

Datenschutz und Datensicherheit

Fachverband Finanzdienstleister

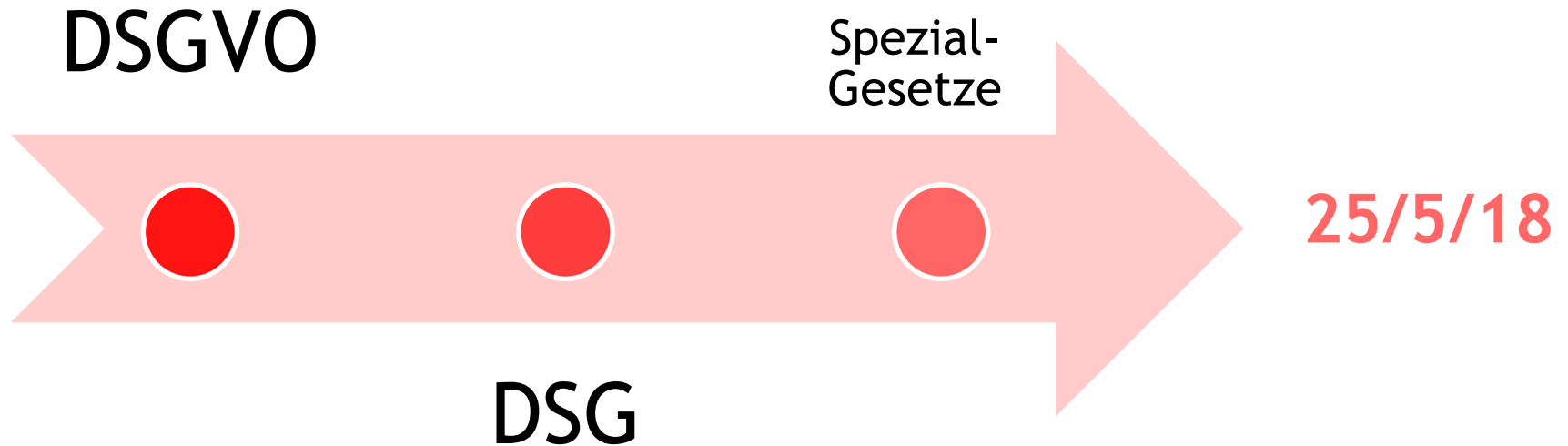
13. März 2018

Mag. Ursula Illibauer

Inhalt

- Zeitplan
- Betroffenheit Finanzdienstleister
- Daten
- Einheitliche Spielregeln
- Rechtmäßigkeit
- Datenweitergabe
- internationale Datenweitergabe
- Verarbeitungsverzeichnis
- Datenschutzbeauftragten
- Self-Assessment
- Betroffenenrechte
- Profiling
- Datensicherheit
- Exkurs: Newsletter
- Strafen
- 10-Punkte Plan für Finanzdienstleister
- Wie hilft die WKO?

