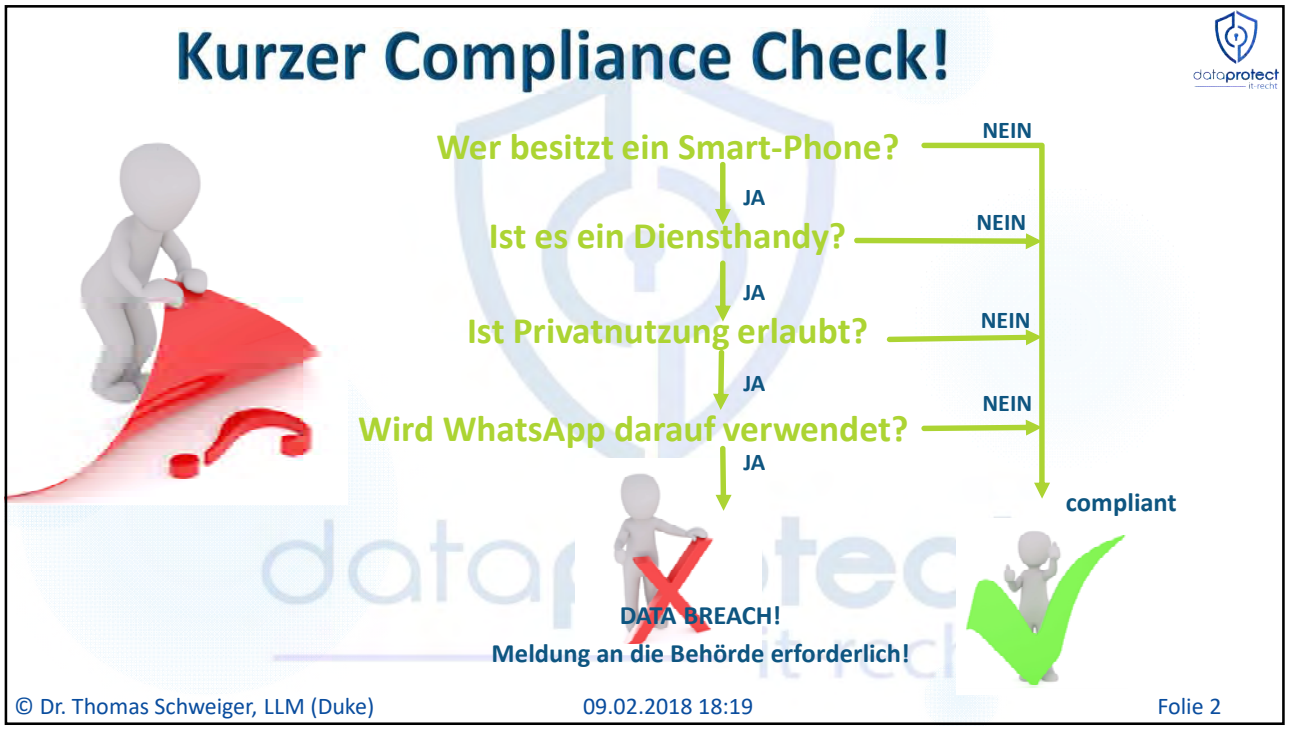

Dr. Thomas Schweiger, LL.M., CIPP/E
Graz, 16.02.2018
weniger als 100 Tage
bis zum 25.05.2018
Datenschutz-Grundverordnung (DSGVO) und Immobilienunternehmen
dataprotect
it-recht


Kurzer Compliance Check!
dataprotect
it-recht
Wer besitzt ein Smart-Phone?
NEIN
JA
Ist es ein Diensthandy?
NEIN
JA
Ist Privatnutzung erlaubt?
NEIN
JA
Wird WhatsApp darauf verwendet?
NEIN
JA
compliant
DATA BREACH!
Meldung an die Behörde erforderlich!
© Dr. Thomas Schweiger, LLM (Duke)
09.02.2018 18:19
Folie 2

Nutzung von WhatsApp am „Diensthandy“

Über unsere Dienste

Registrierung. Du musst dich für unsere Dienste registrieren und dafür korrekte Daten verwenden, deine aktuelle Mobiltelefonnummer angeben und diese im Falle einer Änderung unter Nutzung unserer In-App-Funktion „Nummer ändern“ aktualisieren. Du stimmst zu, SMS und Telefonanrufe mit Codes zur Registrierung für unsere Dienste (von uns oder unseren Drittanbietern) zu erhalten.

Adressbuch. Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können.

© Dr. Thomas Schweiger

Rechtsanwalt Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E

Rechtsanwalt in Linz seit 09.09.1999

vorwiegend im Bereich Beratung tätig

Certified International Privacy Professional

Publikationen im Bereich IT-Recht

Spezialgebiet: Datenschutz

www.dataprotect.at / www.it-recht.at

t: @dataprotect_at

f: dataprotect

historische Einordnung

EMRK	DSRL	DSG
Fußball-WM (Deutschl)	Twitter	iPhone

Herausforderungen nach der DSGVO

Google Analytics Datenschutz?

Die dynamische Internetprotokoll - Adresse eines Nutzers stellt für den Betreiber der Website ein personenbezogenes Datum dar, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, den betreffenden Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen.

