPPING

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Shopping	1	Logging und Tracking (Speicherung und Nachverfolgung von Anmeldedaten)	Lieferanten/ Dienstleister	• Erhobene Daten müssen zumindest nach adäquater Zeit nach Erhebung anonymisiert werden • Die Aufbewahrungsfristen müssen eingehalten werden	■ **Automatische Anonymisierung bei der Erfassung** ■ **Langzeit-Archivierung nur vor gesetzlicher Klärung**
Shopping	2	Double-opt-In (z. B. App mit Inhousenavigation)	Lieferanten/ Dienstleister	• Bewegungsprofile müssen sensibel behandelt werden, dürfen nicht zentral gespeichert werden • Die Daten dürfen nur zweckgebunden verarbeitet werden	■ **Lokale Speicherung der Geodaten** ■ **Auflösung der Geopositionierung möglichst ungenau auch für allgemein zugestimmte Zwecke**
Shopping	3	Nutzung der Beacon-Technologie	Vor allem Kunden (aber natürlich auch alle sonstigen Personen im räumlichen Anwendungsbereich)	Der Beacon versendet von sich aus nur eine Kennung, und dies erst einmal ohne Personenbezug. Daher scheidet § 3a BDSG insoweit aus. Das Gegenstück dazu ist die App, die man sich selbst installieren muss. Diese wertet die Kennung des Beacons aus und stellt über die App einen Bezug zum Angebot, zur Werbung oder zum Anwender her. Hier kann über Benutzerkonten und Endgerät ein Personenbezug hergestellt werden. Daher ist darauf zu achten, dass der Anwender bei der Installation/Einrichtung der App explizit seine Einwilligung zu der Erhebung, Verarbeitung und ggf. auch Speicherung gibt. Das kann in den Nutzungsbedingungen der App geschehen, muss dann aber als Datenschutzhinweis kenntlich gemacht sein. Die rechtlichen Anforderungen ergeben sich hierbei aus dem Telemediengesetz und dem BDSG.	■ **Die Einwilligung ist als Nachweis zu protokollieren**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Shopping	4	Videoüberwachung	• Kunden • Mitarbeiter • Lieferanten/ Dienstleister	§ 6b („Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“)	**Nach derzeitigen Recht ist der Einsatz der Videoüberwachung wohl zumindest in folgenden Bereichen statthaft: Fluchtwege, Kassenautomaten, Kassenbereiche, Anlieferungszonen, Parkbereiche, öffentlich nicht zugängliche Räume (etwa Heizung, EDV, Lager)** ■ **Vor der Einführung der Videoüberwachung Vorabkontrolle durch den zuständigen Datenschutzbeauftragten** *Ferner:* ■ **Videoüberwachung deutlich sichtbar machen (Schilder mit Piktogramm)** ■ **Überwachungsräume und -systeme vor unbefugtem Zutritt und Zugriff schützen** ■ **Aufgezeichneten Daten spätestens automatisch nach 72 Stunden löschen**
Shopping	5	Frequenztechnologie	Vor allem Kunden (aber natürlich auch alle sonstigen Personen im räumlichen Anwendungsbereich)	Solange reine „Kopfzählung“ erfolgt, stellen sich keine Probleme gemäß BDSG	**./.**

Datenschutz ASSET/FONDS

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Asset/Fonds	1	Umgang mit personenbezogenen Daten	• Anwender (intern/ extern) • Mieter • Kreditoren	Sicherstellung der Schutzbedarfe personenbezogener Daten	■ **Vorhalten von personenbezogenen Daten ausschließlich auf Produktivumgebungen mit dezidiertem Berechtigungs- und Archivierungskonzept**

■ **Anonymisierung aller personenbezogenen Daten auf Test-/Abnahmeumgebungen**
■ **Keine personenbezogenen Daten auf Entwicklungsumgebungen**
■ **<u>Grundsätzlich:</u> Trennung Ebene Kapitalverwaltungsgesellschaft und Immobiliensondervermögen**