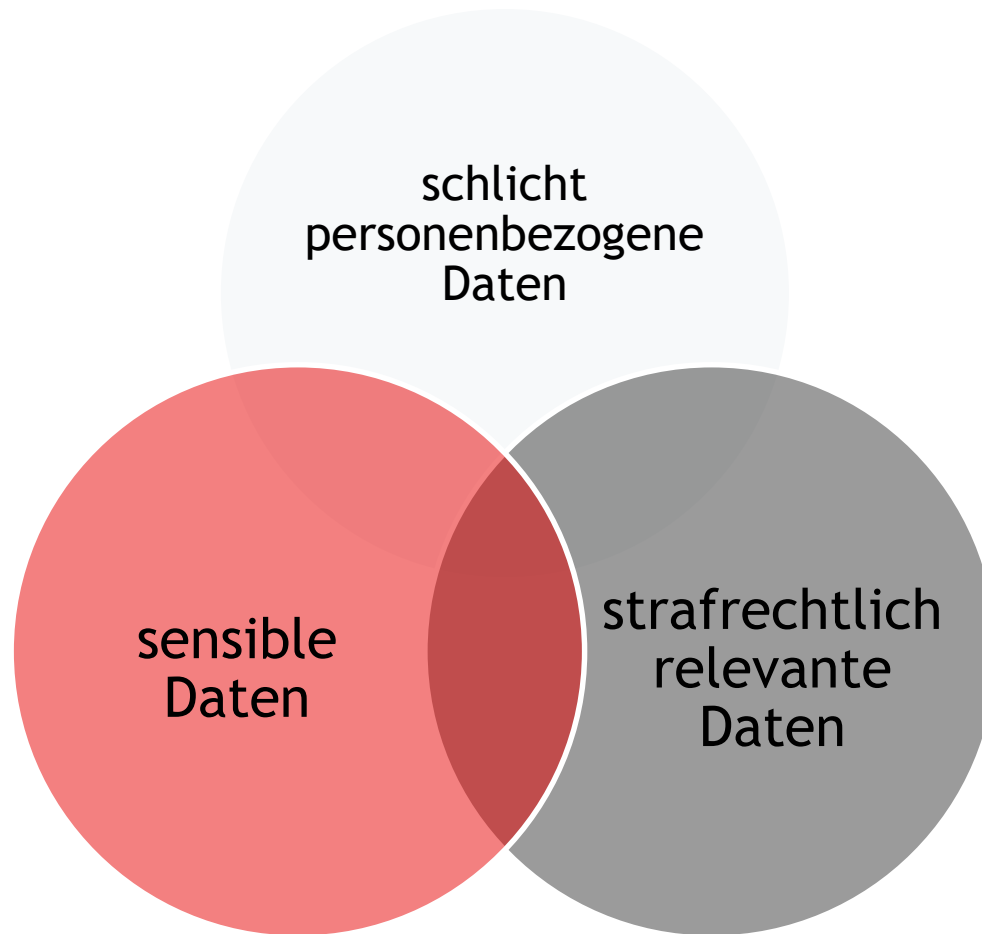
Zeitplan



Betroffenheit Finanzdienstleister

- Verantwortlicher?
 - ✓ JA
- Auftragsverarbeiter?
 - ✓ JA
- Datenverarbeitungen?
 - ✓ JA
- unternehmensbezogen?
 - ✓ JA
- von personenbezogenen Daten?
 - ✓ JA
- automatisiert oder Dateisystem?
 - ✓ JA
- EU-Bezug?
 - ✓ JA

