



# Eine Stunde Datenschutz

## Ausgewählte datenschutzrechtliche Aspekte für Unternehmen

Datenschutz im touristischen Umfeld

Sensible Daten

Auskunftsrecht

# Eine Stunde Datenschutz

---

- Webinar-Reihe des Arbeitskreises Datenschutz sowie des Servicezentrums, Team Rechtsservice, der Wirtschaftskammer Kärnten
- Vortragende:  
*Dr. Patricia Radl-Rebernig / Mag. Stefan Ugovsek*  
*Mag. Judith Leschanz*
- Moderation:  
*Dr. Christina Kitz-Überall*

# Eine Stunde Datenschutz

Unternehmerische Mindestanforderungen aus der Perspektive des Datenschutzes

- Mag. Dr. Patricia Radl-Rebernik, MBA, CMC | radl-rebernik consulting e.U. | +43 (0)650 77 77 324 | Glein 12A, 9431 St. Stefan im Lavanttal | office@radl-rebernik.at
- Mag. Stefan Ugovsek | ICU-Consulting | T + F 0463 204 262 | office@ugovsek.at | Luegerstraße 27, 9020 Klagenfurt | Web: <http://www.icu-consulting.at>
- Mag. Judith Leschanz | Geschäftsführerin Secur-Data Betriebsberatungs-Ges.m.b.H. Fischerstiege 9, 1010 Wien | +43 1 533 4207-0 | office@secur-data.at <https://www.secur-data.at>
- <https://www.wko.at/branchen/k/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/arbeitskreis-datenschutzexperten.html>
- Dr. Christina Kitz-Überall, Servicezentrum, Rechtsservice, Wirtschaftskammer Kärnten [christina.kitz-ueberall@wkk.or.at](mailto:christina.kitz-ueberall@wkk.or.at) | 0590904-723

# Datenschutz im touristischen Umfeld

KommR Dr. Mag. Patricia Radl-Rebernik, MBA, CMC

# Aktuelles

- Zeit für ein **Update**
- Wieso? Es gibt einige Änderungen, die Kunden sind sensibler in Bezug auf „ihre“ Daten.
- **Gelebter Datenschutz** ist „erwachsen“ geworden
- **Kunden/Gäste** fordern es ein
- **Behörde** fordert Umsetzung ein – Prüfungen laufend



# 01

## Tourismusbetriebe und Verarbeitung personenbezogener Daten

# Verarbeitungsbereiche im Tourismus

- Rezeption
- Restaurant
- Etage
- Wellnessbereich
- Fitnessbereich
- Ausflüge, Sportangebote, etc. – intern – extern
- Onlineauftritt

• ...



# Datenschutzerklärung - Homepage

- Alles, was an technischen Tools verwendet wird, muss erklärt werden – einfach, leicht verständlich
- zB Analysetools, Social Media Plugins, Kontaktformular, Newsletter – inkl. Angabe des verwendeten Tools (Auftragsdatenverarbeitung – ggf Datenübermittlung an Drittländer), etc.
- Eingesetztes CMS – aus datenschutzrechtlicher Perspektive (zB Wordpress, Joomla, Wix, etc.)
- Cookie-Erklärung – Cookie Banner

# Datenschutz auf der Website

## *Plugins*

- Google Maps
- Kontaktformular
- Newsletter
- Videodarstellung (zB YouTube)
- Social Media Plugins
- Blogs
- Chats / Chatbots
- ...

**Cookie Consent**

Wir nutzen Cookies auf unserer Website. Einige von ihnen sind technisch unbedingt notwendig, während andere uns helfen die Bedienbarkeit der Website zu verbessern. Für diese technisch nicht unbedingt notwendigen Cookies benötigen wir Ihre Einwilligung.

[Datenschutz](#)

---

**AWS - Technisch notwendige Cookies** ( 0 Service ) nein  ja

Notwendige Cookies, die zum Betrieb der Seite benötigt werden.

---

**AWS - Analyse/Statistik** ( 1 Service ) nein  ja

Matomo ist eine DSGVO-konforme europäische gehostete Analyse-Software welche statistische Daten speichert, damit wir unsere Dienste verbessern können.

Matomo nein  ja

Matomo.org [DETAILS ANZEIGEN](#)

---

**AUSWAHL BESTÄTIGEN** **ALLE ABLEHNEN** **ALLE AKZEPTIEREN**

## Cookie Consent

Wir nutzen Cookies auf unserer Website. Einige von ihnen sind technisch unbedingt notwendig, während andere uns helfen die Bedienbarkeit der Website zu verbessern. Für diese technisch nicht unbedingt notwendigen Cookies benötigen wir Ihre Einwilligung.

### Datenschutz

#### **AWS - Technisch notwendige Cookies** ( 0 Service )

nein  ja

Notwendige Cookies, die zum Betrieb der Seite benötigt werden.

#### **AWS - Analyse/Statistik** ( 1 Service )

nein  ja

Matomo ist eine DSGVO-konforme europäische gehostete Analyse-Software welche statistische Daten speichert, damit wir unsere Dienste verbessern können.

Matomo

nein  ja

Matomo.org

[DETAILS ANZEIGEN](#)

**AUSWAHL BESTÄTIGEN**

**ALLE ABLEHNEN**

**ALLE AKZEPTIEREN**

**Privatsphäre-Einstellungen**

Um Ihnen unsere Druckprodukte bestmöglich präsentieren zu können, verwendet [druck.at](#) Cookies, auch von Drittanbietern. Klicken Sie auf „Alles akzeptieren“ um alle Cookies zu akzeptieren und direkt zur Webseite weiter zu navigieren. Weitere Informationen erhalten Sie in unserer Datenschutzerklärung.

[Datenschutzerklärung](#) [Impressum](#)

[Individuelle Einstellung](#) [Alles akzeptieren](#)

Powered by Usercentrics Consent Management

**Mithilfe von Cookies funktioniert diese Website optimal**

Durch die Auswahl von "Cookies akzeptieren" erlauben Sie der Website, Geräte- und Browserinformationen zu sammeln. Einige dieser Cookies sind für das einwandfreie Funktionieren der Website notwendig (z.B. Sicherheit, Zimmer-Buchung und Anmeldung). Andere Cookies ermöglichen es uns, Ihre Marketingangebote zu personalisieren und die Leistung der Website zu überwachen. Wählen Sie "Cookies verwalten", um die Art von Cookies auszuwählen, die verwendet werden kann. Wir geben einige dieser Daten für Marketingzwecke an Dritte wie Google, Facebook und Instagram weiter. Wählen Sie "Speichern" wenn Sie Ihre Auswahl auf essentielle Cookies beschränken wollen.

Weiter Informationen: [Datenschutzrichtlinien](#)

[Cookies akzeptieren](#)

**Datenschutzeinstellungen**

Wir nutzen Cookies auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern.

