Datenschutz-Grundverordnung (DSGVO)

und deren praktische Umsetzung

IHK

Inhalt

Anwendungsbereich der DSGVO

Personenbezogene Daten (pbD): alle Informationen, die sich auf eine **identifizierte** oder **identifizierbare** natürliche Person beziehen lassen.

Beispiele pdD:

Name	Geburtsdatum	E-Mail	Anschrift

Gesundheitsdaten	Religion	Gewerkschaftszugehörigkeit	Sexualleben

Besondere Schutzbedürftigkeit

Verarbeitung (sehr umfangreiche Definition): jeder – **mit** oder **ohne** Hilfe automatisierter Verfahren – ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit pbD

Grundprinzipien

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  → Daten nur auf Rechtsgrundlage, fair und transparent verarbeiten
- **Zweckbindung**
  → pbD dürfen nur zum angegebenen Zweck verarbeitet werden
- **Datenminimierung**
  → nur benötigte Daten erheben
- **Richtigkeit**
  → auf die Richtigkeit der Daten ist zu achten
- **Speicherbegrenzung**
  → nicht benötigte Daten müssen gelöscht werden
- **Integrität und Vertraulichkeit**
  → Daten müssen vor Zugriff Dritter geschützt werden

Rechenschaftspflicht!

Nachweis muss durch das Unternehmen erbracht werden!

Rechtmäßigkeit der Verarbeitung

Rechtmäßigkeit: Jede Verarbeitung von pbD bedarf einer **Rechtsgrundlage** (Art. 6 Abs.1 DSGVO)

- Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen
- Berechtigtes Interesse
- Einwilligung
- Erfüllung rechtlicher Verpflichtung
- Lebenswichtige Interessen der Betroffenen oder einer anderen natürlichen Person
- Wahrnehmung einer Aufgabe im öffentlichen Interesse

Rechtmäßigkeit der Verarbeitung

Beispiel für Datenverarbeitung aufgrund von berechtigtem Interesse

Direktwerbung per Post	Weihnachtskarten	Onlineshop und Auslieferung über externe Dienstleister

berechtigte Interessen des Verantwortlichen oder eines Dritten **und keine** entgegenstehenden Interessen der betroffenen Personen
→ **Interessenabwägung**

Wichtig!

- Vorabinformation des Betroffenen/Kunden
- Dokumentation der Interessenabwägung

Datenschutzbeauftragter

Benennungspflicht des **Datenschutzbeauftragten**
(Art. 37 Abs. 1 DS-GVO i.V.m. geänderten § 38 Abs. 1 BDSG):

1. Ab **20 Personen**, die ständig mit der automatisierten personenbezogenen Datenverarbeitung beschäftigt sind
2. Kerntätigkeit**:** umfangreiche und systematische Überwachung von Betroffenen oder die Verarbeitung sensibler Daten i.S.d. Art. 9 oder 10 DS-GVO
3. Unabhängig von der Anzahl der Personen, wenn Verarbeitungen von pbD vorliegen, die einer **Datenschutz-Folgeabschätzung** unterliegen

Datenschutzbeauftragter

Liste mit externen Datenschutzbeauftragten:

- Gesellschaft für Datenschutz und Datensicherheit (GDD)
  https://www.gdd.de/
- Berufsverband der Datenschutzbeauftragten Deutschlands
  https://www.bvdnet.de/

Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO

Verpflichtung zur Erstellung entfällt (Art. 30 Abs. 5 DSGVO):

1. Weniger als 250 MA
2. Kein Risiko für Rechte und Freiheiten Betroffener
3. Keine Verarbeitung sensibler pbD nach Art. 9 oder 10 DSGVO
4. Gelegentliche Verarbeitung

→ In der Regel greift die Ausnahme nicht

Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO

1. Welche personenbezogene Daten (pbD) werden verarbeitet?

- Mitarbeiterdaten (Name, Anschrift, Geburtstag etc.)
- Kundendaten (Rechnung, Anschrift, E-Mail etc.)

2. Wo werden die pbD verarbeitet?

- Personalabteilung
- Vertrieb, Buchhaltung

3. Wie werden die pbD verarbeitet?

- Bewerberverwaltung etc.
- Rechnungsstellung, Newsletter-Versand etc.

Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO

4. Auf welcher Rechtsgrundlage werden pbD verarbeitet?

- Vertrag (Arbeitsvertrag, Kaufvertrag)
- Einwilligung (zum Newsletterversand per E-Mail)

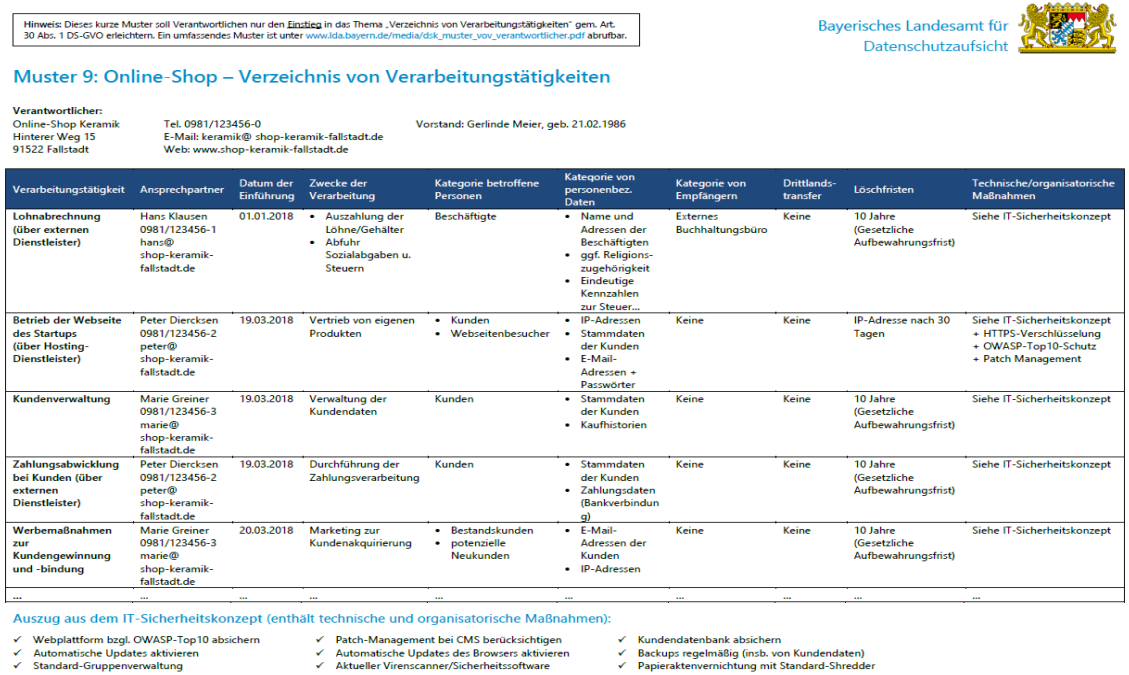
5. An wen werden pbD übermittlet?

- Steuerberater, Deutsche Post
- Auftragsverarbeiter (IT, Lohn- und Gehaltsabrechner)

6. Welches Risiko birgt die Verarbeitung (Datenschutz-Folgeabschätzung)?

- Risikobeurteilung (normal, hoch, sehr hoch)

Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO



Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 9: Online-Shop – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
Online-Shop Keramik
Hinterer Weg 15
91522 Fallstadt

Tel. 0981/123456-0
E-Mail: keramik@ shop-keramik-fallstadt.de
Web: www.shop-keramik-fallstadt.de

Vorstand: Gerlinde Meier, geb. 21.02.1986

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Hans Klausen 0981/123456-1 hans@ shop-keramik-fallstadt.de	01.01.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer...	Externes Buchhaltungsbüro	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Startups (über Hosting-Dienstleister)	Peter Diercksen 0981/123456-2 peter@ shop-keramik-fallstadt.de	19.03.2018	Vertrieb von eigenen Produkten	• Kunden • Webseitenbesucher	• IP-Adressen • Stammdaten der Kunden • E-Mail-Adressen + Passwörter	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung + OWASP-Top10-Schutz + Patch Management
Kundenverwaltung	Marie Greiner 0981/123456-3 marie@ shop-keramik-fallstadt.de	19.03.2018	Verwaltung der Kundendaten	Kunden	• Stammdaten der Kunden • Kaufhistorien	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Zahlungsabwicklung bei Kunden (über externen Dienstleister)	Peter Diercksen 0981/123456-2 peter@ shop-keramik-fallstadt.de	19.03.2018	Durchführung der Zahlungsverarbeitung	Kunden	• Stammdaten der Kunden • Zahlungsdaten (Bankverbindung)	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Werbemaßnahmen zur Kundengewinnung und -bindung	Marie Greiner 0981/123456-3 marie@ shop-keramik-fallstadt.de	20.03.2018	Marketing zur Kundenakquirierung	• Bestandskunden • potenzielle Neukunden	• E-Mail-Adressen der Kunden • IP-Adressen	Keine	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Webplattform bzgl. OWASP-Top10 absichern
- ✓ Automatische Updates aktivieren
- ✓ Standard-Gruppenverwaltung
- ✓ Patch-Management bei CMS berücksichtigen
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Kundendatenbank absichern
- ✓ Backups regelmäßig (insb. von Kundendaten)
- ✓ Papieraktenvernichtung mit Standard-Shredder