Daten



Einheitliche Spielregeln - **bekannt!**

Rechtmäßigkeit,
Treu & Glauben,
Transparenz

Zweckbindung

Richtigkeit

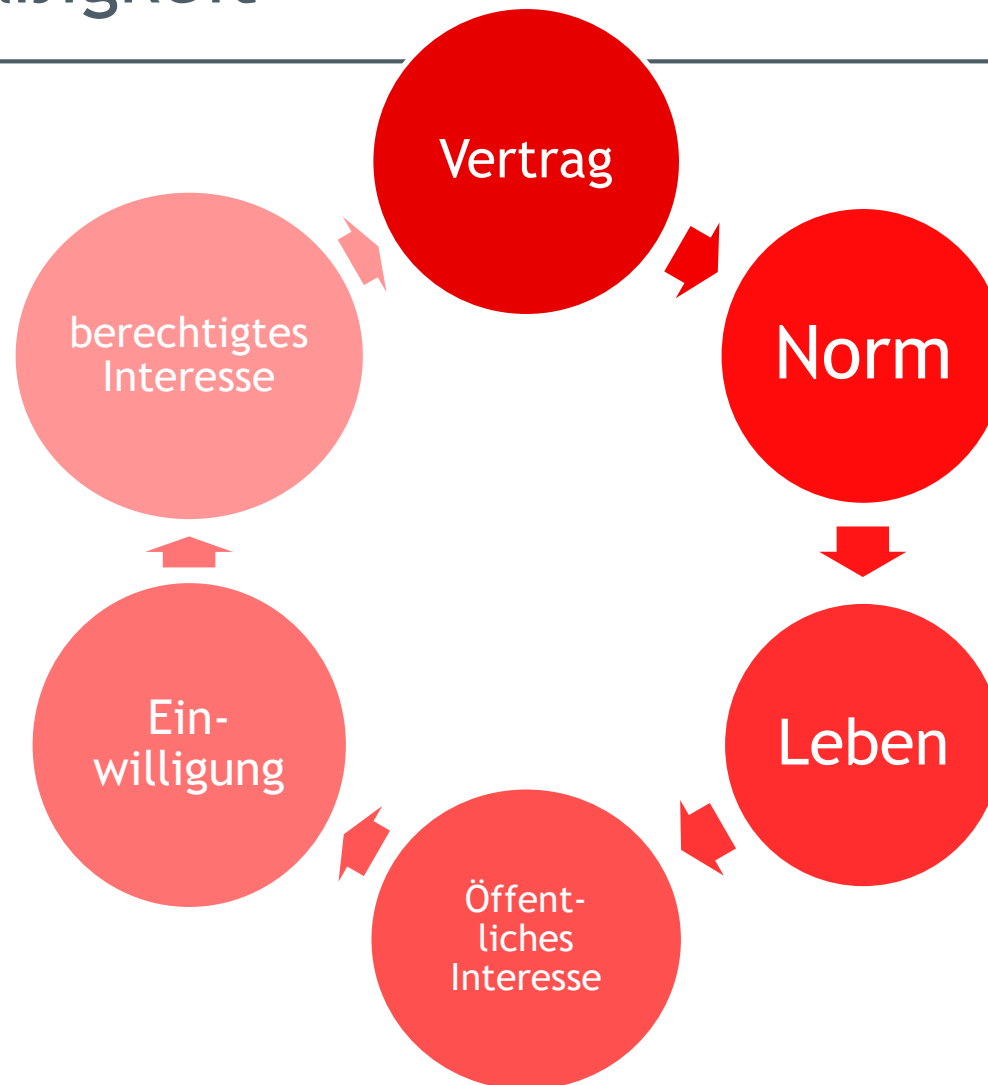
Datenminimierung

Speicherbegrenzung

Integrität und
Vertraulichkeit

Rechenschaft

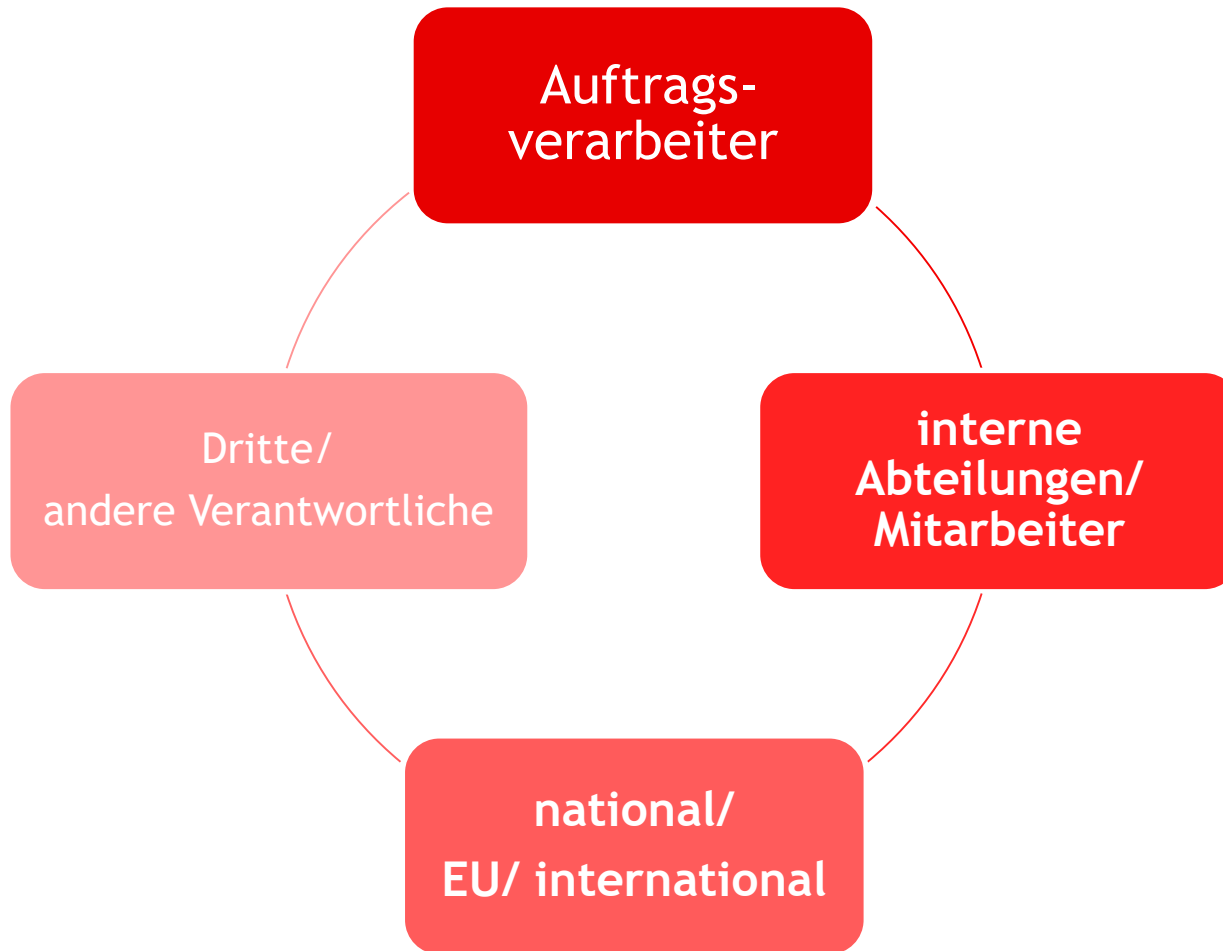
Rechtmäßigkeit



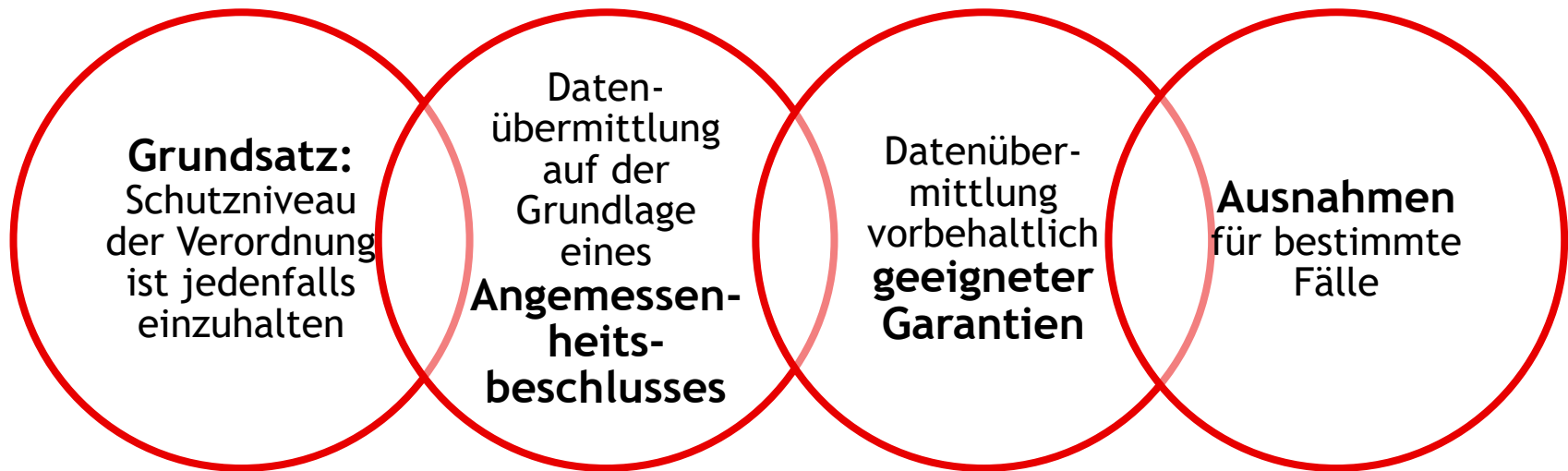
Einwilligungserklärungen

- ☑ freiwillig, für den bestimmten Fall, informiert, unmissverständlich
- ☑ Willensbekundung
- ☑ Erklärung oder sonstige eindeutig bestätigende Handlung
- ☑ getrennt von anderen Sachverhalten (AGB?)
- ☑ jdz Widerrufbarkeit
- ☑ Formulierungsvorschläge auf www.wko.at/datenschutz
- ☑ was tun mit „alten“ Einwilligungen?

Datenweitergabe



Internationale Datenweitergabe



Verarbeitungsverzeichnis - NEU!

- Aufzeichnung aller datenschutzrelevanter Vorgänge im Unternehmen