(EuGH 19.10.2016, C-582/14, RS

DSGVO – Herausforderungen

- Compliance
- Rechenschaftsverpflichtung
- Nachweispflicht
- umfassende Informationspflichten
- Schulung & Training
- Dokumentation
- Revision & Review

Personenbezug ?

alle Informationen → **identifizierte / identifizierbare natürliche Person**

Abgrenzung: natürliche / juristische Person? → wie identifizierbar?

durch wen identifizierbar?

Grundprinzipien der DSGVO

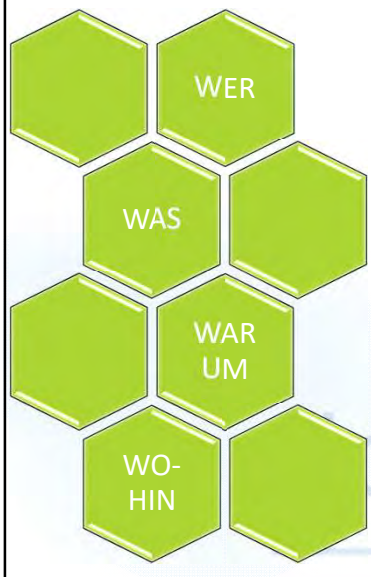
1. Rechtmäßigkeit

- *„the processing shall be lawful only …“* (lawfulness)
- Grundsatz: die Verarbeitung ist verboten
- Grundlage für die (erlaubte) Verarbeitung
  - Einwilligung
  - Vertrag / Vertragsanbahnung
  - rechtliche Verpflichtung
  - lebenswichtige Interessen
  - Wahrnehmung einer Aufgabe im öff Interesse / öffentl Gewalt
  - berechtigte Interessen des Verantwortlichen / eines Dritten

Die Einwilligung im Datenschutz

- Einwilligung:
- jede **freiwillig**
  - für den **bestimmten** Fall,
  - in **informierter** Weise und
  - **unmissverständlich** abgegebene
  - **Willensbekundung**
    - in Form einer Erklärung oder
    - einer sonstigen eindeutigen bestätigenden Handlung

Inhalt einer Einwilligung



- **Verantwortlicher**
- **Welche Daten werden verwendet?**
- **Was geschieht mit den Daten? Warum werden diese verarbeitet?**
- **Werden die Daten an Dritte weitergegeben?**

Einwilligungen richtig gestalten

- Wer / Was / Warum / Wohin?
- Nachweispflicht soll erfüllbar sein
- Freiwilligkeit & Kopplungsverbot
- Widerrufsmöglichkeit

..... (Name)	..... (Vorname)	..... (Postadresse)
..... (Email-Adresse)	..... (Festnetz)	..... (Mobiltelefon)

dataprotect it-recht

erklärt die Einwilligung, dass die oben bekannt gegebenen Daten von XXX XX zu **Werbezwecken** verwendet werden dürfen.

Diese Einwilligung kann jederzeit widerrufen werden. Ein Widerruf kann z.B. auf der Website / im Portal oder per Email an [Email-Adresse] oder auch auf jede andere Art und Weise erfolgen.

Der Widerruf gilt für die Zukunft und hat zur Folge, dass keine weiteren Zusendungen oder Kontaktaufnahmen erfolgen. Die Verarbeitung der Daten vor dem Widerruf ist nicht davon betroffen. Die Daten werden dann lediglich zum Nachweis der korrekten Abwicklung der bisherigen Tätigkeit (z.B. Dokumentation der Einwilligung, bisherige Zusendung der Werbemittel) verwendet. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf verarbeiteten Daten nicht berührt.

Xxx xxxx verarbeitet die Daten in Übereinstimmung mit den datenschutzrechtlichen Bestimmungen. Nähere Informationen sind auch unter [www.[...]/Datenschutz] zu finden.

..... (Unterschrift)

2. Transparenz

- für die betroffene Person nachvollziehbar
- was geschieht mit „meinen Daten“
- umfassende Informationspflichten
  - bei der Erhebung von pb Daten
  - bei der Verwendung von pb Daten
- Datenschutzpolicy & -erklärung
- Rechte der Betroffenen

Wie ist die Informationspflicht zu erfüllen

- „im Zeitpunkt der Erhebung“ -> Wann ist das?
- Wo treffen Sie auf Betroffene?
- Was müssen Sie den Betroffenen mitteilen?
- Wie können Sie es den Betroffenen mitteilen?
  - layered privacy notice / mehrstufige Information
  - Hinweis und Datenschutzinformation auf der Website
- Checkliste
- Datenschutzinformation für Website

Checkliste (Informationspflicht)

WER	DSBA	ZWECK	RECHTS-GRUNDLAGE
Interesse	EMPFÄNGER-KATEGORIEN	Drittland	SPEICHER-DAUER
RECHTE	Widerruf	Vertrags-abschluss	automat. Entscheidung

Wie kann ein Hinweis / Verweis aussehen ?

Wir (Verantwortlicher oder Nennung) verarbeiten
die notwendigen personenbezogene Daten
zur Abwicklung der Geschäftsbeziehung
nach den gesetzlichen Bestimmungen.
Weitere Informationen sind unter www.xxx.at/datenschutz zu finden (Verweis)

- Analyse des Publikums /
- Leitlinien Art 29 DS-Gruppe

dataprotect it-recht

Unterschiedliche Anwendungsfälle

- Ladenlokal / Geschäftslokal
- telefonischer Kontakt
- Email / sonstige Korrespondenz
- Portale / Website
- Besichtigung
- Automaten
- Apps / SMS

dataprotect it-recht

Die Visitenkarte als Datenschutzfalle?

