Datenschutz in der Versicherungsvermittlung

Innsbruck, 25.01.2024

1

Aktuelle Datenschutzlage

Datenschutzrisiko in Zahlen

In Österreich wurden im Jahr 2022

- **1.915 Individualbeschwerden** eingebracht und **6.517** Beschwerden erledigt
- **4.806 Bescheide** aufgrund von Individualbeschwerden
- **133** amtswegige **Prüfverfahren** wurden durchgeführt
- **122 Verwaltungsstrafverfahren** beendet, **63** davon mit Bescheid (=Strafe)

Im Zeitraum von **25.05.2018 bis Januar 2022** wurden in Österreich **3.644 Data Breach Notifications** getätigt.

Im Durchschnitt benötigt ein Unternehmen **287 Tage** um einen Data Breach zu erkennen und einzugrenzen.

Double-Extortion-Ransomware ist eine der größten Gefahren für Unternehmen derzeit. Hierbei werden Daten vor der Verschlüsselung kopiert um eine Lösegeldzahlung der Opfer zu gewährleisten bzw die Daten im Darknet zu verkaufen.

Bußgelder – Ein Auszug

- **EUR 9.500.000,00:** Keine Möglichkeit, datenschutzrechtliche Anfragen per E-Mail zu stellen (Österreich)
- **EUR 4.000.000,00:** Irrtümlicher Versand einer Excel-Datei mit Daten von ca. 6 Tsd. Kunden an 234 Personen (Österreich)
- **EUR 216.550,00:** Unbefugter Zugriff auf Kundendatenbank durch fehlende Schutzmaßnahmen ermöglicht (Ungarn)
- **EUR 200.000,00:** Erfassung sensibler Daten von Mitarbeitern und mangelnde Kooperation mit der Datenschutzbehörde (Frankreich)
- **EUR 20.000,00:** Keine vollständige Auskunftserteilung (Italien)
- **EUR 10.000,00:** Fehlerhafte Übermittlung von Gesundheitsdaten an die E-Mail Adresse eines Dritten (Italien)
- **EUR 3.500,00:** Versand unerwünschter Werbe-E-Mails (Zypern)
- **EUR 3.373,00:** Datenpanne aufgrund von Dienstlaptopdiebstahl (Polen)
- **EUR 1.500,00:** Versenden einer E-Mail ohne Blind Copy Funktion mit Stelleninformationen (Spanien)

Aktuelle Entscheidungen der Datenschutzbehörde

23.03.2023 (GZ: 2023-0.227.168) Verletzung des Rechts auf Auskunft:
Verantwortlicher muss Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form übermitteln („**Genauigkeits- und Verständlichkeitsgebot“**). Er hat der betroffenen Person die Ausübung ihrer Betroffenenrechte zu erleichtern („Erleichterungsgebot“). Er hat auf den Antrag auf Auskunft – grundsätzlich – unverzüglich, in jedem Fall aber innerhalb eines Monats, zu reagieren („**Reaktions- und Beschleunigungsgebot**“).