Datenschutz ALLGEMEIN

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Allgemein	1	• Weitergabe von Zugangsdaten/Passwörtern durch Mitarbeiter an Vertretung bei Abwesenheit • Email Weiterleitung bei Abwesenheit	• Mitarbeiter • Externe Emailabsender	Möglicherweise Verletzung des Fernmeldegeheimnisses	■ **Klare Passwortregelung** ■ **Verbot der Weitergabe von Passwörtern** ■ **Abwesenheitsnotiz – keine Weiterleitung**
Allgemein	2	Human Resources	• Mitarbeiter • Bewerber	• Rechtsgrundlage für die Erhebung von Bewerberdaten • Active Sourcing • Löschfristen beim Austritt • Entsorgung von Dokumenten in der HR Abteilung • Internet & Emailnutzung • Datenübertragung an Konzern- und Drittunternehmen (bspw. Datev) • Leistungs- und Verhaltenskontrolle	**./.**

Datenschutz ALLGEMEIN

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Kategorien betroffener Personen	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Allgemein	3	Recht auf Vergessen-werden	• Kunden • Kontaktper-sonen • Ex-Mitarbeiter	Unmöglichkeit der Lö-schung aufgrund diverser Speicherorte und Backups	■ **Datenmanagementsystem mit automatischer Löschung nach Fristablauf**
Allgemein	4	Auskunftsrechte	Personen, die persönliche Daten zur Verfügung gestellt haben, wie z. B. • Kunden • Ex-Mitarbeiter • abgelehnte Bewerber	• Betroffene können Aus-kunft verlangen • Bei unrechtmäßiger Verarbeitung Schadens-ersatzanspruch	■ **Datenmanagementsystem**
Allgemein	5	Informationspflicht	• Potenzielle Ansprechpart-ner auf Kun-denseite • Potenzielle Kandidaten für zu besetzende Stellen	Betroffene müssen in erheblichem Umfang infor-miert werden, wenn ihre Daten erhoben werden (Zweck, Dauer der Spei-cherung, Rechtsgrundlage usw.)	■ **Standardprozesse**
Allgemein	6	Recht auf Datenüber-tragbarkeit	Vertragspartner, die im Rahmen von Geschäfts-zwecken Daten zur Verfügung stellen	Unmöglichkeit der Er-füllung aufgrund unter-schiedlicher Speicherorte, Datenformate etc. Betroffene können ver-langen, alle von ihnen zur Verfügung gestellten Daten in einem struktu-rierten, gängigen und maschinenlesbaren For-mat zu erhalten.	■ **Standardisiertes Datenma-nagement, klare Verfahrens-übersicht**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Allgemein	1	Buchhaltung, Jahres-abschlussprüfung	• Datenverlust • Datenveränderung bei vollständigem Zugriff in das Produktivsystem	■ **Vollständiger „Datenabzug“ für WP zur Bearbeitung im abgeschlossenen System**
Allgemein	2	Bewirtschaftung von Liegenschaften	Beeinträchtigung von Integrität, Verfügbarkeit, Verbindlichkeit und Zurechenbarkeit der Kommunikation	■ **Krypto-Konzept, als Anwendungen z. B. digitale Signatur, De-Mail**
Allgemein	3	Steuerverfahren: Grundsteuer, Grunderwerbsteuer, Umsatzsteuer, Kfz-Steuer	• Datenverlust • Datenveränderung	■ **Verkehr mit Finanzamt nur durch Steuerberater**
Allgemein	4	Beziehungen zu Verwaltungen (Genehmigungen), z. B.: Baugenehmigung, Sondernutzungserlaubnis, Wasserrechtliche Erlaubnisse	Automatisierter Abruf ohne Beschränkung	■ **Einschränkung der Berechtigung durch organisatorische Maßnahmen**
Allgemein	5	Besondere Bedürfnisse der öffentlichen Hand durch Geheimschutz	Missbrauch von Sicherheitslücken	■ **Sicherheitsüberprüfung (SÜG)** ■ **sichere Netze** ■ **VPN** ■ **Ende-zu-Ende-Verschlüsselung** ■ **digitale Signatur**
