

# DSGVO Update

Ursula Illibauer

Fachgruppentagung Finanzdienstleister Niederösterreich

17.09.2019

# Aktuelles

# Zahlen nach 1 Jahr DSGVO

- **Stand Mai 2019**
- 1.969 Beschwerden  
(davon 241 international)
- über 600 „Data Breach Notification“
- 164 amtswegige Prüfverfahren
- 11 Anträge auf Genehmigung von Verhaltensregeln
- 189 Verwaltungsstrafverfahren

# Strafen

- **Ö:** bislang eine Hand voll Strafen zur Bildverarbeitung / Videoüberwachung ausgesprochen,
  - EUR 6.700 wg einer verdeckten, langfristig angelegten VÜ durch einen Privatdetektiv (rechtskräftig)
  - EUR 11.000 wg heimlichen Filmens zweier Fußballspielerinnen unter der Dusche (nicht rechtskräftig)
  - **EUR 50.000** gegen „Unternehmen aus dem medizinischen Bereich“ wg fehlendem DSBA und mangelhafter Erfüllung der Informationspflichten (vgl [Schmidl](#))

# Strafen

- **Norwegen:** EUR 170.000
- **Polen:** EUR 220.000
- **GB:** Pfund 120.000
- **Deutschland:** EUR 15.000
- **Frankreich:** EUR 50 Mio
- **GB:** EUR 205 Mio
- **Griechenland:** EUR 150.000

# Umfragewerte

- nur **ein Viertel** der Unternehmen DSGVO-konform?
  - Quelle: [Bitkom](#)
  - 27.09.2018
  
- nur **jedes zweite** österreichische Unternehmen ausreichend vorbereitet?
  - Quelle: [Deloitte](#)
  - 25.1.2019
  
- Unternehmen sind **nicht sicherer** geworden?
  - Quelle: [KSV1870](#)
  - 28.5.2019

# Aktuelle Entscheidungen

- Speicherung von Bewerberdaten für die Dauer von 7 Monaten ist gerechtfertigt (27.8.2018, DSB-D123.085/0003-DSB/2018)
- Anonymisieren statt Löschen ist zulässig (5.12.2018, DSB-D123.270/0009-DSB/2018)
- kein Konsultationsverfahren der DSB, wenn Datenschutzfolgenabschätzung kein hohes Risiko ergibt (18.12.2018, DSB-D485.001/0003-DSB/2018)
- 1xige Zustellung postalischer Werbung pro Jahr ist unproblematisch (23.4.2019, DSB-D123.626/0006-DSB/2018)

# Aktuelle Entscheidungen

- **Entscheidungen zu Kreditauskunfteien:**
  - 5. 12. 2018, DSB-D123.211/0004-DSB/2018: zu weitgehende Löschung aus Datenbank einer Kreditauskunftei und Antrag auf Berichtigung (nicht rechtskräftig)
  - 7. 12. 2018, DSB-D123.193/0003-DSB/2018: keine automatischen 7 Jahre bei KKE (nicht rechtskräftig)
  - 11.12.2018, DSB-D123.194/0003-DSB/2018: rechtliche Grundlage in § 152 GewO für Verarbeitung bonitätsrelevanter Daten durch Kreditauskunfteien

„Da die Ausübung dieser ... Tätigkeit ohne Sammlung, Aufbewahrung und Weitergabe von ... Daten nicht sinnvoll vorstellbar ist, muss auch angenommen werden, dass der Gesetzgeber in bestimmten Fallkategorien ein die Betroffeneninteressen überwiegendes berechtigtes Interesse dieser Gewerbetreibenden an einer Verwendung von Daten über „Kreditverhältnisse“ als gegeben erachtete“



# Aktuelle Entscheidungen

- Entscheidungen zu **Kreditauskunfteien**:
  - 20.02.2019, DSB-D123.319/0002-DSB/2019: wie lange dürfen Zahlungserfahrungsdaten nach Begleichung der Forderung gespeichert werden?

