

# Allgemeine Informationen zur praktischen Anwendung der DSGVO

Informationsveranstaltungsreihe  
DSGVO & Geldwäsche

Mag. Ursula Illibauer

# Inhalt

---

- Was ist neu?
- Wer ist betroffen?
- Was ist...?
- **8-Punkte-Plan:**
  1. Einheitliche Grundsätze
  2. Datenschutzerklärung / Einwilligung
  3. Was ist neu?
  4. Verarbeitungsverzeichnis
  5. Risikoanalyse
  6. Datenschutzfolgenabschätzung
  7. Betroffenenrechte
  8. Datensicherheit
- Was ist zu tun?
- Strafen
- Wie hilft die WKO?

# Was ist neu?

---

## ■ einheitliches Recht in der EU?

- ▶▶ EU - Datenschutz - Grundverordnung (DSGVO)
- ▶▶ österreichisches Datenschutz-Anpassungsgesetz 2018 (DSG)

## ■ wieviel Zeit zur Umsetzung?

- ▶▶ Umsetzung bis 25. Mai 2018!

# Wer ist betroffen?

---

- **Was:** Datenverarbeitungen von **personenbezogenen Daten**
  - automatisiert oder
  - nicht automatisiert, aber in einem Dateisystem gespeichert
  
- **Wo:**
  - **Europabezug**
  - Unternehmen mit Sitz außerhalb Europas, wenn personenbezogene Daten von **Betroffenen der EU** verarbeitet werden
  
- **Wer: JEDER** der Daten nicht nur zu privaten Zwecken verarbeitet

# Was ist...?

<b>DSGVO</b>	<b>DSG 2000</b>
personenbezogene Daten	personenbezogene Daten
besondere Kategorien von Daten	sensible Daten
verarbeiten	verwenden
<b>Verantwortlicher</b>	Auftraggeber
<b>Auftragsverarbeiter</b>	Dienstleister
Profiling	-
-	Übermitteln / Überlassen
Empfänger, Dritter	-
Pseudonymisierung	indirekt personenbezogene Daten
Dateisystem	-

---

# 8-Punkte-Plan

# 1. Grundsätze einhalten

---

Rechtmäßigkeit,  
Treu & Glauben,  
Transparenz

Zweckbindung

Richtigkeit

Datenminimierung

Rechenschaft

Speicherbegrenzung

Integrität und  
Vertraulichkeit

## 2. Einwilligungen richtig einholen

---

- ☑ freiwillig, für den bestimmten Fall, informiert, unmissverständlich
- ☑ Willensbekundung (Checkbox?)
- ☑ Erklärung oder sonstige eindeutig bestätigende Handlung
- ☑ getrennt von anderen Sachverhalten (AGB?)
- ☑ jdz Widerrufbarkeit



- 
- Formulierungsvorschläge zB auf [www.wko.at/datenschutz](http://www.wko.at/datenschutz):

*„Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich ... (die Datenarten genau aufzählen, z.B. „Name“, „Adresse“, etc) zum Zweck der ... (genaue Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte der Firma ...“) bei der Firma NN gespeichert werden. Diese Einwilligung kann jederzeit bei ... (Angabe der entsprechenden Kontaktdaten) widerrufen werden.“*

### 3. Datenschutzbeauftragten bestellen?

- Verpflichtung sowohl für **Verantwortlichen** als auch **AV**
- verpflichtend für Behörde oder öffentlichen Stelle und
- verpflichtend für Unternehmen,
  - **Kerntätigkeit** = umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen **oder**
  - **Kerntätigkeit** = umfangreiche Verarbeitung **strafrechtlich relevanter/ sensibler Daten**
- **erfasst**: Kreditauskunfteien, Standorttracking, Banken, Versicherungen,...
- **nicht erfasst**: Unternehmen, die nur in einer **untergeordneten Weise** diese Kerntätigkeiten durchführen

## 4. Verarbeitungsverzeichnis erstellen!

---

- Aufzeichnung aller datenschutzrelevanter Vorgänge im Unternehmen
- Pflicht für Verantwortlichen und Auftragsverarbeiter
- Inhalt äußerst weitreichend
- Aufzeichnungen haben schriftlich oder elektronisch zu erfolgen
- sehr eingeschränkte Ausnahme für wenige
- Muster unter [wko.at/datenschutz](https://wko.at/datenschutz)

