HERZLICH WILLKOMMEN

zur DSGVO-Veranstaltung für Versicherungsagenten

Montag, 11. Juni 2018

ALLES UNTERNEHMEN.

WKO VA
WIRTSCHAFTSKAMMER OBERÖSTERREICH
Die Versicherungsagenten

VABELHAFT KOMPETENT!
Meine Versicherungs-Agentur.

Ihre Ansprechpartner

KommR Martin Kirchmayr
Obmann

DI Bernadette Hinterdorfer
Geschäftsführerin

Anna Rosenauer
Assistentin

- Wir sind bei Fragen gerne für Sie da!
  Ihr Landesgremium OÖ der Handelsagenten

VABELHAFT KOMPETENT!
Meine Versicherungs-Agentur.

SAVE THE DATE

TOP-VA Gala am **Donnerstag, 22. November 2018**

DSGVO für Versicherungsagenten

- **Rechtsanwalt Dr. Thomas Schweiger, LL.M.**
- **Erik Rusek**

VACE
IT & SECURITY SERVICES

DATENSCHUTZ

in der **Praxis**

dataprotect
it-recht

Datenschutz Grundverordnung EU-DSGVO

Für welche Unternehmen ist die Europäische Datenschutz-Grundverordnung gültig?

- Es gelten grundsätzlich **alle Pflichten** der EU-DSGVO für **alle Unternehmen**!
- Alle Regeln sowie der **Haftungsrahmen** gelten gleichermaßen für alle Unternehmensgrößen!
- Die Ausnahme für den Entfall des „Verzeichnis der Verarbeitungstätigkeiten“ bei **Unternehmen unter 250 Mitarbeitern** gilt nur dann, wenn die Verarbeitung von personenbezogenen Daten nur **gelegentlich** geschieht.
- **Sonstige Verpflichtungen** sind zu erfüllen (Infopflicht, Betroffenenrechte …)

VACE
IT & SECURITY SERVICES

DSGVO im Überblick

Grundrecht für EU Bürger

Die Europäische Union verankert den Schutz, **natürlicher Personen** betreffende, personenbezogene Daten auf **Grundrechtsebene**

EU-weites Datenschutzrecht

Die Verordnung ist der Versuch alle 28 bestehenden, nationalen Gesetze zu vereinheitlichen – auf Grund der **Öffnungsklauseln** unzureichend

Rechtmäßigkeit und Zweckbindung

Personenbezogene Daten natürlicher Personen dürfen nur zu definierten Zwecken verarbeitet werden. Dabei ist die Rechtmäßigkeit der Verarbeitung sicherzustellen.

Beweislastumkehr

Der Verantwortliche muss die Rechtskonformität seiner Datenverarbeitung nachweisen.

dataprotect
it-recht

Was sind personenbezogene Daten?

Daten mit denen eine Person identifizierbar ist

Name, Geburtsdatum, Geburtsort, Anschrift, Beruf, Staatsangehörigkeit, Geschlecht, Größe, Gewicht, Haar- und Augenfarbe, Kleidergröße, Familienstatus, wirtschaftliche Lage, Vorlieben und Freizeitverhalten, Standortdaten, Lebenslauf, Kontaktdaten (wie Telefonnummer, Email), usw.

Daten die einer identifizierten Person zugeordnet sind

Polizze, Schadensmeldungen, usw.

Sonderfall: besondere Kategorien personenbezogener Daten:

rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** (Verletzungen bei Unfall, Krankengeschichte, SVNR) oder Daten zum Sexualleben oder der sexuellen Orientierung

Es betrifft nur Daten natürlicher Personen, die elektronisch oder in analoger, strukturierter Form verarbeitet werden!