**Einzelfallbeurteilung** unter Berücksichtigung aller maßgeblichen Umstände, wie bspw:

- die **Höhe** der einzelnen Forderungen,
- das „**Alter**“ der Forderungen (sohin das Datum der Eintragung in die Datenbank),
- **Anzahl** der im Wege eines Inkassounternehmens eingetriebenen Forderungen,
- die **Zeit**, die seit Begleichung einer Forderung verstrichen ist,
- die **Herkunft** der Daten.

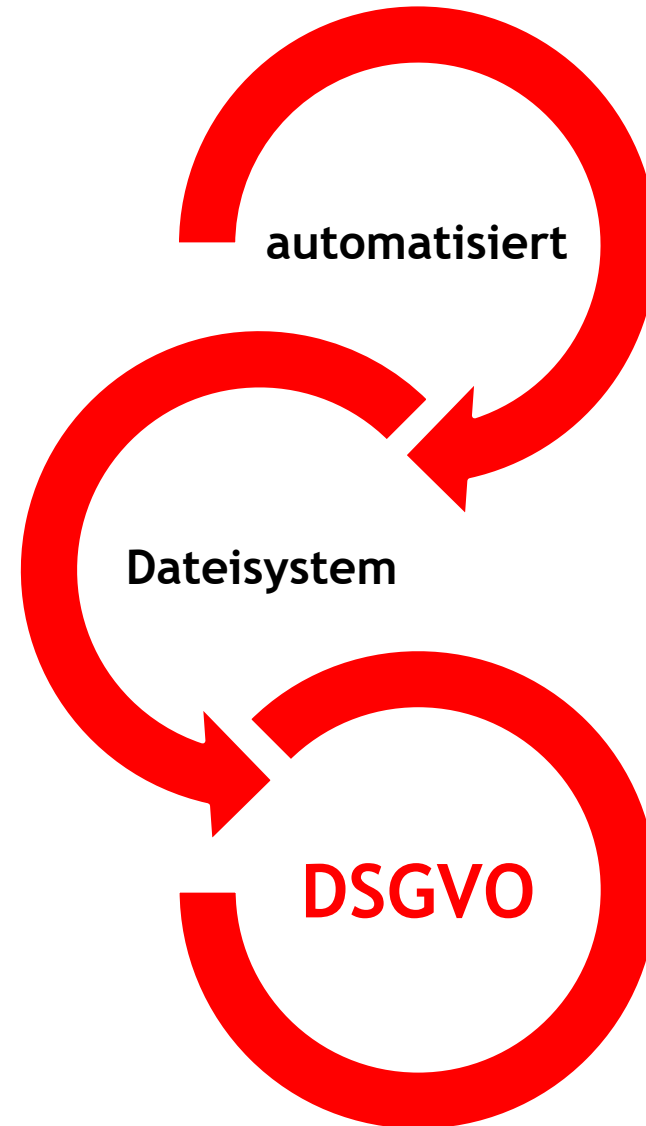
- weitere Entscheidungen abrufbar unter [ris.bka.gv.at](https://ris.bka.gv.at)

# Mythen & No-Gos

# We have updated our privacy policy...

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

# DSGVO bei Papierschilddern?!



# Ich darf Daten verarbeiten, wenn...

1. Einwilligung,
2. für die Vertragserfüllung,
3. rechtliche Verpflichtung,
4. Schutz lebensnotwendiger Interessen,
5. im öffentlichen Interesse,
6. im berechtigten Interesse.

# Ich darf besondere / sensible Daten verarbeiten, wenn...

1. **ausdrückliche Einwilligung,**
2. **arbeits- oder sozialrechtliche Verpflichtungen,**
3. für Zwecke der **Gesundheitsvorsorge** oder Arbeitsmedizin,
4. **gesetzliche Verpflichtung,**
5. Schutz **lebensnotwendiger** Interessen,
6. von der Person **selbst veröffentlichte** Daten,
7. Verarbeitung zur Geltendmachung / Ausübung / Verteidigung von **Rechtsansprüchen,**
8. Verarbeitung durch politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht.