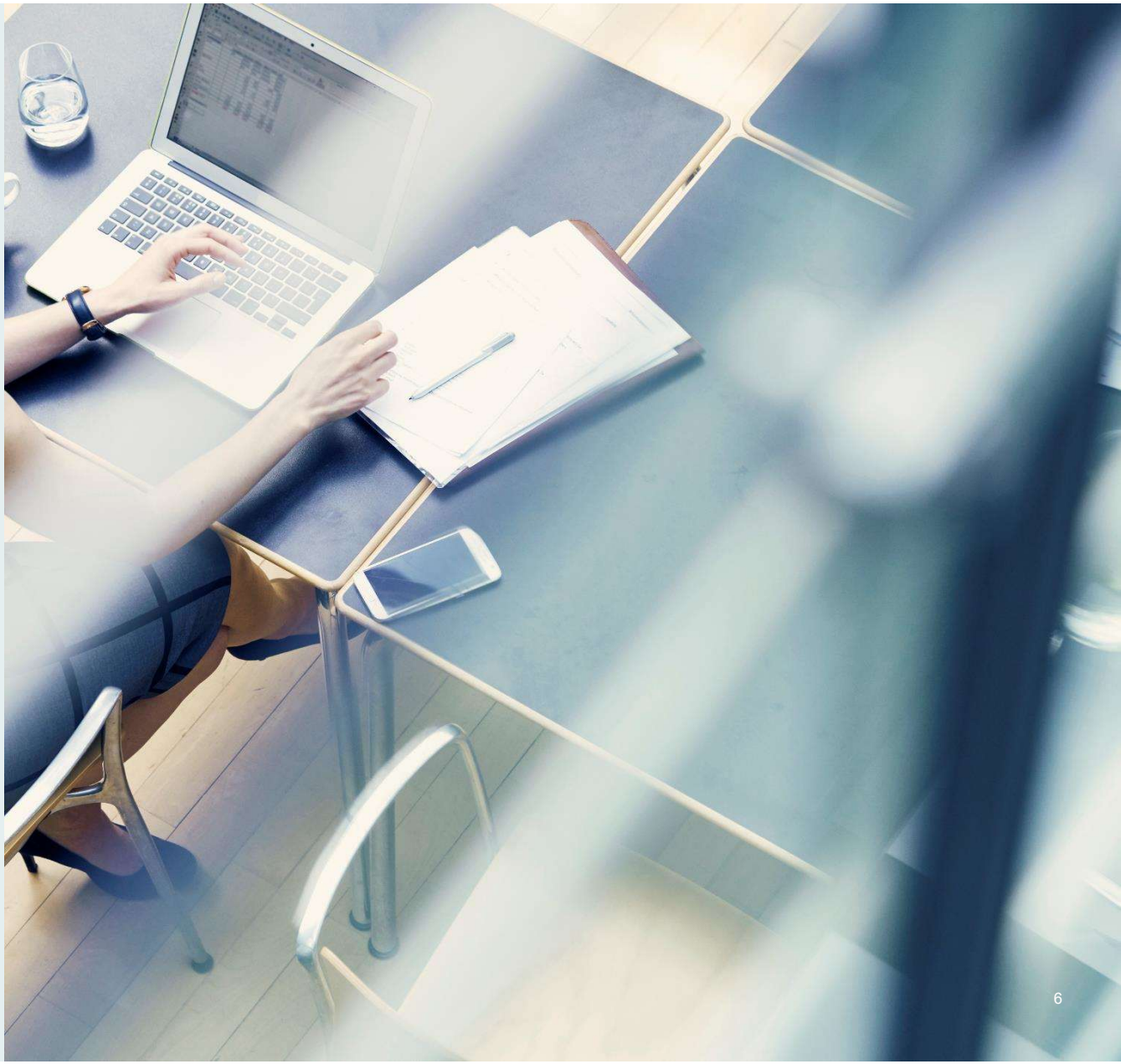
21.02.2023 (GZ: 2023-0.137.735) Unredliche Beschwerdeerhebung:
Eine betroffene Person weist kein tatsächliches Rechtsschutzbedürfnis auf, wenn sie gegen **Bezahlung eines Geldbetrages** von der Erhebung ihres Beschwerderechts vor der Datenschutzbehörde Abstand nehmen würde.

30.01.2023 (GZ: 2023-0.046.014) Nachholung Data Breach Notification (Gesundheitsdaten):
Die Benachrichtigung der betroffenen Person ist nicht nur zur Vermeidung weiterer Verletzung ihrer persönlichen Rechte und Freiheiten erforderlich, sondern hat **auch im Nahhinein zu erfolgen**. Die Benachrichtigung betroffener Personen von der Verletzung hat grundsätzlich unverzüglich zu erfolgen. Die Benachrichtigung innerhalb einer Frist von **zwei Wochen** scheint als angemessen.

04.02.2022 (GZ: 2021-0.347.702) Recht auf Löschen – Rechtsverteidigung:
Beschränkungen des Anspruchs auf Geheimhaltung ist nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig (Interessenabwägung). Ein **zweckmäßiges Prozessvorbringen** gilt als Grundlage für eine **rechtmäßige Datenverarbeitung**. Das (offenkundige) Interesse des Beschwerdeführers die Beschwerdegegnerin an einem Tatsachenvorbringen zu hindern, um deren Prozesserfolg zu schaden, begründet kein schutzwürdiges Geheimhaltungsinteresse.

2

Datenschutz für Versicherungsvermittler



Verhaltensregeln – Code of Conduct (CoC)

Verhaltensregeln

Versicherungsmakler und Berater in Versicherungsangelegenheiten

Navigation

Code of Conduct bringt mehr Rechtssicherheit für Versicherungsmakler

Datenschutzbehörde genehmigt datenschutzrechtliche Verhaltensregeln

Die EU-Datenschutzgrundverordnung (DSGVO) brachte für Versicherungsmakler und Berater in Versicherungsangelegenheiten viele neue Herausforderungen mit sich. Die neuen Datenschutz-Regularien waren für die Anwender teils auch mit großer Rechtsunsicherheit verbunden.

Agiert etwa ein Versicherungsmakler im Rahmen seiner Agenden als datenschutzrechtlich Verantwortlicher oder als Auftragsverarbeiter? Auf welcher Basis werden personenbezogene Daten, sensible Daten von einer Versicherungsmaklerin oder einem Makler verarbeitet? Dies waren nur einige Fragen, die die DSGVO nach sich gezogen hat.