Wann dürfen personenbezogene Daten verarbeitet werden

Zweckbindung

- Zweckfestlegung & Zweckbindung

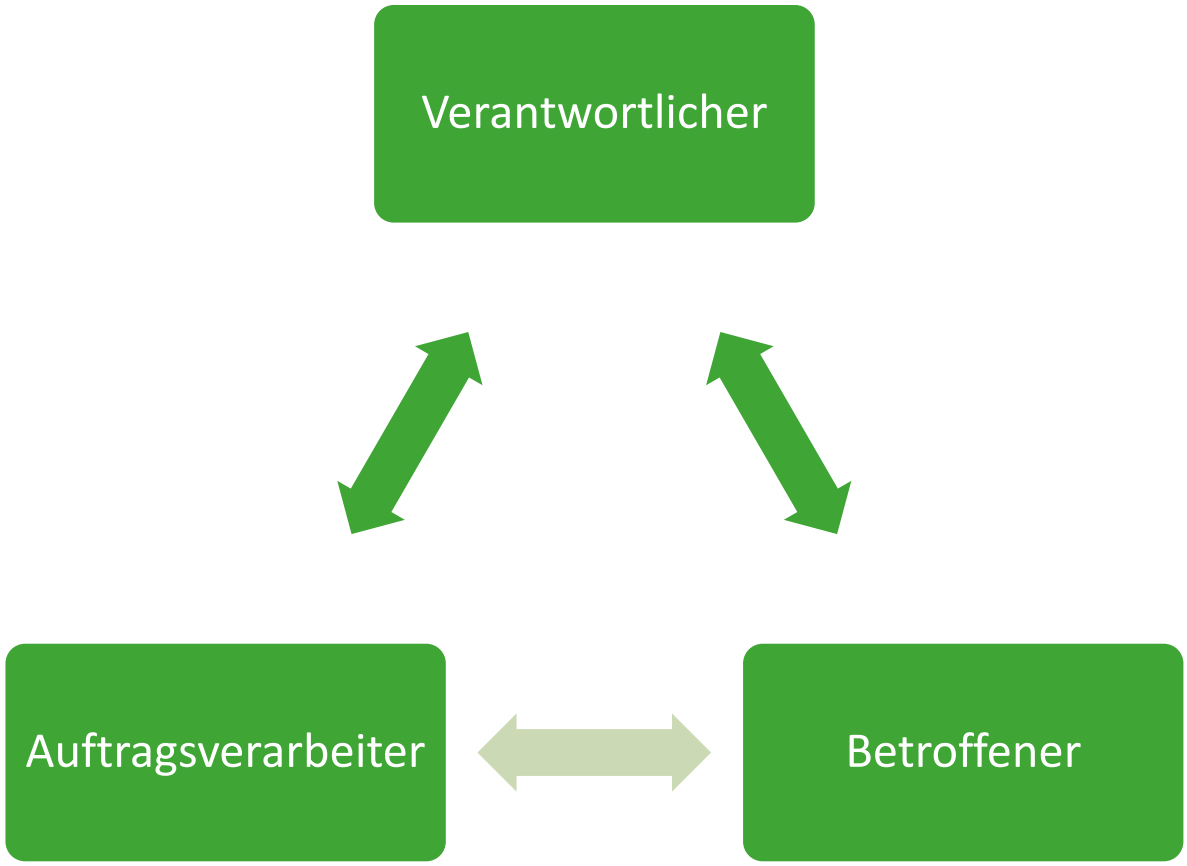
Rechtmäßigkeit (schlichte Daten)

- Vertrag/Vertragsanbahnung
- rechtliche/gesetzliche Verpflichtung
- Lebenswichtiges Interesse
- berechtigtes Interesse der Organisation/eines Dritten
- Einwilligung
- Öffentliches Interesse / Öffentliche Gewalt

Relevante Aspekte

- Freiwilligkeit & Nachweisbarkeit der Einwilligung
- Kopplungsverbot bei Einwilligung
- Widerspruchsmöglichkeit bei berechtigtem Interesse
- ausdrückliche Einwilligung bei Gesundheitsdaten

Rollen im „Datenschutz“



Privacy by Design / Default

Privacy by Design

Datenschutzvorschriften bereits bei der Entwicklung neuer Applikationen/Prozesse/ Technologien berücksichtigen

- **Datensparsamkeit** nur jene Daten welche dem Zweck entsprechend erhoben wurden
- **Löschfristen** automatische Löschung von Personendaten und Verifizierung ihrer Aktualität
- **Datenkorrekturen** entsprechend dem Recht auf Richtigstellung
- **Auskunftspflicht** Benachrichtigung welche personenbezogenen Daten sind gespeichert?