# Ich darf strafrechtliche Daten verarbeiten, wenn...

1. unter behördlicher **Aufsicht**,
2. ausdrückliche **gesetzliche** Ermächtigung / Verpflichtung,
3. gesetzlichen **Sorgfaltspflichten**,
4. zur Wahrung überwiegender berechtigter **Interessen**.

# Aufbewahrungsfristen

- ✓ Steuerrechtliche Aufbewahrungspflicht (§ 132 Abs 1 BAO): **7 Jahre**
- ✓ Gewährleistung (§ 933 ABGB): **2 Jahre / 3 Jahre**
- ✓ Allgemeiner Schadenersatz (§ 1489 ABGB): **30 Jahre**
- ✓ Ausstellung eines Dienstzeugnis (§ 1478 ABGB): **30 Jahre**
- ✓ Ersatz wg diskriminierender Ablehnung einer Bewerbung (§§ 15 Abs 1 und 29 Abs 1 GlbG sowie § 7k Abs 1 iVm Abs 2 Z 1 BEinstG): **6 Monate**

weitere Aufbewahrungsfristen: [wko.at/datenschutzservice](https://wko.at/datenschutzservice)



# No-Gos

- Anruf zu Werbezwecken ohne vorherige Einwilligung
- Datenfriedhöfe
- Datenweitergabe „ohne Nachdenken“
- Mitarbeiter nicht informieren
- Websites nicht ordentlich ausgestalten
- Datensicherheit vernachlässigen
- auf Stellungnahme-Ersuchen der DSB nicht reagieren
- auf Betroffenenanfragen nicht reagieren

# Finanzdienstleistungen

# Profiling

= jede Art von automatisierter 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, wenn das Profiling mit Direktmarketingmaßnahmen in Verbindung steht

# „Schweres“ Profiling (Art 22 DSGVO)

- **Problem:** ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung, die rechtliche Wirkung entfaltet oder in ähnlicher Weise erheblich beeinträchtigt
  - spezielle Rechtfertigungsgrundlage
  - Informationsverpflichtung über involvierte Logik & Tragweite der angestrebten Auswirkungen
  - Datenschutz-Folgenabschätzung
  - geeignete mathematische oder statistische Verfahren, technische und organisatorische Maßnahmen, mit denen sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird
  - **Beispiel:** Kundenbindungs- und Bonussysteme?

# Black-List - Risikoanalyse

- = 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-Kreditanspruchs, 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**

# Datenschutz-Folgenabschätzung

- **Prüfschritte:**

1. Datenverarbeitung definieren
2. Kriterien der Blacklist prüfen
3. Rechtsgrundlagen und Grundsätze prüfen
4. Verarbeitungsvorgänge und Zwecke prüfen
5. Bewertung Notwendigkeit und Verhältnismäßigkeit
6. Schutz- und mögliche Angriffsziele definieren
7. Risikoanalyse (Black List BFDI)
8. Eintrittswahrscheinlichkeit und Schwere des Risikos
9. Abhilfemaßnahmen und Maßnahmenplan definieren
10. Konsultation DSBA
11. Dokumentation

vgl auch:

- [EU-Datenschutz-Grundverordnung \(DSGVO\): Ablaufplan Datenschutz-Folgenabschätzung](#)
- [Online-Ratgeber zur Datenschutz-Folgeabschätzung](#)

# Rollenbild



© Designed by  
Macrovector / Freepik

- **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: Clouds, IT-Dienstleistungen

# Rollenbild



© Designed by  
Macrovector / Freepik

- Was ist Ihre Kerntätigkeit und ist die Verarbeitung der Daten hierfür erforderlich?
- Wer hat die Entscheidungsbefugnis über die Datenverarbeitung (über Mittel und Zwecke)?
- Woher stammen die Daten?
- Haben Sie direkten Kundenkontakt oder treten Sie im Namen eines anderen auf?
- Können Sie die Daten jederzeit löschen?

