



# Eine Stunde Datenschutz

## Unternehmerische Mindestanforderungen aus der Perspektive des Datenschutzes

Juristische Mindestanforderungen

Technische Mindestanforderungen

Organisatorische Mindestanforderungen

# Eine Stunde Datenschutz

---

- Webinar-Reihe des Arbeitskreises Datenschutz sowie des Servicezentrums, Team Rechtsservice, der Wirtschaftskammer Kärnten
- Vortragende:  
*Dr.iur. Ludwig Notsch | Ing. Christian Kügerl*  
*DKff. Anke Obersteiner*
- Moderation:  
*Dr. Christina Kitz-Überall*

# Eine Stunde Datenschutz

Unternehmerische Mindestanforderungen aus der Perspektive des Datenschutzes

- Dr. Ludwig Notsch | Internetjurist | geprüfter Datenschutzexperte  
+43/463/310 557 | E: kontakt@internetjurist.at | A: Lastenstraße 14,  
A-9020 Klagenfurt a. WS. | M:+43/676/660 93 99 | <https://www.INTERNETJURIST.at>
- DKff. Anke Obersteiner | Geschäftsführerin der DDSB.AT Beratung GmbH  
Datenschutzexpertin und ISMS - Managerin & -Auditorin nach ISO 27001 TÜV  
+43 676 7278708 | T:+43 1 4200050 20 | M: [anke.obersteiner@ddsb.at](mailto:anke.obersteiner@ddsb.at) | [www.ddsb.at](http://www.ddsb.at)
- Ing. Christian Kügerl | perfect solutions e.U.  
Pörtschach am Berg 8, 9063 Maria Saal | +43 664 545 80 60  
[office@perfect-solutions.at](mailto:office@perfect-solutions.at)
- <https://www.wko.at/branchen/k/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/arbeitskreis-datenschutzexperten.html>
- Dr. Christina Kitz-Überall, Servicezentrum, Rechtsservice, Wirtschaftskammer Kärnten  
E [christina.kitz-ueberall@wkk.or.at](mailto:christina.kitz-ueberall@wkk.or.at) | T 05 90 90 4 - 723



**Unternehmerische  
Mindestanforderungen  
aus datenschutzrechtlicher Sicht**

**Dr.iur. Ludwig Notsch**

# Die Außenwirkung

## Datenschutzerklärung auf der Homepage

- Erfüllung der Informations**pflichten** nach Art 13 und 14 DSGVO
- Personenbezogene Daten, die direkt bei der „betroffenen Person“ erhoben werden
- **Zwingende Inhalte sind beispielsweise**
  - Name und Kontaktdaten des Verantwortlichen bzw. seines Vertreters und / oder Namen und Kontaktdaten eines gemeldeten Datenschutzbeauftragten
  - Zweck der Datenverarbeitung
  - Rechtsgrundlagen der Datenverarbeitung
  - Dauer der Datenspeicherung bzw. Kriterien für die Dauer

# Die Außenwirkung

## Datenschutzerklärung auf der Homepage

- Zwingende Inhalte (Teil II) sind beispielsweise

Empfänger/ Kategorien der erhobenen Daten

Absicht die Daten in **Drittländer** zu übertragen (sicheres/ unsicheres Drittland)

berechtigtes Interesse (Argumentationskette erforderlich)

# Die Außenwirkung

## Warum ist die Datenschutzerklärung so wichtig?

- Für jeden unmittelbar einsehbar = **öffentlich**
- **Aktualität** sofort erkennbar
- Erste **Angriffsfläche** für Wettbewerb, unzufriedene „Ex“-Mitarbeiter, Kunden, etc