Wenn Sie unter 16 Jahre alt sind und Ihre Zustimmung zu freiwilligen Diensten geben möchten, müssen Sie Ihre Erziehungsberechtigten um Erlaubnis bitten.

Wir verwenden Cookies und andere Technologien auf unserer Website. Einige von ihnen sind essenziell, während andere uns helfen, diese Website und Ihre Erfahrung zu verbessern. Personenbezogene Daten können verarbeitet werden (z. B. IP-Adressen), z. B. für personalisierte Anzeigen und Inhalte oder Anzeigen- und Inhaltsmessung. Weitere Informationen über die Verwendung Ihrer Daten finden Sie in unserer [Datenschutzerklärung](#). Sie können Ihre Auswahl jederzeit unter [Einstellungen](#) widerrufen oder anpassen.

Einige Services verarbeiten personenbezogene Daten in den USA. Mit Ihrer Einwilligung zur Nutzung dieser Services stimmen Sie auch der Verarbeitung Ihrer Daten in den USA gemäß Art. 49 (1) lit. a DSGVO zu. Das EuGH stuft die USA als Land mit unzureichendem Datenschutz nach EU-Standards ein. So besteht etwa das Risiko, dass US-Behörden personenbezogene Daten in Überwachungsprogrammen verarbeiten, ohne bestehende Klagemöglichkeit für Europäer.

Essenziell  Statistiken  Marketing

[Alle akzeptieren](#)

[Speichern](#)

[Individuelle Datenschutzeinstellungen](#)

[Cookie-Details](#) | [Datenschutzerklärung](#) | [Impressum](#)

02



**DATA PRIVACY  
FRAMEWORK  
PROGRAM**

**EU-US**

# Datenschutzerklärung

*Hinweis Privacy Shield = Geschichte*



The screenshot shows the Privacy Shield Framework website. At the top left is the logo for the Privacy Shield Framework. To the right is a search bar with the text 'Search' and a magnifying glass icon, and a 'Log In' link. Below the logo are navigation links: 'Self-Certify', 'Privacy Shield List', and 'Audiences'. A search bar contains the text 'dropbox'. Below the search bar are two tabs: 'ACTIVE' (selected) and 'INACTIVE'. To the right of the tabs is an 'Advanced' button. Below the search results, a card for 'Dropbox, Inc.' is visible. The card includes the company name, location 'San Francisco, California', a green dot indicating it is 'Active', and a list of frameworks: 'EU-U.S. Privacy Framework' and 'Swiss-U.S. Privacy Framework'. To the right of the card, it says 'Covered Data' and 'Non-HR'. At the bottom right of the card is a link for 'Questions or Complaints'.

# EU-US Data Privacy Framework

**NEU**

- Seit 10.07.2023
- Angemessenheitsentscheidung der EU
- Angemessenes Schutzniveau für personenbezogene Daten
- 2-stufiges Rechtsschutzsystem in US
  - 1. Stufe: Civil Liberties Protection Officer (US Geheimdienst)
  - 2. Stufe: unabhängiges u. unparteiisches Datenschutzprüfungsgericht (Data Protection Review Court) wird eingerichtet – für Beschwerden von Zugriffen durch US-Sicherheitsbehörden
- Selbst Zertifizierung: Data Privacy Framework

<https://www.dataprivacyframework.gov/s/participant-search>



**DATA PRIVACY  
FRAMEWORK  
PROGRAM**

Search

Home Self-Certify Data Privacy Framework List Audiences ▾ About ▾

ACTIVE INACTIVE

🔍 dropbox

Advanced Search

**Dropbox, Inc.**

San Francisco, California

Active

**Framework**

EU-U.S. Data Privacy Framework  
Swiss-U.S. Data Privacy Framework  
UK Extension to the EU-U.S. Data Privacy Framework

**Covered Data**

HR  
Non-HR

**Dropbox, Inc.**

Active Participant

Industries

Participation

Privacy Policy

Dispute Resolution

**Industries**

Information and Communications Technology  
Information Technology Services

Information and Communications Technology  
Software

**Participation**

**UK Extension to the EU-U.S. Data Privacy Framework: Active**

Original Certification Date: 10/02/2023  
Next Certification Due Date: 05/14/2024  
Data Collected: HR, NON-HR

**Swiss-U.S. Data Privacy Framework: Active**

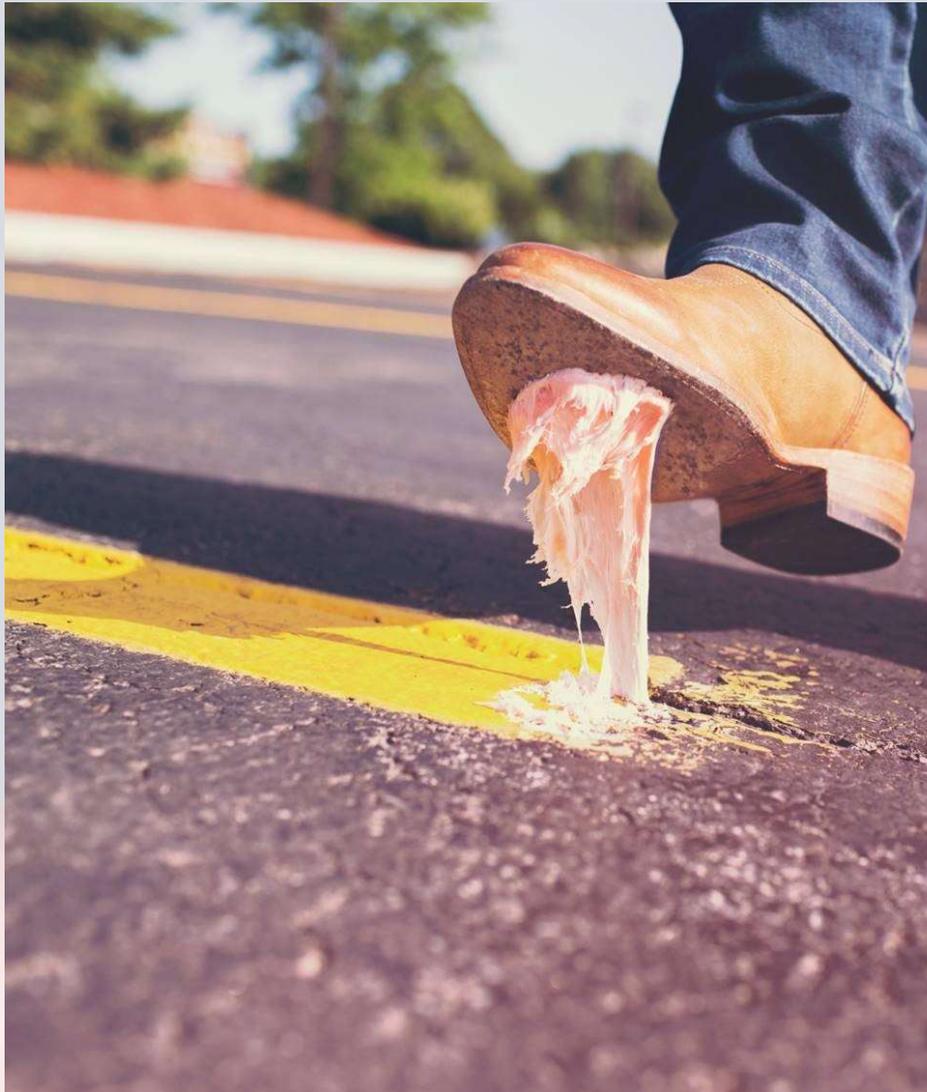
Original Certification Date: 05/24/2017  
Next Certification Due Date: 05/14/2024  
Data Collected: HR, NON-HR