Datenschutz-Verhaltenskodex offiziell genehmigt

Um die Besonderheiten der einzelnen Verarbeitungsbereiche der Branche und die Anwendung der DSGVO sowie deren Umsetzungsbestimmungen im Datenschutzgesetz (DSG) zu präzisieren, wurden vom Fachverband Versicherungsmakler und Berater in Versicherungsangelegenheiten, in Zusammenarbeit mit Vertretern der Branche sowie der Bundessparte Information und Consulting der WKÖ, Verhaltensregeln gem. Art 40 DSGVO als Code of Conduct bei der Datenschutzbehörde eingereicht und von dieser nun behördlich genehmigt.

"Wir Versicherungsmakler sind stets umsichtig im Umgang mit Datenschutz und Datensicherheit. Nach der Umsetzung der Vorgaben der DSGVO wurden die unterschiedlichen Rechtsauslegungen in der Praxis aber zum Problem. Große Unsicherheit und viel Bürokratie waren die Folge. Als Interessensvertretung haben wir uns daher entschlossen, diese Schwierigkeiten durch Verhaltensregeln mit der Datenschutzbehörde zu klären und Rechtsicherheit für die Branche herzustellen", betont Christoph Berghammer, Fachverbandsobmann der Versicherungsmakler am Donnerstag im Rahmen eines Online-Pressegespräches.

Klarheit über die Rechtsstellung von Versicherungsmaklern

Kontakt

Stubenring 16 / Top 7
1010 Wien

Telefon +43 5 90 900 4816
E-Mail ihrversicherungsmakler@wko.at
Web https://wko.at/ihrversicherungsmakler

Detaillierte Kontaktseite

FAQ zum Code of Conduct

Antworten auf Fragen zu den Verhaltensregeln für Versicherungsmakler

Downloads

Bescheid der Datenschutzbehörde über die Genehmigung des Code of Conduct

Inhalt

Rollenbild

Die CoC normieren die Rollenbilder des Versicherungsmaklers.

Rechtmäßigkeit der Datenverarbeitung

Die CoC legen die Rechtfertigungsgründe für die Verarbeitung personenbezogenen Daten fest.

Sonderfall Betriebsübergabe

Die CoC regeln die Rechtmäßigkeit der Datenverarbeitung im Falle einer Betriebsübergabe.

Speicherbegrenzung & Löschkonzept

Die CoC tragen zur Rechtssicherheit in Bezug auf den Grundsatz der Speicherbegrenzung bei.

Informationspflichten

Die CoC lösen die Probleme bei der Informationserteilung.

Datenschutzbeauftragter

Die CoC geben Aufschluss darüber ob ein Datenschutzbeauftragter benötigt wird.

IT- &Datensicherheitsmaßnahmen

Die CoC enthalten einen Maßnahmenkatalog in Bezug auf die technischen und organisatorischen Maßnahmen gemäß der DSGVO

Code of Conduct –Vorteile

- CoC stellen Interpretationshilfen für die für die Auslegung der DSGVO dar
- Fragestellungen der Praxis und Graubereiche werden durch CoC geklärt
- CoC schaffen Rechtssicherheit für die jeweilige Branche
- Einhaltung der CoC wird von einer unabhängigen Überwachungsstelle geprüft

für alle	für jene, die weiter investieren:
✓ Codes of Conduct (CoC) sind offizielle durch die Behörde abgesegnet	✓ Überprüfung der individuellen Datenschutz-Compliance
✓ Rechtsicherheit für die Branche	✓ Erleichterungen der Nachweispflicht
✓ keine Kosten für Unternehmen	✓ Wettbewerbsvorteile durch CoC-Gütesiegel
✓ keine Verpflichtung	

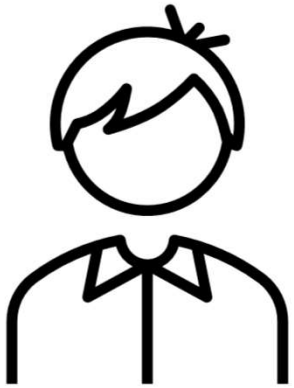
Plus an Rechtsicherheit und Sicherheit im Geschäftsverkehr

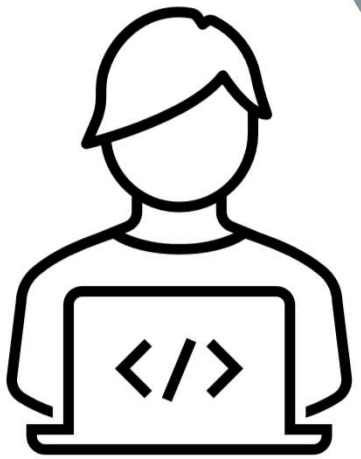
AON

Rollenbild

Standardfall: eigenständige Verantwortliche

- Versicherungsmakler treffen eigenständige Entscheidungen über die Verarbeitung, Erhebung und Speicherung der Daten Ihrer Kunden.
- Der Versicherungsmakler ist dem Versicherungskunden gegenüber verantwortlich für die ordnungsgemäße Verarbeitung seiner Daten.
- Versicherungsmakler benötigen die durch sie verarbeiteten Daten um ihren Rat (persönliche Empfehlung) nachweisen zu können.