- Pflicht für **Verantwortlichen & Auftragsverarbeiter**
- Inhalt äußerst weitreichend
- Aufzeichnungen schriftlich oder elektronisch
- sehr eingeschränkte Ausnahme für wenige
- Muster unter wko.at/datenschutz

Verarbeitungsverzeichnis - Verantwortlicher

- **Namen und Kontaktdaten des Verantwortlichen / ggf Vertreters / ggf Datenschutzbeauftragten,**
- **Zweck** der Datenverarbeitung,
- **Kategorien betroffener Personen,**
- **Kategorien personenbezogener Daten,**
- **Kategorien von Empfänger von Daten, Empfänger in Drittländern oder internationalen Organisationen,**
- ggf Übermittlungen von personenbezogenen Daten an ein **Drittland** oder an eine internationale Organisation, Angaben des Drittlands oder der betreffenden internationalen Organisation,
- **Fristen für die Löschung** der verschiedenen Datenkategorien (nach Möglichkeit),
- allgemeine Beschreibung der **technischen und organisatorischen Datensicherheitsmaßnahmen**

Verarbeitungsverzeichnis - Verantwortlicher

Name und Kontaktdaten des/ der Verantwortlichen	Max Mustermann GmbH Neuer Weg 1 ZZZZ Musterdorf
Name und Kontaktdaten des Datenschutzbeauftragten	Franz Fachmann e. U. Datenstraße 5 YYYY Datenstadt

Zwecke der Datenverarbeitung	Kategorien der Betroffenen	Kategorien personenbezogener Daten	Kategorien von Empfängern	Empfänger in Drittländern	Fristen für die Löschung	technischen und organisatorischen Datensicherheitsmaßnahmen
Personalverwaltung	Mitarbeiter	Name, Adresse,...	GKK, Finanzamt,...	✕	gesetzliche Aufbewahrungsfristen	Zutrittskontrolle, Zugriffskontrolle,...

Achtung: Nur für Vorführzwecke!