Privacy by Default

- datenschutzfreundliche Voreinstellungen

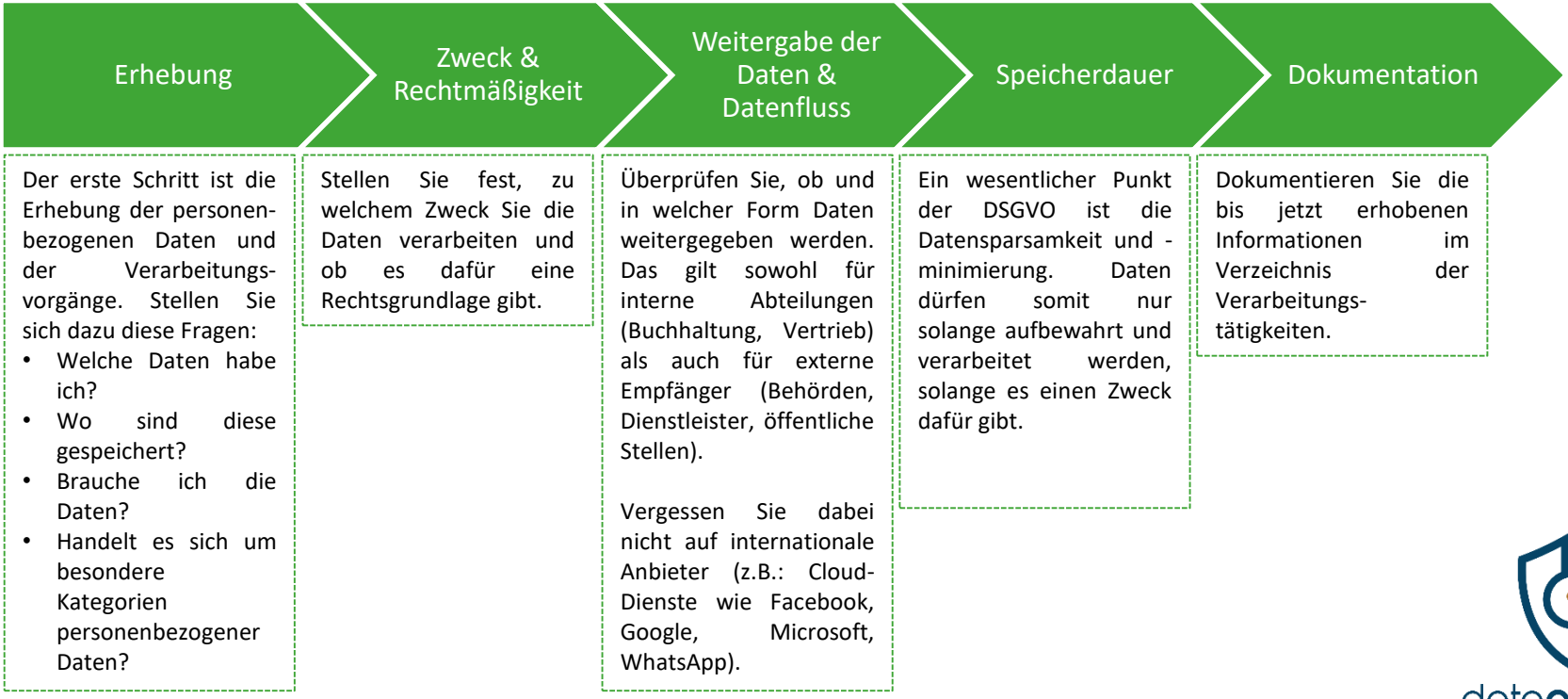
Datenschutz in der Praxis

Wesentliche Aufgaben

Verzeichnis der Verarbeitungstätigkeiten	Betroffenenrechte
Technische und Organisatorische Maßnahmen (TOMs)	Datenschutzbeauftragter & Data-Breach

Ablauf

Wie gehe ich die DSGVO an?

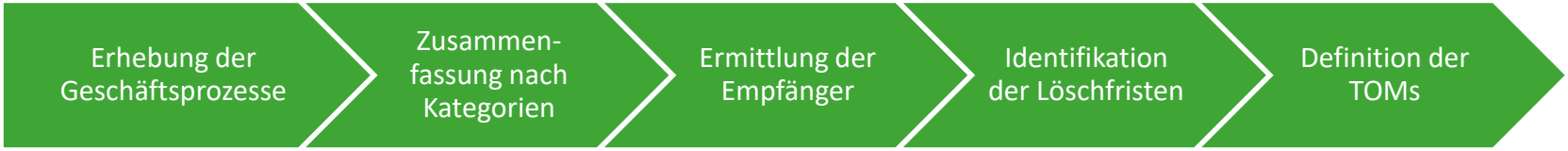


Verzeichnis der Verarbeitungstätigkeiten

Verzeichnis der Verarbeitungstätigkeiten

Jeder „Verantwortliche“ führt ein Verzeichnis aller Verarbeitungstätigkeiten:

- **Name** und **Kontaktdaten** des Verantwortlichen
- **Zweck** der Verarbeitung
- Kategorien **betroffener Personen und Daten**
- Kategorien der **Empfänger**
- Übermittlung personenbezogener Daten in ein **Drittland**
- **Fristen** für die Löschung der Daten
- Beschreibung der getroffenen **technischen und organisatorischen Maßnahmen**



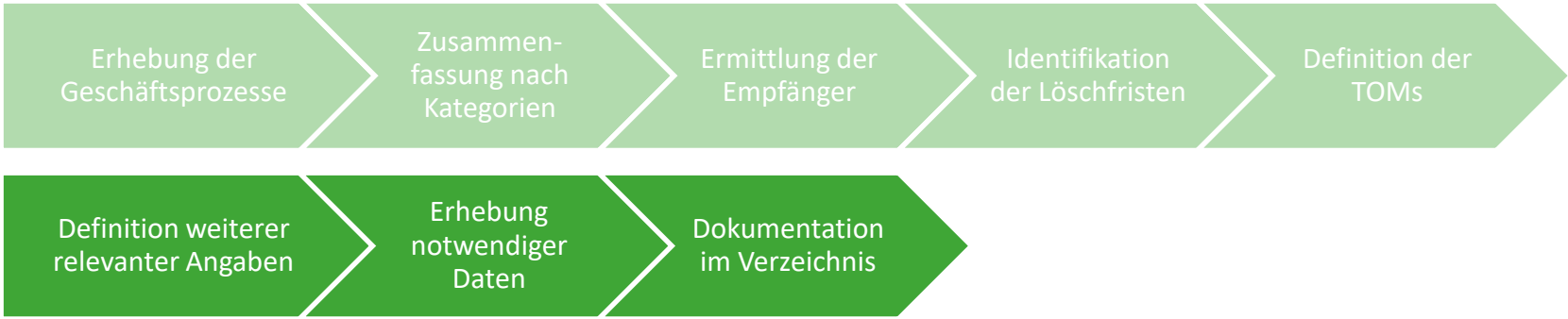
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html

Verzeichnis der Verarbeitungstätigkeiten - Erweiterung

Verzeichnis der Verarbeitungstätigkeiten

Das Verzeichnis kann darüber hinaus auch freiwillige Angaben enthalten.

