



# Datenschutz-Stolperfallen bei Webseiten und Online-Shops

Rechtssicher durchstarten!

# Inhalt

- I. Datenschutz-Anwendungsbereich, Rechtsgrundlagen
- II. Datenschutzerklärung
- III. Informationspflichten
- IV. Auftragsverarbeitung
- V. Aktuelle Themen
  - 1. Tracking-Tools
  - 2. Cookies
  - 3. Social Plugins
  - 4. Kontaktformular
  - 5. Video
  - 6. Sicherheit der Webseite
- VI. Weiterführende Informationen

## Anwendungsbereich der Datenschutzgesetze

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

**Verarbeitung pbD** = jeder – **mit** oder **ohne** Hilfe automatisierter Verfahren – ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit pbD

**Beispiele pdD:**

Name

Bestellverlauf

E-Mail

IP-Adresse

## Anwendungsbereich der Datenschutzgesetze

Identifizierbare personenbezogene Daten, z. B.:

Dynamische IP-Adresse

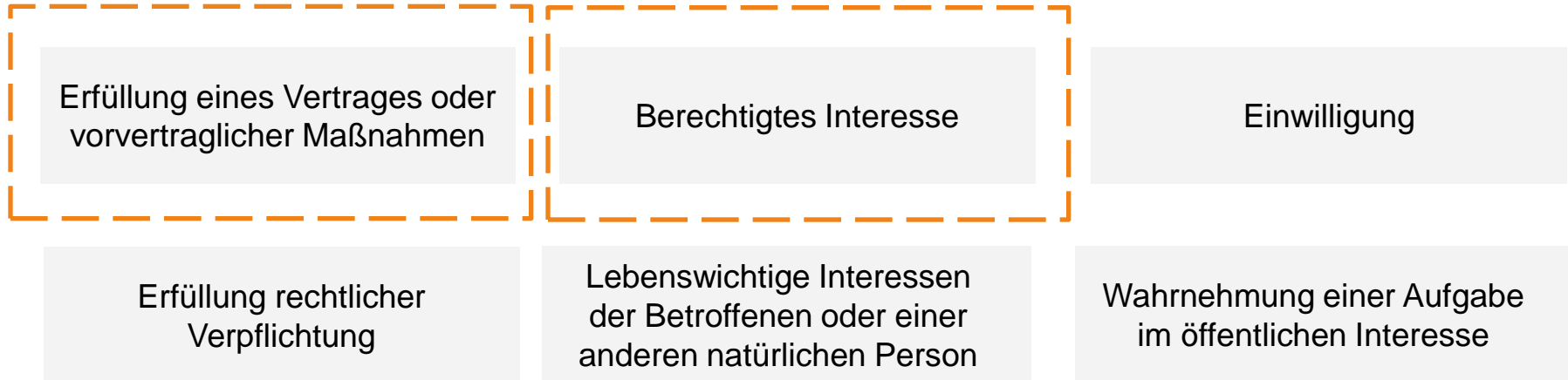


**EuGH Urteil vom 19.10.2016 –  
C 582/14 Dynamische IP-Adresse = pbD**

Begründung:  
**Nicht** alle zur Identifikation notwendigen  
Mittel müssen **in einer Hand** sein.  
Es genügt, dass der Webseite-Betreiber  
(Verantwortlicher) potenziell **legale**  
**Möglichkeiten** hat, an die  
Identifizierungsmerkmale heranzukommen.

## Rechtmäßigkeit der Verarbeitung

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



## 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

### Datenschutzerklärung – Pflichtangabe auf der Webseite

- Jede Webseite muss verfügen über:
  - Impressum
  - Datenschutzerklärung
  - 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](#)“

### Pflichtangaben im Internet-Impressum (nach TMG)

#### Muster-Impressum für Einzelunternehmen:

Muster-Shop

Max Mustermann

Musterstr. 2

80123 München

Tel: 089-1234567

Email: mustermann@muster-shop.de

USt-IdNr.: DE 9876543 (soweit vorhanden)

Nähere Informationen zum Internet-Impressum und weitere Muster unter:

<https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Internetrecht/Impressum-im-Internet/>



# Informationspflichten - Datenschutzerklärung

## Informationspflichten

- geben Auskunft darüber, welche pbD auf welcher Rechtsgrundlage, zu welchem Zweck mit welcher Speicherdauer etc. **im 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

### Datenschutzerklärung – IHK-Handreichungen

- Auf der IHK-Homepage finden Sie:
  - IHK-Checkliste
  - IHK-Leitfaden  
→ „Dokumente und Downloads“
  - Muster von Prof. Hoeren  
→ „weitere externe Informationen“
  