# Verarbeitungsverzeichnis

## - Verantwortlicher

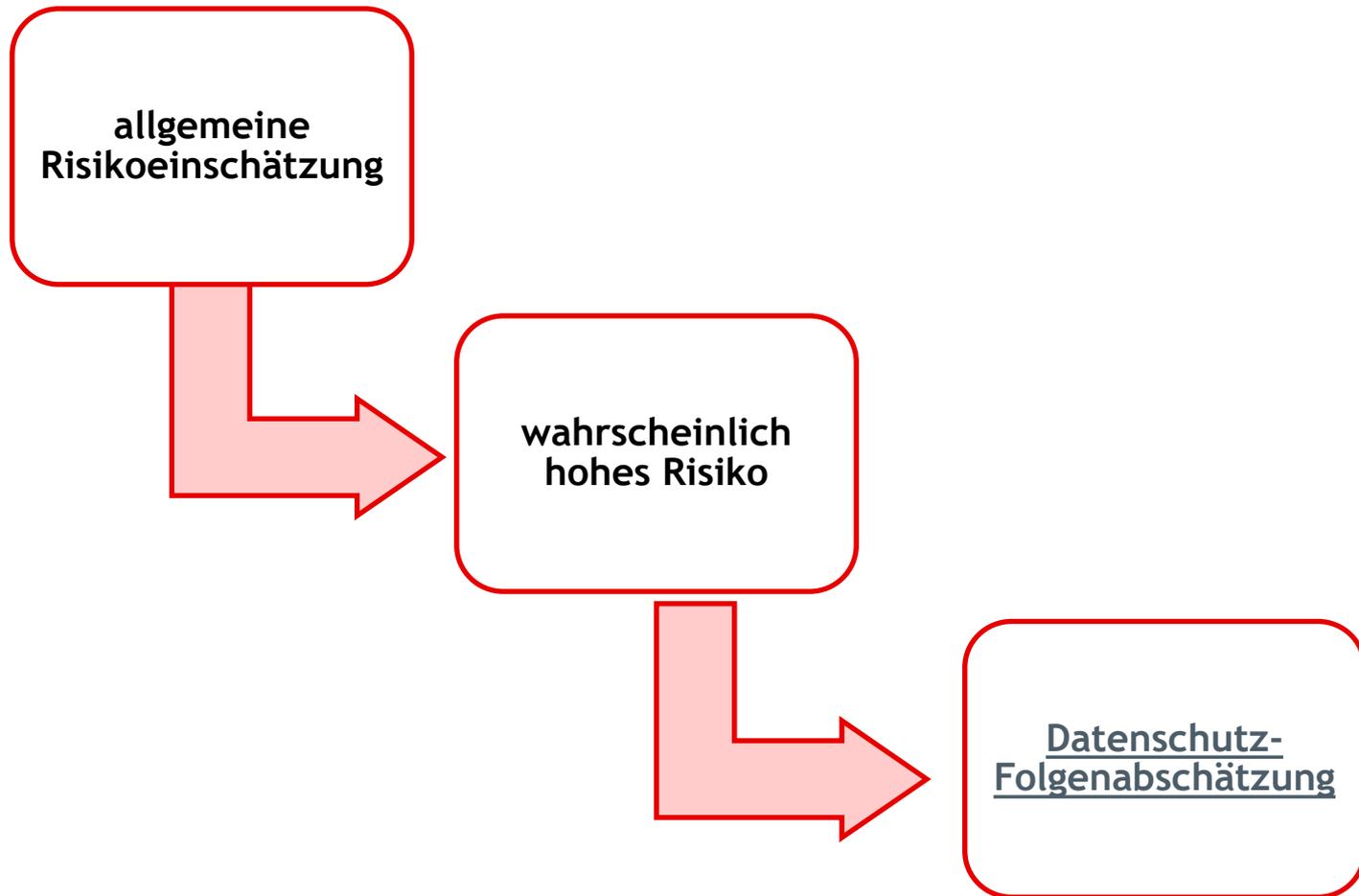
- **Namen und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,**
- **Zweck** der Datenverarbeitung,
- Beschreibung der **Kategorien betroffener Personen** und der **Kategorien personenbezogener Daten** (z.B. Kunden und Lieferanten; Rechnungsdaten, Adressdaten),
- **Kategorien von Empfängern** von Daten (z.B. Sozialversicherung, Finanzamt, Rechtsanwalt, Steuerberater), **Empfänger in Drittländern** oder internationalen Organisationen (z.B. Konzernmutter in USA),
- ggf Übermittlungen von personenbezogenen Daten an ein **Drittland** (z.B. USA) oder an eine internationale Organisation, Angaben des Drittlands oder der betreffenden internationalen Organisation,
- die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien (nach Möglichkeit),
- allgemeine Beschreibung der **technischen und organisatorischen Datensicherheitsmaßnahmen**