Ausnahmefall: Auftragsverarbeiter

- Verarbeitet die Daten ausschließlich für den Verantwortlichen, in dessen Interesse zB bei Eingabe von Daten in das Portal des Versicherers

Rechtfertigungsgründe

Schlichtpersonenbezogene Daten

- **Vertragserfüllung** oder Erfüllung vorvertraglicher Pflichten
- Einzelfall: überwiegende berechtigte Interessen des Versicherungsmaklers
- Einzelfall: Einwilligung (zB Anmeldung Newsletter)

Sensible Daten

- Makler als gewillkürter Vertreter des Kunden
- **Gesetzliche Ermächtigung** (§ 28 MaklerG und § 11c Ziff. 5 VersVG)
- Sensible Daten können auch mit dem Versicherer ausgetauscht werden

Betriebsübergabe

- Berechtigtes Interesse oder Vertragserfüllung
- **Bedingung**: Zustimmung zur Rechtsnachfolge in Vollmacht des Vormaklers
- Käufer sollte sich aus Transparenzgründen dennoch darum kümmern,
  - eine erneuerte Vollmacht für die Verarbeitung der Daten einzuholen und
  - die Kunden über den Unternehmensübergang informieren

Informationspflichten

Grundsatz: der Betroffene muss vor der Verarbeitung über die Verarbeitung informiert werden

- Umfang, Zweck und Dauer der Verarbeitung
- Rechtfertigungsgründe und Datenübermittlung

Zusatz: Daten aus anderen Quellen → besonderer Hinweis (Art 14 DSGVO)

- Bekanntgabe der Datenkategorie und der Quelle

Sonderfälle

- **Gruppenversicherung:** Versicherungsmakler muss nicht informieren, sofern der Versicherungsnehmer (zB Arbeitgeber, Hausverwaltung etc.) die Versicherten bereits über den Datenaustausch informiert hat

- **Drittschäden:** Versicherungsmakler kann von einer Unterrichtung des geschädigten Dritten Abstand nehmen (unverhältnismäßiger Aufwand)

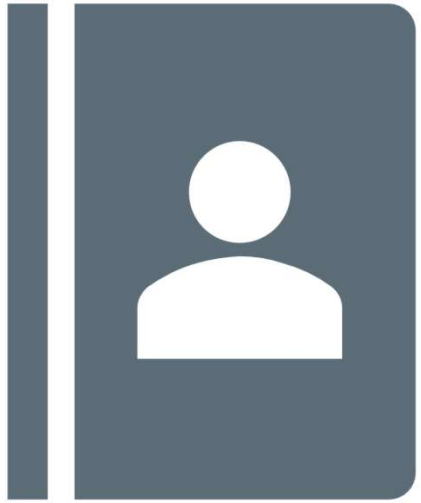
- **Sofortabschluss per Telefon**: zweistufige Informationserteilung → zuerst mündlich danach schriftlich

Verarbeitungsverzeichnis

Verantwortliche sind zur Führung eines Verarbeitungsverzeichnisses verpflichtet

Inhalt:

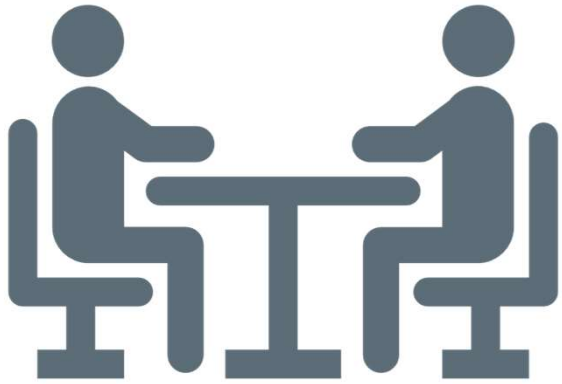
- Allgemeine Informationen
  - Angaben zum Verantwortlichen
  - Angaben zum Datenschutzkoordinator
- Zwecke der Datenverarbeitung (Versicherungsvermittlung, Vertragsverwaltung, Schadenberatu Newsletter-Versand, Personalverwaltung etc.)
- Rechtfertigungsgründe der Verarbeitung (Vertragserfüllung, gesetzliche Ermächtigung, Einwilligung etc.)
- Datenkategorien
- Empfängerkategorien
- Datenübermittlung
- Speichermedium (Kundenverwaltungssystem, Online-Portal, Handakte etc.)
- Löschfristen