# Internationaler Datenverkehr

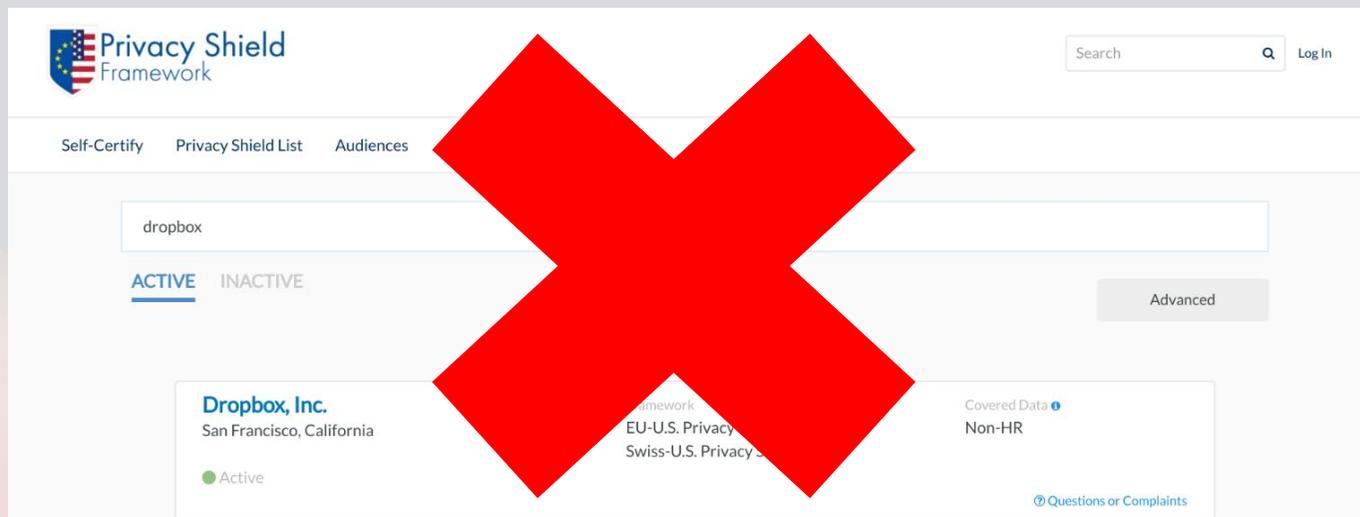


# Drittstaaten-Thematik am Beispiel USA

## Privacy Shield = Geschichte

**ACHTUNG:** Der Privacy Shield ist seit **16.7.2020** außer Kraft!

Es ist somit eine eigene AVV bei Datenübermittlung an Drittstaat USA erforderlich, um rechtskonform zu arbeiten



# Drittstaaten-Thematik am Beispiel USA

## NEU = E.U. – U.S. Data Privacy Framework

Angemessenheitsbeschluss der Europäischen Kommission

U.S. Diensteanbieter muss entsprechend als **AKTIV** gelistet sein

Auftragsdatenverarbeitungsvereinbarung muss abgeschlossen sein

# Drittstaaten-Thematik am Beispiel USA

**Ist mein U.S. Diensteanbieter gelistet?  
ZB Microsoft, Apple, Google, etc**

Direkter Check über:

<https://www.dataprivacyframework.gov/s/>



Log in

ACTIVE   INACTIVE

Advanced Search

< Previous

Next >

[Self-Certify](#)

[Data Privacy Framework List](#)

[Audiences](#)

- [U.S. Businesses](#)
- [European Businesses](#)
- [European Individuals](#)
- [Data Protection Authorities](#)

[About](#)