# Verarbeitungsverzeichnis

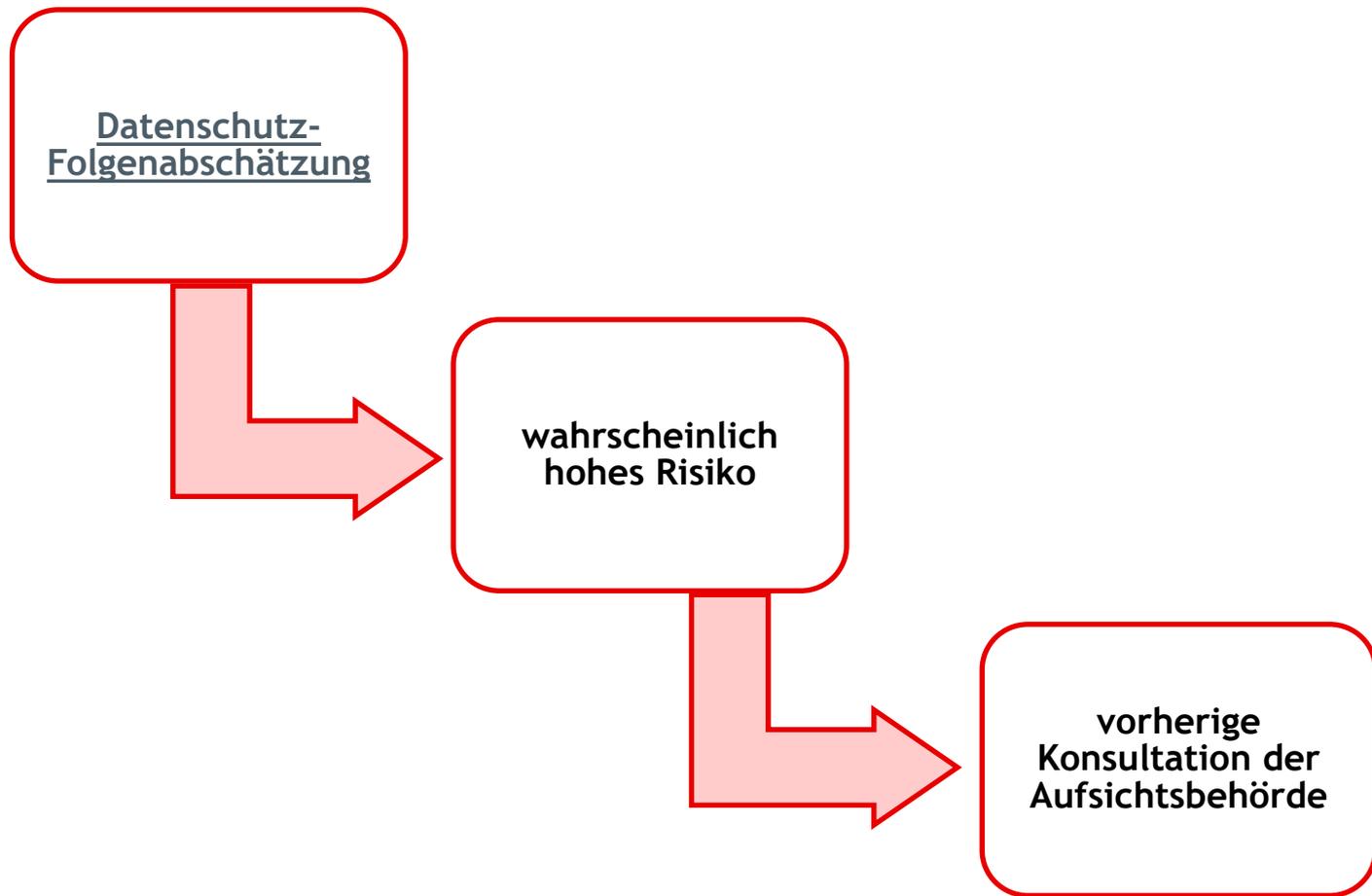
## - Auftragsverarbeiter

- **Name und Kontaktdaten des Auftragverarbeiters** und jedes **Verantwortlichen**, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie ggf des **Vertreters** des Verantwortlichen oder des Auftragverarbeiters und eines etwaigen **Datenschutzbeauftragten**,
- **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden,
- ggf Übermittlungen von personenbezogenen Daten an ein **Drittland** oder eine internationalen Organisation, Angabe des Drittlands oder der betreffenden internationalen Organisation,
- allgemeine Beschreibung der **technischen und organisatorischen Datensicherheitsmaßnahmen**

# 5. Risiken analysieren!



## 6. Datenschutzfolgenabschätzung erstellen?



# 7. Betroffenenrechte beachten!





## 8. Datensicherheit einhalten!

geeignete technische, organisatorische  
Maßnahmen zum Schutz vor Zerstörung,  
Verlust, Zugang durch Unbefugte

Art, Umfang,  
Umstände, Zweck  
der Verarbeitung

Stand der  
technischen  
Möglichkeiten

Eintrittswahrschein-  
lichkeit, Schwere  
der Risiken

Implementierungs-  
kosten

Datenleck

Information  
an Betroffene

Meldung  
Aufsichtsbehörde

# Was ist zu tun?

---

## 1. Bedarf im Betrieb feststellen

- Zeit & Budget
- Maßnahmenplan
- Zuständigen/ Ansprechpartner für die weitere Abwicklung nominieren

## 2. „IST-Stand“ erheben:

- Datenanwendungen im Unternehmen JETZT prüfen (DVR, Standardanwendungen)
- Zuständigen für „Datenschutz“ nominieren
- Speicherdauer von Daten prüfen
- Zustimmungserklärungen, AGB, DS-Erklärungen, laufende Verträge überprüfen
- Informationen auf Websites, Mails, etc