Übergabe einer Visitenkarte → personenbezogene Daten?

Erhebung von Daten? → Information gem. Art 13 DSGVO

Prozess? Wie soll das erfolgen? → Email bei Aufnahme ins CRM-System?

3. Zweck(e) der Verarbeitung

- jede Verarbeitung verfolgt einen Zweck
- Zweckfestlegung
- Zweckbindung (ieS)
- Informationspflichten
  - individuell nach Art 13 / 14: Zweck
  - Verzeichnis von Verarbeitungstätigkeiten: Zweck

3. Zweck(e) der Verarbetung

- jede Verarbeitung verfolgt einen Zweck
- Zweckfestlegung
- Zweckbindung (ieS)
- Informationspflichten
  - individuell nach Art 13 / 14: Zweck
  - Verzeichnis von Verarbeitungstätigkeiten: Zweck

4. Datenminimierung

- ausgehend vom Zweck
- angemessen
- erforderlich
- auf das notwendige Maß beschränkt

5. Richtigkeit

- sachlich richtige Daten
- aktuelle Daten
- Löschung / Berichtigung unrichtiger Daten

6. Speicherbegrenzung

- zeitlicher Bezug
- Relevanz für den Zweck der DV
- Löschroutinen (-fristen)
- Aufbewahrungspflichten (gesetzliche)
- Recht auf Löschung / Vergessenwerden

7. Vertraulichkeit & Integrität

- Datensicherheit
- Schutz vor
  - unbefugter / unrechtmäßiger Verarbeitung
  - unbeabsichtigem Verlust
  - unbeabsichtiger Zerstörung
  - unbeabsichtiger Schädigung
- technische & organisatorische Maßnahmen (TOMs)

Kurz-Info
Datenschutz-AnpassungsG 2018

DSGVO <> DSG (ab 25.05.2018)

- Öffnungsklausel: Kinder – ab 14. Lebensjahr
- keine Geldbußen für Behörden / öff Stellen
- Ergänzungen:
  - Verweis auf ArbVG als „Norm“ iSd Art 88
  - Datengeheimnis für Beschäftigte
  - Bildverarbeitung
  - Straftatbestand

Was bringt die DSGVO Neues für Organisationen

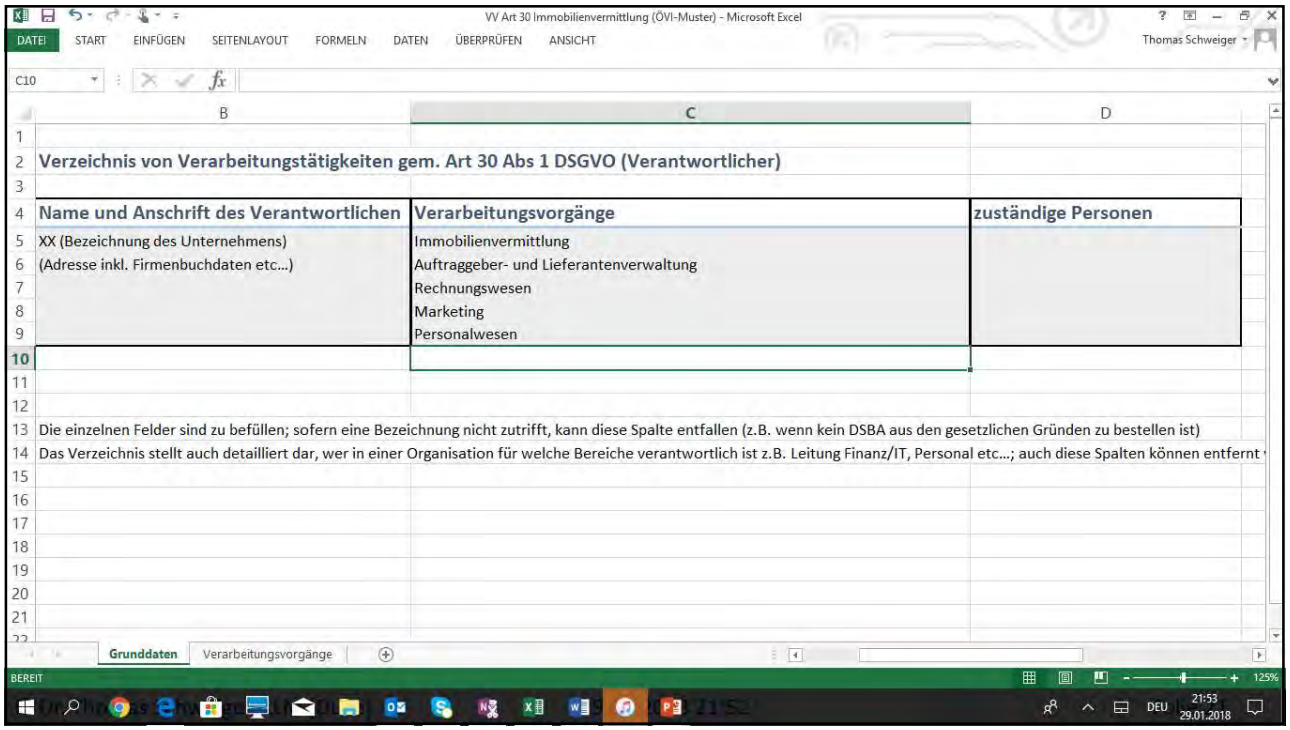
- VV (Verz. von Verarbeitungstätigkeiten) / ROPA – Art 30
- DSFA (Datenschutz-Folgenabschätzung) / (D)PIA– Art 35 ff
- DSB (Datenschutzbeauftragter) / DPO - Art 37 ff
- DBN (Data Breach Notification) – Art 33 ff
- Geldbußen (gg Unternehmen) – Art. 83 / § 11 DSG