Allgemein	6	Finanz-Transaktionen (z. B. bei Immobilienankäufen)	Betrugsversuch durch Phishing und Social Engineering	■ **Mitarbeiter-Sensibilisierung** ■ **Markierung externer Mails**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Allgemein	7	Abschluss Rahmenvertrag mit IT-Dienstleistern inklusive Prüfberechtigung vorab und laufender Betrieb	Wird die Prüfberechtigung seitens des Auftragsgebers nicht vertraglich abgesichert, kann der Dienstleister die Prüfung verweigern	■ **Anstatt einer eigenen Prüfung kann auch die jährliche Vorlage eines Testats gemäß ISO 27001 oder vergleichbar ausreichend sein**
Allgemein	8	Anforderungen an die physikalische Sicherheit müssen dokumentiert werden	Verfügbarkeit und Integrität und Belastbarkeit müssen nachgewiesen werden. Insbesondere für webbasierte Applikationen	■ **Prüfung nach BSI Grundschutz katalog, Pentest gemäß OWASP TOP 10 bei Cloud-Services**
Allgemein	9	Anforderungen an die logische Sicherheit	Anforderung an die Vertraulichkeit müssen nachgewiesen werden (z. B. Verschlüsselung sensibler Daten)	■ **Rechte-/Rollenkonzept gemäß dem Prinzip „Nur so viele Rechte wie nötig“** ■ **Verschlüsselung von sensiblen Benutzerdaten bei der Speicherung und der Datenübertragung**
Allgemein	10	Abbildung von portfolioübergreifenden Immobilienstamm- und -bewegungsdaten sowie Buchungsbelegen	Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten	■ **Einsatz eines zentralen ERP-Systems mit dezidiertem Berechtigungssystem und Zugriffsmöglichkeiten von externen Dienstleistern**
Allgemein	11	Bereitstellung relevanter Dokumente im Bestand/für Transaktionen	Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Dokumente	■ **Nutzung von (virtuellen) Datenräumen zur Bereitstellung relevanter Dokumente der Objekte/Liegenschaften** ■ **Einheitliche, portfolioübergreifende Ablagestruktur** ■ **Dezidiertes Berechtigungskonzept mit Zugriffsmöglichkeiten von intern/extern**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Allgemein	12	Dokumentenmanagement	Beurteilung der Vertraulichkeit	■ **Deklaration der Vertraulichkeitsstufe bei allen internen Dokumenten**
Allgemein	13	Immobilienbewertung	Sicherstellung der organisatorischen Unabhängigkeit der Sachverständigen im Bewertungsprozess	■ **Informationssystem zur Integration der externen Sachverständigen** ■ **Systemgestützte Signierung von Gutachten** ■ **Organisatorische Trennung der Sachverständigen durch cloudbasierte Komponente (Voraussetzung: Systembetreiber in Deutschland)**
Allgemein	14	Entscheidungen in kritischen Geschäftsprozessen	Sicherstellung der Nachvollziehbarkeit von kritischen Entscheidungen und Integrität des Ergebnisses	■ **Etablierung des 4-Augen-Prinzips bzw. kompetenzgerechte Freigaben in kritischen Geschäftsprozessen**
Allgemein	15	Management von Systemberechtigung	Transparenz über Systemberechtigungen	■ **Definition von fachlichen Rollen und deren Zugriffsberechtigungen über die gesamte Systemlandschaft** ■ **Zentrales Repository zur Abbildung der Anwender und deren fachliche Rollen bezogen auf alle (kritischen) Systeme** ■ **Internes Kontrollsystem**
Allgemein	16	Umgang mit individueller Datenverarbeitung (IDV, bspw. Excel o.ä.)	Sicherstellung der Ordnungsmäßigkeit sowie eines geregelten IT Software-Entwicklungs- und -betriebsprozesses von IDV bei Rechnungslegungs-, Aufsichtsrechts- oder Steuerungsrelevanz	■ **Inventarisierung und Klassifizierung der eingesetzten IDV** ■ **Schutzbedarfsfestlegung der IDV mit Rechnungslegungs- und Steuerungsrelevanz bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit** ■ **Ableitung von Maßnahmen zur Sicherstellung der Schutzbedarfe**