© BayLDA
Muster-Handreichungen für kleine Unternehmen

Link:
https://www.lda.bayern.de/de/kleine-unternehmen.html

Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO

1. Konstellation: gemeinsam Verantwortliche

2. Konstellation: keine gemeinsamen Verantwortlichen

3. Konstellation: Auftragsverarbeitung

Auftragsverarbeitung – Art. 28 ff. DSGVO

Auftragsverarbeitung (AV)

- Weisungsgebundenes Outsourcing einer Datenverarbeitung
- Hilfstätigkeit = keine eigenständige Dienstleistung!
- Rechtsgrundlage für Datenverarbeitung durch AVer in der EU/EWR

  → bei Drittland zusätzlich gesonderte Garantien* notwendig

Beispiele

- Webseiten-Hoster
- Tracking-Tools: sofern Nutzerdaten auf Webservern des Dienstleisters gespeichert werden

  → nicht bei Speicherung auf eigenem Webserver

zusätzlich gesonderte Garantien*

- Angemessenheitsbeschluss der Kommission (z. B. Schweiz, Israel, Argentinien)
- Standarddatenschutzklauseln
- Speziell für USA: EU-US Privacy Shield → Liste
- Verbindliche interne Datenschutzvorschriften
- genehmigte Verhaltensregeln / Zertifizierungsmechanismen

Auftragsverarbeitung – Art. 28 ff. DSGVO

Abschluss

- in schriftlicher oder
- in **elektronischer** Form

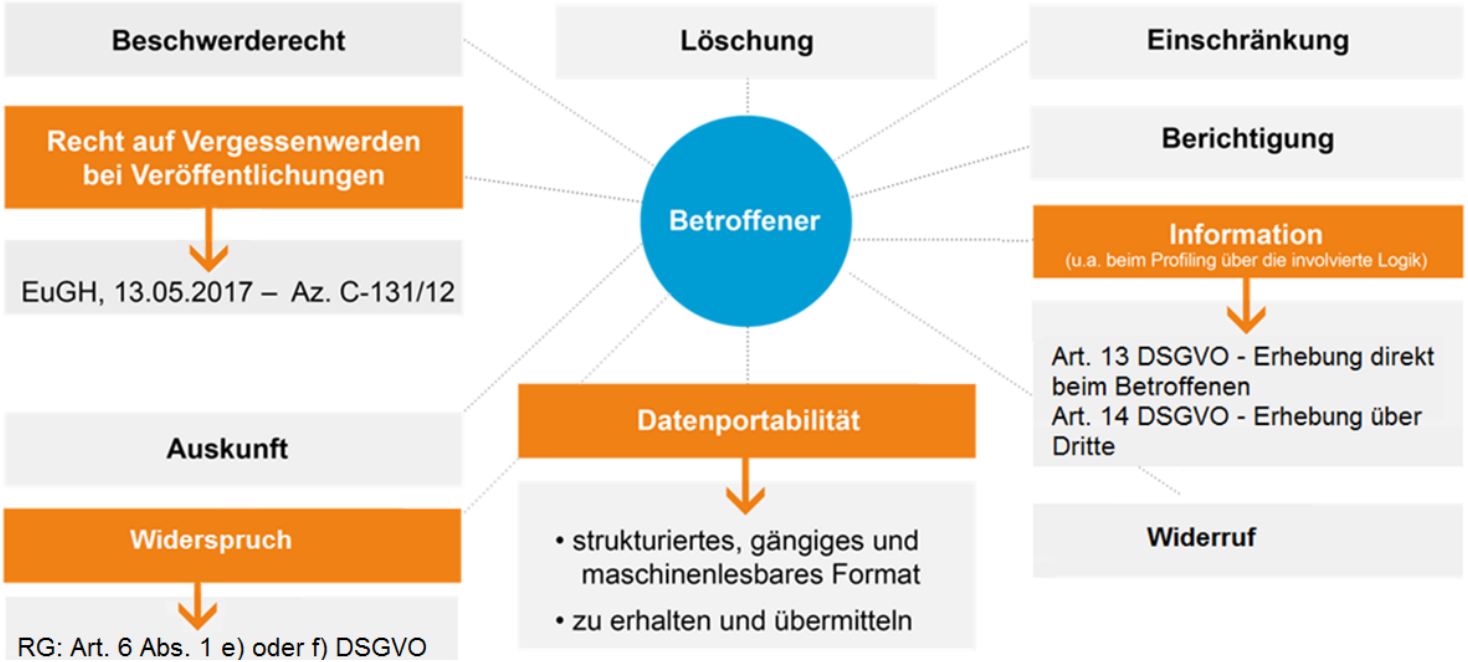
  → Signatur oder Unterschrift nicht notwendig