Auftragsverarbeiter

Auftragsverarbeiter verarbeiten personenbezogene Daten im Auftrag und auf Weisung des Verantwortlichen

- Zwischen dem Verantwortlichen und dem Auftragsverarbeiter wird ein sogenannter Auftragsverarbeitervertrag geschlossen
- Den Auftragsverarbeiter treffen geringere Pflichten als den Verantwortlichen
- Auftragsverarbeiter sind verpflichtet den Verantwortlichen bei der Erfüllung der Betroffenenrechte zu unterstützen
- Auftragsverarbeiter haben ein vereinfachtes Verarbeitungsverzeichnis zu führen
- Auftragsverarbeiter sind dazu verpflichtet TOMs umzusetzen
- Verantwortliche sind dazu verpflichtet die Einhaltung der datenschutzrechtlichen Vorschriften zu überprüfen



Betroffenenrechte

Recht aus Auskunft

- Beantwortung binnen 1 Monat → Frist kann in Ausnahmefällen auf weitere 2 Monate verlängert werden
- Kostenlos
- Betroffener hat ein Recht auf Kopie seiner Daten

Recht auf Löschung

- Kann der Verantwortliche nur verweigern, wenn die Daten noch benötigt werden

Recht auf Berichtigung der Daten

- Verantwortlicher hat die Daten unverzüglich zu berichtigen bzw zu vervollständigen

Recht auf Datenübertragbarkeit

- Recht auf Erhalt und – sofern technisch machbar – Übermittlung der Daten an einen anderen Verantwortlichen

Recht auf Einschränkung der Datenverarbeitung

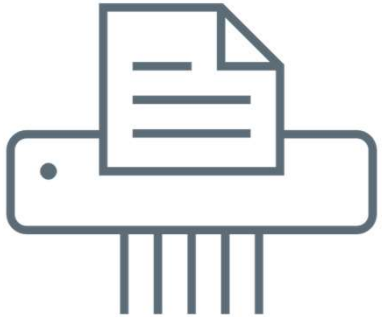
- Sofern der Betroffene die Richtigkeit der Daten bestreitet bzw Widerspruch gegen die Datenverarbeitung erhebt

Datenschutzbeauftragter

- Schwerpunkt der Tätigkeit des Versicherungsmaklers liegt
- in der Kranken- Unfall-, Ärztehaftpflicht oder Lebensversicherung und
- es gibt mindestens 20 Vollzeit-Mitarbeitern,
- welche überwiegend sensible Daten verarbeiten,
- dann ist ein Datenschutzbeauftragter zu benennen.

