Datenschutz – UPDATE

Erste Erfahrungen mit der DSGVO

Ursula Illibauer
Bundessparte Information & Consulting

BildungsKickOff 2019
15. Jänner 2019

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Seit 25. Mai 2018…

- über 1.200 Beschwerden bei der DSB anhängig (**Stand**: 21.12.2018)
- über 250 Meldungen von Datenschutzverletzungen („data breach“)
- über 60 amtswegige Prüfverfahren

- nur **ein Viertel** der Unternehmen DSGVO-konform?
  (Quelle: https://www.bitkom.org/Presse/Presseinformation/Kaum-Fortschritt-bei-der-Umsetzung-der-Datenschutz-Grundverordnung.html, Stand: 27.09.2018)

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Wenig Neues…

- **Rechtmäßigkeit** („warum darf ich das?“)
- **Speicherdauer** („wie lange?“)
- **Verarbeitungsverzeichnis** („Protokoll“)
- **Informationspflicht** („Datenschutzerklärung“)
- **Datensicherheit / IT-Sicherheit** („wie sicher?“)

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Wenig Neues, dennoch neue Probleme…

- Handhabe mit Betroffenenrechten
- Informationspflichten
- Aufbewahrungsfristen bestimmen
- Abgrenzung im DSGVO Rollenbild
- Abgrenzung mit Telekommunikationsgesetz (TKG)
- Unsicherheit bei IT- bzw Datensicherheit Sicherheit
- Warten auf aktuelle Entscheidungen

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Aufbewahrungsfristen

- ✓ **Steuerrechtliche Aufbewahrungspflicht (**§ 132 Abs 1 BAO): 7 Jahre
- ✓ Allgemeiner **Schadenersatz** (§ 1489 ABGB): 30 Jahre
- ✓ Anspruch auf Ausstellung eines **Dienstzeugnisses** (§ 1478 ABGB): 30 Jahre
- ✓ Ansprüche auf Ersatz wegen **diskriminierender Ablehnung einer Bewerbung** (§§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG): 6 Monate
- ✓ **Geldwäschebestimmungen** (§ 365y GewO): 5 Jahre
- ✓ **Aufbewahrungspflicht** (§ 98 VAG): 7 Jahre

weitere Aufbewahrungsfristen: wko.at/datenschutzservice

Rollenbild…

- **Verantwortlicher** = jemand, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- **Auftragsverarbeiter** = jemand, der personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet

Beispiele:
- Verantwortlicher: Rechtsanwälte, Steuerberater
- Auftragsverarbeiter: externer Buchhalter, Clouds

FDL: grundsätzlich (immer im Anwendungsfall zu prüfen) eigenständige Verantwortliche

Vgl: Steuerberater – Lohnverrechnung (GZ: DSB-D122.767/0001-DSB/2018)

Datenschutzerklärung…

- wie weitreichend / wann noch transparent / wann überbordend?
- Visitenkarten
- postalische Werbung
- Informationen im Geschäftslokal
- Verlinkungen / QR-Codes / Comics

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Abgrenzung zum TKG…

1. Anrufe **zu Werbezwecken und**

1. Telefaxe und **elektronische Post** (zB E-Mails, SMS, Social Media Nachrichten) zu Direktwerbezwecken (**Achtung!** NEU)

bedürfen der **vorherigen, jederzeit widerruflichen Zustimmung** des Empfängers (§ 107 TKG)

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Newsletter

Ausnahme von der Einwilligungsnotwendigkeit für elektronische Post im **aufrechten Kundenverhältnis** unter den Voraussetzungen:

- die E-Mail-Adresse des Kunden wird beim Verkauf einer Ware oder einer Dienstleistung erhoben; und
- die Zusendung erfolgt zur Direktwerbung für eigene, ähnliche Produkte; und
- der Kunde erhält bei Erhebung der E-Mail-Adresse die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen; und
- der Kunde erhält bei jeder Zusendung die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen; und
- der Kunde ist nicht in die sog **„ECG-Liste“** (https://www.rtr.at/de/tk/TKKS_ECGListe) eingetragen.