Verzeichnis von Verarbeitungstätigkeiten

Verzeichnis von Verarbeitungstätigkeiten (VV)

- Ausnahme: < 250 MA, kein Risiko, Verarbeitung gelegentlich, keine Art. 9 / 10 Daten
- Inhalt:
  - Namen und Kontaktdaten des Verantwortlichen
  - Zweck(e) der Verarbeitung
  - Kategorien der betroffenen Personen & Daten
  - Kategorien der Empfänger
  - Löschungsfrist
  - technische u organisatorische Maßnahmen (TOMs)

VV-Muster
Immobilienmaklertätigkeit



VV Art 30 Immobilienvermittlung (ÖVI-Muster) - Microsoft Excel

DATEI START EINFÜGEN SEITENLAYOUT FORMELN DATEN ÜBERPRÜFEN ANSICHT Thomas Schweiger

C10

Verzeichnis von Verarbeitungstätigkeiten gem. Art 30 Abs 1 DSGVO (Verantwortlicher)

Name und Anschrift des Verantwortlichen	Verarbeitungsvorgänge	zuständige Personen
XX (Bezeichnung des Unternehmens) (Adresse inkl. Firmenbuchdaten etc...)	Immobilienvermittlung Auftraggeber- und Lieferantenverwaltung Rechnungswesen Marketing Personalwesen	

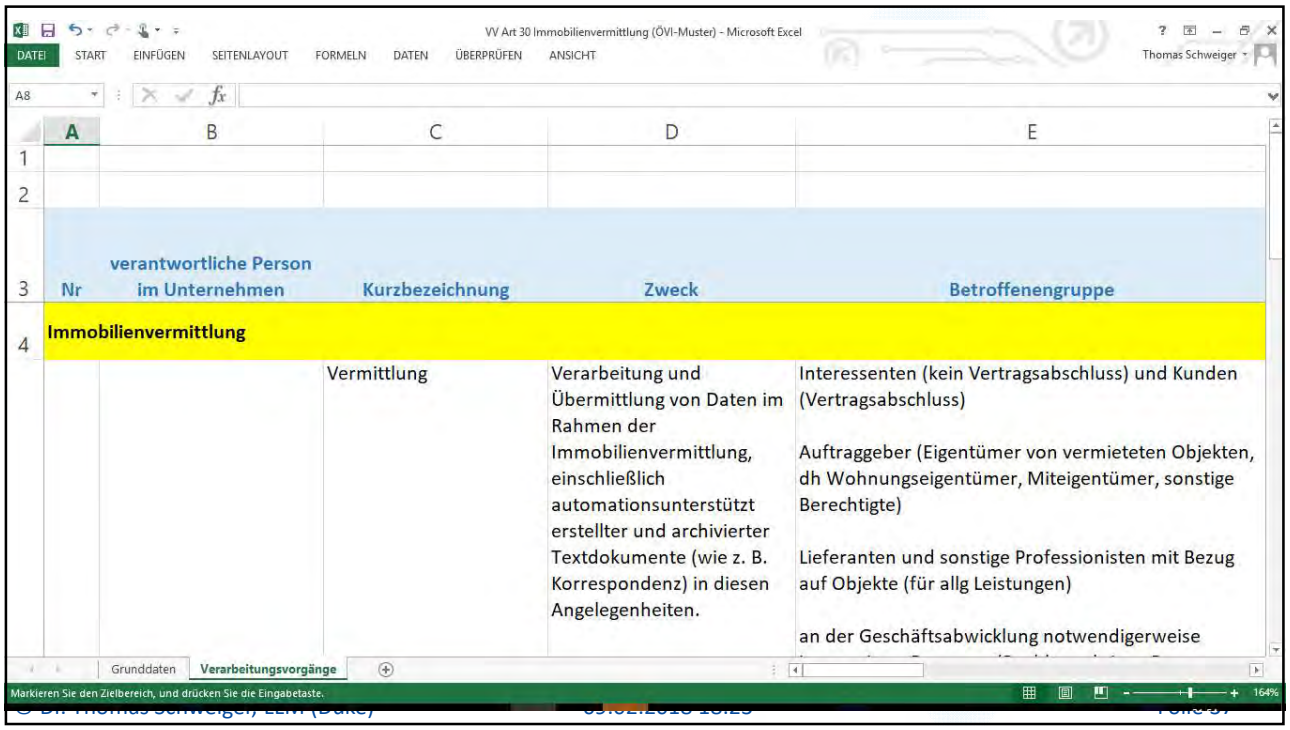
Die einzelnen Felder sind zu befüllen; sofern eine Bezeichnung nicht zutrifft, kann diese Spalte entfallen (z.B. wenn kein DSBA aus den gesetzlichen Gründen zu bestellen ist)

Das Verzeichnis stellt auch detailliert dar, wer in einer Organisation für welche Bereiche verantwortlich ist z.B. Leitung Finanz/IT, Personal etc...; auch diese Spalten können entfernt