- **Kostenlose Generatoren** für die Datenschutzerklärung  
→ „Datenschutz-Generatoren“

#### Links

[ihk-muenchen.de/  
dsgvo-datenschutz-webseite](https://ihk-muenchen.de/dsgvo-datenschutz-webseite)

[www.ihk-muenchen.de/dsgvo](https://www.ihk-muenchen.de/dsgvo)

### Checkliste nach DSGVO: **Stets** zu veröffentlichende Angaben

#### 1. Name und Kontaktdaten des Unternehmers als Verantwortlicher

→ hierzu gehören Angaben wie Anschrift, E-Mail Adresse, ggf. Telefonnummer und Fax

#### 2. Zwecke, für die die personenbezogenen Daten verarbeitet werden

→ zu beachten: sofern die Verarbeitung auch für andere Zwecke erfolgen soll, so ist die betreffende Person vor der Weiterverarbeitung darauf hinzuweisen

#### 3. Rechtsgrundlage der Verarbeitung personenbezogener Daten

→ z. B. Einwilligung oder gesetzliche Vorschrift wie z. B. Abschluss eines Vertrages

#### 4. Speicherdauer oder Kriterien für die Festlegung der Speicherdauer

→ wie z. B. bis zur Newsletter Abmeldung

### Checkliste nach DSGVO: **Stets** zu veröffentlichende Angaben

#### 5. Bestehen der Betroffenenrechte

- Recht auf Auskunft, Berichtigung, Löschung, Recht auf Vergessenwerden, Einschränkung oder Datenübertragbarkeit und Recht auf Widerspruch bei erteilten Einwilligungen

#### 6. Beschwerderecht bei der Aufsichtsbehörde

- wenn der Betroffene der Ansicht ist, dass die Verarbeitung seiner personenbezogenen Daten rechtswidrig erfolgt

Sie sind verpflichtet, die oben genannten Angaben 1-6 zu veröffentlichen. Sollten Sie einen Punkt noch nicht veröffentlicht haben, müssen Sie dies umgehend veranlassen.

### Checkliste nach DSGVO: **Fall bezogen** zu veröffentlichende Angaben

#### 1. Kontaktdaten des Datenschutzbeauftragten

→ sofern Sie einen Datenschutzbeauftragten bestellt haben

#### 2. Berechtigte Interessen, die mit der Verarbeitung verfolgt werden

→ anzugeben, wenn die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist

#### 3. Empfänger oder Kategorien von Empfängern (d. h. Gruppen wie Hosters, Lettershops) der personenbezogenen Daten

→ sofern personenbezogene Daten an „Dritte“ übermittelt wurden

#### 4. Absicht, die personenbezogenen Daten in ein Nicht-EU-Ausland (Drittland) zu übermitteln und die Garantie für ein angemessenes Datenschutzniveau hierfür (wie z. B. Standardvertragsklausel, EU-US Privacy Shield)

### Checkliste nach DSGVO: **Stets** zu veröffentlichende Angaben

#### 5. Verpflichtung zur Bereitstellung personenbezogener Daten seitens des Betroffenen und die möglichen Folgen der Nichtbereitstellung

→ erforderlich sind personenbezogene Daten z. B. für einen Vertragsabschluss. Diese Verpflichtung findet sich auch im Gesetz wieder.

#### 6. Automatisierte Entscheidungsfindung und Profiling

→ sofern eingesetzt, sind die besondere Tragweite und die angestrebten Auswirkungen sowie die verwendete Logik oder Algorithmus anzugeben

Je nach Einzelfall können Sie verpflichtet sein, weitere Angaben zu veröffentlichen. Prüfen Sie daher nach, ob dieses auf Sie zutrifft.

## 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:

- Grundangaben\* direkt auf dem Dokument (z. B. Vertrag, Einwilligung)
- Im Übrigen Verweis auf die Homepage zu den gesamten Informationspflichten (Grundangaben\* und weitere allgemeine Pflichtangaben\*)

\* Begriffe – vgl. S. 18



**Wahlmöglichkeit**



d. h. Keine Pflicht zur  
Angabe auf der Homepage

 [ihk-muenchen.de/dsgvo](https://ihk-muenchen.de/dsgvo)

### Informationspflichten nach Art. 13, Art. 14 DSGVO

#### Grundangaben

- Name und Kontaktdaten Ihres Unternehmens
- Name und Kontaktdaten des DSB (soweit vorhanden, Funktionsangabe reicht)
- Zwecke und Rechtsgrundlagen der Verarbeitung
- Kategorien pbD (**nur bei Art. 14**)
- (Kategorien von) Empfänger pbD
- Übermittlung pbD an ein Drittland