Verarbeitungsverzeichnis - Auftragsverarbeiter

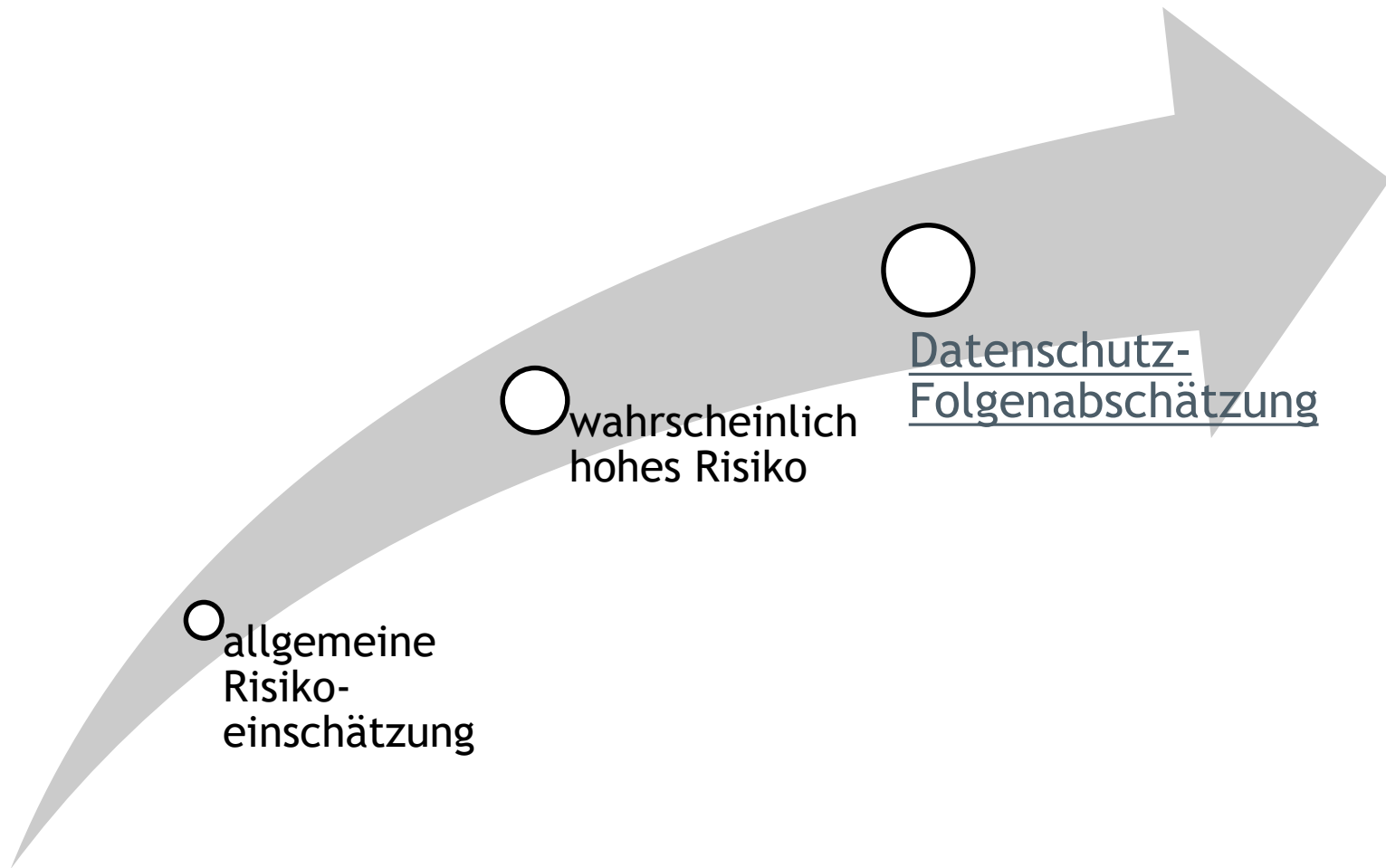
- **Name und Kontaktdaten des Auftragverarbeiters** und jedes **Verantwortlichen**, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie ggf des **Vertreters** des Verantwortlichen oder des Auftragverarbeiters und eines etwaigen **Datenschutzbeauftragten**,
- **Kategorien von Verarbeitungen**, 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**
- **Muster:** <https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-auftragsverarbeite.html>

Datenschutzbeauftragter - NEU!