**EU-U.S. Data Privacy Framework: Active**

Original Certification Date: 09/23/2016  
Next Certification Due Date: 05/14/2024  
Data Collected: HR, NON-HR

**PURPOSE OF DATA COLLECTION**

Dropbox provides a website, software, and mobile applications which allow people to store files, synchronize files across multiple devices, and collaborate with others. Dropbox offers services to individual users on both a free and paid subscription basis (Dropbox Basic, Dropbox Plus, Dropbox Professional, Dropbox Family, Dropbox Transfer, and Dropbox Backup). Dropbox also offers services intended for use within teams and organizations on a paid subscription basis (Dropbox Standard, Dropbox Advanced, Dropbox Enterprise, Dropbox Advanced Server Integration, Dropbox Enterprise Server Integration, and Dropbox Education). Certain Dropbox services may also be accessed by Application Programming Interfaces (APIs), which taken together, are elements of the Dropbox Developer Platform. Dropbox, through Dropbox Sign Services, provides a website, software, and mobile applications which allow people to streamline complex transactions through innovative digital solutions such as electronic fax, electronic signature, and workflow automation. Dropbox Sign Services offers services to individual users on both a free and paid subscription basis (Dropbox Sign Free, Dropbox Sign Essentials, Dropbox Sign Dropbox + ESign, Dropbox Sign Standard, Dropbox Premium, Dropbox Fax Free, Dropbox Fax Home Office, Dropbox Fax Professional, Dropbox Fax Small Business, Dropbox Forms Free and Dropbox Forms Standard). Dropbox Sign Services also provides Application Programming Interfaces (the "API") that allow Customers to build integrated fax, signature, or workflow automation solutions within a Customer's websites, applications, or other properties. Dropbox collects personal data from individuals in the European Union, European Economic Area



03

Zweck  
Einwilligung  
Löschung

# Zweckbindung

- Jede Verarbeitung von Daten bedarf eines Zwecks.
- Zweckbindung: pickt
- Zwecke/Rechtmäßigkeit der Verarbeitung Art. 6 DSGVO
  - Vertrag (Abs. 1, b)
  - Rechtliche Verpflichtung (Abs. 1, c)
  - Öffentliches Interesse (Abs. 1, d)
  - berechtigtes Interesse (Abs. 1, e)
  - Einwilligung (Abs. 1, a)
- Zweck erweitern: berechtigtes Interesse – solide Informationskette, die entsprechend Dokumentiert werden muss! Ist Tricky – weil: es muss halten!

# Einwilligung

- Schwächste Rechtsgrundlage bei Verarbeitung von personenbezogenen Daten
- Nur im „Notfall“
- Jederzeit zurücknehmbar – ohne Gründe
- Besser: gesetzliche Verpflichtung oder Vertrag
- Alternativ: berechtigtes Interesse (muss nachvollziehbar begründet und dokumentiert werden)
- Check, ob Einwilligung tatsächlich notwendig ist – oder ob Vertragsgrundlage, etc. vorhanden ist

# Vertrag

***Vertragsgrundlage: kommt sehr oft vor – daher: keine Einwilligung notwendig***



## **Hotel/Gastro**

- Beherbergungsvertrag
- Verköstigungsvertrag
- ...

## **Seilbahn**

- Transportvertrag
- Nutzungsvertrag
- Mietvertrag
- ...
- ...

## **Ausflugsziel**

- Transportvertrag
- Mietvertrag
- ...



# Gesetzliche Grundlagen

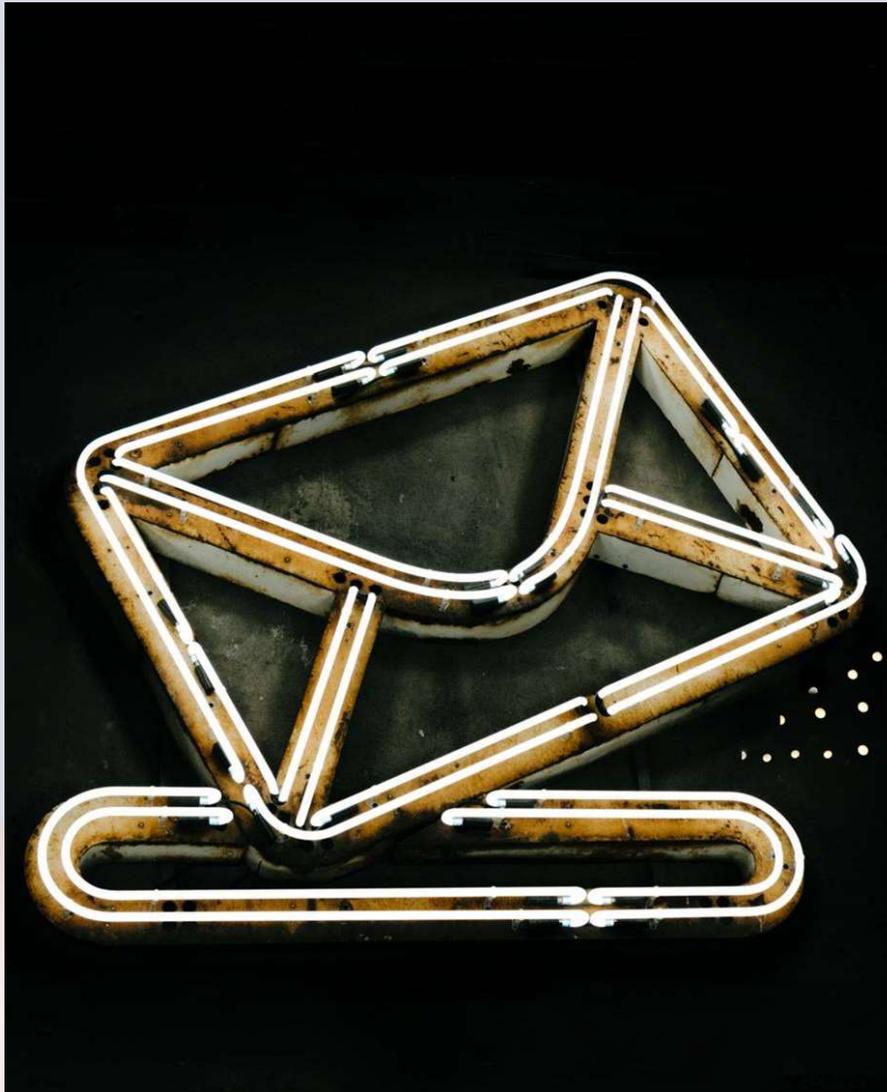
**Per Gesetz vorgeschrieben: kein Vertrag und keine Einwilligung notwendig**