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

IMMER unzulässig:

- Versenden anonymer elektronischer Post
- kommerzielle Kommunikation muss so gestaltet sein, dass diese (§ 6 Abs 1 ECG)
  - als solche erkennbar ist,
  - natürliche oder juristische Person, die die kommerzielle Kommunikation in Auftrag gegeben hat, erkennen lässt,
  - Angebote zur Absatzförderung (Zugaben, Geschenke) als solche erkennen lässt und einfachen Zugang zu den Bedingungen enthält sowie
  - Preisausschreiben/ Gewinnspiele als solche erkennen lässt und einfachen Zugang zu Teilnahmebedingungen enthält

- der Empfänger wird aufgefordert, Websites zu besuchen, die gegen § 6 Abs 1 ECG verstoßen oder
- keine authentische Adresse vorhanden, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann

Einwilligung-Formulierungsvorschlag:

O Hiermit stimme ich …. zu, den Newsletter des Unternehmens … an folgende E-Mail-Adresse zugestellt zu erhalten: ……..

Ich kann meine Zustimmungserklärung jederzeit widerrufen; am einfachsten, indem ich den Widerruf an folgende E-Mail-Adresse schicke: ….

Durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Zustimmung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Datenschutzrechtlich verantwortlich: …. Wenn Sie Fragen haben, kontaktieren Sie uns unter: …. Die Rechtsgrundlage für die Datenverarbeitung zum Zweck des Newsletter-Versandes ist Ihre Zustimmung. Wir verarbeiten Ihre Daten zum Zweck des Newsletter-Versandes bis zum Widerruf Ihrer Zustimmung. Zur Abwicklung des Newsletter-Versandes arbeiten wir mit einem Betreiber eines Newsletter-Managementsystems mit Sitz in der EU zusammen. Ihnen stehen bezüglich Ihrer bei uns gespeicherten Daten grundsätzlich das Recht auf Auskunft, Richtigstellung, Einschränkung und Widerspruch zu einer Datenverarbeitung sowie Löschung und Übertragbarkeit Ihrer Daten zu. Wenn Sie glauben, dass wir gegen datenschutzrechtliche Vorschriften verstoßen, können Sie sich bei uns … oder bei einer Datenschutzbehörde beschweren.

(Datum, Unterschrift)

Webtracking / Websites

- **„Cookie-Regelung“** (§ 96 Abs 3 TKG)

- **Informationsverpflichtung:**

1. welche personenbezogenen Daten werden ermittelt, verarbeitet und übermittelt,
2. auf welcher Rechtsgrundlage,
3. für welche Zwecke,
4. für wie lange die Daten gespeichert werden,
5. über die Nutzungsmöglichkeiten auf Grund der in elektronischen Fassungen der Verzeichnisse eingebetteten Suchfunktionen.
6. Information in geeigneter Form und spätestens bei Beginn der Rechtsbeziehungen (Pop-Up)
7. Auskunftsrecht „nach dem Datenschutzgesetz“

- **Einwilligung** nötig, **außer**:
  - technischen Speicherung oder Zugang,
  - wenn alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder,
  - wenn dies unbedingt erforderlich ist, damit der Dienst, der vom Benutzer ausdrücklich gewünscht wurde, zur Verfügung gestellt werden kann.

- Änderung der Browsereinstellungen auf **„privacy by default“**
- Einwilligung **über Pop-Up über Website selbst** (Link zur Datenschutzerklärung!)
- „Anpingen“ des Browsers, iSe Einwilligung über die jeweilige Website (verschiedene Modelle am Markt erst verfügbar)
- alle nicht-technisch notwendigen Cookies werden **erst ab dem Zeitpunkt der Einwilligung gesetzt** (Cookie zum Nachweis der Einwilligung = notwendig)

Wann kommt die neue ePrivacy?

- Überarbeitung der geltenden ePrivacy RL (Richtlinie 2002/58/EG) durch die **ePrivacy VO**
- **sektorspezifischer** Datenschutz
  - Telekommunikation
  - Datenverarbeitung zu Werbezwecke
  - Cookies / Webtracking
  - Verzeichnisse
- **„Nachbessern** und **Aufholbedarf** im Hinblick auf DSGVO“

Aktuelle Entscheidungen

- erste **Strafbescheide**:
  - hauptsächlich „Bildverarbeitung“
  - bis zu 4.800 EUR (DSB-D550.038/0003-DSB/2018)

- Entscheidung zum **Auskunftsbegehren** (GZ: DSB-D122.844/0006-DSB/2018):
  - Bank muss kostenlos Auskunft über Bankdaten der letzten Jahre erteilen (5 Jahre).
  - Ein derartiges Auskunftsbegehren ist nicht exzessiv.
  - noch nicht rechtskräftig