- **Datenanwendungen**, die bei der Verarbeitung eine Rollen spielen
- **Datenherkunft**
- **Rechtliche Basis**, auf der die Datenverarbeitung erfolgt
- **Auftragsverarbeiter** und **gemeinsame Datenverarbeitung**



https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html

Informationspflicht & Betroffenenrechte

Rechte der betroffenen Personen

Notwendigkeit zur Planung für die Abarbeitung

Identifikation

Personenbezogene Daten im Unternehmen erheben
Verarbeitungsvorgänge identifizieren

Planung

Ablauf der Betroffenenrechte und Verantwortlichkeiten planen
Umsetzung der Maßnahmen und Information an Mitarbeiter

Test

Durchführung eines Plan-Spiels „Betroffenenrecht“

Betroffenenrechte - Dokumentation

Dokumentation der Betroffenenrechte

Autor		Klassifikation	
Organisation	Musterfirma GmbH	Version	0.9
Datum	15.03.2018	Kontaktdaten	

Nr.	Datum der Inanspruchnahme	Identität des Betroffenen	Kategorie der Personen	Art des Ansuchens	Anmerkung	Identitätsfeststellung	Übermittlung	Bearbeitender MA
1	12.03.2018	Max Mustermann, 01.01.2000	Bewerber	Auskunft	Daten wurden aus Excel kopiert und in eigener Datei übermittelt	FS: 696969	verschlüsseltes ZIP; Passwort via SMS	ERU

Technische und Organisatorische Maßnahmen

Verfügbarkeit, Integrität & Vertraulichkeit	Sicherheit am Stand der Technik
Privacy by Design & Privacy by Default	Dokumentation

Technische und Organisatorische Maßnahmen - Beispiele

VERTRAULICHKEIT

- Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, der unbefugten Benutzung und Manipulation (**Zutritts-, Zugangs- und Zugriffskontrolle**)
- Gesonderte Aufbewahrung und Verarbeitung von personenbezogenen Daten (**Pseudonymisierung**)
- Sichere Aufbewahrung und Übermittlung von personenbezogenen Daten (**Verschlüsselung**)

INTEGRITÄT

- Kein unbefugtes Manipulieren oder Entfernen bei elektronischer Übertragung oder Transport (**Weitergabekontrolle**)
- Verhinderung und Erkennung von unbefugten Eingaben (**Eingabekontrolle**)

VERFÜGBARKEIT UND BELASTBARKEIT

- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (**Verfügbarkeit & Wiederherstellbarkeit**)

VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen (**Rechenschaftsverpflichtung**)
- Incident-Response-Management und Notfallplan (**Meldepflicht**)
- Kontrolle bei den Auftragsverarbeitern (**Rechenschaftsverpflichtung**)

Auftragsverarbeiter

Beschäftigung von Dienstleistern im Zuge der Verarbeitung personenbezogener Daten

Identifikation

- Identifizieren Sie Ihre Auftragsverarbeiter
- Als Basis dienen die Verarbeitungsvorgänge und eine Liste von Lieferanten

Vertragliche Regelung

- Ablauf der Betroffenenrechte und Verantwortlichkeiten planen
- Umsetzung der Maßnahmen und Information an Mitarbeiter

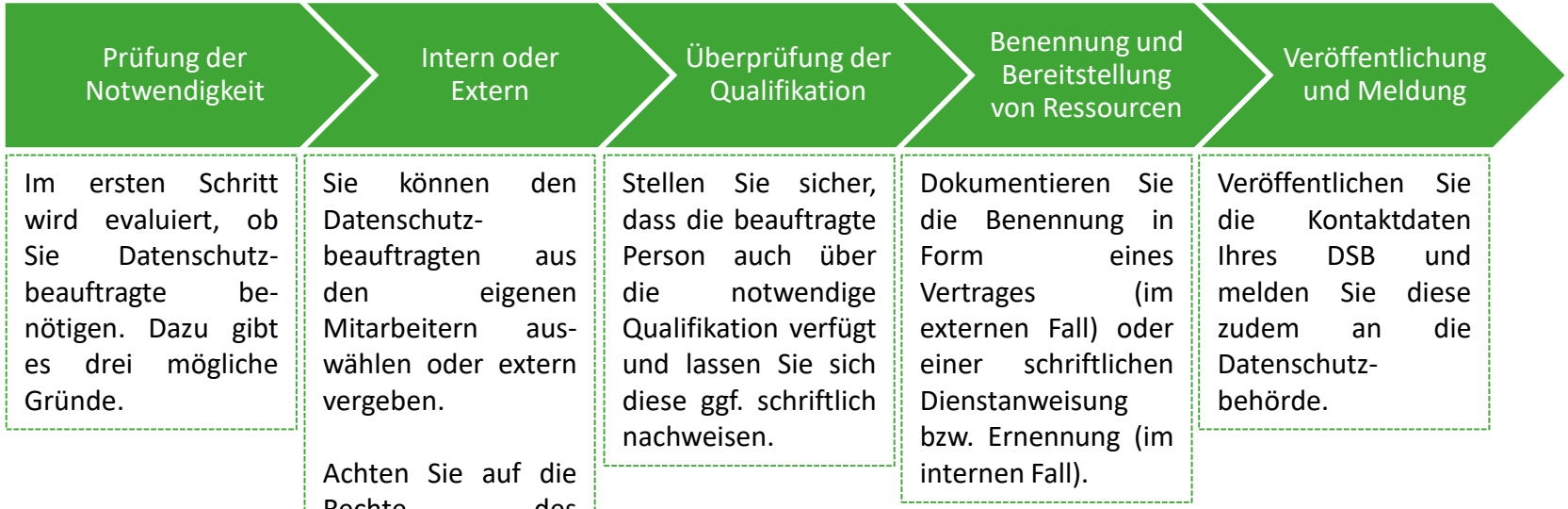
Software-Hersteller sind auch von der DSGVO betroffen.