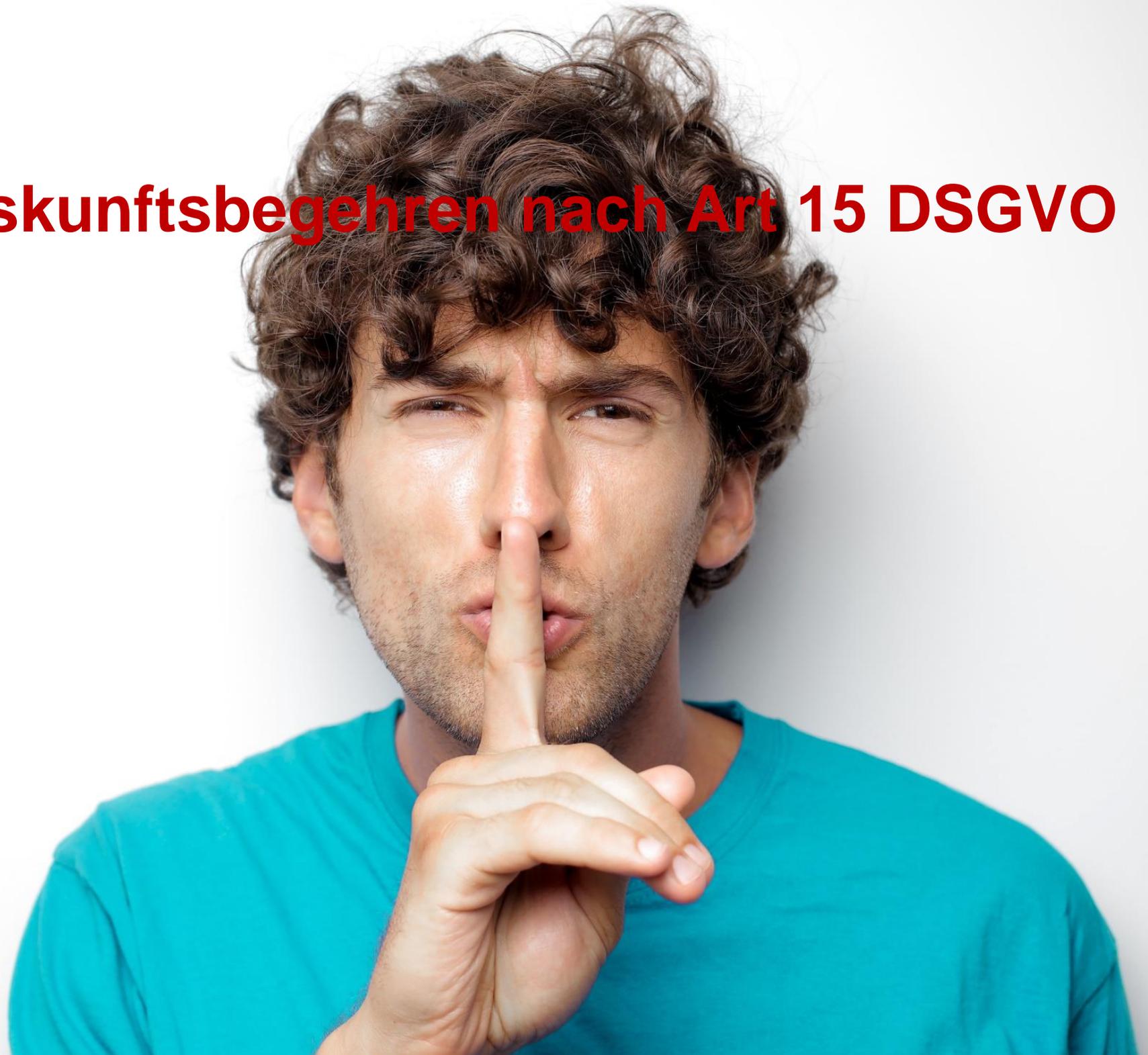
- [Program Overview](#)
- [Framework Text](#)
- [Inactive Participants](#)
- [News & Events](#)
- [Contact](#)
- [Privacy Program](#)



The [International Trade Administration \(ITA\)](#), U.S. Department of Commerce manages this site to facilitate the Data Privacy Framework program in the United States. External links to other Internet sites should not be construed as an endorsement of the views or privacy policies contained therein. This site contains PDF documents. A [PDF Reader](#) is available from Adobe Systems Incorporated.

U.S. Department of Commerce | Data Privacy Framework Program | 1401 Constitution Avenue, N.W. | Room 11018 | Washington, D.C. 20230

# Auskunftsbegehren nach Art 15 DSGVO



# Auskunftsbegehren nach Art 15 DSGVO

## Das Betroffenenrecht auf „Auskunft“

- Bei Inanspruchnahme des Auskunftsrechts sind dem Betroffenen alle ihn betreffenden pers.bez. Daten als **Kopie** (schriftlich, elektronisch) **kostenlos** zur Verfügung zu stellen
- Die Rechte und Freiheiten anderer Personen dürfen nicht beeinträchtigt werden

# Auskunftsbegehren nach Art 15 DSGVO

- Grundsätzlich ist die Auskunft **schriftlich** zu erteilen, und zwar in einer kompakten, transparenten, verständlichen und leicht zugänglichen Form.
- Frist **1 Monat** (begründete Verlängerung möglich)
- Frist beginnt ab **Zugang des Auskunftsbegehrens im Unternehmen** zu laufen
- 1 Monat/ 4 Wochen, klingt lange, ist es aber nicht!



# **DANKE!** für die **Aufmerksamkeit**

**Weiter geht es mit:**

**„Unternehmerische Mindestanforderungen aus technischer Sicht -  
Ing. Christian Kügerl“**

# Unternehmerische Mindestanforderungen aus **technischer** Sicht

**Ing. Christian Kügerl**

# Übersicht

**Technische Grundlagen und Standards**

**Ratsame Anschaffungen**

**Regelmäßige Aufgaben**

# Technische Grundlagen und Standards

## Datensicherheit

- Passwörter
- Backups
- Verschlüsselung
- Zugangsberechtigungen
- MFA (bzw. 2FA)

# Technische Grundlagen und Standards

## Passwörter

- Länge > Komplexität
- Änderungszyklen (Pro / Contra)
- Erstellung und Merkbarkeit
- Verwaltung / Weitergabe

# Technische Grundlagen und Standards

## Backups

- 3-2-1 Regel
- Intervalle / Datenverlust
- Unterschied Daten / Systeme
- Verpflichtung laut DSGVO