AVs vor dem 25.05.2018

- Rat: **Neuerstellung**

  → Änderung der gesetzlichen Mindestinhalte
- online sehr gute Muster verfügbar

Betroffenenrechte – Art. 15 ff. DSGVO



Auskunftsersuchen

- Beantwortungsfrist: **1 Monat** (Fristverlängerung mit Begründung)
- **Prozess** implementieren
- Bei fehlenden pbD →**Negativauskunft**
- Keine Auskunft bei **unbegründeten und exzessiven Anfragen**
- Keine Kopien bei **Beeinträchtigung** der Rechte und Freiheiten anderer Personen
- Stets auf alle **Betroffenenrechte** hinweisen

Informationspflichten vs. Datenschutzerklärung

Informationspflichten

- geben Auskunft darüber, welche pbD auf welcher Rechtsgrundlage, zu welchem Zweck mit welcher Speicherdauer etc. in dem Unternehmen verarbeitet werden

Datenschutzerklärung

- gibt Auskunft darüber, welche pbD auf welcher Rechtsgrundlage, zu welchem Zweck mit welcher Speicherdauer etc. beim Besuch der Unternehmenswebsite verarbeitet werden

Informationspflichten nach Art. 13, Art. 14 DSGVO

- Informationspflichten nach Art. 13 DSGVO
  - Informationserhebung **direkt** beim Betroffenen
  - Informationen müssen Betroffene zum Zeitpunkt der Datenerhebung mitgeteilt werden
- Informationspflicht nach Art. 14 DSGVO
  - Informationserhebung **über Dritte**
  - Mitteilungspflicht gegenüber Betroffenen binnen eines Monats

Informationspflichten nach Art. 13, Art. 14 DSGVO

Ausnahme (keine Informationspflicht)

- Art. 13 DSGVO – der Betroffene verfügt bereits über diese Information
- Art. 14 DSGVO – u.a. dann, wenn die Informationserteilung
  - unmöglich wäre
    oder
  - einen unverhältnismäßigen Aufwand bedeuten würde

Informationspflichten nach Art. 13, Art. 14 DSGVO

Gesamtinformation oder Medienbruch

Medienbruch:

1. Stufe: **Grundangaben** im Dokument (z. B. Vertrag)

2. Stufe: Verweis auf die Homepage zu den gesamten Informationspflichten (**Grundangaben und weitere allgemeine Pflichtangaben**)

→ **Wahlmöglichkeit**

↓

d. h. Keine Pflicht zur Angabe auf der Homepage

ihk-muenchen.de/dsgvo

Informationspflichten nach Art. 13, Art. 14 DSGVO

Muster

Umsetzung von Informationspflichten durch die IHK für München und Oberbayern

→ z. B. für Vertragspartner, Einwilligung

- DSK-Kurzpapier Nr. 10 Info (u. a. zu Visitenkarten): www.dsgvo-verstehen-bayern.de/kleine-unternehmen/

Datenschutzaufsicht für Unternehmen in Bayern:

Bayerisches Landesamt für Datenschutzaufsicht:

www.lda.bayern.de

ihk-muenchen.de/informationspflichten-datenschutz

Datenschutzerklärung – Pflichtangabe auf der Webseite

- Jede Webseite muss verfügen über:
  - Impressum
  - Datenschutzerklärung
  - Medienbruch: Informationspflichten nach Art. 13, 14 DSGVO

- Datenschutzerklärung
  - Pflichtangaben – Umfang, Art und Weise der Verarbeitung von pbD auf Webseiten
  - Transparent, d. h. auf der ersten Seite und von der Unterseite erreichbar, einfache Sprache, z. B. „Impressum/Datenschutz“ oder „Datenschutz“

Datenschutzerklärung – IHK-Handreichungen

- Auf der IHK-Homepage finden Sie:
  - IHK-Checkliste für eine Datenschutzerklärung
  - IHK-Leitfaden zur Datenschutzerklärung
    → „Dokumente und Downloads“
  - Muster von Prof. Hoeren
    → „weitere externe Informationen“

- **Kostenlose Generatoren** für die Datenschutzerklärung
  → „Datenschutz-Generatoren“

Links

- ihk-muenchen.de/dsgvo-datenschutz-webseite
- www.ihk-muenchen.de/dsgvo

Datenpannen – Art. 33 DS-GVO

- Datenpanne: **Verletzung des Schutzes pbD**
  - Verlust von Hardware (mobile Endgeräte)
  - gezielte Angriffe von außen oder versehentlich durch Mitarbeiter (Hacking)
  - unsachgemäße Verschrottung von Datenträgern
  - unrechtmäßige Übermittlung pbD (falscher Briefempfänger)
  - Offener E-Mail Verteiler (CC statt BC) etc.
- **Meldepflicht:** sobald der Schutz der pbD verletzt wurde wurde; **nicht erst bei Schäden**

Datenpannen – Art. 33 DS-GVO

- Implementierung eines Prozesses mit Umgang mit Datenpannen
  - Erarbeitung eines **Rechtekonzepts**
  - Empfehlung: Entscheidung über die (Nicht)Meldung Geschäftsführer
  - **Dokumentation** (auch jedwede Entscheidung)
- Meldeberechtigt: zuständige Datenschutzaufsichtsbehörde → für Unternehmen in Bayern ist Bayerisches Landesamt für Datenschutzaufsicht (BayLDA) zuständig (Online Tool)
- Zeitrahmen: unverzüglich, d.h. **innerhalb von 72 Stunden**
- **Bei hohen Risiken** für die Betroffenen: Meldung an die Betroffenen

Die wichtigsten Themen

- Datenschutzerklärung
- Informationspflichten
- Verzeichnis von Verarbeitungstätigkeiten
- Übermittlung pbD bzw. Auftragsverarbeitung
- Prozess des Umgangs mit Datenpannen
- Auskunftsersuchen

Tipps, Infos zur DSGVO

IHK für München und Oberbayern
- www.ihk-muenchen.de/dsgvo
- www.ihk-muenchen.de/dsgvo-datenschutz-webseiten

BayStMII
- www.dsgvo-verstehen-bayern.de

BayLDA
- www.lda.bayern.de
- www.lda.bayern.de/de/kleine-unternehmen.html

Praxishilfen GDD
- www.gdd.de/gdd-arbeitshilfen

Bitkom
- www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz-Sicherheit/index.jsp

Broschüre
„Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine – Das Sofortmaßnahmen-Paket“
(Hrsg. Bayerische Landesamt für Datenschutzaufsicht, C. H. Beck Verlag, Kosten: 5,50€)

Tipps, Infos zum rechtssicheren Internetauftritt

DSK

- www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
  Orientierungshilfe für Anbieter von Telemedien

- www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf
  Kurzpapier Nr. 3 – Werbung

- www.datenschutzkonferenz-online.de/media/en/Entschlie%C3%9Fung%20Pandemie%2003_04_2020_final.pdf
  Datenschutzgrundsätze bei der Bewältigung der Corona-Pandemie

Tipps, Infos zum rechtssicheren Internetauftritt

Rechtssichere Internetseite / Onlineshop

- www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Internetrecht/Rechtssichere-Internetseite/
- www.ihk-muenchen.de/rechtsgrundlagen-ecommerce/
- www.ihk-muenchen.de/haftung-internet

Marketing und Werbung im Internet

- www.ihk-muenchen.de/marketing-internet

Richtig Werben von A - Z

- www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Werbung-Fairer-Wettbewerb/Richtig-Werben-von-A-Z/

Abmahnung – was tun?