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

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



# Newsletter

# Elektronische Werbung

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)

# 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](https://www.rtr.at/de/tk/TKKS_ECGListe)) eingetragen.

# Newsletter

## 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:

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)

# Onlinewerbung

# Webtracking

= Informationen, die vom Informationsanbieter mit Hilfe des Browsers auf der Festplatte des PC des Kunden abgespeichert werden, um Daten mit dem Computer des Kunden zu verknüpfen

- ePrivacy Richtlinie (in Zukunft: ePrivacy Verordnung?)
- § 96 Telekommunikationsgesetz (TKG)

# Webtracking

- **„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“



# Webtracking

- **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)

# Social Media Marketing

- **Social Plugins:**
  - Problem der Datenweitergabe ohne zeitgerechte Information / konforme Rechtsgrundlage?
  - „Zwei-Klick-Lösung“ als pragmatischer Ansatz
  - gemeinsam Verantwortliche? EuGH: Social Pluggins (zB Facebook - Like-Button), Schlussanträge Generalanwalt in der Rechtssache C-40/17 „Fashion ID“
- **Facebook Fanpages:**
  - gemeinsam Verantwortliche?
  - EuGH: Facebook - Fanpages (EuGH vom 05.06.2018 C-210/16)
- **Datenschutzerklärungen!!!**

## Standards:

- <https://www.facebook.com/business/help/2001034850142726?helpref=search&sr=2&query=datenschutz>
- [https://business.instagram.com/advertising?locale=de\\_DE](https://business.instagram.com/advertising?locale=de_DE)
- <https://business.twitter.com/de/help/troubleshooting/how-twitter-ads-work.html>