# Technische Grundlagen und Standards

## Verschlüsselung

- Stand der Technik (SSL, Bitlocker, etc.)
- Einrichtung
- Vorteile abseits DSGVO
- E-mails (sensible Daten)

# Technische Grundlagen und Standards

## Zugangsberechtigungen

- Was ist der „Admin“ ?
- Vorteile
- Sinnvolle Beschränkungen
- Vertretungen

# Technische Grundlagen und Standards

## MFA (bzw. 2FA)

- Was ist eine MFA / 2FA ?
- Anwendungsbereiche
- Varianten
- Vorsicht bei Phishing

# Ratsame Anschaffungen

## Übersicht

- Windows Professional  
(Bitlocker, Zugangsberechtigungen, ...)
- Backup-Systeme und Medien (Inhouse, Offsite, Cloud, ...)
- Schutz vor Schadsoftware (Varianten, Bedrohungen)

# Regelmäßige Aufgaben

## Übersicht

- Betriebssysteme updaten !
- Virenschutz updaten !
- Programme updaten
- Backups erstellen und regelmäßig prüfen
- E-mails archivieren
- Zugangsberechtigungen evaluieren

# **DANKE!** **für die** **Aufmerksamkeit**

**Weiter geht es mit:**

**„Unternehmerische Mindestanforderungen aus organisatorischer Sicht – DKff. Anke Obersteiner“**

# **Unternehmerische Mindestanforderungen**

## **aus organisatorischer Sicht**

### **DKff. Anke Obersteiner**

# Datenschutz durch Organisationsgestaltung

- [ ] Datenschutzbeauftragten bestimmen, falls gesetzlich erforderlich oder aus organisatorischen Gründen sinnvoll.
- [ ] Datenschutzverantwortlichkeiten im Unternehmen klar definieren und kommunizieren.
- [ ] Regelmäßige Treffen des Datenschutzteams etablieren, um Datenschutzthemen zu besprechen.
- [ ] Datenschutzmanagementsystem (DSMS) implementieren und pflegen.
- [ ] Datenschutzstrategie entwickeln, die mit den Geschäftszielen in Einklang steht.

# Mitarbeiterschulung und -bewusstsein

- [ ] Regelmäßige Datenschutzs Schulungen für alle Mitarbeiter planen und durchführen.
- [ ] Datenschutz-Handbuch und Richtlinien für Mitarbeiter bereitstellen.
- [ ] Datenschutzbewusstsein durch interne Kampagnen stärken.
- [ ] Sicherheitsbewusste Unternehmenskultur fördern.

# Datenschutzrichtlinien und -verfahren

- [ ] Datenschutzrichtlinien erstellen, regelmäßig aktualisieren und allen Mitarbeitern zugänglich machen.
- [ ] Verfahren für die Datenerhebung, -verarbeitung und -löschung definieren.
- [ ] Prozesse für die Reaktion auf Anfragen von Betroffenen gemäß DSGVO (z.B. Auskunftsrecht) etablieren.
- [ ] Verfahren für die Meldung und Handhabung von Datenschutzvorfällen entwickeln.

# Verträge und Zusammenarbeit

- [ ] Datenschutzklauseln in Verträge mit Dritten (z.B. Lieferanten, Partner) aufnehmen.
- [ ] Auftragsverarbeitungsverträge (AVV) mit externen Dienstleistern abschließen.
- [ ] Prozess für die Auswahl und Überprüfung von Auftragsverarbeitern etablieren.

Diese Auszüge der Datenschutz - Checkliste dient als Grundlage für organisatorische Datenschutzmaßnahmen. Für eine vollständige und wirksame Datenschutzstrategie sollten Unternehmen jedoch immer individuell prüfen, welche Maßnahmen aufgrund ihrer spezifischen Situation, Größe und Branche notwendig sind.

# Social Engineering: Die Psychologie des Datenschutzes



# Clean Desk



# Drucker und sonstige Geräte



# Datenschutzkonforme Entsorgung



**DANKE!**  
**für die**  
**Aufmerksamkeit**

# Terminavisos

Nächste Folge „1 Stunde Datenschutz“ am 23.01.2024 von 09:00 bis 10:30 Uhr

Thema: Ausgewählte datenschutzrechtliche Aspekte für Unternehmen

Vortragende:

Mag. Judith Leschanz (Auskunftsrecht)

Dr. Patricia Radl-Rebernicg (Datenschutz im touristischen Umfeld)

Mag. Stefan Ugovsek (Umgang mit sensiblen Daten)