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html

VACE
IT & SECURITY SERVICES

Datenschutzbeauftragte

Muss ich einen Datenschutzbeauftragten benennen?



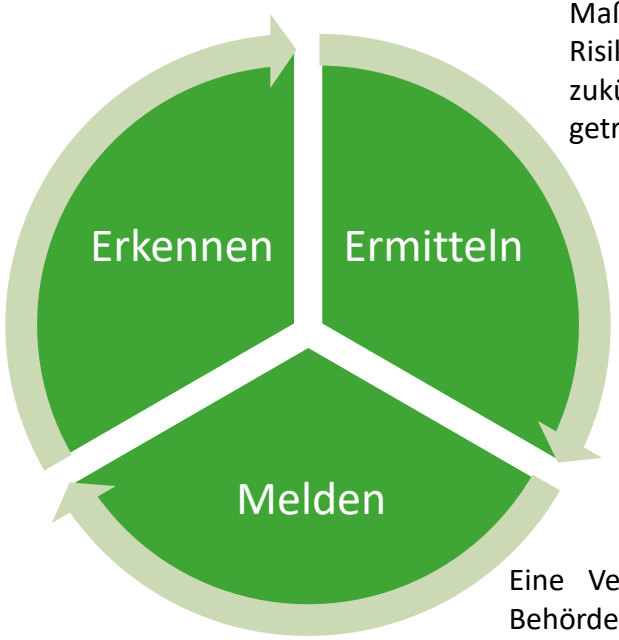
dataprotect
it-recht

Verletzung des Schutzes personenbezogener Daten

Sicherheitsvorfall mit personenbezogenen Daten

Bearbeitung eines Data-Breach

Die Erkennung eines Sicherheitsvorfalls, in den personenbezogene Daten involviert sind, ist der Ausgangspunkt für die Zeitdauer bis zur notwendigen Meldung.



Die Analyse des Vorfalls liefert Maßnahmen, die zur Eindämmung des Risikos sowie zur Steigerung der zukünftigen Sicherheit der Daten getroffen werden sollten.

Eine Verletzung des Datenschutzes ist an die Behörde zu melden. Bei einem hohen Risiko für die Rechte und Freiheiten der Betroffenen, sind diese ebenfalls zu informieren.

Meldung der Verletzung

Name und Kontaktdaten des **Verantwortlichen**
Name und Anschrift:
E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.) des **Datenschutzbeauftragten / Datenschutz-Koordinators**
Name und Anschrift:
E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:
Kategorien und ungefähre Zahl der **betroffenen Personen**:
betroffene Kategorien und ungefähre Zahl der **personenbezogenen Datensätze:**

Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:
ggf **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

Datum und Uhrzeit des Vorfalls:
Begründung, falls die Meldung länger als 72h nach dem Vorfall erfolgte:

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html

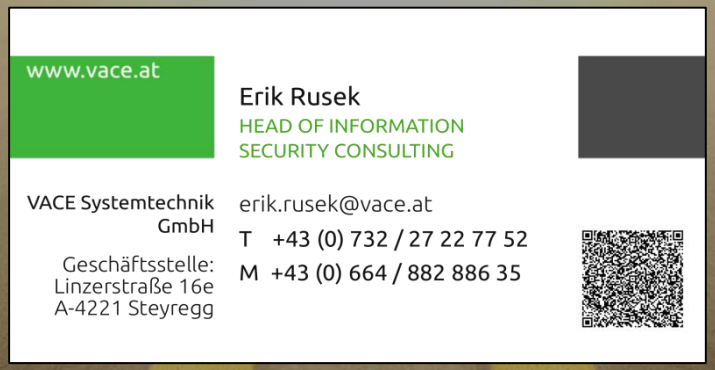
Weitere Maßnahmen & Tipps

BEZEICHNUNG	ERKLÄRUNG
Schulung & Sensibilisierung	Die mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiter sollten regelmäßig hinsichtlich derer Pflichten und Verantwortung geschult werden.
Datenübermittlungen	Identifizieren Sie Verarbeitungsvorgänge, im Zuge derer personenbezogene Daten an Organisationen in Drittländern übermittelt werden. Prüfen Sie die Rechtsgrundlage der Übermittlung gesondert.
Dokumentation	Dokumentieren Sie alle Tätigkeiten im Zusammenhang mit personenbezogenen Daten, um den Nachweispflichten der EU-DSGVO nachkommen zu können.
Transparenz	Führen Sie die Verarbeitung personenbezogener Daten in transparenter Art und Weise durch und informieren Sie die betroffenen darüber (**Informationspflicht**).
Zweckbindung	Stellen Sie sicher, dass die Verarbeitungsvorgänge in Ihrer Organisation immer auf Basis eines rechtmäßigen Zweckes durchgeführt werden und achten Sie auf Koppelungen.
Hinweispflichten	Erfüllen Sie Ihre Hinweispflichten und veröffentlichen Sie die Betroffenenrechte auf der Webseite. Integrieren Sie diese zudem in Ihre Vereinbarungen mit natürlichen Personen.
Prüfung der Wirksamkeit	Stellen Sie durch laufende Prüfungen sicher, dass Ihre Datenschutzmaßnahmen sinn- und wirkungsvoll sind. Eventuelle Verbesserungen oder Erweiterungen sollten umgesetzt werden.