Grunddaten Verarbeitungsvorgänge

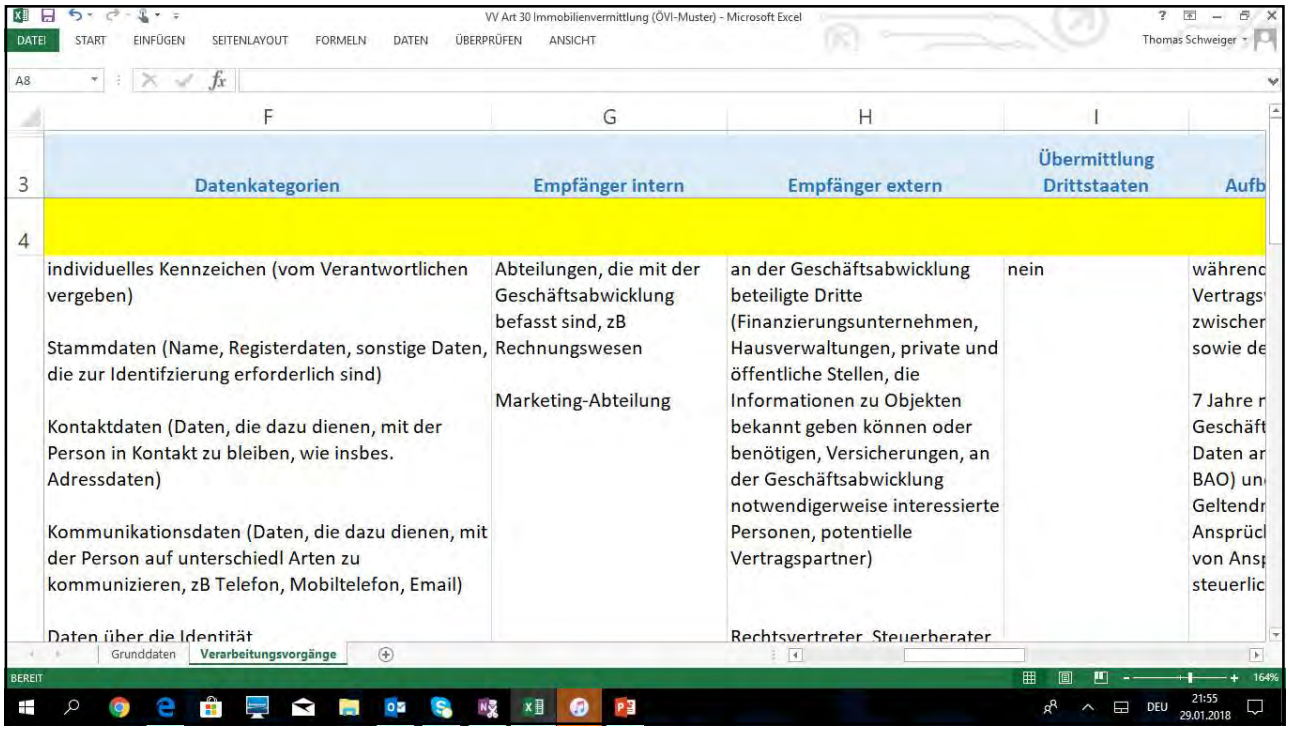
BEREIT 125%

DEU 21:53 29.01.2018



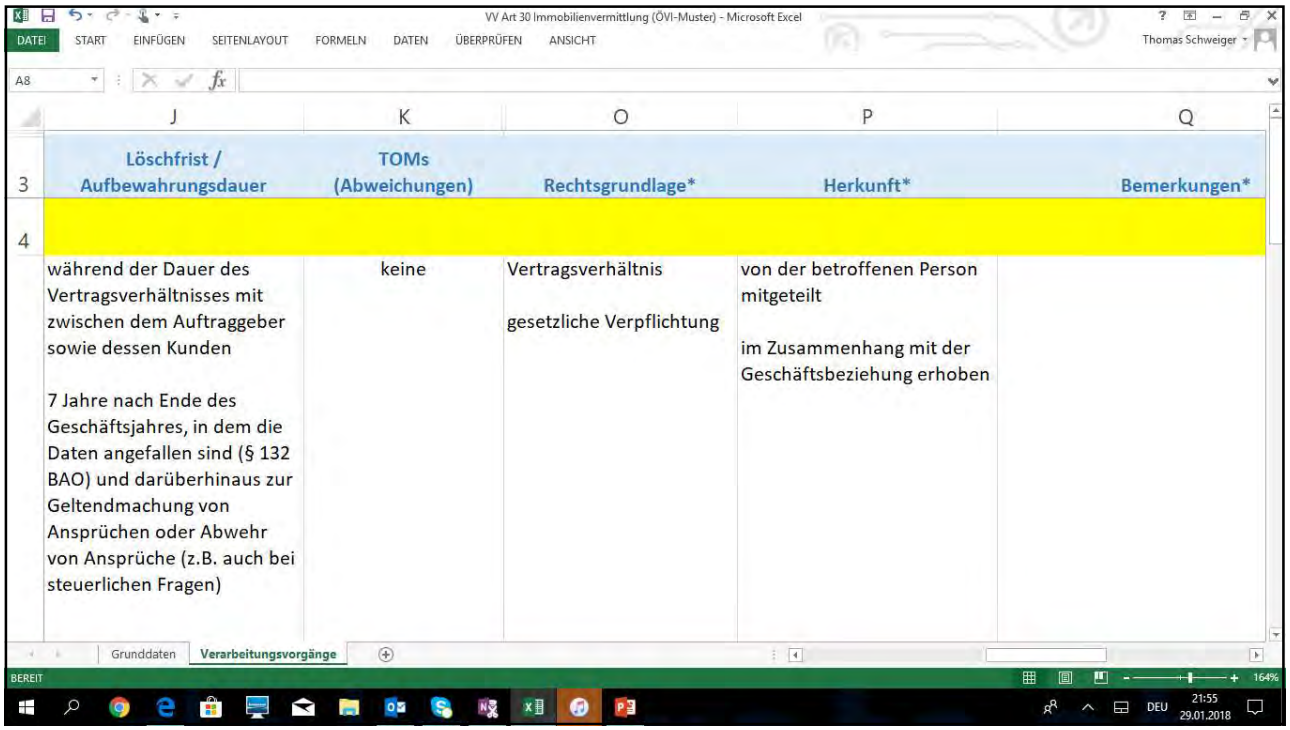
VV Art 30 Immobilienvermittlung (ÖVI-Muster) - Microsoft Excel