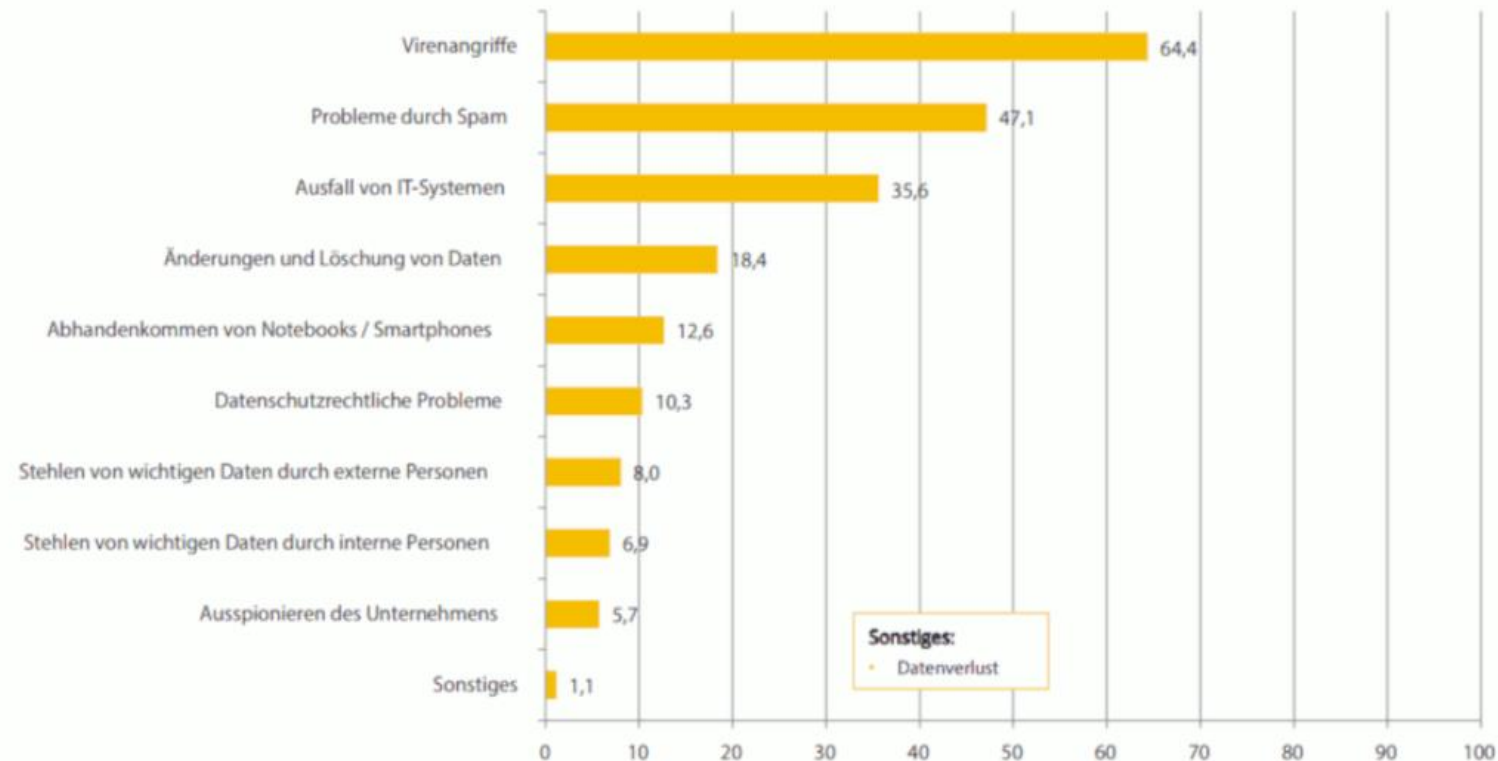
# Ausblick

# Datensicherheit wird immer wichtiger!

## ART DER IT-SECURITY VORFÄLLE IN DEN LETZTEN 2 JAHREN

„Welche IT-Security-Vorfälle waren das?“

Frage wurde nur jenen gestellt, in deren Unternehmen es in den letzten 2 Jahren einen IT-Vorfall gab.



Grafik & Studie:  
Techbold



© Designed by Macrovector / Freepik

## Basics:

- ✓ Information und Schulung der Mitarbeiter
- ✓ ausdrückliche Festlegung Aufgabenverteilung zwischen Mitarbeitern
- ✓ Zutrittsberechtigungen
- ✓ Zugriffberechtigungen (Firewall, Virenschutz, Passwörter, Fernwartungstools)
- ✓ Protokollierung der Datenverwendung/ Zugriffe
- ✓ Verschlüsselung / Pseudonymisierung (zB VeraCrypt, SSL)
- ✓ Datensicherungen
- ✓ Überprüfungen der Datensicherungen

# it-safe.at



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](mailto:ic@wko.at)

[Detaillierte Kontaktseite](#)