- Datensicherheitsmaßnahmen überprüfen
- protokollieren

# Was kann passieren?



© Tetra Images/Corbis

Strafen bis zu **EUR 20 Mio** oder **4 %** des weltweiten Konzernumsatzes des vorangegangenen Geschäftsjahres



**KEINE PANIK!**  
Durchatmen, sacken  
lassen

Datenanwendungen  
im Unternehmen in  
Ruhe prüfen und  
einschätzen

und bei Fragen...

# Hilfestellung durch die WKO

---

- [www.wko.at/datenschutz](http://www.wko.at/datenschutz)
  - ✓ Überblicksseite mit Kurzzusammenfassung
  - ✓ Checklisten
  - ✓ Muster
  - ✓ Informationsdokumente
  - ✓ Ansprechpersonen je Bundesland
  - ✓ 2 Onlineratgeber
  - ✓ Informationsfolder
  - ✓ Broschüren
- [www.wko.at/it-sicherheit](http://www.wko.at/it-sicherheit)



Machen Sie Ihr Unternehmen  
IT-sicher!



IT-Sicherheit ist für jedes  
Unternehmen überlebenswichtig!

Die Sicherheit der IT-Systeme, aber auch die Kompetenz im Umgang damit, ist wesentlich für die moderne, digitale Wirtschaft. Mit der Aktion „it-safe.at“ bietet die Bundessparte Information und Consulting (BSIC) in der WKÖ vor allem kleinen Unternehmen Hilfestellung.

Auf dieser Website finden Sie praxisnahe Online-Ratgeber sowie Informationen und konkrete Tipps rund um IT-Sicherheit in Ihrem Unternehmen. Gemeinsam gehen wir's an und machen auch Ihr Unternehmen IT-sicher!

Kontakt

Bundessparte Information und  
Consulting

Wiedner Hauptstraße 63  
1045 Wien

Telefon: +43 5 90 900 3175  
E-Mail: [ic@wko.at](mailto:ic@wko.at)

[Detaillierte Kontaktseite](#)

- ✓ Blog
- ✓ EPU Checkliste
- ✓ Online-Ratgeber
- ✓ Handbuch KMU
- ✓ Handbuch Mitarbeiter
- ✓ Tagesaktuelles
- ✓ Veranstaltungen
- ✓ ...





---

Vielen Dank für Ihre Aufmerksamkeit!