Nr	verantwortliche Person im Unternehmen	Kurzbezeichnung	Zweck	Betroffenengruppe
Immobilienvermittlung				
		Vermittlung	Verarbeitung und Übermittlung von Daten im Rahmen der Immobilienvermittlung, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten.	Interessenten (kein Vertragsabschluss) und Kunden (Vertragsabschluss) Auftraggeber (Eigentümer von vermieteten Objekten, dh Wohnungseigentümer, Miteigentümer, sonstige Berechtigte) Lieferanten und sonstige Professionisten mit Bezug auf Objekte (für allg Leistungen) an der Geschäftsabwicklung notwendigerweise



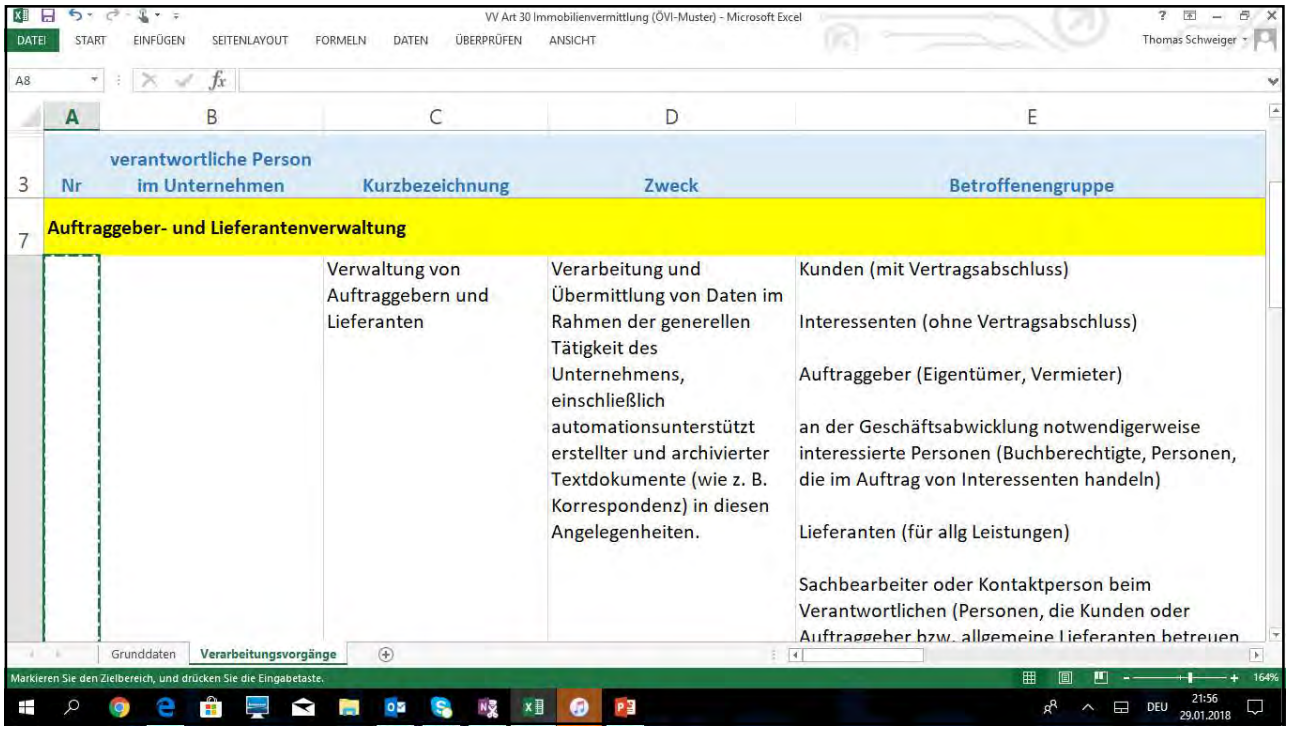
VV Art 30 Immobilienvermittlung (ÖVI-Muster) - Microsoft Excel