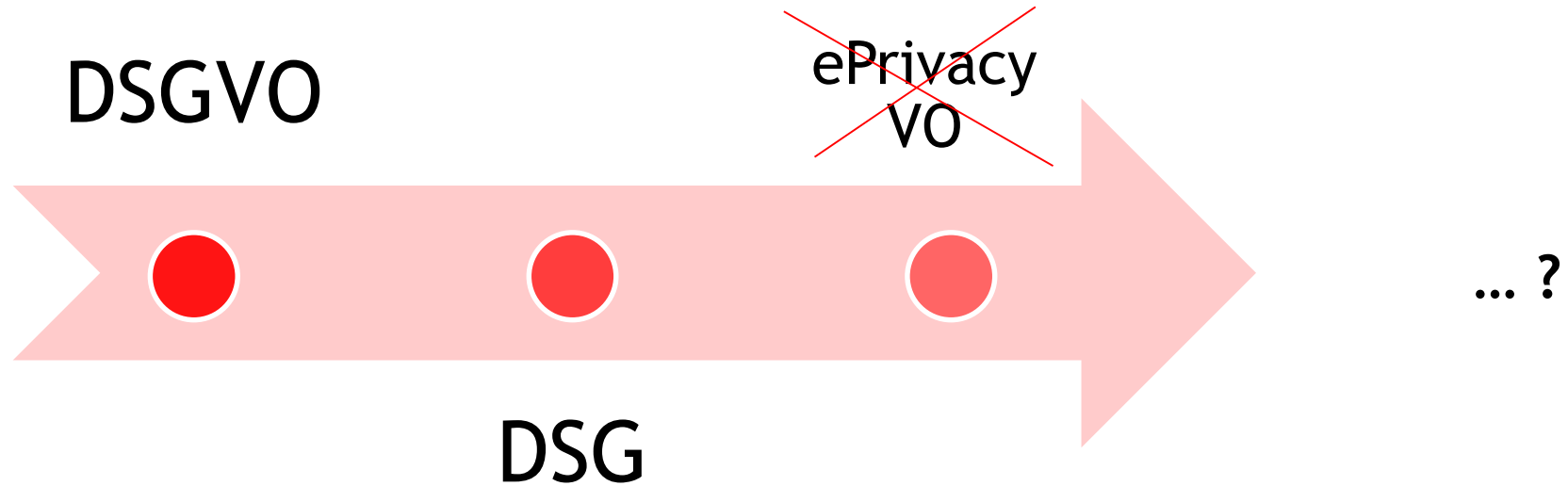


- ✓ Blog
- ✓ Erklärvideos
- ✓ EPU Checkliste
- ✓ Online-Ratgeber
- ✓ Handbuch KMU
- ✓ Handbuch Mitarbeiter
- ✓ Tagesaktuelles
- ✓ Veranstaltungen
- ✓ Leitfaden TOMs
- ✓ ...

# 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**“

# Zeitplan





# Fragen?

# wko.at/datenschutzservice werbungwien.at | recht.werbungwien.at

The screenshot shows the WKO website interface. At the top left is the WKO logo with a red and white Austrian flag. A yellow circle highlights the 'Wien' dropdown menu. To the right are 'Kontakt' and 'mehr WKO' links. Below is a navigation bar with 'Meine Branche', 'Themen', 'Veranstaltungen', and 'Die Wirtschaftskammer'. A search bar contains 'Suchbegriff ...'. The breadcrumb trail reads: 'Themen > Wirtschaftsrecht und Gewerberecht > Datenschutz > Unterstützung zur Umsetzung der DSGVO'. The main heading is 'Unterstützung zur Umsetzung der DSGVO' with the subtitle 'Alle Serviceangebote Ihrer Wirtschaftskammer im Überblick'. Below this is the date 'Stand: 23.04.2019' and social media icons. A section 'So unterstützen wir Sie:' lists several services. A yellow circle highlights a 'Kontakt' card for 'Rechtsservice - Wirtschafts- und Gewerberecht' with address, phone, and email, and a 'Detaillierte Kontaktseite' link. Below is a 'Links' section with a link to 'zur DSGVO-Infoseite'.

WKO Wien

Kontakt mehr WKO

Meine Branche Themen Veranstaltungen Die Wirtschaftskammer

Suchbegriff ...

Themen > Wirtschaftsrecht und Gewerberecht > Datenschutz > Unterstützung zur Umsetzung der DSGVO

## Unterstützung zur Umsetzung der DSGVO

Alle Serviceangebote Ihrer Wirtschaftskammer im Überblick

Stand: 23.04.2019

So unterstützen wir Sie:

- [Online Ratgeber](#)
- [FAQ zur DSGVO](#)
- [Webinare](#)
- [Informationsdokumente](#)
- [Beratung](#)
- [Experten für Datenschutz](#)
- [Aktuelle Veranstaltungen](#)
- [Branchenspezifische Informationen](#)

**Kontakt**

**Rechtsservice - Wirtschafts- und Gewerberecht**

Straße der Wiener Wirtschaft 1  
1020 Wien

Telefon: +43 1 514 50 1615  
E-Mail: [rechtspolitik@wkw.at](mailto:rechtspolitik@wkw.at)

[Detaillierte Kontaktseite](#)

**Links**

[zur DSGVO-Infoseite](#)

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

# Kontakt

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