- Entscheidung zu **Aufbewahrungsfristen** (GZ: DSB-D216.471/0001-DSB/2018):
  - Löschungsbegehren für Stammdaten
  - § 207 Abs 2 BAO: Aufbewahrungsfrist 10 Jahre
  - § 132 Abs 1 BAO, § 212 UGB: Aufbewahrungsfrist 7 Jahre
  - DSB: Aufbewahrungsdauer in diesem Fall 7 Jahre

- weitere Entscheidungen abrufbar unter ris.bka.gv.at

Black-List

- = Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V): Black-List & Erläuterungen

- Datenverarbeitung zur **Bewertung oder Einstufung natürlicher Personen** (inkl Profiling)
  - hinsichtlich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort, Ortswechsel und
  - ausschließlich auf einer automatisierten Verarbeitung beruhend und
  - Potential für negative rechtliche, physische oder finanzielle Auswirkungen
  - **mögliche Anwendungsfälle**: Ablehnung eines Online-Kreditantrags, Bonitätsdatenbanken, Datenbank für die Bekämpfung der Geldwäscherei und der Terrorismusbekämpfung, Verhaltens- oder Marketingprofile (ausgenommen personalisierte Werbung)

- Verarbeitungen von **Daten zur Bewertung des Verhaltens und anderer persönlicher Aspekte** von natürlichen Personen
  - und die von Dritten dazu genutzt werden können, automatisierte Entscheidungsfindungen zu treffen,
  - die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen
  - **mögliche Anwendungsfälle**: Big Data Analysen Banken- und Finanzsektor, Gesundheitswesen, Steuerwesen, Versicherungen, Marketing und Werbung

- **Zusammenführung / Abgleich von Datensätzen** aus zwei oder mehreren Verarbeitungen, die zu unterschiedlichen Zwecken oder von verschiedenen Verantwortlichen durchgeführt wurden
  - im Rahmen einer Datenverarbeitung, die über die von einer betroffenen Person üblicherweise zu erwartenden Verarbeitungen hinausgeht,
  - sofern durch die Anwendung von Algorithmen Entscheidungen getroffen werden können, welche die betroffene Person in erheblicher Weise beeinträchtigen
  - mögliche Anwendungsfälle: Scoringmethoden, Fraud-Prevention-Systeme

- **2 Kriterien müssen erfüllt sein:**
  - umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten,
  - umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten,
  - Erfassung von Standortdaten
  - Verarbeitung von Daten schutzbedürftiger betroffener Personen
  - Zusammenführung / Abgleich von Datensätzen aus zwei oder mehreren Verarbeitungen, die zu unterschiedlichen Zwecken oder von verschiedenen Verantwortlichen durchgeführt wurden
    - im Rahmen einer Datenverarbeitung, die über die von einer betroffenen Person üblicherweise zu erwartenden Verarbeitungen hinausgeht,
    - sofern diese für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei der betroffenen Person erhoben wurden.

Prüfschritte:

- Datenverarbeitung definieren
- DFA Kriterien der Blacklist prüfen
- Rechtsgrundlagen und Grundsätze prüfen
- Verarbeitungsvorgänge und Zwecke prüfen
- Bewertung Notwendigkeit und Verhältnismäßigkeit
- Schutz- und mögliche Angriffsziele definieren
- Risikoanalyse (Black List BFDI)
- Eintrittswahrscheinlichkeit und Schwere des Risikos
- Abhilfemaßnahmen und Maßnahmenplan definieren
- Konsultation DSBA
- Dokumentation

vgl auch: EU-Datenschutz-Grundverordnung (DSGVO): Ablaufplan Datenschutz-Folgenabschätzung