zB

- Tourismusabgabe
- Meldepflichten gegenüber Gemeinde/Land
- Sozialversicherung
- Finanzamt
- Telekommunikationsgesetz (TKG) 2021
- Mediengesetz
- E-Commerce Gesetz (ECG)
- ...

# Löschung personenbezogener Daten

- Es gibt Löschfristen!
- Wenn die Aufbewahrungsfrist abgelaufen ist – ist auch die Rechtsgrundlage weg. (Art. 5 Abs. 1 lit. b DSGVO)
- FAZIT: ich MUSS löschen
  - Digital – überall: Festplatten, Handies, Laptops, ...
  - Physisch
- Vorsicht beim BACKUP – digitale Löschlogik muss Backups inkludieren
- DAHER: rechtzeitig auch die Prozesse definieren, damit aus Backups Daten gelöscht werden können
- ERSTER SCHRITT: Speicherkonzept – Löschkonzept
- Physische Speicher-/Löschlogik muss mit digitaler übereinstimmen
- Startschuss: Aufräumen



04

# Newsletter

TKG 2021

# TKG 2021 (vorher TKG 2003)

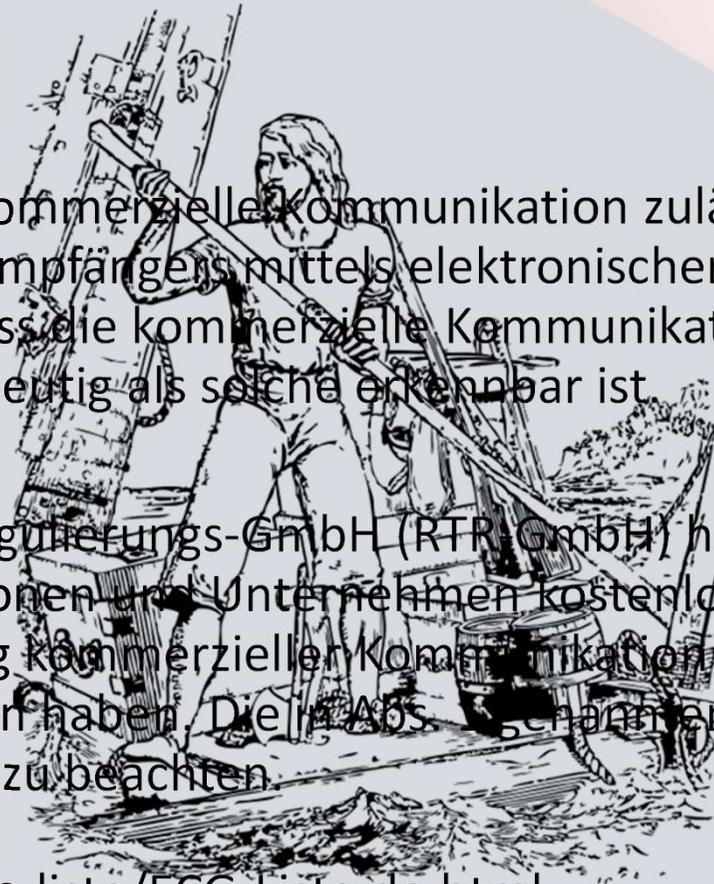
- TKG 2021 - **§ 174 TKG** – unerbetene Nachrichten
- In Kraft getreten am **01.11.2021**
- „Abs. (2) Die Zusendung einer elektronischen Post – einschließlich SMS –
- ist ohne vorherige Einwilligung des Empfängers unzulässig, wenn die Zusendung zu Zwecken der Direktwerbung erfolgt.“
- Unter welchen Bedingungen ist E-Mail-Werbung erlaubt?
- Bis auf wenige Ausnahmen: Nur mit vorheriger Einwilligung
- **Einwilligung:** Nur mit Widerrufshinweis und Koppelungsverbot einhalten

# TKG 2021

- **Achtung!**
- Bereits die Einwilligung per E-Mail ist idR ein – verbotenes – Werbe-Mail!
- **Werbezwecke** – was versteht man darunter?
  - Alle Aktivitäten im Zusammenhang mit Werbenachrichten
  - schon ein bloßes Angebot gilt als Werbung und fällt darunter
- **ALLE E-Mails haben nach UGB ein Impressum zu enthalten**

# Robinsonliste ECG-Liste RTR

- **§ 7 ECG**
- (1) Ein Diensteanbieter, der eine kommerzielle Kommunikation zulässigerweise ohne vorherige Zustimmung des Empfängers mittels elektronischer Post versendet, hat dafür zu sorgen, dass die kommerzielle Kommunikation bei ihrem Eingang beim Nutzer klar und eindeutig als solche erkennbar ist.
- (2) Die Rundfunk- und Telekom Regulierungs-GmbH (RTR-GmbH) hat eine Liste zu führen, in die sich diejenigen Personen und Unternehmen kostenlos eintragen können, die für sich die Zusendung kommerzieller Kommunikation im Weg der elektronischen Post ausgeschlossen haben. Die in Abs. 1 genannten Diensteanbieter haben diese Liste zu beachten.



<https://www.rtr.at/TKP/service/ecg-liste/ECG-Liste.de.html>



08

# Digitaler Auftritt und Social Media

# Texte, Fotos und Videos

- Rechtsgrundlagen (zB Urheberrecht, Recht am eigenen Abbild)
- Ideal: Eigene Fotos/Videos  
Alternativ: Rechtsgrundlage (zB Mitarbeiterfotos, Kundenfotos)
- Offizieller Ankauf:  
Rechte für Verwendung definieren

# Facebook-Fanpage und Instagram Businessaccount

Es braucht eine eigene DSE für die Facebook-Fanpage  
(Unternehmensseite) und den Instagram-Businessaccount

**Auslöser:** Urteil des EuGH 05.06.2018 - C-210/16

Link zum Originalurteil:

[https://curia.europa.eu/juris/document/document.jsf?docid=202543  
&doclang=DE](https://curia.europa.eu/juris/document/document.jsf?docid=202543&doclang=DE)

**Conclusio:** *Der Betreiber einer Facebook-Fanpage ist gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher seiner Seite verantwortlich*

# DATENSCHUTZERKLÄRUNG

## Facebook-Fanpage und Instagram Businessaccount



**Praxis:**

Erstellung der erforderlichen Datenschutzerklärungen für

**Facebook-Fanpage** und **Instagram-Businessaccount**

Einpflegen als Link auf der **Facebook-Fanpage** und **Instagram**



# 07

## DATENVERLUST

Was ist zu tun?

