15. Österreichischer IT-&Beratertag 2017

Der Branchenevent für Ihren Erfolg

„Datenschutz – NEU“

Die DSGVO und das österr. Datenschutzgesetz ab Mai 2018

Ursula Illibauer

Bundessparte Information & Consulting

WKO WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung · Buchhaltung · IT

Inhalt

1. Was ist „neu“?
2. Betroffenheit
3. Einheitliche Grundsätze
4. Auftragsverarbeiter
5. Datenschutzbeauftragter
6. Verarbeitungsverzeichnis
7. Risikoanalyse / Datenschutzfolgenabschätzung
8. Betroffenenrechte
9. Grenzüberschreitender Datenverkehr
10. Datensicherheit
11. Strafen
12. Datenschutz-Anpassungsgesetz 2018
13. 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:

- **EU-Bezug**
- Unternehmen mit Sitz außerhalb Europas, wenn personenbezogene Daten **von Betroffenen der EU verarbeitet werden**

Wer:

- **JEDER** der Daten nicht nur zu privaten Zwecken verarbeitet!
- Verantwortlicher
- Auftragsverarbeiter

Einheitliche Spielregeln

Rechtmäßigkeit, Treu & Glauben, Transparenz

Zweckbindung

Richtigkeit

Datenminimierung

Speicherbegrenzung

Integrität und Vertraulichkeit

Rechenschaft

Auftragsverarbeiter

- Verarbeitung erfolgt **im Auftrag** eines Verantwortlichen
- **haftet** wie der Verantwortliche für Nichteinhaltung von Bestimmungen
- **keine Sub-Auftragsverarbeiter** ohne Zustimmung des Verantwortlichen
- Verpflichtung zur Implementierung von **Sicherheitsmaßnahmen**
- technische und organisatorische **Unterstützung** des Verantwortlichen
- Pflicht zur Führung eines **Verzeichnis von Verarbeitungstätigkeiten** (**Achtung**: für sich selbst und Verantwortlichen)

Auftragsverarbeiter

- Verpflichtung zur **Risikoabschätzung**
- ggf Verpflichtung zur Benennung eines **Datenschutzbeauftragten**
- Warnpflicht ggü Verantwortlichem
- schriftlicher (/elektronischer) **Vertrag** mit Verantwortlichem
- **Muster**:
  - ✓ **wko.at/datenschutz:** https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html https://www.dsb.gv.at/dokumente (bereits DSGVO-konform)
  - ✓ **Datenschutzbehörde**: https://www.dsb.gv.at/dokumente (Dienstleistervertrag nach § 10 DSG 2000, noch nicht adaptiert)

Datenschutzbeauftragter

- Verpflichtung sowohl für **Verantwortlichen** als auch **Auftragsverarbeiter**
- 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**

Datenschutzbeauftragter

- keine spezielle Haftung angeordnet
- Kenntnisse, praktische Erfahrung im Datenschutz
- handelt unabhängig und weisungsfrei
- Mitarbeiter/ freier Mitarbeiter/ Dienstleister
- kein Interessenkonflikt mit andern Aufgaben
- Einbindung im Betrieb
- Unterstützung durchs Unternehmen
- Ansprechpartner/ Schnittstelle
- Verpflichtung zur Geheimhaltung

Datenschutzbeauftragter

- **Aufgaben:**
  - **Unterrichtung** und Beratung
  - **Überwachung** der Einhaltung datenschutzrechtlicher Verpflichtungen (einschließlich Kontrolle der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter)
  - **Beratung** im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung auf Anfrage
  - **Zusammenarbeit** mit der Aufsichtsbehörde
  - **Anlaufstelle** für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen

Verarbeitungsverzeichnis

- Aufzeichnungspflicht / Protokollierungspflicht
- Pflicht für Verantwortlichen und Auftragsverarbeiter
- Inhalt äußerst weitreichend (zB Kontaktdaten, Datenkategorien, Löschfristen,…)
- Aufzeichnungen schriftlich oder elektronisch