Datensicherheit

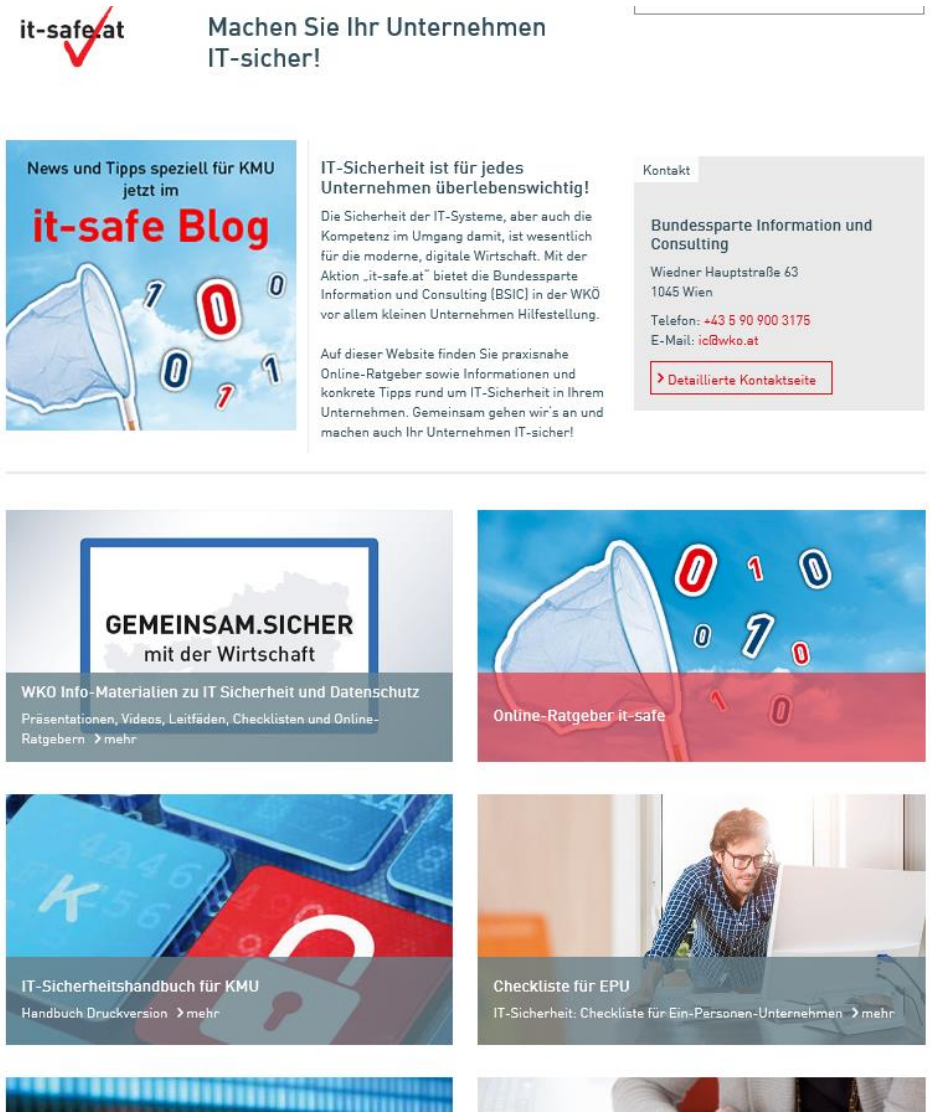
- data breach notification (Art 33 und 34 DSGVO)
- neues Formular der DSB selbst
- tlw Einstellungen, tlw Aufforderung zur Nachreichung von Dokumenten
- wann liegt ein Risiko vor, wann ein hohes Risiko?
- **Leitfaden** der Artikel 29 Gruppe (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052) bringt nur tlw Hilfestellung, mehr Praxisbeispiele wären hilfreich
- **Meldung an Betroffene**: EU-Datenschutz-Grundverordnung (DSGVO): Data Breach Notification - Muster Benachrichtigung der betroffenen Person

- **Anhaltspunkt**: Leitfaden IT-Sicherheit in Kreditinstituten – FMA
- **IT-Safe.at** (Leitfäden, Mitarbeiterhandbücher, KMU-Handbücher

Basics:

- ✓ ausdrückliche Festlegung Aufgabenverteilung zwischen den Mitarbeitern;
- ✓ Bindung der Datenverwendung an einen gültigen Auftrag z.B. eines oder einer Vorgesetzten;
- ✓ Information und Schulung der Mitarbeiter über ihre Pflichten und internen Datensicherheitsvorschriften;
- ✓ Zutrittsberechtigungen zu Räumen, in denen Daten verarbeitet werden;
- ✓ Schutz der IT-Systeme und Datenträger vor unbefugten Zugriffen;
- ✓ Schutz der IT-Systeme vor unbefugter Inbetriebnahme;
- ✓ Protokollierung der Datenverwendung;
- ✓ die Dokumentation der oben angeführten Sicherheitsmaßnahmen in Form eines Datensicherheitshandbuchs