## DATENVERLUST

- **Data Breach Meldung** muss innerhalb von 72 Stunden ab Kenntnis erfolgen
- Direkt an die **Datenschutzbehörde** [www.dsb.gv.at](http://www.dsb.gv.at)
- Je nach Schwere des Vorfalls auch direkt an **ALLE Betroffenen**
- **Die Meldepflicht hat der Verantwortliche!**

### Was ist zu melden?

- Hackangriffe auf die Webseite, wenn...
- Cryptolocker-Erpressungsversuche ... Hackermails
- Hackerangriff auf Zutrittssystem
- Massenmails via CC statt BCC, Irrläufer...
- gestohlene Zeitaufzeichnungen von MitarbeiterInnen
- ...



# KONTAKT

KommR Mag. Dr. Patricia Radl-Rebernick MBA, CMC  
radl-rebernick consulting e.U.

geprüfte Datenschutzexpertin  
Zertifizierte Datenschutzbeauftragte  
Förderexpertin  
E-Learning Spezialistin

[office@radl-rebernick.at](mailto:office@radl-rebernick.at)

+43 650 77 77 324

[www.radl-rebernick.at](http://www.radl-rebernick.at)



**SCAN ME**

# Umgang mit sensiblen Daten

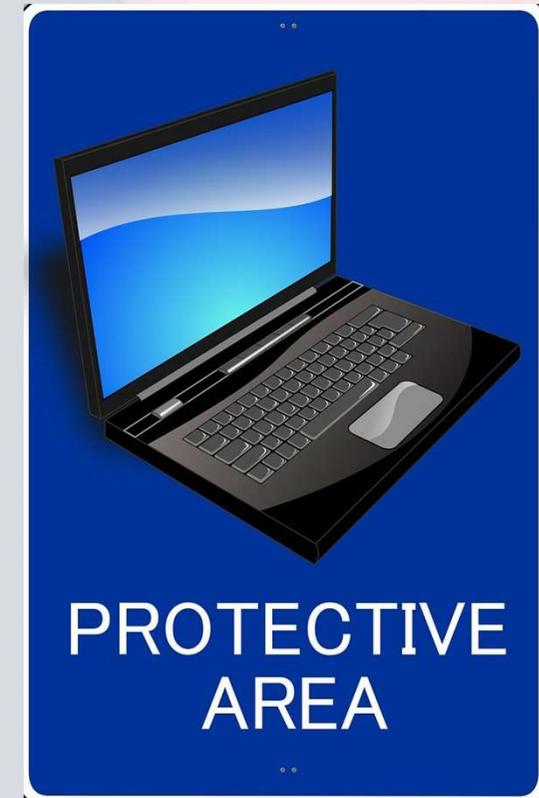
## Verarbeitung besonderer Kategorien personenbezogener Daten – Art 9 DSGVO

- **Was sind sensible Daten**
- **Wer ist betroffen**
- **Auf was ist zu achten**
- **Abgrenzung zur Bildverarbeitung (Fotos + Video)**

**Mag. Stefan Ugovsek**

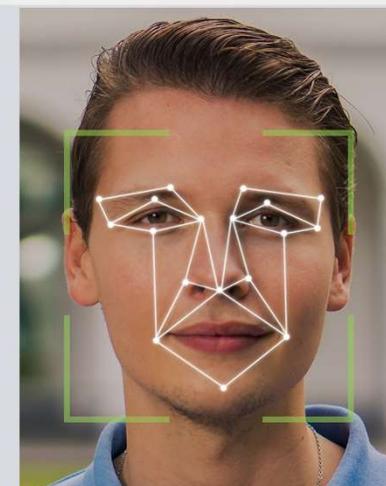
## Checkliste iZm sensiblen Daten

- Werden sensible Daten im Unternehmen verarbeitet?
- Sind diese Daten für den Geschäftsbetrieb erforderlich?
- Welche Auswertungsabsichten bestehen?
- Prüfung der Rechtsgrundlage für die Verarbeitung
- Wie sicher sind diese Daten
- Muss eine Datenschutzfolgeabschätzung durchgeführt werden?



## Was sind sensible Daten (Art. 9 DSGVO)

- **Gesundheitsdaten** (körperliche und geistige Gesundheit)
  - Unverträglichkeiten, Allergien (zB in der Hotellerie oder Werkskantinen)
  - Daten von Mitarbeiter:innen bezüglich Arbeitsfähigkeit
  - Aufzeichnungen iZm Beratungsgesprächen oder Coaching
  - uvm
- **biometrische Daten** (Menschen sind eindeutig identifizierbar)
  - Fingerabdruck (zB Zugangsberechtigung, Arbeitszeiterfassung, Smartphone, Laptop)
  - Gesichtserkennung (Face-ID) am Smartphone und im öffentlichen Raum (Flughafen)
  - Augen – Iris-Scan
  - Im High-Tech-Bereich – Venenscan
- genetische Daten
- Daten zum Sexualleben und zur sexuellen Orientierung einer Person (EuGH Urteil vom 01.08.2022 - Rechtssache C-184/20)
- Daten zu religiösen oder weltanschaulichen Überzeugungen, Zugehörigkeit zu einer Gewerkschaft, rassische und ethnische Herkunft, politische Einstellung



## Welche Unternehmen sind betroffen?

### Sensible Daten finden sich in fast jedem Unternehmen

- Mitarbeiter:innen – Aufzeichnungen (Gesundheit, Religion, Gewerkschaft, politische Gesinnung)
- Bestimmte Daten in der Kundendatenbank
- Digitale Zugangs- bzw. Zutrittsberechtigungen

### Gesundheitsdaten:

- Tourismus (Beeinträchtigungen, Unverträglichkeiten, Gesundheitszeugnisse)
- Gesundheitsberufe (Optiker, Hörakustiker, Orthopädietechniker, Zahntechniker)
- Humanenergetiker, LSB, Masseur, Fußpfleger, Kosmetiker
- Gesundheitsbetriebe (Altenbetreuung, Kurhäuser uä)
- Fitnessstudios mit digitalen Hilfestellungen
- Versicherungsmakler

## Wann dürfen sensible Daten verarbeitet werden?

Ist gem. Art. 9 generell untersagt!