Im Standardfall ist kein Datenschutzbeauftragter zu bestellen

Speicherbegrenzung & Löschkonzept



Grundsatz der Datenminimierung

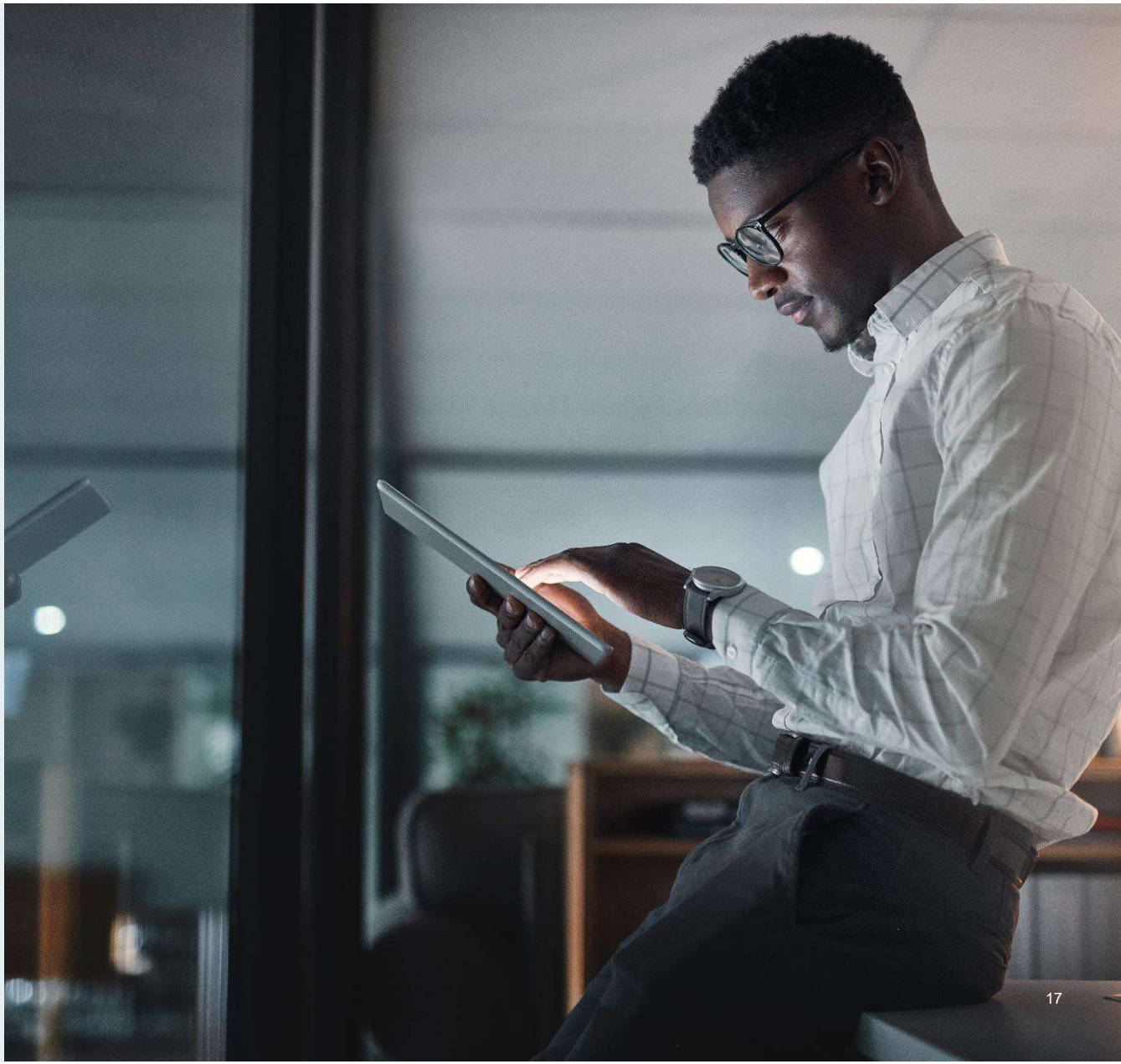
- Es sollen nur Daten verarbeitet werden, die benötigt werden
- Aufbewahrung zum Nachweis der bestmöglichen Beratung → Frist bis zu 30 Jahre (ABGB)

IT- & Datensicherheitsmaßnahmen (TOMs)

- Information und Schulung der Mitarbeiter
- Aufgabenverteilung zwischen den Mitarbeitern
- Zutrittsberechtigungen (u.a zu Betrieb, Büro, Aktenschrank, Serverraum etc.)
- Zugriffsberechtigungen (u.a. Firewall, Virenschutz, Passwörter, Fernzugrifftools etc.)
- Protokollierung der Datenverwendung/ Zugriffe
- Verschlüsselung / Pseudonymisierung soweit möglich
- regelmäßig erfolgte Datensicherungen
- regelmäßig erfolgte Überprüfungen der Datensicherungen

3

Zertifizierung



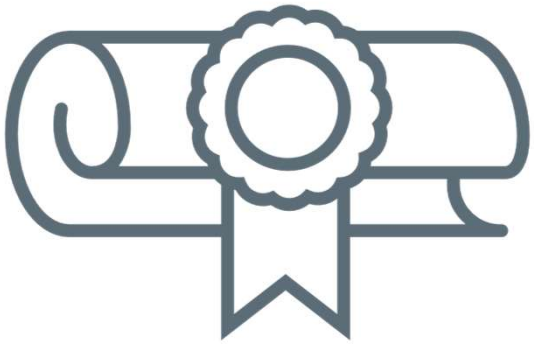
Ablauf der Zertifizierung

Verpflichtungserklärung

- an den Fachverband Versicherungsmakler per E-Mail ihrversicherungsmakler@wko.at
- alternativ kann die Verpflichtungserklärung auch direkt gegenüber der gewählten Überwachungsstelle abgegeben werden
- Die Erklärung hat zumindest zu umfassen
  - die ausdrückliche Mitteilung, sich zur Anwendung der Verhaltensregeln zu verpflichten,
  - den Namen oder die Firma des Berufsberechtigten, den Sitz oder die Geschäftsanschrift,
  - die firmenmäßige Zeichnung,
  - die Kontaktdaten des Berufsberechtigten.

Prüfung

- Die Überwachungsstelle nimmt eine individuelle Prüfung vor (Audit) und prüft hierbei insbesondere:
  - Das Verarbeitungsverzeichnis, inklusive dem Löschkonzept
  - Informationsblätter und Vollmacht
  - Auftragsverarbeitervereinbarungen

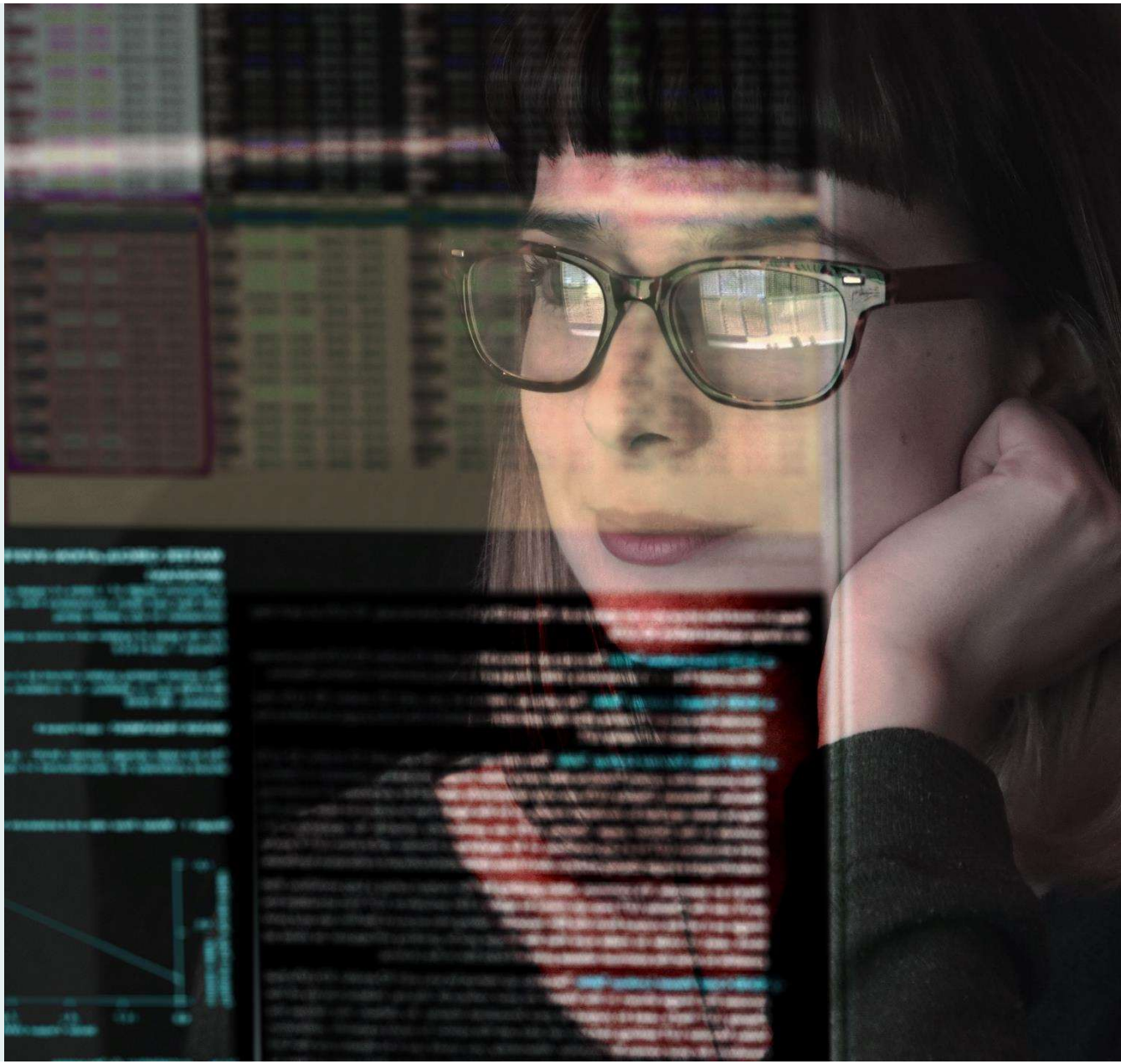


Zertifikat

- Nach Prüfung durch die Überwachungsstelle wird dem Versicherungsmakler bei Vorliegen der Voraussetzungen eine Bestätigung über die Anwendbarkeit der Verhaltensregeln per E-Mail an die bekanntgegebenen Kontaktdaten übermittelt
- Aufnahme in das konstitutive öffentliche Verzeichnis