#### Weitere Pflichtangaben

- Quelle der Daten (**nur bei Art. 14**)
- Speicherdauer
- Betroffenenrechte
- Widerrufsrecht bei Einwilligung
- Sonderfälle**
  - Spätere Zweckänderung
  - Automatisierte Entscheidungsfindung oder Profiling

## Informationspflichten nach Art. 13, Art. 14 DSGVO

### Muster

Umsetzung von Informationspflichten  
durch die IHK für München und Oberbayern

→ z. B. für Vertragspartner, Einwilligung

Datenschutzaufsicht für Unternehmen in Bayern:  
Bayerisches Landesamt für Datenschutzaufsicht:  
[www.la.da.bayern.de](http://www.la.da.bayern.de)

 [ihk-muenchen.de/informationspflichten-datenschutz](http://ihk-muenchen.de/informationspflichten-datenschutz)

# 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

## 1. Tracking Tools

### Zur Reichweitenmessung

- Zur ausschließlich **statistischen Analyse** zulässig
- Rechtsgrundlage  
Art. 6 Abs. 1 f DSGVO  
(„berechtigtes Interesse“)
  - Vorabinformation, z. B. über Datenschutzerklärung
  - Möglichkeit zum Widerspruch

### Rechtskonformer Einsatz

- Hinweis in der Datenschutzerklärung
- Anonymisierung der IP-Adresse
- Möglichkeit zum Widerspruch gegen pseudonymisiertes Tracken
- Vertrag über Auftragsverarbeitung (AV)
  - sofern pbD auf Server des Tracking-Tool-Anbieters gespeichert werden

## 1. Tracking Tools

### Sonstige Tools zum Tracking

Sofern

- webseiten- oder geräteübergreifend Nutzungsprofile erstellt
- Daten an Dritte übermittelt
- Daten für andere Zwecke eingeholt werden
  - Markt- und Meinungsforschung
  - Werbung

### Rechtskonformer Einsatz

- Rechtsgrundlage: Einwilligung des Betroffenen
  - Vorabinformation des Betroffenen (z. B. über Cookie-Banner)
  - Aktive Zustimmung (z. B. Anklicken, *nicht: Opt-out!*)
  - Hinweis auf jederzeitigen Widerruf der Einwilligung (z. B. Datenschutzerklärung)

## 2. Cookies

### Definition & Anwendung

- Cookies =  
kleine Textdateien, die Informationen auf dem Rechner eines Webseitenbesuchers ablegen
- Webseiten benutzen Cookies, um
  - Besucher zu identifizieren
  - Besucher wiederzuerkennen

### Cookie-Hinweis

- Cookie-Banner auf der Webseite
- Hinweis in der Datenschutzerklärung
  - über „Datenschutz-Generator“



## 2. Cookies

### Grundsatz

- Cookies sind zulässig, soweit diese für **notwendige** oder **nützliche** Funktionen erforderlich sind.
- Sonst nur mit Einwilligung
  - **strittig** (fehlt Regelung über eine ePrivacy-VO)

### Beispiele

Notwendig oder nützlich sind z. B.

- Gewährleistung der
  - Sicherheit der Website oder
  - der Seitennavigation
- Warenkorbfunktion im Onlineshop

## 2. Cookies

### Beispiel für „Eingesetzte Cookies“

Typ	Name	Funktion/Zweck	Speicherdauer
Funktionscookie	cookieconsent_dismissed	Dieses Cookie verhindert, dass der Hinweis zur Cookie Nutzung bei jedem Websitebesuch angezeigt wird.	1 Jahr
Funktionscookie	spamshield	Schutz vor Spam	Dieser wird nach Schließen des Browsers gelöscht.

### 3. Social Plugins

#### Social Plugins

= Schaltflächen, über die Besucher Inhalte einer Webseite bewerten und dieses zudem ihren Kontakten auf Social Media mitteilen können

#### Datenschutzrelevanz

- Social Media erhält pbD der Webseitenbesucher, wenn sich die Seite lädt und dies unabhängig davon, ob User dort registriert ist oder nicht.
  