✓ **Muster** unter www.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**

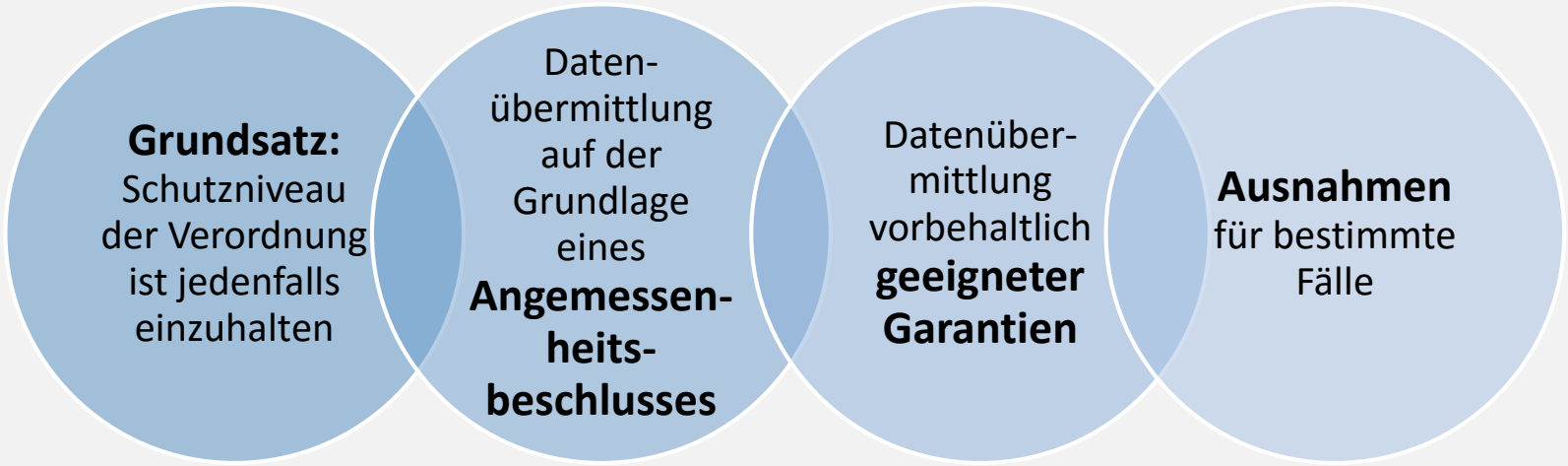
Verarbeitungsverzeichnis

- **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**

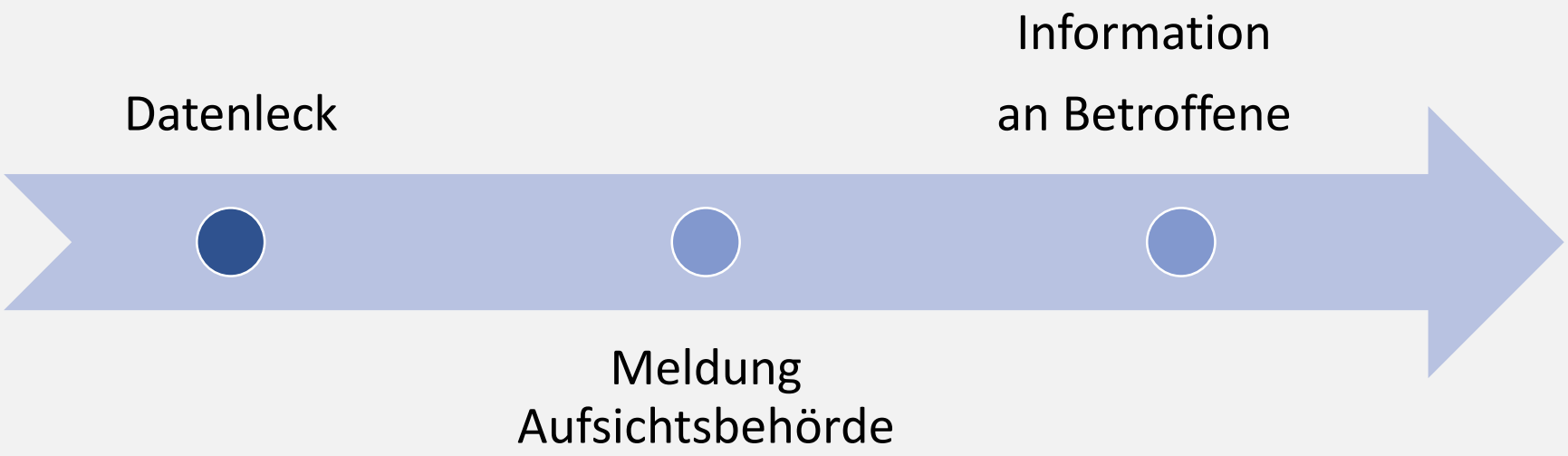
Betroffenenrechte

- Auskunft
- Richtigstellung
- Löschung / Mitteilungspflicht
- Widerspruch
- data portability
- Einschränkung
- Information

Grenzüberschreitender Datenverkehr



Datensicherheit



Datensicherheit

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

Art, Umfang, Umstände, Zweck der Verarbeitung

Eintrittswahrscheinlichkeit & Schwere der Risiken

Stand der technischen Möglichkeiten

Implementierungs-kosten

Strafen

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

- Beschwerde
- Schadenersatz
- Wettbewerbsrecht

Datenschutz-Anpassungsgesetz 2018

- **Grundrecht** auf Datenschutz bleibt
- **Berichtigung oder Löschung** von automationsunterstützt verarbeiteten personenbezogenen Daten nur zu einem gewissen Zeitpunkt möglich
- **Altersgrenze** für die Einwilligung eines Kindes bei Angebot von Diensten der Informationsgesellschaft auf 14. Lebensjahr fixiert
- Möglichkeiten der Verarbeitung **strafrechtlich relevanter Daten**
- **Strafen**:
  - Verwaltungsstrafbestimmungen bis zu EUR 50.000
  - Verfall von Datenträgern, Programmen und Bildübertragungs- und Bildaufzeichnungsgeräten
  - Freiheitsstrafe bis zu einem Jahr oder eine Geldstrafe bis zu 720 Tagessätzen verhängen, wenn Datenverarbeitung in Gewinn- oder Schädigungsabsicht

Datenschutz-Anpassungsgesetz 2018

- **Datengeheimnis =** Geheimhaltungsverpflichtung für Verantwortliche, AV und Mitarbeiter betreffend Daten, die aufgrund der Beschäftigung anvertraut oder zugänglich wurden, soweit kein rechtlich zulässiger Grund für eine Übermittlung besteht
- **Datenverarbeitungsregister**
  - zu Archivzwecken bis zum 31.12.2019, keine Standard- und Musteranwendungsverordnung mehr
  - „Black und White-List“ zur Datenschutz-Folgenabschätzung
  - DVR ist exportierbar
- **Bildverarbeitung**
  - geeignete Datensicherheitsmaßnahmen
  - Protokollierung (außer Echtzeit)
  - nach 72h löschen
  - Kennzeichnung (inkl Nennung des Verantwortlichen)

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
- www.it-safe.at

Vielen Dank für Ihre Aufmerksamkeit.