Marktsegment	Nr.	Bezeichnung Prozess/ Anwendung/Tätigkeit	Risiken/Anforderungen Datenschutz/IT-Sicherheit	Best Practice
Allgemein	17	IT-Governance	Sicherstellung der Nachvollziehbarkeit aller Systemanpassungen	■ **Vollständige, prozessbegleitende Dokumentation aller Systementwicklungstätigkeiten, fachliche Abnahme(-tests) sowie Inbetriebnahmen**
Allgemein	18	Auswahl von Systembetreibern	Sicherstellung aller aufsichtsrechtlicher Anforderungen	■ **Richtlinien für Outsourcingpartner** ■ **Pre-Audit und regelmäßige Audits nach Vergabe aller beteiligten Geschäftspartner in Bezug auf Datenschutz und Informationssicherheit**

GLOSSAR

Anonymisierung	Das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können
Authentizität	Gewissheit über die Herkunft der Daten
BDSG	Bundesdatenschutzgesetz
Beacon-Technologie	Positionsbestimmung in geschlossenen Räumen mittels Smartphone-App und kleinen, im Raum platzierten Sendern, sog. Beacons
BK	Betriebskosten, die im konkreten Zusammenhang für die Weitergabe personenbezogener Daten an im wesentlichen Abrechnungsdienstleister stehen.
BSI Grundschutzkatalog	Sammlung von Empfehlungen zur IT Sicherheit des Bundesministeriums für Sicherheit in der Informationstechnologie (BSI)
cloudbasiert	s. Cloud-Services
Cloud-Services	Bereitstellung informationstechnischer Ressourcen über das Internet (bspw. Online-Speicherplatz)
Datenräume	Geschützte virtuelle Räume zur Bereitstellung von Unterlagen für die Due-Diligence-Prüfung im Rahmen von An- oder Verkaufsverhandlungen
DATEV	Software zur Buchführung, Gehaltsabrechnung u.ä.
De-Mail	Sicheres Online-Kommunikationsmittel ähnlich E-Mail
Double-opt-In (s. auch Opt-In)	Verfahren zur Erteilung von Einwilligungen, bei dem der Nutzer wie beim Opt-In ausdrücklich zustimmen muss (gewöhnlich per E-Mail Link)
DSGVO	Datenschutzgrundverordnung – gilt EU-weit ab Mai 2018
Due-Diligence	Sorgfältigkeitsprüfung des Kaufobjekts im Rahmen von An- oder Verkaufsverhandlungen
EDV	Elektronische Datenverarbeitung
Erhebung	Das Beschaffen bzw. die Kenntniserlangung von personenbezogenen Daten über den Betroffenen
ERP	Enterprise Ressource Planning

GLOSSAR

ERP-System	Softwarelösung zur Ressourcenplanung eines Unternehmens
Fernmeldegeheimnis	Strafrechtliches Verbot des unbefugten Abhörens, Unterdrückens, Verwertens oder Entstellens, von Fernmelde- (Fernschreib-, Fernsprech-, Funk- und Telegrafen-) Botschaften
Frequenztechnologie	Aufzeichnung und Analyse von Daten über Besucherströme in Shopping Centern
Geodaten	Standortkoordinaten
Geopositionierung	Bestimmung des Standorts
HR	Human Resources = Personalabteilung
IDV	Individuelle Datenverarbeitung – durch Fachabteilung selbst programmierte Anwendungen
Integrität	Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen
ISO 27001	ISO Standard zu Informationssicherheit
IT	Information Technology – Informationstechnik
IT-Governance	Führung, Organisationsstrukturen und Prozesse, die sicherstellen, dass die Informationstechnik (IT) die Unternehmensstrategie und -ziele unterstützt
Kryptokonzept	Konzept zum Einsatz von Verschlüsselungsverfahren
logische Sicherheit	Im Gegensatz zur physischen Sicherheit betrifft die logische Sicherheit die Maßnahmen, welche organisatorischer Natur sind
Löschung	In diesem Zusammenhang ist Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten, also jede Handlung die bewirkt, dass die Information endgültig nicht mehr aus den Daten gewonnen werden kann
MV	Mietvertrag
Opt-In (s. auch Double-opt-In)	Verfahren zur Erteilung von Einwilligungen, bei dem der Nutzer ausdrücklich zustimmen muss
OWASP TOP 10	Liste der 10 wichtigsten Sicherheitsrisiken für Webapplikationen