Datenkategorien	Empfänger intern	Empfänger extern	Übermittlung Drittstaaten	Aufb
individuelles Kennzeichen (vom Verantwortlichen vergeben) Stammdaten (Name, Registerdaten, sonstige Daten, die zur Identifzierung erforderlich sind) Kontaktdaten (Daten, die dazu dienen, mit der Person in Kontakt zu bleiben, wie insbes. Adressdaten) Kommunikationsdaten (Daten, die dazu dienen, mit der Person auf unterschiedl Arten zu kommunizieren, zB Telefon, Mobiltelefon, Email) Daten über die Identität	Abteilungen, die mit der Geschäftsabwicklung befasst sind, zB Rechnungswesen Marketing-Abteilung	an der Geschäftsabwicklung beteiligte Dritte (Finanzierungsunternehmen, Hausverwaltungen, private und öffentliche Stellen, die Informationen zu Objekten bekannt geben können oder benötigen, Versicherungen, an der Geschäftsabwicklung notwendigerweise interessierte Personen, potentielle Vertragspartner) Rechtsvertreter, Steuerberater	nein	während Vertrags zwischer sowie de 7 Jahre r Geschäft Daten ar BAO) un Geltendr Ansprüc von Ans steuerlic



VV Art 30 Immobilienvermittlung (ÖVI-Muster) - Microsoft Excel

	J	K	O	P	Q
3	Löschfrist / Aufbewahrungsdauer	TOMs (Abweichungen)	Rechtsgrundlage*	Herkunft*	Bemerkungen*
4					
	während der Dauer des Vertragsverhältnisses mit zwischen dem Auftraggeber sowie dessen Kunden 7 Jahre nach Ende des Geschäftsjahres, in dem die Daten angefallen sind (§ 132 BAO) und darüberhinaus zur Geltendmachung von Ansprüchen oder Abwehr von Ansprüche (z.B. auch bei steuerlichen Fragen)	keine	Vertragsverhältnis gesetzliche Verpflichtung	von der betroffenen Person mitgeteilt im Zusammenhang mit der Geschäftsbeziehung erhoben	



VV Art 30 Immobilienvermittlung (ÖVI-Muster) - Microsoft Excel

	A	B	C	D	E
3	Nr	verantwortliche Person im Unternehmen	Kurzbezeichnung	Zweck	Betroffenengruppe
7	**Auftraggeber- und Lieferantenverwaltung**				
			Verwaltung von Auftraggebern und Lieferanten	Verarbeitung und Übermittlung von Daten im Rahmen der generellen Tätigkeit des Unternehmens, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten.	Kunden (mit Vertragsabschluss) Interessenten (ohne Vertragsabschluss) Auftraggeber (Eigentümer, Vermieter) an der Geschäftsabwicklung notwendigerweise interessierte Personen (Buchberechtigte, Personen, die im Auftrag von Interessenten handeln) Lieferanten (für allg Leistungen) Sachbearbeiter oder Kontaktperson beim Verantwortlichen (Personen, die Kunden oder Auftraggeber bzw. allgemeine Lieferanten betreuen

Geldbußen (Strafen)

Geldbußen

- werden auf das **800-fache** erhöht
- **4 %** des weltweiten / jährlichen Gesamtvorjahres**umsatzes** bzw. **EUR 20.000.000,--**
- **wirksam, verhältnismäßig & abschreckend**
- **Strafzumessungsgründe**
- **Geldbuße gg Unternehmen (wie § 99d BWG)**
- **keine Geldbußen gg Behörden / öffentliche Stellen**

Geldbußen

- siehe Art. 83 DSGVO – Höchstausmaß
- Strafzumessungsgründe sind maßgebend
- Österreich: Geldbußen gegen Unternehmen („Hauptadressat“):
  - Personen in Führungspositionen begehen die Tat
  - mangelnde Überwachung oder Kontrolle ermöglicht die Begehung des Verstoßes (Verstoß gegen Internes Kontrollsystem)

DSGVO-Projektplan

Dr. Thomas Schweiger, LL.M. (Duke), CIPP/E

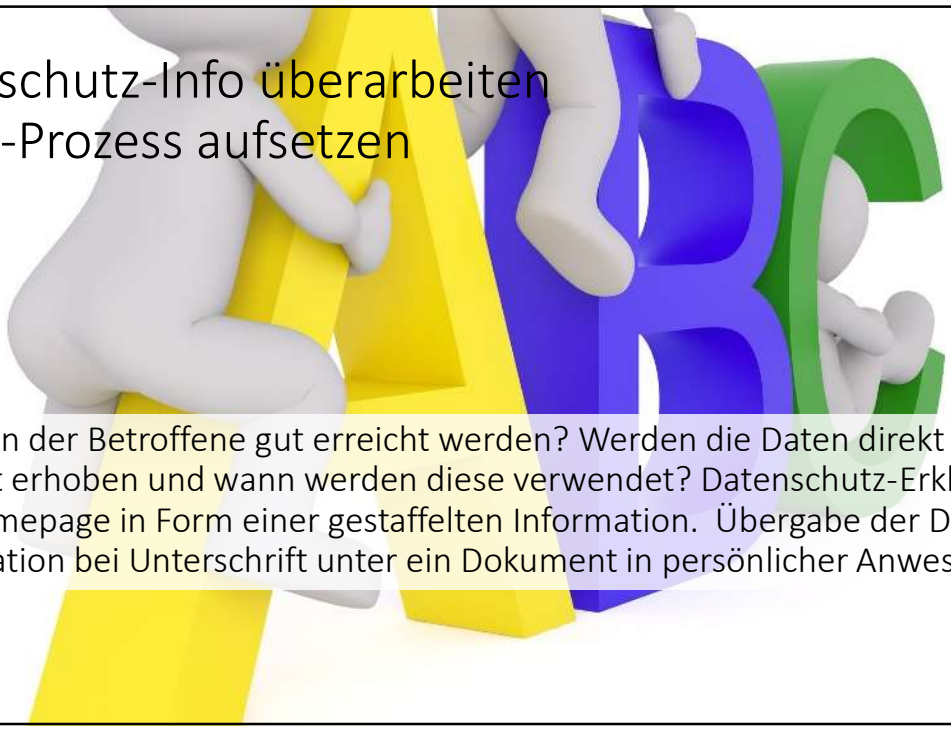
DataManager benennen & Ressourcen bereitstellen

