



# **Datenschutz nach neuem Recht Wirtschaftsjunioren Wetterau**



Industrie- und Handelskammer  
**Gießen-Friedberg**

Die Unternehmer-Mitmachorganisation



# DSGVO und BDSG

- DSGVO und BDSG seit 25. Mai 2018 in Kraft
- Umfassende Reform des Datenschutzrechts mit unzähligen Änderungen, Neuerungen, neuen Anforderungen und Verpflichtungen für datenverarbeitende Stellen!
- Möglichkeit der Verhängung drastischer Bußgelder

# Auskunfts – und Betroffenenrechte

- Informationspflichten, Auskunftsrecht, Recht auf Berichtigung, Recht auf „Vergessenwerden“(Löschung)
- Recht auf „Transportabilität“ der Daten
- Datensparsamkeit
- Technische und organisatorische Maßnahmen der Datenverarbeitung
- Datenschutzfolgeabschätzung bei besonders sensiblen Daten
- Meldung von Datenschutzverstößen („Datenpannen“)

# „TOMs“



## 1) Vertraulichkeit (Art. 32 Abs.1 lit. B) DS-GVO)

- Zutrittskontrolle  
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle  
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle  
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle  
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden;
- Pseudonymisierung (Art. 32 Abs.1 lit. a) DS-GVO; Art. 25 Abs.1 DS-GVO)  
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehen zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

# TOMs



## 2) Integrität (Art. 32 Abs. 1 lit. b) DS-GVO)

- Weitergabekontrolle  
Kein unbefugtes Lesen, Kopieren, Veränderung oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle  
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement

## 3) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DS-GVO)

- Verfügbarkeitskontrolle  
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verluste, z.B.: Backup-Strategie ( online/offline; on-Site/off-Site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;  
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DS-GVO)

## 4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle

# Dokumentation anhand Verarbeitungsverzeichnis

- Alle Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden
- Schwellenwert: mehr als 249 Mitarbeiter
- Aber: Rückausnahme, wenn Datenverarbeitung nicht nur *gelegentlich* erfolgt
- Keine Erläuterung, was gelegentlich bedeutet!
- Lohnbuchhaltung durch Steuerbüro wohl davon ausgenommen

# Der betriebliche Datenschutzbeauftragte (DSB)

- BDSG: Schwellenwert 10 Personen, die ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind
- Auskunfteien, Adresshändler oder Markt- und Meinungsforschungsinstitute immer!
- DSGVO: Wenn die Kerntätigkeit in einer Datenverarbeitung besteht, die aufgrund ihres Zwecks oder Umfangs eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen erfordert, oder
- Eine umfangreiche Verarbeitung von besonders schutzwürdigen Daten (Bsp: Gesundheitsdaten)

# Wer kann zum DSB benannt werden?

- Mitarbeiter des Betriebs (= interner DSB) oder ein außenstehender Dienstleister (= externer DSB)
- Fachliche Qualifikationen auf dem Gebiet des Datenschutzes
- Kein Interessenskonflikt (z.B. Geschäftsführung)
- Kontaktdaten des DSB sind zu veröffentlichen und der Landesdatenschutzbehörde zu melden



# Muster Verarbeitungsverzeichnis

Briefkopf der Firma

## Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO

Abteilung \_\_\_\_\_ lfd. Nr. \_\_\_\_\_

<b>Verantwortlicher</b>	<b>Angaben zur Person des Datenschutzbeauftragten</b>
Name und Anschrift der Firma Name <u>Geschäftsführer</u>	Falls vorhanden
<b>Name u. Anschrift des Auftragnehmers, wenn die Daten im Auftrag verarbeitet werden:</b>  _____	
Auftragsdatenverarbeitungsvereinbarung vom: <u>TT.MM.JJJJ</u>	

Datum der Anlegung: TT.MM.JJJJ  
Datum der letzten Änderung: TT.MM.JJJJ  
Revisionszyklus: 12 Monate

<b>Verantwortliche Fachabteilung:</b>	
Ansprechpartner: Telefon: E-Mail:	

# Muster Verarbeitungsverzeichnis

## 1. Bezeichnung der Verarbeitungstätigkeit

<p><b>Bezeichnung der Verarbeitungstätigkeit</b>  <i>Die Bezeichnung der Tätigkeit soll allgemein verständlich sein.                  Für Außenstehende unverständliche Abkürzungen sind zu vermeiden.</i></p>

## 2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

Zwecke (Aufgabe(n)), zu deren Erfüllung die personen- bezogenen Daten erhoben, verarbeitet oder genutzt werden	Rechtsgrundlagen Gesetz, das die Aufgabenwahrnehmung legitimiert und die Datenverarbeitung rechtfertigt ( ggf. <u>Einwilligung</u> § 6 DSGVO)
	Spezialgesetzliche Regelung: <input type="checkbox"/>  Einwilligung des Betroffenen: <input type="checkbox"/>  Vertrag oder Vertragsanbahnung: <input type="checkbox"/>  Interessenabwägung (Art. 6 Abs. 1f) : <input type="checkbox"/> DSGVO):   Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses: <input type="checkbox"/>



# Muster Verarbeitungsverzeichnis

## 3. Beschreibung der Kategorien betroffener Personen

lfd. Nr.	Bezeichnung der Betroffenen Bspw. Gewerbetreibende, Auszubildende, Versicherungsvermittler, etc.

## 4. Beschreibung der Datenkategorien



lfd. Nr.	Bezeichnung der Daten Aussagekräftige Oberbegriffe, z. B. Namen, Anschriften, Staatsangehörigkeit;

## 5. Quelle der Daten

lfd. Nr.	

# Muster Verarbeitungsverzeichnis

## 6. Zugriffsberechtigte Personengruppen

Benennung Personengruppen	<input type="text"/>
Umfang des Datenzugriffs	<input type="text"/>
Zweck des Datenzugriffs	<input type="text"/>
Berechtigungskonzept	<input type="text"/>

## 7. Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden

<b>intern</b> <input type="checkbox"/>	Abteilung/Funktion	<input type="text"/>
	Zweck der Übermittlung	<input type="text"/>
<b>extern</b> <input type="checkbox"/>	Empfängerkategorie	
	(öffentliche Stelle, z.B. Amtshilfe)	<input type="text"/>
	(nicht-öffentliche Stelle)	<input type="text"/>
	Zweck der Übermittlung	<input type="text"/>
	Rechtsgrundlage	<input type="text"/>
	Häufigkeit	<input type="text"/>

# Muster Verarbeitungsverzeichnis

## 8. Übermittlung in Drittländer oder internationale Organisation, Garantien

Übermittlung findet nicht statt und ist auch nicht geplant

lfd. Nr.	Datenübermittlung findet wie folgt statt

lfd. Nr.	Empfänger(kategorie)

Sofern es sich um eine in Art. 49 Abs. 1 Unterabs 2 DS-GVO genannte Datenübermittlung handelt.	<b>Dokumentation geeigneter Garantien:</b>
--	--

## 9. Regelfristen für die Löschung der Daten und die Prüfung der Löschung

lfd. Nr. von 4.	Frist für Löschung der verschiedenen Datenkategorien:

, den XX.XX.20XX

# Muster Einwilligungserklärung

In unserem Werbenewsletter informiert die Mustermannbetrieb GmbH ihre Kunden postalisch oder per E-Mail über Aktionsrabatte, aktuelle Leistungen und Neuigkeiten. Dies ist ein kostenloser Service für Sie.

Ja, ich/wir bin/sind damit einverstanden, dass meine/unsere Kontaktdaten (Name, Adresse, Faxnummer und E-Mail-Adresse) zum Zweck der Produktwerbung und Informationen zum Leistungsspektrum des Betriebs gespeichert und zur Kontaktaufnahme genutzt werden.

Mir/uns ist dabei klar, dass diese Einwilligungen freiwillig und jederzeit widerruflich sind.

Der Widerruf ist per E-Mail zu richten an: [info@mustermannbetrieb.de](mailto:info@mustermannbetrieb.de) oder postalisch an: Mustermannbetrieb GmbH, Musterstraße 1, 12345 Musterstadt

Nach Erhalt des Widerrufs werden wir die betreffenden Daten nicht mehr nutzen und verarbeiten bzw. löschen.

---

Ort, Datum, Unterschrift

## Weiterführende Hinweise

Musterdatenschutzerklärungen:

- <https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/>
- [www.e-recht24.de/muster-datenschutzerklaerung.html](http://www.e-recht24.de/muster-datenschutzerklaerung.html)
- <https://shop.trustedshops.com/de/rechtstexter-fuer-ihre-datenschutzerklaerung>
- Weitere Infos:  
[https://www.giessen-friedberg.ihk.de/Geschaeftsbereiche/Recht\\_und\\_Steuern](https://www.giessen-friedberg.ihk.de/Geschaeftsbereiche/Recht_und_Steuern)

# Datenschutz nach neuem Recht

- Vielen Dank für Ihre Aufmerksamkeit!
- Dr. Sven Sudler  
Industrie- und Handelskammer Gießen-Friedberg  
Tel.: 0641-7954-4010  
[sudler@giessen-friedberg.ihk.de](mailto:sudler@giessen-friedberg.ihk.de)