GLOSSAR

Pentest	= Penetrationstest – umfassender Sicherheitstest zur Aufdeckung von Sicherheitslücken und Schwachstellen in informationtechnischen Systemen
Phishing	Identitätsdiebstahl mithilfe gefälschter Webseiten und E-Mails
Smartcard mit Pin	Individuelle Chipkarte zur Identifikation, welche nur genutzt werden kann, wenn die PIN (persönliche Identifikationsnummer) bekannt ist
Social Engineering	Manipulation von Personen mit dem Ziel, diese zu einem bestimmten Verhalten zu bewegen, häufig um einen Betrug zur ermöglichen
SÜG	Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867), das zuletzt durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732) geändert worden ist
Telemediengesetz	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBl. I S. 1766) geändert worden ist
VPN	Virtual Private Network – in sich geschlossenes Computernetzwerk in welchem die Teilnehmer über das Internet verschlüsselt kommunizieren können
WP	Wirtschaftsprüfer
Zweifaktor-Authentifizierung	Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten

ANMERKUNG

Diese Compliance-Risikoübersicht beschreibt aus der Sicht des Arbeitskreises „Compliance“ problematische Situationen und Verhaltensweisen, die einen Compliance-Verstoß im Bereich Datenschutz und IT-Sicherheit nahelegen, jedoch ohne dabei den besonderen Umständen des Einzelfalls stets gerecht werden zu können.
Sie stellt daher keine abschließende Würdigung des beschriebenen Vorgangs dar und weder die Mitglieder des Arbeitskreises „Compliance“ noch das Institut für Corporate Governance in der deutschen Immobilienwirtschaft e.V. übernehmen irgendeine Haftung für die Richtigkeit und Vollständigkeit der in der Risikoübersicht vorgeschlagenen Beurteilungen der dort behandelten Situationen und Verhaltensweisen.

FACHLICHE LEITUNG
Dr. Ingo Seidner, Jones Lang LaSalle SE

ORGANISATORISCHE LEITUNG
Karin Barthelmes-Wehr, ICG

MITGLIEDER
Dr. Wulff Aengevelt, Aengevelt Immobilien GmbH & Co. KG
Jochen Bär, Union Asset Management Holding AG
Katja Dobberow, KPMG
Susanne Eickermann-Riepe, PwC PricewaterhouseCoopers GmbH
Henry Hillmann, Bundesanstalt für Immobilienaufgaben
Kevin Justen, Savills Immobilien Beratungs-GmbH
Rolf Kollmannsperger, Union Investment Real Estate GmbH
Carsten Labinski, Apleona GmbH
Anne Lindner, CBRE
Dr. Hans-Udo Richarz, ECE Projektmanagement G.mb.H. & Co. KG
Andreas Scheer, STADT UND LAND Wohnbauten-Gesellschaft mbH
Hans Richard Schmitz, Hamborner REIT AG
Karsten Schweigkofler, Colliers International Deutschland GmbH
Malte Tober, Jones Lang LaSalle SE
Alexander Tobiason, CBRE GmbH
Christian Valenthon, Savills Immobilien Beratungs-GmbH
Holger Weiß, Vonovia SE
Mathias Wendt
Dr. Volker Wiegel, LEG Immobilien AG
Ralf Zieren, Deutsche Annington Immobilien GmbH

ICG

Institut für Corporate Governance
in der deutschen Immobilienwirtschaft

Wir stehen für werteorientierte Unternehmensführung

■■■■■

Professionalität
Transparenz
Integrität
Nachhaltigkeit

■■■■■

Institut für Corporate Governance in der deutschen Immobilienwirtschaft e.V.
Unter den Linden 42 • 10117 Berlin
Phone: +49 (0)30 202 1585 55 • Fax: +49 (0)30 202 1585 29
E-Mail: info@icg-institut.de
www.icg-institut.de

Druck/Stand: März 2018

ICG in Kooperation mit ZIA Die Immobilienwirtschaft