- 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:** Standorttracking, Banken, Versicherungen,...
- **nicht erfasst:** Unternehmen, die nur in einer **untergeordneten Weise** diese Kerntätigkeiten durchführen

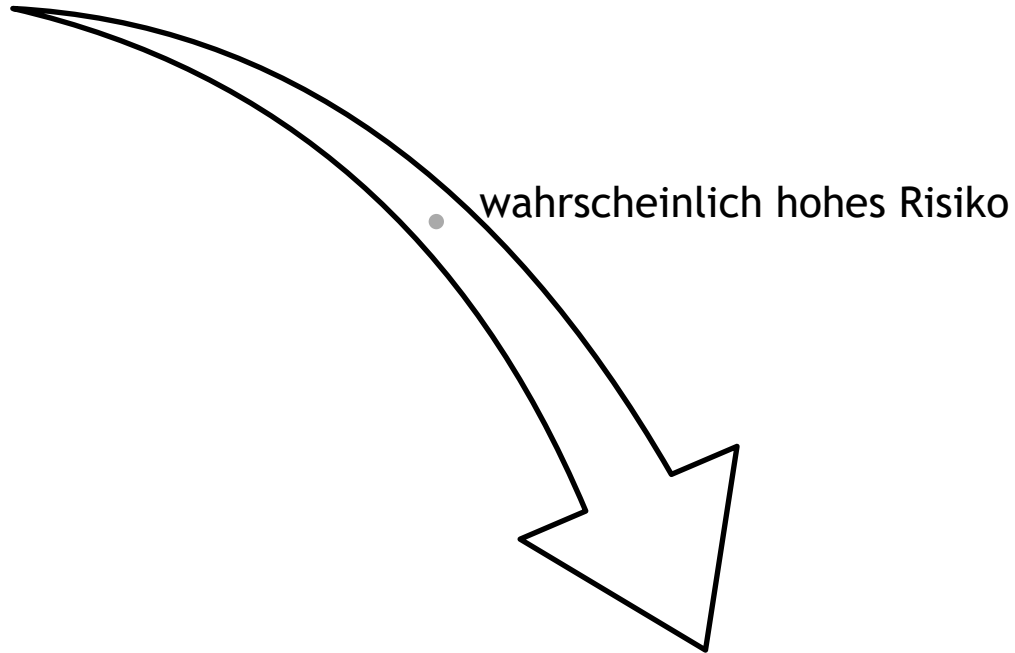
- **Finanzdienstleister: im Standardfall nein**

Self-Assessment - NEU!



Self-Assessment - NEU!

Datenschutz-
Folgenabschätzung



vorherige Konsultation der
Aufsichtsbehörde

Betroffenenrechte - tlw bekannt!

- Information
- Auskunft
- Richtigstellung
- Löschung
- Widerspruch
- Datenübertragbarkeit
- Einschränkung

Profiling - tlw bekannt!

- automatisierte Verarbeitung personenbezogener Daten, um bestimmte persönliche Aspekte zu bewerten
 - zB Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel
 - bewerten, analysieren oder vorhersagen
 - Widerspruchsrecht
- **Problem:** ausschließlich auf einer automatisierten Verarbeitung - einschließlich Profiling - beruhende Entscheidung, die rechtliche Wirkung entfaltet oder in ähnlicher Weise erheblich beeinträchtigt
 - spezielle Rechtfertigungsgrundlage
 - Informationsverpflichtung (vorab)

Datensicherheit - tlw bekannt!