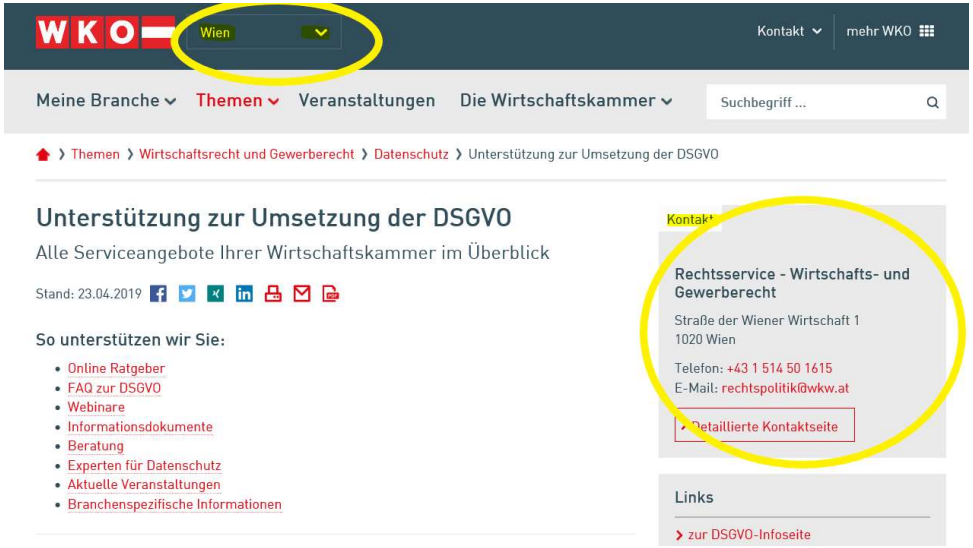
4

Informationen zum Thema Datenschutz

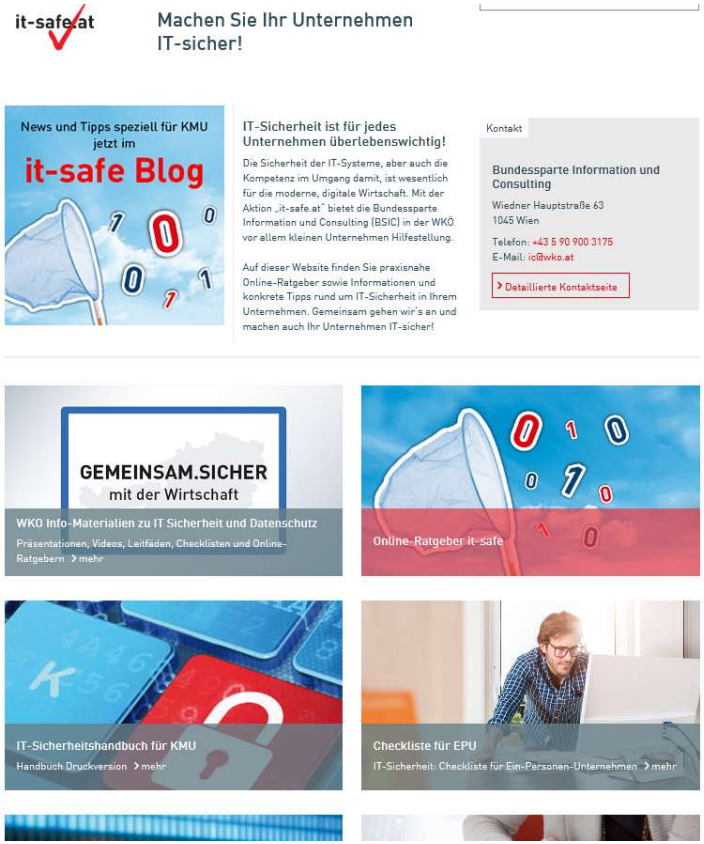


wko.at/datenschutzservice

- ✓ Überblicksseite
- ✓ Checklisten
- ✓ Muster
- ✓ Informationsdokumente
- ✓ Ansprechpersonen je Bundesland
- ✓ Onlineratgeber
- ✓ Informationsfolder
- ✓ Broschüren
- ✓ Webinare
- ✓ FAQ
- ✓ externe Experten
- ✓ aktuelle Veranstaltungen
- ✓ Praxisleitfaden
- ✓ Förderungen (KMU Digital)
- ✓ …



it-safe.at



- ✓ Blog
- ✓ Erklärvideos
- ✓ EPU Checkliste
- ✓ Online-Ratgeber
- ✓ Handbuch KMU
- ✓ Handbuch Mitarbeiter
- ✓ Tagesaktuelles
- ✓ Veranstaltungen
- ✓ Leitfaden TOMs
- ✓ …

Ich freue mich auf einen Austausch mit Ihnen!

Mag. Kerstin Keltner
Director Financial Lines & Cyber

t +43 676 830 425 337
kerstin.keltner@aon-austria.at