**Ausnahmen sind:** (Auszug)

- ausdrücklich **Einwilligung** (kann jederzeit widerrufen werden!)
- Daten, die offensichtlich **selbst öffentlich gemacht** wurden
- Verpflichtung aus **arbeits- und sozialrechtlichen Bestimmungen**. (zB Krankmeldung, Gesundheitszeugnis)
- im Rahmen der **Gesundheitsvorsorge** oder Arbeitsmedizin
- zum Schutz lebenswichtiger Interessen
- im Kontext von Rechtsansprüchen

**Berechtigtes Interesse kann NICHT ins Treffen geführt werden**

Daten dürfen nur für einen **klar formulierten Zweck und definierte Dauer** verarbeitet werden!

## Deutlich höheres Schutzniveau

Es sind geeignete technische und organisatorische Maßnahmen und Verfahren zu treffen, damit die Verarbeitung den Anforderungen des erhöhten Risikos genügt:

**Art und Ort der Speicherung**

**Zugriffs- und Zugangskontrolle**

**Datenweitergabe**

**Datenschutzbeauftragter** (umfangreiche Verarbeitung)

**Datenschutzfolgeabschätzung (DSFA)** (umfangreiche Verarbeitung)

- Mit Datenschutzexperten abklären
- Details unter: <https://www.wko.at/datenschutz/eu-dsgvo-datenschutz-folgenabschaetzung-konsultation>

**Datenverlust**

- Meldung an die Datenschutzbehörde
- Benachrichtigung der betroffenen Person(en)
- Details unter: <https://www.wko.at/datenschutz/eu-dsgvo-meldung-von-datenschutzverletzungen>



## Sind Bildaufzeichnungen biometrische Daten?

- Fotos und Videos sind in der DSGVO nicht explizit als sensible Daten definiert
- Zweckbindung und Auswertungsabsicht ist ausschlaggebend
- Biometrie liegt vor, wenn Gesichtssymmetrie verarbeitet wird (Clearview, FB, Smartphone)
- Mehr als 50% der Beschwerden bei der DSB beziehen sich auf Videoüberwachung

## Bildaufzeichnungen

### Fotos

- Klare **Definition des Zwecks und der Dauer** der Verarbeitung
- Überwiegend ist **Einwilligung** erforderlich
  - Mitarbeiter:innen-Fotos auf Webseite oder Social Media
  - Auf Kundenausweisen, Eintrittskarten (zB Fitnessstudios)
  - Abbildungen von Kindern → ausschließlich mit Einwilligung der/des Erziehungsberechtigten
- Überwiegend berechtigtes Interesse bei **Veranstaltungen** → **Informationspflicht**
- Fotos zu **Marketingzwecken** → **Vertrag** ist einer Einwilligung vorzuziehen
- Auch **Urheberrecht und Recht am eigenen Bild** ist miteinzubeziehen
- Details unter: <https://www.wko.at/oe/information-consulting/werbung-marktkommunikation/fotografie-und-werbung>

## Bildaufzeichnungen

### Videoüberwachung

- berechtigtes Interesse gegeben?
- sensible Daten sind es nur, wenn das Videomaterial verarbeitet wird, um besondere Datenkategorien abzuleiten bzw. diese auszuwerten
- Kennzeichnungs- und Informationspflicht (Piktogramm + Info)
- Speicherdauer max. 72 Stunden
- Details unter: <https://www.wko.at/datenschutz/eu-dsgvo-bildverarbeitung>



# Eine Stunde Datenschutz

## Auskunftsrecht

Mag. Judith Leschanz

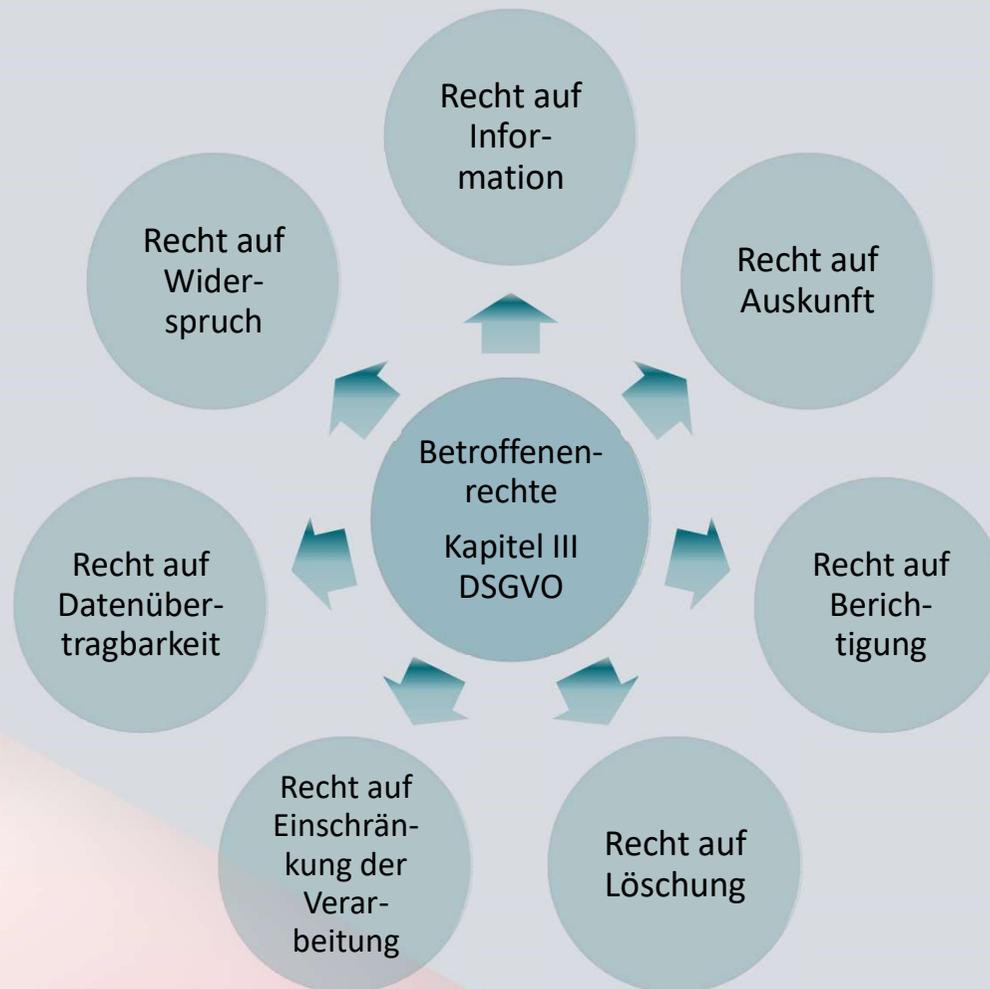
23. Jänner 2024

## Ansprechpartner



- Geschäftsführerin der Secur-Data Betriebsberatungs-GmbH
- Data Protection Officer der A1 Group
- Vorstandsvorsitzende des Vereins österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at
- Mitgründerin des Datenschutzvereins Privacy Ring
- Vortragende an der Universität für Weiterbildung Krems

## Betroffenenrechte



Betroffenenrechte können in **Beschwerdeverfahren** oder auf dem **Klageweg** geltend gemacht werden.