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

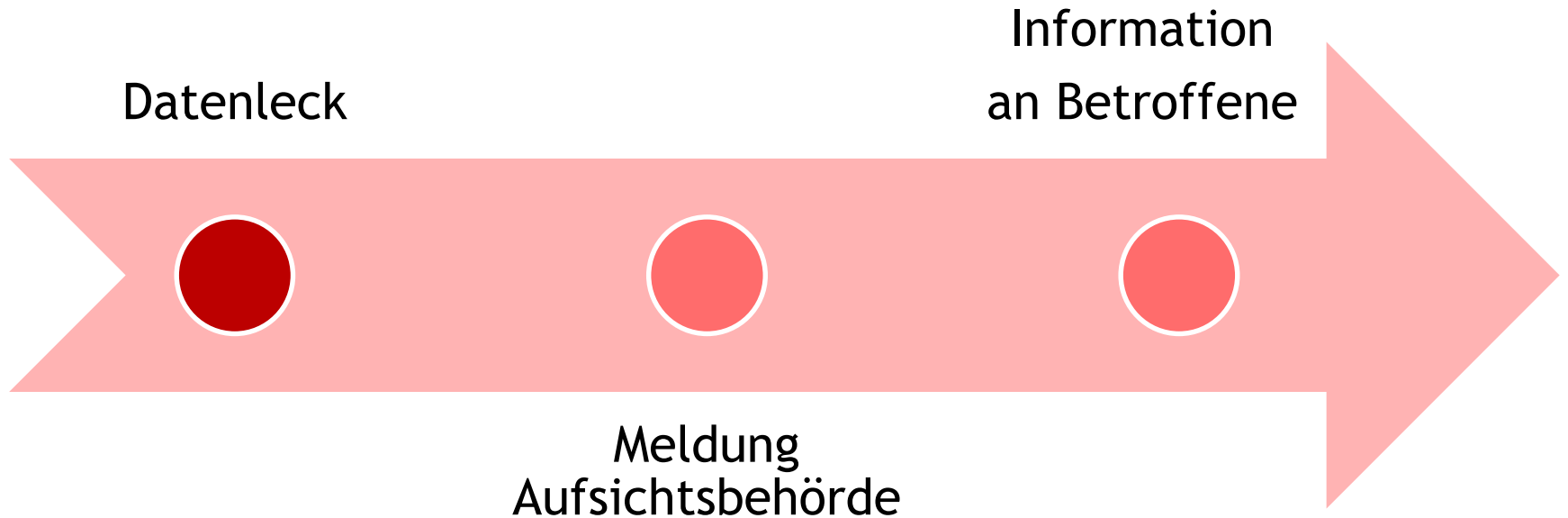
Art, Umfang,
Umstände, Zweck
der Verarbeitung

Eintrittswahrschein-
lichkeit, Schwere
der Risiken

Stand der
technischen
Möglichkeiten

Implementierungs-
kosten

Datensicherheit - NEU!



Newsletter

- **unerbetene Kommunikation (§ 107 TKG):**
 - ✓ Anrufe, Telefaxe und elektronische Post
 - ✓ als Massensendung **oder**
 - ✓ zu Werbezwecken
 - ✓ bedürfen der vorherigen, jederzeit widerruflichen Zustimmung des Empfängers
- **Ausnahme:** für elektronische Post im aufrechten Kundenverhältnis
 - ✓ Abbestellmöglichkeit
 - ✓ Werbung für eigene ähnliche Produkte/Dienstleistungen
 - ✓ ECG Liste ist zu beachten
- Versendung **anonymer** elektronischer Post ist verboten

TO DO - 10 Punkte!

1. Dateninventur
2. Zeit & Budget bestimmen
3. Maßnahmenplan
4. Zuständigen/ Ansprechpartner für „Datenschutz“ nominieren / Datenschutzbeauftragten bestellen
5. Datenanwendungen im Unternehmen prüfen (DVR, Standardanwendungen)
6. Speicherdauer von Daten prüfen
7. Zustimmungserklärungen, AGB, DS-Erklärungen, laufende Verträge überprüfen
8. Informationen auf Websites, Mails, etc
9. Datensicherheitsmaßnahmen überprüfen
10. protokollieren

Strafen - was kann schlimmstenfalls passieren?



© Tetra Images/Corbis

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

Hilfestellung durch die WKO

- www.wko.at/datenschutz
 - ✓ Überblicksseite mit Kurzzusammenfassung
 - ✓ Checklisten
 - ✓ Muster
 - ✓ Informationsdokumente
 - ✓ Ansprechpersonen je Bundesland
 - ✓ 2 Onlineratgeber
 - ✓ Informationsfolder
 - ✓ Broschüren
- 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

[Detaillierte Kontaktseite](#)

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



Keep calm - it ' s only GDPR ...

Mag. Ursula Illibauer

Bundessparte Information und Consulting

E ursula.illibauer@wko.at

T +43 (0)5 90 900 3151