Quellen & Musterformulierungen

BEZEICHNUNG	ERKLÄRUNG	QUELLE
Verzeichnis der Verarbeitungstätigkeiten	Vorausgefülltes Muster für das Verzeichnis der Verarbeitungstätigkeiten	https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html
Auftragsverarbeiter-vereinbarung	Mustervorlage für die gesetzlich notwendige Auftragsverarbeitervereinbarung.	https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html
IT-Safe	Online-Ratgeber zur Evaluierung der IT-Sicherheit und Tipps zur Umsetzung.	https://itsafe.wkoratgeber.at/
IT-Sicherheitshandbuch	Ein Informationssicherheitshandbuch für KMUs zur Dokumentation von Maßnahmen im Unternehmen.	https://www.wko.at/site/it-safe/sicherheitshandbuch.html
DSGVO Umsetzung	Unterstützende Links und Ratgeber zur generellen Umsetzung der DSGVO.	https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unterstuetzung-zur-Umsetzung-der-DSGVO.html

VACE
IT & SECURITY SERVICES



Das Angebot an Dienstleistern für Human Resources, Engineering, Training und Education, Netzwerk- und IT-Security ist groß,…

…wir vereinen all diese Kompetenzen zum einzigartigen Nutzen für Sie!

Geldwäsche Terrorismusbekämpfung

- **Mag. Dr. Roland Koppler, MBA**

GELDWÄSCHE TERRORISMUSBEKÄMPFUNG WIEREG

SORGFALTSPFLICHTEN DES VERSICHERUNGSAGENTEN

Roadshow 2018

Linz – Braunau – Gmunden - Steyr

Anforderungen an den Versicherungsagenten

- Rechtsgrundlage(n)
- Zielsetzung und Grundlagen
- Adressatenkreis (persönlicher / sachlicher Geltungsbereich)
- Sorgfaltspflichten
- Register der wirtschaftlichen Eigentümer
- Sanktionen

Rechtsgrundlagen

- §§ 365m – 365z , 366b GewO (BGBl I 95/2017, Geldwäsche-Novelle)
  - In Kraft seit 18. Juli 2017 (!!)
  - Umsetzung der 4. GW-RL ((EU)RL 2015/849)
- WiEReG (BGBl I 136/2017)
  - Einsichtsmöglichkeit seit Mai 2018
  - Meldefristerstreckung auf 16. 8. 2018

Zielsetzung und Grundlagen (1)

- Ziel / Zweck
  - Hintanhaltung der Nutzung des Finazsystems zu Geldwäsche und Terrorismusbekämpfung
  - Prävention, Aufdeckung und Untersuchung von möglicher Geldwäsche
- Geldwäsche

  => Verschleierung der Herkunft von Geld aus illegalen Tätigkeiten wie Korruption, Bestechung, Raub, Erpressung, Drogen- und Waffenhandel oder Steuerhinterziehung (!!!!)

Zielsetzung und Grundlagen (2)

- Geldwäschemeldestelle
  => Einheit im BM für Inneres
- Politisch exponierte Person („PEP“)
  - Hochrangige Politiker
    - Staats-, Regierungschefs, Minister , Staatssekretäre
    - Abgeordnete und Mitglieder von Gesetzgebungsorganen (Nationalrat, Bundesrat, Landtage)
    - Mitglieder der Führungsgremien von politischen Parteien
  - Oberste Richter
  - Vorstände und Aufsichtsräte von staatseigener Betriebe
- Familienmitglieder und „ bekanntermaßen nahestehende Personen“

Geltungsbereich

- Persönlicher Geltungsbereich (u.a)
  - Versicherungsvermittler
    - Makler
    - Echte Mehrfachagenten
    - Exklusivagenten **mit** „Inkasso und Exkasso“
  - Ausnahme für Exklusivagenten **ohne** „In- und Exkasso“ und „Nebengewerbliche (§137a GewO)“ (§ 365m Abs 2 Zif 4 GewO)
- Sachlicher Geltungsbereich
  - Lebensversicherungen mit Anlagezweck

Sorgfaltspflichten

- Unternehmenseigenes Risikoprofil (365n1Abs 1 GewO)
- GW-Policy (365n1Abs 3 und 4 GewO)
- Info- und Feststellungspflichten nach dem KYC – Prinzip
  - Identitätsfeststellungspflicht
    - Kunde / Vertragspartner
    - Bezugsberechtigter
    - Treugeber
    - Wirtschaftlicher Eigentümer
- Dokumentations- und Archivierungspflicht

Unternehmenseigenes Risikoprofil

- **§ 365n1.** (1) Der Gewerbetreibende **hat** angemessene Schritte zu unternehmen, um die **für ihn bestehenden Risiken der Geldwäsche und Terrorismusfinanzierung** unter Berücksichtigung von Risikofaktoren, einschließlich in Bezug auf seine Kunden, Länder oder geografische Gebiete, Produkte, Dienstleistungen, Transaktionen oder Vertriebskanäle **zu ermitteln und zu bewerten**. ……
- (2) Die in Abs. 1 genannten Risikobewertungen sind **nachvollziehbar aufzuzeichnen**, auf aktuellem Stand **evident zu halten** und der **Behörde** auf Anfrage in einem allgemein gebräuchlichen Format **zur Verfügung zu stellen**. ……