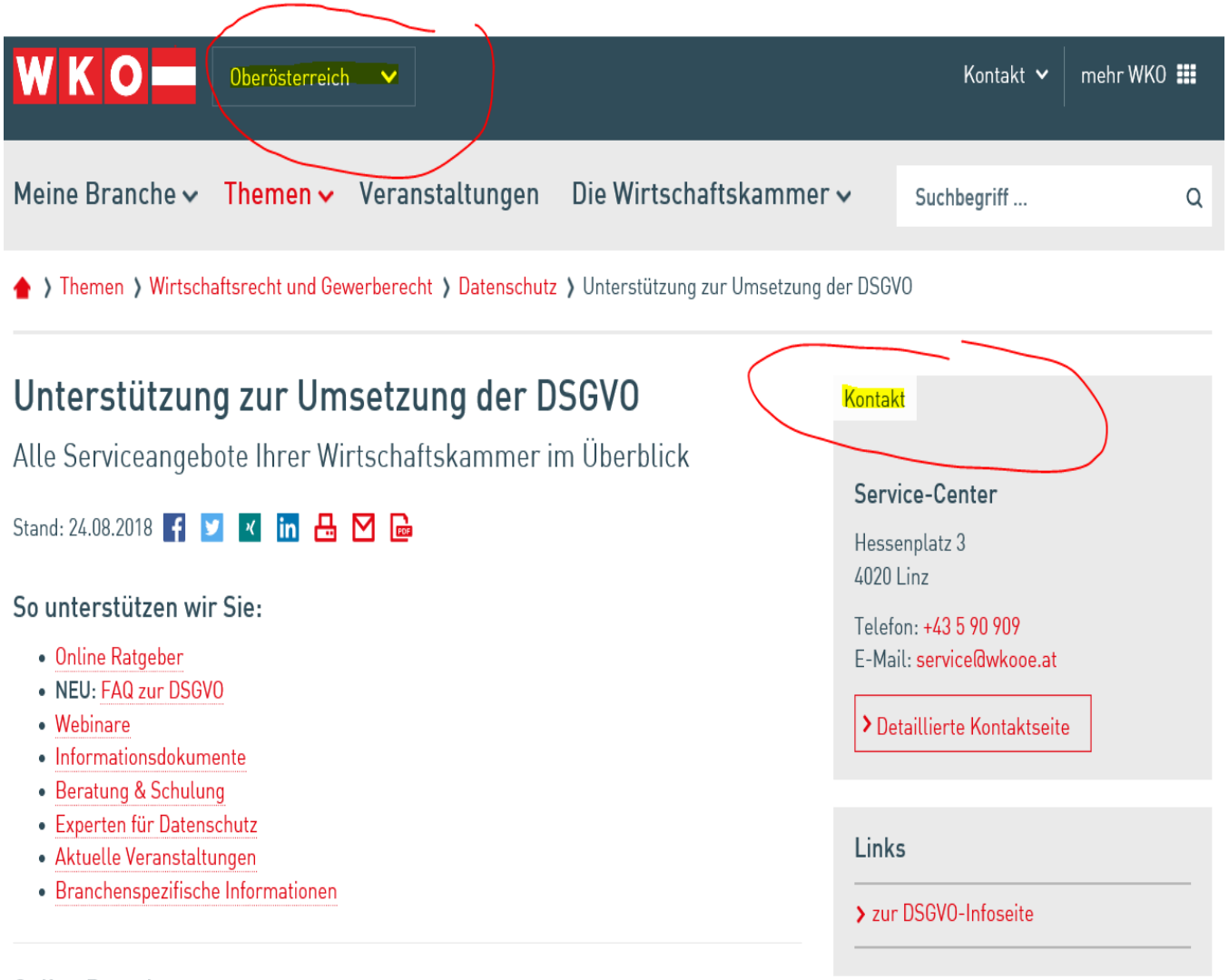
it-safe.at



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

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

wko.at/datenschutzservice



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

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Kontakt

Mag. Ursula Illibauer
Bundessparte Information und Consulting
E ursula.illibauer@wko.at
T +43 (0)5 90 900 3151
www.wko.at/ic / www.it-safe.at

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH