Datenschutz-Grundverordnung (DS-GVO)

Worauf Sie als Unternehmer achten sollten

IHK

Inhalt

I. Datenschutz-Überblick

II. Die DSGVO und ihre praktische Umsetzung

1. Benennungspflicht des Datenschutzbeauftragten
2. Überblick über personenbezogene Daten verschaffen
3. Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO
4. Übermittlung personenbezogener Daten (pbD)
5. Auftragsverarbeitung – Art. 28 ff. DSGVO
6. Betroffenenrechte Art. 15 ff. DSGVO
7. Informationspflichten Art. 13, Art. 14 DSGVO
8. Datenschutzerklärung
9. Datenpannen

III. Weiterführende Informationen

Datenschutz – ein Grundrecht

Grundrecht → Informationelle Selbstbestimmung

Ab 25.05.2018 → Recht auf Privatheit

„Jeder Mensch hat grundsätzlich das Recht, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

BVerfG, u.a. „Volkszählungsurteil" vom 15. Dezember 1983

DS-GVO (Art. 1 DS-GVO)

Schützt die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten

- Inkrafttreten: 25.05.2016
- Wirksam ab: 25.05.2018

BDSG-neu

- Wirksam ab: 25.05.2018

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

Anwendungsbereich der DS-GVO

Identifizierbare personenbezogene Daten, z.B.:

- Dynamische IP-Adresse
- Akteneinsicht in Strafverfahren
- Werturteile (Zeugnisse etc.)
- Bestellverlauf (Onlineshop)

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 Website-Betreiber (Verantwortlicher) potenziell **legale Möglichkeiten** hat, an die Identifizierungsmerkmale heranzukommen.

pbD – weit zu fassender Begriff

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

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

Benennungspflicht des Datenschutzbeauftragten

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

→ Ab **10 Personen**, die **ständig** mit der automatisierten personenbezogenen Datenverarbeitung beschäftigt sind

→ Kerntätigkeit: umfangreiche und systematische Überwachung von Betroffenen oder die Verarbeitung sensibler Daten i.S.d. Art. 9 oder 10 DS-GVO

→ Unabhängig von der Anzahl der Personen, wenn Verarbeitungen von pbD vorliegen, die einer Datenschutz-Folgeabschätzung unterliegen

Überblick über personenbezogene Daten verschaffen

1. **Welche pbD werden verarbeitet?**
   - Mitarbeiterdaten (Name, Anschrift, Geburtstag etc.)
   - Kundendaten (Rechnung, Anschrift, E-Mail etc.)
   - Systemwartung, Einzelgesprächsnachweise etc.
2. **Wo werden die pbD verarbeitet?**
   - Personalabteilung
   - Vertrieb, Buchhaltung
   - IT-Abteilung
3. **Wie werden die pbD verarbeitet?**
   - Bewerberverwaltung etc.
   - Rechnungsstellung, Newsletter-Versand etc.
   - Wartung etc.

Grundlage für:
- Betroffenenrechte
- Erstellung von Verzeichnissen von Verfahrenstätigkeiten
- Meldung von Datenpannen
- Erfüllung von Dokumentationspflichten etc.

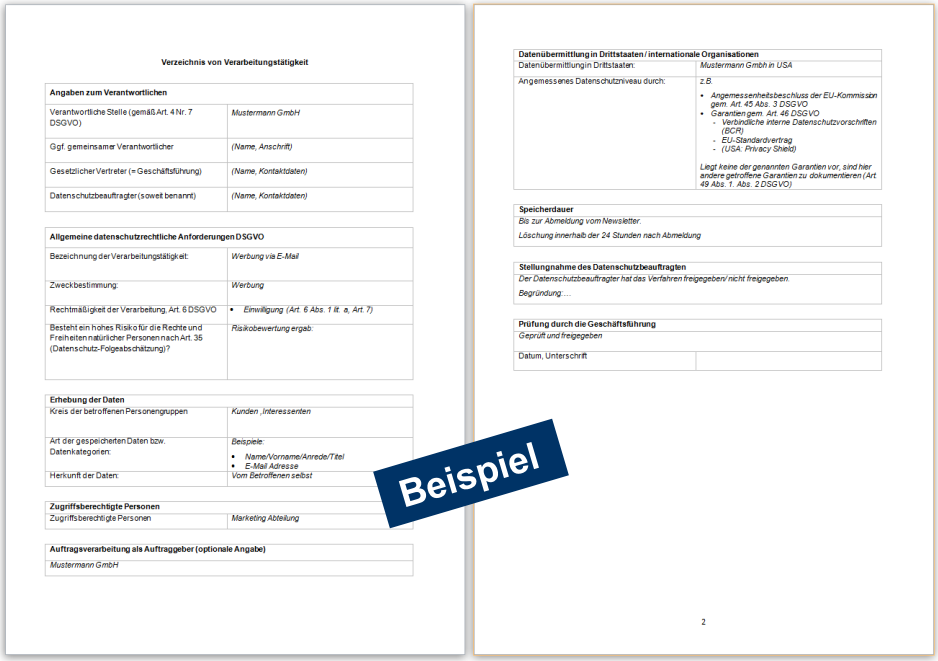
Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO

1. Welche pbD werden verarbeitet?
2. Wo werden die pbD verarbeitet?
3. Wie werden die pbD verarbeitet (zu welchem Zweck)?
4. Auf welcher Rechtsgrundlage werden die pbD verarbeitet?
5. An wen werden die pbD übermittelt?
6. Welches Risiko birgt die Verarbeitung (Datenschutz-Folgeabschätzung)?

Kein VvV gemäß Art. 30 Abs. 5 DS-GVO notwendig, wenn:
(greift jedoch in der Regel nicht → siehe Punkt 4)

- Weniger als 250 MA
- Kein Risiko für Rechte und Freiheiten Betroffener
- Keine Verarbeitung sensibler pbD nach Art. 9 oder 10 DS-GVO
- **Gelegentliche** Verarbeitung

Verzeichnis von Verarbeitungstätigkeiten (VvV) – Art. 30 DSGVO



Verzeichnis von Verarbeitungstätigkeit

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	*Mustermann GmbH*
Ggf. gemeinsamer Verantwortlicher	*(Name, Anschrift)*
Gesetzlicher Vertreter (= Geschäftsführung)	*(Name, Kontaktdaten)*
Datenschutzbeauftragter (soweit benannt)	*(Name, Kontaktdaten)*

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Bezeichnung der Verarbeitungstätigkeit:	*Werbung via E-Mail*
Zweckbestimmung:	*Werbung*
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	• *Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7)*
Besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 35 (Datenschutz-Folgeabschätzung)?	*Risikobewertung ergab:*

Erhebung der Daten	
Kreis der betroffenen Personengruppen	*Kunden ,Interessenten*
Art der gespeicherten Daten bzw. Datenkategorien:	*Beispiele:* • *Name/Vorname/Anrede/Titel* • *E-Mail Adresse*
Herkunft der Daten:	*Vom Betroffenen selbst*

Zugriffsberechtigte Personen	
Zugriffsberechtigte Personen	*Marketing Abteilung*

Auftragsverarbeitung als Auftraggeber (optionale Angabe)
Mustermann GmbH

Beispiel

Datenübermittlung in Drittstaaten / internationale Organisationen	
Datenübermittlung in Drittstaaten:	*Mustermann Gmbh in USA*
Angemessenes Datenschutzniveau durch:	*z.B.* • *Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO* • *Garantien gem. Art. 46 DSGVO* - *Verbindliche interne Datenschutzvorschriften (BCR)* - *EU-Standardvertrag* - *(USA: Privacy Shield)* *Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. Abs. 2 DSGVO)*

Speicherdauer
Bis zur Abmeldung vom Newsletter:
Löschung innerhalb der 24 Stunden nach Abmeldung

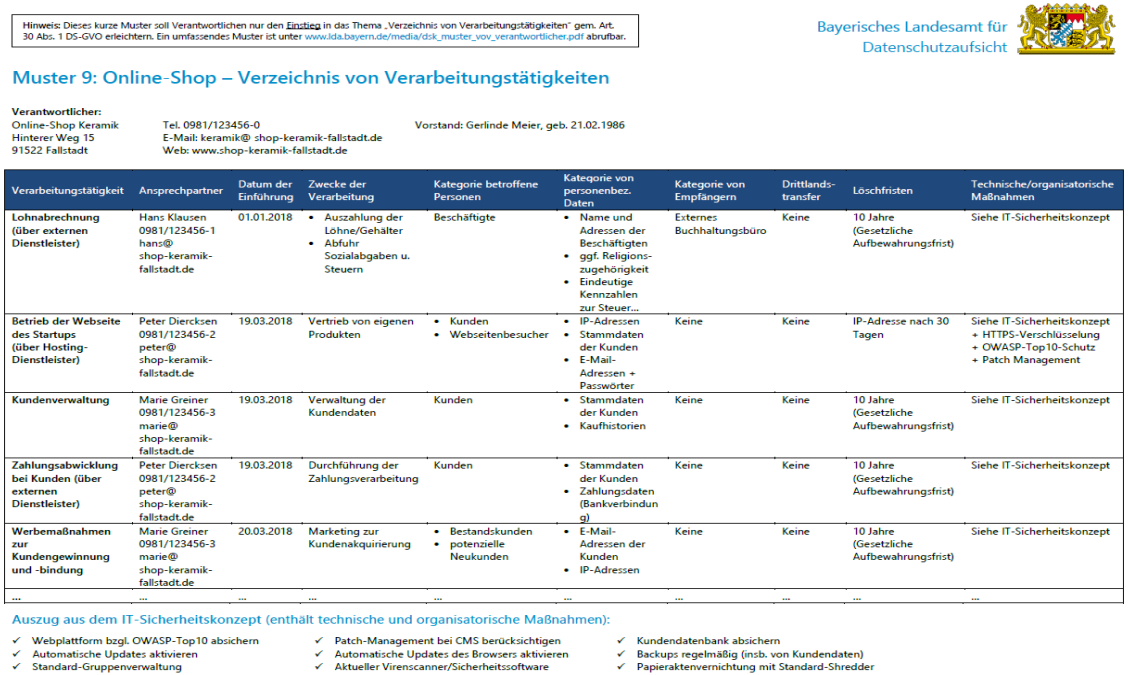
Stellungnahme des Datenschutzbeauftragten
Der Datenschutzbeauftragter hat das Verfahren freigegeben/ nicht freigegeben
Begründung:...

Prüfung durch die Geschäftsführung	
Geprüft und freigegeben	
Datum, Unterschrift	

2

Viele sehr gute Muster online verfügbar. In der Suchmaschine Begriffe wie „Muster Verzeichnis von Verarbeitungstätigkeit“ eingeben.

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

Übermittlung pbD: Verantwortliche und Auftragsverarbeitung

1. Konstellation: gemeinsam Verantwortliche

Verantwortlicher Unternehmen A ⟷ Verantwortlicher Unternehmen B → Joint Controller-Vertrag Art. 26 DS-GVO

2. Konstellation: keine gemeinsamen Verantwortlichen

Verantwortlicher Unternehmen A → Verantwortlicher Unternehmen B → Rechtsgrundlage

3. Konstellation: Auftragsverarbeitung

Verantwortlicher Unternehmen A → Auftragsverarbeiter Dienstleister → Auftragsverarbeitungs-vertrag (AV) Art. 28 DS-GVO

Auftragsverarbeitung – Art. 28 ff. DSGVO

Auftragsverarbeitung (AV)

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

  → bei Drittland zusätzlich gesonderte Garantien notwendig

Beispiele

Typische Auftragsverarbeiter:

- IT Dienstleister beim Zugriff auf pbD
- Lohn und Gehaltsabrechnungsbüro
- Cloud-Anbieter

Keine Auftragsverarbeiter:

- Steuerberater (da Berufsgeheimnisträger)
- Post oder Banken (da Infrastruktur-Dienstleistungen)

Auftragsverarbeitung – Art. 28 ff. DSGVO

Abschluss

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

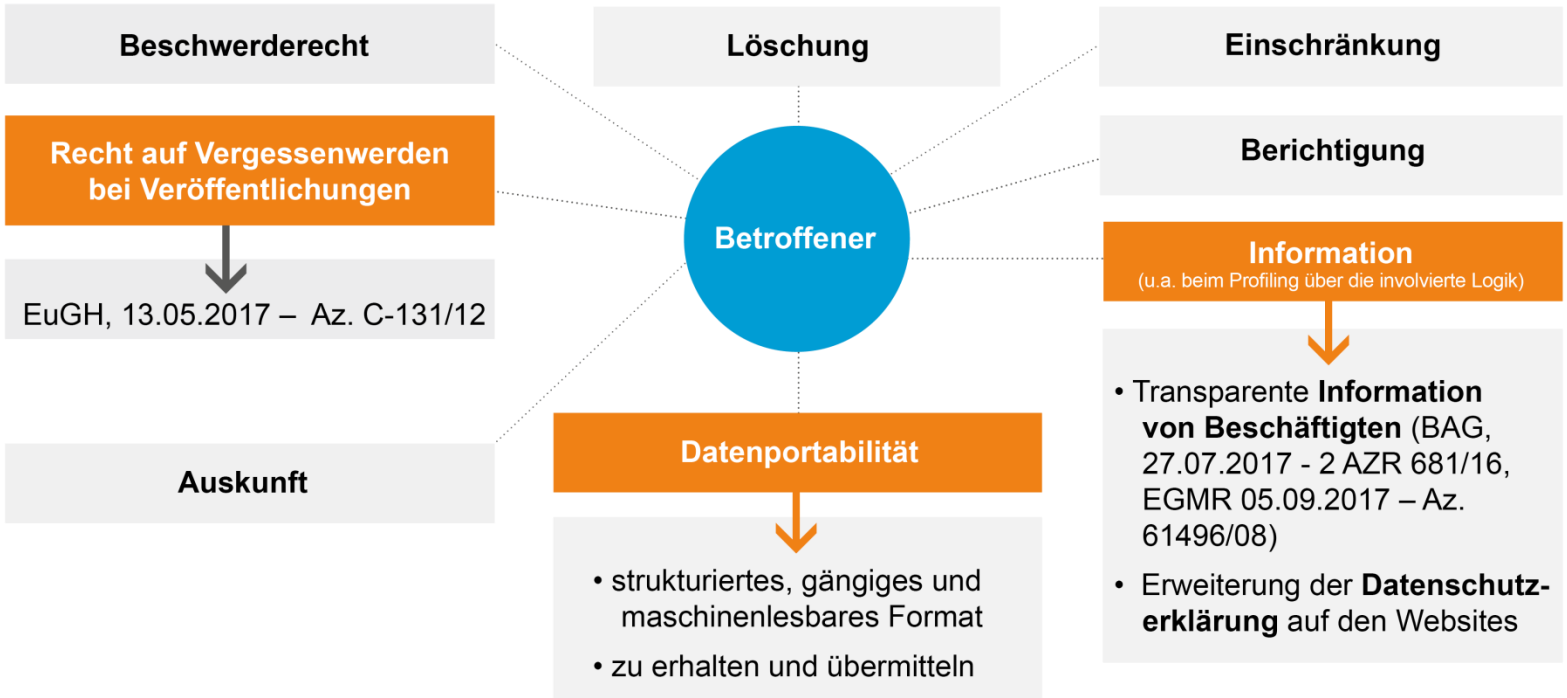
  → Signatur oder Unterschrift nicht notwendig

AVs vor dem 25.05.2018

- Rat: **Neuerstellung**

  → Änderung der gesetzlichen Mindestinhalte
- online sehr gute Muster verfügbar

Betroffenenrechte – Art. 15 ff. DSGVO



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 und Umsetzung

BayLDA

- 2. Stufe
  Bereithalten oder Verlinken auf eine Gesamt-Information nach Art. 13/14 DSGVO genügt regelmäßig
- 1. Stufe
  Immer ist zu informieren, soweit sich dies nicht bereits aus der Situation heraus ergibt:
  - Über die Identität des Verantwortlichen
  - Verarbeitungszwecke
  - Soweit sachgereicht, zudem über Betroffenenrechte

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

- Bezeichnung der Verarbeitung
- 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

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)

→ **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):
  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:** liegt bei Verletzung des Schutzes pbD vor
  → z. B. Verlust von Hardware (mobile Endgeräte), gezielter Angriffe von außen oder versehentlich durch Mitarbeiter, unsachgemäße Verschrottung von Datenträgern, unrechtmäßige Übermittlung pbD etc.
- **Meldepflicht: sobald jede Verletzung des Schutzes der pbD** festgestellt wurde; nicht erst bei Schäden
- 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

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€)

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

Fragen?