- www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Werbung-Fairer-Wettbewerb/Abmahnung-was-tun/

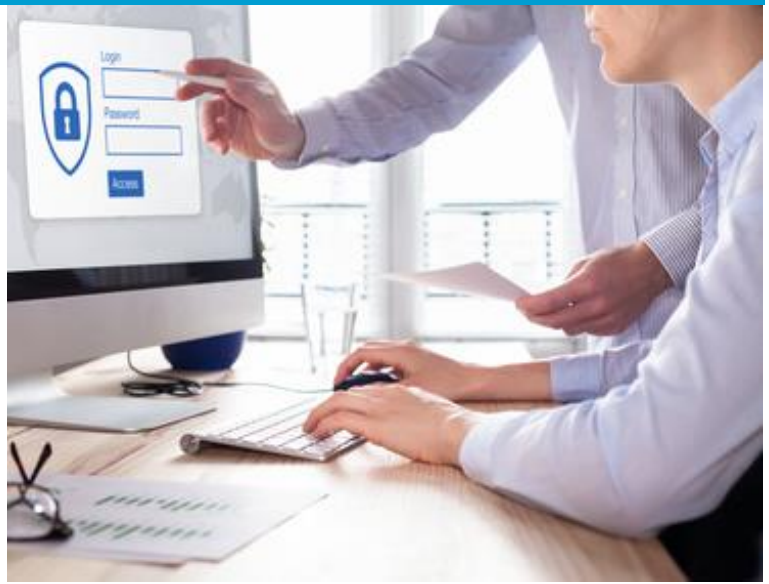
Sicherheit der Webseite // Links

BayLDA

- https-Check der Verschlüsselung der eigenen Webseite
  → www.lda.bayern.de/de/httpscheck.html

Verschlüsselung, BSI für Bürger

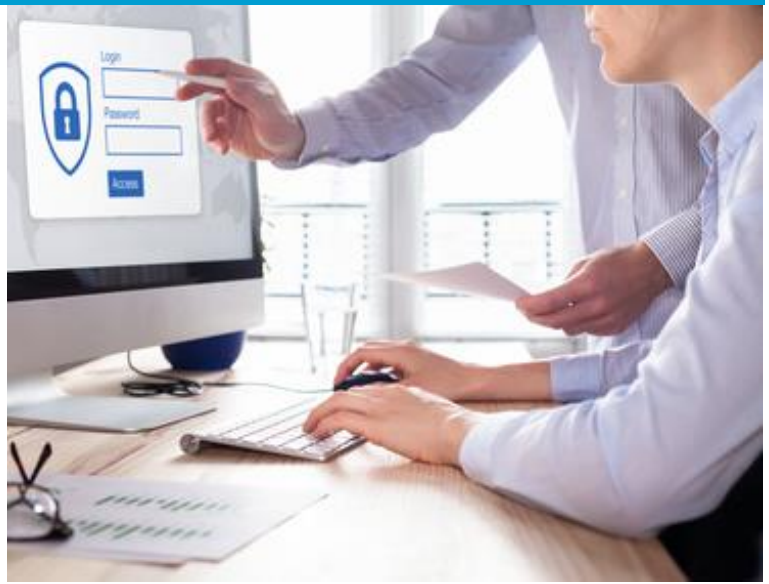
→ https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html



Tipps und Infos – Home Office und Videokonferenz

Dienstleister in Drittländern

- IHK für München und Oberbayern
  https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Daten%C3%BCbermittlung-in-Drittstaaten/
- Angemessenheitsbeschlüsse für Drittstaaten mit angemessenem Datenschutzniveau
  https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de
- Standardvertragsklauseln (SCC)
  https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087
- EU-US Privacy Shield
  https://www.privacyshield.gov/list



Angemessene Garantien nach Art. 44 DSGVO

Datenschutz – IHK-Ansprechpartner

Datenschutzbeauftragte der IHK für München und Oberbayern und des BIHK e.V.

Rita Bottler

089-5116-0

rita.bottler@muenchen.ihk.de

Referentin für Datenschutzrecht

Julia Franz

089-5116-0

franzj@muenchen.ihk.de