Unternehmenseigenes Risikoprofil

- **Risikofaktoren**
  - standortbezogenes Risiko
  - kundenbezogenes, geografisches Risiko
  - dienstleistungsbezogen (Produktart)
  - Vertriebskanalrisiko
- Ermittlung und Bewertung
- Dokumentation
  - nachvollziehbare Aufzeichnung
  - allgemein gebräuchliches Format
  - laufende Aktualisierung und Evidenzhaltung

Unternehmenseigenes Risikoprofil

- **Hilfestellung durch Risikoraster**
  (Excel-Datei lt WKO-Muster)
  - **gilt als allgemein gebräuchliches Format**
  - **von Behörden anerkannt, aber auch gefordert (!!!)**
  - **Best Practice - Standard für Branche**
- **Ausfüllhilfe**

4. ML-Dir. Art. 8 + Anhang II und III Risikofaktor	Versicherungsvermittler, wenn sie Lebensversicherungen oder andere Produkte mit Anlagezweck vermitteln (Versicherungsagent,	Risiko	Zutreffendes Bitte mit **X** markieren
1. Standort,	ländliche Gebiete	1	
	Außenbezirke von Städten	2	
	Geschäftsstraßen	3	
	exquisite Lage (zB Innenstadt, Fußgängerzone)	4	x
2. Vertriebskanalrisiko	Betrieb mit einem Standort	1	
	Filialnetz vorhanden (mehrere Standorte)	2	x
	im gesamten Unternehmen weniger als 5 Mitarbeiter	1	
	im gesamten Unternehmen 5-10 Mitarbeiter	2	
	im gesamten Unternehmen mehr als 10 Mitarbeiter	3	x
3. Kunden; kundenbezogen; kundenbezogenes geographisches Risiko	mehrheitlich Lebensversicherungen Produkte mit Anlagezweck mit Kunden/Firmen aus Inland/öffentliche Verwaltungen oder öffentliche Unternehmen, börsennotierte Unternehmen	1	
	mehrheitlich Lebensversicherungen Produkte mit Anlagezweck mit Kunden/Firmen aus EU-Raum	2	
	mehrheitlich Lebensversicherungen Produkte mit Anlagezweck mit Kunden/Firmen aus Drittländern	3	
	Lebensversicherungen Produkte mit Anlagezweck mit PEPs/Kunden aus Hochrisikoländern/mehrheitlich juristische Personen oder unklare Eigentumsstruktur	4	x
4. Dienstleistungen; dienstleistungsbezogenes Risiko	ausschließlich klassische Lebensversicherungen mit Jahresprämie unter 1000€ oder Verträge ohne Rückkaufsklausel, die nicht als Sicherheit für Darlehen dienen können	1	
	mehrheitlich ("51%-99%") klassische Lebensversicherungen mit Jahresprämie unter 1000€ oder Verträge ohne Rückkaufsklausel, die nicht als Sicherheit für Darlehen dienen können	2	
	25% - 50% klassische Lebensversicherungen mit Jahresprämie unter 1000€ oder Verträge ohne Rückkaufsklausel, die nicht als Sicherheit für Darlehen dienen können	3	
	unter 25% klassische Lebensversicherungen mit Jahresprämie unter 1000€ oder Verträge ohne Rückkaufsklausel, die nicht als Sicherheit für Darlehen dienen können	4	x
Summe		17	5
Durchschnitt (Summe markierter Zahlen in risk - Spalte/Anzahl markierter Zahlen in Risiko - Spalte) - bei jedem Risikofaktor ist **mindestens eine Zahl** zu markieren		**3,4**	Durchschnitt berechnet sich nach Eingabe der "X" automatisch

GW – Policy (1)

- § 365n1 (3) Der Gewerbetreibende **hat über Strategien, Kontrollen und Verfahren** zur wirksamen Minderung und Steuerung der auf Unionsebene, auf mitgliedstaatlicher Ebene und bei sich selbst ermittelten Risiken von Geldwäsche und Terrorismusfinanzierung **zu verfügen**. ,,,

  ……………………………………………………

  in einem angemessenen Verhältnis nach Art und Größe des Unternehmens.

GW – Policy (2)

§ 365n1 (4) Die in Abs. 3 genannten Strategien, Kontrollen und Verfahren umfassen

- 1. die Ausarbeitung interner Grundsätze, Kontrollen und Verfahren, unter anderem in Bezug auf eine vorbildliche Risikomanagementpraxis, Sorgfaltspflichten gegenüber Kunden ……., Verdachtsmeldungen, Aufbewahrung von Unterlagen, interne Kontrolle, Einhaltung der einschlägigen Vorschriften …… und regelmäßige Überprüfung der Arbeitsausführungen durch Mitarbeiter;
- 2. eine unabhängige Prüfung, ……, sofern dies im Hinblick auf Art und Umfang der Geschäftstätigkeit angemessen ist

GW – Policy (3)

- Verpflichtung zur Erstellung einer GW-Policy
  - auf Basis des Risikoprofils lt. Raster
  - Verhältnismäßigkeitsprinzip
- Inhalt und Zweck:
  - Dokumentation
  - Strategien, Kontrollen, Verfahren
  - Interne organisatorische Regeln
  - Verdachtsmeldungen
  - Schulungsmaßnahmen