- Finanzmittel und Humanressourcen sind bereitzustellen
- DM übernimmt die Projektplanung & -leitung
- DM weist die „To-Dos“ zu und fordert diese zeitgerecht ein
- DM berichtet an das Board über die Fortschritte (Zwischenberichte)

Datenlandkarte erheben

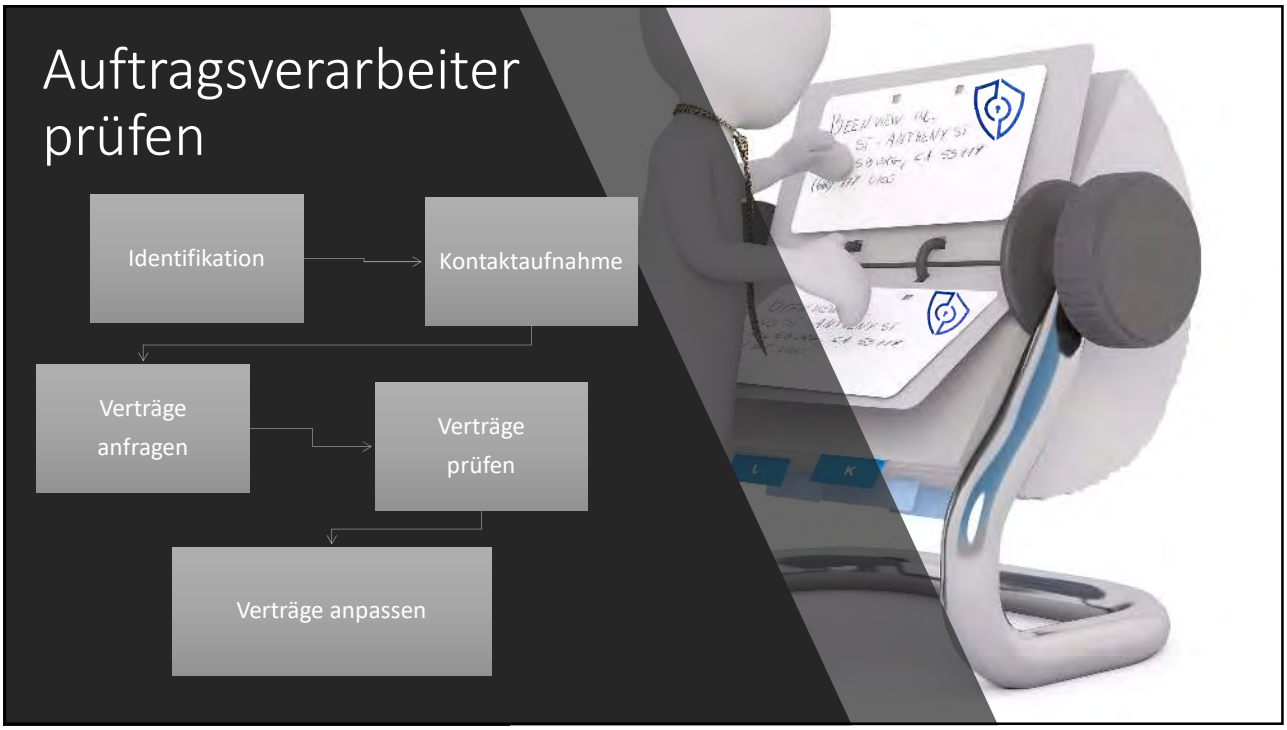
- Verzeichnis gem. Art 30
- Zweck
- Betroffene
- Daten
- Empfänger
- Drittländer
- Löschfrist
- TOMs
- **Zusätze**
- Rechtsgrundlage
- Herkunft

Datenschutz-Info überarbeiten & Info-Prozess aufsetzen



Wo kann der Betroffene gut erreicht werden? Werden die Daten direkt oder indirekt erhoben und wann werden diese verwendet? Datenschutz-Erklärung auf der Homepage in Form einer gestaffelten Information. Übergabe der DS-Information bei Unterschrift unter ein Dokument in persönlicher Anwesenheit?

Auftragsverarbeiter prüfen



Data Breach Notification – Prozess erstellen

Meldung an die Aufsichtsbehörde (wenn Risiko nicht ausgeschlossen)

Meldung an die betroffenen Personen (wenn hohes Risiko)

Leitfaden für Betroffenenrechte erstellen

Bestätigung & Auskunft
Berichtigung, Einschränkung & Löschung
Datenübertragbarkeit
Eingriff in automatisierte Entscheidungsfindung
Widerruf & Beschwerde

Awareness schaffen

Beschäftigte schulen

Review-Cycle implementieren

dataprotect | knowledge pack IMMO

- Verzeichnis (Muster)
- Transparenzpaket
- Daten-geheimnis
- Vertrag Auftrags-datenverarbeitung
- Standard-Toms (KMU)
- Leitfaden:
  - Betroffenenrechte
  - Datenschutzvorfall