## Transparenz und Informationspflichten

### Was muss ich im Vorhinein tun?

Informationspflichten gem. Art. 13 und 14 DSGVO und Rechtebelehrung gem. Art. 15 bis 22 DSGVO in

- präziser,
- transparenter,
- verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitstellen

### Wo muss ich die Informationen bereitstellen?

Die Informationen können schriftlich oder elektronisch bereitgestellt werden (*Website, Signatur, Papier*)

### Wie viel Zeit habe ich für die Erfüllung von Betroffenenrechten?

Grundsätzlich **unverzögerlich, spätestens** 1 Monat ab Kenntnis/Zugang (**Beweislast bei Verantwortlichem**)

Fristverlängerung bei hoher Komplexität oder Anzahl an Anträgen auf weitere 2 Monate möglich (insgesamt max. 3 Monate Zeit)

Angabe von **Grund der Verzögerung** und Beschwerderecht bei Datenschutzbehörde

# Betroffenenrechte

## Auskunftsrecht – Inhalt

[EDPB Guideline 01/2022 zur Auskunft \(V 2.0\)](#)

### Allgemeiner Inhalt

- Verarbeitungszwecke und Rechtsgrundlagen
- Datenkategorien
- Empfänger (inkl. Auftragsverarbeiter + Drittland-Übermittlung)
- Dauer der Speicherung
- Weitere Betroffenenrechte
- Beschwerderecht bei der DSB

### Inhalt bei Dritten erhoben

- Herkunft der Daten
- Logik und Tragweite einer autom. Entscheidungsfindung
- Bei Drittland-Übermittlung – getroffene geeignete Garantien

### Kopie des Datenbestandes

- Auch elektronisch möglich
- Ohne Rechte und Freiheiten Dritter zu beeinträchtigen



Eine „**Nullauskunft**“ ist ebenfalls verpflichtend! Bei der Anfrage nach Auskunft werden zudem immer personenbezogene Daten verarbeitet.

# Betroffenenrechte

## Auskunftsrecht – Die telefonische Anfrage

### Wer stellt die Anfrage?

- Name der Anrufer / Besucher
- Funktion der Anrufer
- ggf. Name der Behörde
- Rückrufnummer und andere Kontaktmöglichkeiten

### Um welchen Sachverhalt geht es?

- Zweck der Anfrage
- Begründung, warum diese Anfrage vom Verantwortlichen beantwortet werden soll

### Welche Informationen müssen Sie zusätzlich festhalten?

- Identität der Betroffenen, deren Daten gewünscht werden
- Art und Umfang der Informationen
- Rechtsgrundlage der Anfrage

Wie gehen Sie mit einer telefonischen Anfrage um?

- Es sollten **keine** telefonischen Auskünfte erteilt werden
- Verweisen Sie auf den **Schriftweg** mit Angabe von Rechtsgrundlage und Identifikationsnachweis
- **Dokumentieren** Sie die Anfrage intern
- Für die weitere Vorgehensweise, insbesondere zur Klärung der Berechtigung der Anfrage, ist unverzüglich der **Datenschutzbeauftragte** beizuziehen.

## Betroffenenrechte

### Darf ich Geld für die Erfüllung von Betroffenenrechten verlangen?

Nein, außer Anträge werden **exzessiv** (zB häufig wiederholend) oder offenkundig **unbegründet**

Dann angemessenes Entgelt oder Verweigerung.

**Grund** für Ausübung eines Betroffenenrechts **unerheblich**

[EuGH 26.10.2023 - C 307/22](#)

[BVwG 24. 5. 2019 - W258 2205602-1/8E](#)

**Wichtig:** Dokumentation anlegen und Aufbewahrungsfristen festlegen.

Betroffenenbegehren können auch Gegenstand eines längeren Beschwerdeverfahrens oder einer amtswegigen Prüfung werden.

### Identifizierung von Betroffenen?

**Einzelfallbeurteilung** – nur bei begründeten Zweifeln dürfen nähere Informationen verlangt werden.

## Betroffenenrechte

### Ist eine Ausweiskopie zwingend einzuholen?

Bestehen **begründete** Zweifel über die Identität der betroffenen Person, kann eine Ausweiskopie ein taugliches Mittel sein. Es ist nicht zwingend vorgesehen, wenn Identität anders bestätigt werden kann.

### Rechtsprechung:

Eindeutig identifizierbare Person durch Standort, familiäre, wirtschaftliche und soziale Identität der Beschwerdeführerin begründet keine Zweifel über die Identität.

Bescheid vom 14. 1. 2019, GZ DSB-D123.224/0004-DSB/2018

### Bußgeld: EUR 525.000

Strafe für DPG Media Magazines B.V. für die Bearbeitung von Auskunfts- und Löschanfragen von Kunden nur, wenn eine Kopie des Ausweises in einem Portal hochgeladen oder postalisch an das Unternehmen gesendet wurde. Verstoß gegen Art. 12 Abs. 2 DSGVO

## Betroffenenrechte

### LArbG Baden-Württemberg Urteil vom 27.7.2023, 3 Sa 33/22

**Sachverhalt:** Ausgeschiedener AN verlangt zweitinstanzlich die Erteilung von Auskunft nach Art. 15 DSGVO und macht immateriellen Schadensersatz wegen Verletzung der Auskunftspflicht und wegen der Verwendung von Video- und Fotoaufnahmen mit Abbildungen von ihm nach Beendigung des Arbeitsverhältnisses geltend.

1. Die verspätete Auskunftserteilung auf ein Verlangen nach Art. 15 Abs. 1 DSGVO stellt als solche keinen **immateriellen Schaden** dar. Ein bloßer Verstoß gegen die Vorgaben der Datenschutzgrundverordnung genügt nicht, um einen Schadensersatzanspruch gemäß **Art. 82 Abs. 1 DSGVO** zu begründen.
2. Art. 82 Abs. 1 DSGVO enthält auch **keine Vermutung** dahingehend, dass der mit einem Verstoß gegen die Datenschutzgrundverordnung einhergehende Kontrollverlust über die eigenen Daten als solcher zu einem ersatzfähigen immateriellen Schaden führt.
3. Ein Antrag gemäß Art. 15 Abs. 1 Satz 1 Hs 2 DSGVO auf Auskunftserteilung über „sämtliche personenbezogenen Daten“ genügt regelmäßig nicht dem **Bestimmtheitserfordernis** des § 253 Abs. 2 Nr. 2 ZPO.