Sorgfaltspflichten
im
Geschäftsverkehr

- Grundsatz des KYC-Prinzips
- Vereinfachte Sorgfaltspflichten
  - in Ausnahmefällen, wenn geringes Risiko
  - Eigeneinschätzung
  - Dokumentation der Gründe für diese Einschätzung

Sorgfaltspflichten im Geschäftsverkehr

- Erhöhte Sorgfaltspflichten
  - Geschäftsbeziehung zu PEPs, deren Familienmitglieder und „bekanntermaßen nahestehenden Personen“
  - Zustimmung der Führungsebene
  - Prüfung der Mittelherkunft und Transaktionen
  - Verstärkte fortlaufende Überwachung

KYC – Prinzip (1)

- Wann:
  - Bei bzw vor jeder Geschäftsbegründung
  - Bei Zweifel an Echtheit oder Angemessenheit der Kundenidentifikationsdaten
  - Bei Verdacht bezüglich GW oder Terrorismusfinanzierung
  - Auch bei bestehenden Kunden auf risikobaiserter Grundlage

KYC – Prinzip (2)

- Gegenstand und Umfang
  - Feststellung der Kundenidentität (inkl. BB !!)
  - Feststellung des **wirtschaftlichen Eigentümers (s.u)**
  - Art und Zweck des Geschäfts
  - Laufende Überwachung des Geschäfts inklusive Mittelherkunft (!!!) und Art der Geldtransaktionen
  - Plausibilität des Geschäfts unter Berücksichtigung der Kenntnisse über den Kunden, seine Geschäftstätigkeit und sein Risikoprofil
  - Verdachtsmeldung an Geldwäschestelle

WiEReG (2)

- Begriff des wirtschaftlichen Eigentümers
  - direkter wirtschaftlicher Eigentümer
  - indirekter wirtschaftlicher Eigentümer
  - oberster Rechtsträger
  - Subsidiäre Meldung
- Fallbeispiele
  - https://www.bmf.gv.at/finanzmarkt/register-wirtschaftlicher-eigentuemer/Uebersicht/Fallbeispiele_BMF_2.pdf?6floyf

WiEReG (3)

- direkter wirtschaftlicher Eigentümer

  => natürliche Person , die an einer Gesellschaft mit mehr als 25% beteiligt ist

  => Eigentum, Stimmrecht, Kontrolle, Angehöriger der Führungsebene, Sonstige Weise

WiEReG

- indirekter wirtschaftlicher Eigentümer

=> Variante 1:

natürliche Person übt **Kontrolle** über einen Rechtsträger aus, der seinerseits mit mehr als 25% an der betroffenen Gesellschaft beteiligt ist

=> Variante 2:

natürliche Person übt **Kontrolle** über mehrere Rechtsträger aus, die zusammen mehr als 25 % an der betroffenen Gesellschaft beteiligt sind

WiEReG (4)

- Ab der 2. Beteiligungsebene ist das Vorliegen der Kontrolle für den indirekten wirtschaftlichen Eigentümer erforderlich

- Kontrolle bedeutet
  - mehr als 50% Beteiligung an dem in der 1. Ebene beteiligten Rechtsträger
  - sonstige Kontrolle
    (§ 244 UGB, § 2 WiEReG), Treuhand, ..)

WiEReG (5)

- Oberster Rechtsträger
  - Rechtsträger in einer Beteiligungskette, die von indirekten wirtschaftlichen Eigentümern kontrolliert werden

    sowie

  - Rechtsträger, an denen ein indirekter wirtschaftlicher Eigentümer direkt eine Beteiligung hält, die zusammen mit dem anderen Rechtsträgers(s.o.) das wirtschaftliche Eigentum begründet

WiEReG (6)

- Subsidiäre Meldung
  - wenn keine natürliche Person als wirtschaftlicher Eigentümer existiert bzw nicht festgestellt werden kann
  - dann subsidiär die Mitglieder der obersten Führung
- Pflicht zur Meldung : Geschäftsführung !!
  - Ausgenommen OG / KG mit ausschließlich natürlichen Personen als Gesellschafter

WiEReG (7)

- Ausnahme von der Meldepflicht
  - OG, KG, GmbH, wenn ausschließlich natürliche Personen Gesellschafter sind
    - Meldepflicht jedoch, wenn andere Personen direkt oder indirekt Kontrolle ausüben
- Achte: Meldepflicht daher für GmbH & Co KG

Strafsanktionen
(§366b GewO)

- Bei einfachen Verstößen
  - bis zu 20.000.- EURO

- Bei besonders schwerwiegenden, wiederholten oder systematischen (!!!) Verstößen
  - Öffentliche Bekanntmachung auf Homepage der Behörde („Pranger“ !!)
  - bis zu 5,0 Mio EURO oder 10 % des Jahresumsatzes

Hilfestellung und Service der WKO

https://www.wko.at/branchen/information-consulting/finanzdienstleister/geldwaesche-und-terrorismusfinanzierung.html

DANKE

Mag. Dr. Roland Koppler MBA
r.koppler@ooev.at

Danke für Ihre Aufmerksamkeit!

ALLES UNTERNEHMEN.

WKO
WIRTSCHAFTSKAMMER OBERÖSTERREICH
Die Versicherungsagenten