- Rechtskonformer Einsatz
  - Keine direkte Einbindung
  - Einbindung nur über „2-Klick-Methode“ oder über „Shariff“

## 4. Kontaktformular

### Webformular

= Möglichkeit der Kontaktaufnahme für den Webseitenbesucher

### Datenschutzvorgaben

- Nur notwendige Angaben abfragen (Grundsatz der Datenminimierung)
- Bei der Abfrage optionaler Angaben diese als freiwillig kennzeichnen
- Übermittlung der Daten möglichst über eine verschlüsselte Datenleitung
- Hinweis in der Datenschutzerklärung

### 5. Videos

- Einbindung von Videos in Webseiten  
→ datenschutzkonform,  
d. h. keine direkte Einbettung auf die  
eigene Website

Denn Videokanäle würden die  
IP-Adresse eines Users bereits beim  
Laden der Seite speichern.

#### Rechtskonformer Einsatz

- Keine direkte Einbindung
- Einbindung von Videos nur  
- als sog. „2-Klick-Lösung“ oder  
- als „erweiterte Datenschutzeinstellung“
- Hinweis in der Datenschutzerklärung

## 6. Sicherheit der Webseite

- Art 32 DSGVO – angemessenes Schutzniveau ist zu gewährleisten
  - durch geeignete technische (z. B. Verschlüsselung) und organisatorische Maßnahmen
  
- Kriterien
  - **Nach dem** Stand der Technik **angemessener** Schutz, nicht immer neuester Stand!
  - Implementierungskosten
  - Art, Umfang, Umstände und Zwecke der Verarbeitung
  - Unterschiedliche Eintrittswahrscheinlichkeit sowie Risiko (normal/hoch/sehr hoch) für Betroffene
  
- Hinweis in der Datenschutzerklärung (verschlüsselt/unverschlüsselt)

## 6. Sicherheit der Webseite // Links

### BayLDA

- https-Check der Verschlüsselung der eigenen Webseite  
→ [www.lda.bayern.de/de/httpscheck.html](http://www.lda.bayern.de/de/httpscheck.html)

### Verschlüsselung, BSI für Bürger

- [https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/erschluesselung\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/erschluesselung_node.html)



### Tipps, Infos zur DSGVO

#### IHK für München und Oberbayern

- [www.ihk-muenchen.de/dsgvo](http://www.ihk-muenchen.de/dsgvo) und
- [www.ihk-muenchen.de/dsgvo-datenschutz-webseite](http://www.ihk-muenchen.de/dsgvo-datenschutz-webseite)

#### BayStMII

- [www.dsgvo-verstehen.bayern.de](http://www.dsgvo-verstehen.bayern.de)

#### BayLDA

- [www.lda.bayern.de/de/datenschutz\\_eu.html](http://www.lda.bayern.de/de/datenschutz_eu.html) und
- [www.lda.bayern.de/de/kleine-unternehmen.html](http://www.lda.bayern.de/de/kleine-unternehmen.html)

#### Bitkom

- [bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html](http://bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html)

#### Praxishilfen GDD

- [www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo](http://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo)





### Tipps, Infos zum rechtssicheren Internetauftritt

#### DSK

- [www.datenschutzkonferenz-online.de/media/oh/20190405\\_oh\\_tmg.pdf](http://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](http://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](http://www.datenschutzkonferenz-online.de/media/en/Entschlie%C3%9Fung%20Pandemie%2003_04_2020_final.pdf)  
Datenschutzgrundsätze bei der Bewältigung der Corona-Pandemie



# 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 angemessenen Datenschutzniveau  
[https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\\_de](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

### Tipps, Infos zum rechtssicheren Internetauftritt

#### Rechtssichere Internetseite / Onlineshop

- [www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Internetrecht/Rechtssichere-Internetseite/](http://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Internetrecht/Rechtssichere-Internetseite/)
- [www.ihk-muenchen.de/rechtsgrundlagen-ecommerce/](http://www.ihk-muenchen.de/rechtsgrundlagen-ecommerce/)
- [www.ihk-muenchen.de/haftung-internet](http://www.ihk-muenchen.de/haftung-internet)

#### Marketing und Werbung im Internet

- [www.ihk-muenchen.de/marketing-internet](http://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/](http://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/](http://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Werbung-Fairer-Wettbewerb/Abmahnung-was-tun/)



## Datenschutz – IHK-Ansprechpartner

### Rita Bottler

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

[rita.bottler@muenchen.ihk.de](mailto:rita.bottler@muenchen.ihk.de)  
[dsb\\_bihk\\_ev@muenchen.ihk.de](mailto:dsb_bihk_ev@muenchen.ihk.de)  
089-5116-1683



### Julia Franz

Referentin für Datenschutzrecht

[franzj@muenchen.ihk.de](mailto:franzj@muenchen.ihk.de)  
089-5116-2065



# Fragen?