### Siehe auch: LArbG Düsseldorf Urteil vom 28.11.2023, 3 Sa 285/23

# Betroffenenrechte: Auskunft

## Verfahren EuGH

- **C-154/21 vom 12. 1 . 2023 (Vorlage von OGH 18. 2. 2021, 6 Ob 159/20f) – RW gegen Österr. Post AG**

Der Verantwortliche muss dem Betroffenen im Falle einer Anfrage gem. Art. 15 DSGVO die Identität der Empfänger mitteilen,

- wenn der Betroffene dies wünscht
- die Identifizierung des Empfängers für den Verantwortlichen möglich ist und
- die Anfrage des Betroffenen nicht offensichtlich unbegründet und exzessiv ist.

### **Der Verantwortliche hat kein Wahlrecht!**

- **C-487/21 vom 4. 5. 2023 (Vorlage von BVwG, W211 2222613-2/12, 9. 8. 2021) – CRIF GmbH**
  - Der Betroffene hat das Recht eine originalgetreue und verständliche Reproduktion aller personenbezogenen Daten zu erhalten, wenn dies unerlässlich ist um ihm die wirksame Ausübung der durch die DSGVO verliehenen Rechte zu ermöglichen.
  - Der Begriff „Kopie bezieht sich nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen.

## Prozess für Betroffenenrechte

### Datenschutzbeauftragter/Datenschutzkoordinator

Eingang eines Antrags für Betroffenenrechte  
Entgegennahme über zentralen Kanal im Unternehmen

Prüfung der Anfrage auf ihren Inhalt  
Identitätsprüfung – im Zweifel: Ausweiskopie einholen  
Workflow für Abteilungen einleiten

- Auskunft: Kopie der Daten oder Nullauskunft  
- Löschung: Prüfung lösch hemmender Aufbewahrungsfristen  
Sperrung in CRM veranlassen

Beantwortung des Betroffenenbegehrens binnen offener Frist  
Aktvermerk über etwaige Handlung im Akt / Reporting anlegen

**Best Practice:**

Postfach mit [datenschutz@unternehmen.at](mailto:datenschutz@unternehmen.at) anlegen und zentrale Verwaltung.

Eingang nach Erhalt bestätigen  
„Sehr geehrter Kunde/et al, wir bestätigen den Eingang Ihrer Anfrage“

Fristenlauf notieren =  
zwei Fristen: Erledigung bis 1 Woche vor Fristende, Absendung zum Stichtag.

**Best Practice:**

Identität der Betroffenen sicherstellen mittels Vorname-Nachname-Adresse-E-Mail

Vorlagen für Auskunftsbegehren und Löschanträge erstellen

Bei Abteilungen Verantwortliche für Bearbeitung der Anfrage benennen

**Best Practice:**

Im Workflow beachten:

- Einwilligungen bei Marketing/Sales widerrufen
- Löschung oder Sperrung im CRM

Bei Buchhaltung und Controlling gilt Aufbewahrungsfrist nach BAO für Verrechnungsdaten

Prüfung, ob berechtigte Interessen für etwaige Rechtsverteidigung bestehen (AN-Daten, Beschwerdefall bei DSB etc.)

**Best Practice:**

Einhaltung der Fristen durch gezielte Erinnerung im Kalender  
Ausendung über zentrale Stelle für sichergestellte und dokumentierte Beantwortung

Errichtung eines Kontroll- und Reportingsystems (Dokumentation)

Aktvermerk für etwaige Ansprüche aus der Beantwortung

# Betroffenenrechte

## Best Practices

### Vorlagen für Betroffenenrechte bereithalten

- Einheitliches Formular für Auskunftsrechte etc. erstellen
- Vorlage für Antwort-Formular mit Belehrung über Rechtsweg zu DSB erstellen
- Richtlinien für Mitarbeiter im Umgang mit personenbezogenen Daten erstellen

-> Papierrichtlinie, Lösch-Richtlinie, CRM-Richtlinie für Datenrichtigkeit

### Verarbeitungsverzeichnis als zentraler Anknüpfungspunkt

- Abbildung der Datenanwendungen, Empfänger, Speicherdauer
- Zuständige Abteilung und Mitarbeiter laufend schulen
- Verzeichnisse stets aktualisieren

### Dokumentationspflichten beachten

- Dauer der Aufbewahrung nach Betroffenenbegehren idR bis Abschluss der Verjährung vgl. § 24 Abs. 4 DSG: 1 Jahr, längstens 3 Jahre (siehe [RS Wolfgang Fellner – Anspruch verjährt](#))

Sehr geehrte Frau, sehr geehrter Herr!

Wir haben Ihren Antrag auf Auskunft nach Art. 15 DSGVO am [Datum] erhalten.

Sie haben darin Ihre Identität ausreichend nachgewiesen.

Hiermit beantworten wir Ihren Antrag in offener Frist von einem Monat mit einer Liste der zu Ihnen verarbeiteten Daten und relevanten Datenverarbeitungen.

In der Anlage ist eine Kopie zu Ihren Daten angefügt.

[...]

Ihnen stehen grundsätzlich die Rechte auf Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch zu.

Wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, besteht ein Beschwerderecht bei der Österreichischen Datenschutzbehörde.

# Betroffenenrechte

## Neues zum Auskunftsrecht

- große Anzahl von Entscheidungen seitens DSB und der datenschutzrechtlichen Aufsichtsbehörden
- Guidelines der [EDSA \(01/2022 on data subject rights\)](#)
- Judikatur: EuGH **RS C-487/21** vom 4. Mai 2023, CRIF/DSB [„Kopie oder nicht Kopie?“](#)
  - Art. 15 Abs. 1 S 3 DSGVO bedeutet, dass der betroffenen Person eine **originalgetreue und verständliche Reproduktion aller seiner personenbezogenen Daten** zu erhalten hat.
  - Dieses Recht setzt das Recht voraus, eine Kopie von Auszügen oder Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken zu erlangen, wenn die **Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch die DSGVO verliehenen Rechte zu ermöglichen.**
  - Der iSd Art. 15 Abs. 3 S 3 DSGVO verwendete Begriff „**Informationen**“ bezieht sich ausschließlich auf personenbezogene Daten.
- [Reichweite des Auskunftsanspruchs](#)  
C-154/21, 12. Jänner 2023, RW/Österreichische Post AG  
Verantwortlicher ist verpflichtet, auf Anfrage die **Identität** der Empfänger mitzuteilen  
(**Kategorien** nicht ausreichend)

# Terminavisos

**KOSTENLOSER** Datenschutzsprechtag  
am 06. Februar 2024, ab 11:00 Uhr in Spittal | Drau

Nächste Folge „Eine Stunde Datenschutz“  
am 13. März 2024 von 09:00 bis 10:30 Uhr