EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Datenverarbeitungsverzeichnis nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO)
Verantwortlicher

Eine komplette Anleitung „Was ist zu tun“, erhalten Sie unter:
https://business-view.photo/2018/03/14/eu-dsvgo-nur-bis-zum-25-mai-haben-sie-zeit/

Verarbeitungstätigkeit - Formblatt (PDF Ausfüllbar)
https://business-view.photo/formblatt-verarbeitungstaetigkeit/

Ich/Wir übernehmen keine Gewähr für die Aktualität, Vollständigkeit und Richtigkeit der bereitgestellten Informationen. Dies bezieht sich auf eventuelle Schäden materieller oder ideeller Art Dritter, die durch die Nutzung dieses Dokumentes, oder der beschriebenen Techniken verursacht wurden.

Über eine Rückmeldung würden wir uns freuen. Wünsche, Anregungen, Erfahrungen bei der Arbeit mit den Unterlagen werden gerne entgegengenommen. Bitte auch nicht mit Kritik sparen.

Gerichtsurteile und rechtliches dienen nur Informationszwecken und erheben keinen Anspruch auf Vollständigkeit. Die Artikel / Links zu Recht und verwandten Themen dienen der allgemeinen Bildung und Weiterbildung und nicht der Beratung im Falle eines individuellen rechtlichen Anliegens. Wie alle Projektbereiche sind sie ständigen Veränderungen unterworfen. Diese Artikel / Links entstehen offen und ohne redaktionelle Begleitung und Kontrolle. Es ist möglich, dass Sie hier auf unrichtige, unvollständige, veraltete, widersprüchliche, in falschem Zusammenhang stehende oder verkürzte Angaben treffen. Das gilt auch für Texte auf Diskussions-, Hilfe- und sonstigen Internet Seiten, zu dieser Publikation.

Internet Verweise / Links
Bei “Links” handelt es sich stets um “lebende” (dynamische) Verweisungen. Der/die Autor(en) hat bei der erstmaligen Verknüpfung zwar den fremden Inhalt daraufhin überprüft, ob durch ihn eine mögliche zivilrechtliche oder strafrechtliche Verantwortlichkeit ausgelöst wird. Er überprüft aber die Inhalte, auf die er in seinem Angebot verweist, nicht ständig auf Veränderungen, die eine Verantwortlichkeit neu begründen könnten. Wenn feststellt wird oder von anderen darauf hingewiesen wird, dass ein konkretes Angebot, zu dem er einen Link bereitgestellt hat, eine zivil- oder strafrechtliche Verantwortlichkeit auslöst, wird der Verweis auf dieses Angebot aufgehoben, und in den Social Media Kanälen des Autors bekannt gegeben.

Inhaltsverzeichnis

Es wird darauf hingewiesen, dass es sich hier um ein fiktives Beispiel handelt. Bei der praktischen Umsetzung ist auf die konkreten Anwendungsfälle im Unternehmen abzustellen.

A. Stammdatenblatt

Name und Kontaktdaten des (der) für die Verarbeitung (gemeinsam) Verantwortlichen

(a) Name(n) und Anschrift(en):
Max Mustermann GmbH
Neuer Weg 1
DE-XXXXX Musterdorf

(b) E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.):
max@example.com

(c) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.) des Datenschutzbeauftragten[1]:
Franz Fachmann RA
Datenstraße 5
AT-YYYYY Datenstadt

(d) Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie z.B. Tel. Nr.) des Vertreters des (der) Verantwortlichen:[2]
KEINER

1 Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde. HINWEIS: Wenn keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht, der Verantwortliche aber freiwillig einen bestellen möchte, müssen trotzdem alle den Datenschutzbeauftragten betreffenden Bestimmungen der DSGVO eingehalten werden; möchte man das nicht, darf die bestellte Person nicht „Datenschutzbeauftragter“ genannt werden, sondern sollte eine andere Bezeichnung gewählt werden (z.B. „Datenschutzkoordinator“). Dieser kann, muss aber nicht ins Verfahrensverzeichnis aufgenommen werden. Siehe dazu das zur Auslegung der Bestimmungen zum Datenschutzbeauftragten in der DSGVO sowie zu dessen Aufgaben können die Guidelines der Art 29-Gruppe zum Datenschutzbeauftragten herangezogen werden, die auf der Website der EU-Kommission abrufbar sind. http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

2 Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

B. Datenverarbeitungen/Datenverarbeitungszwecke

(a) Zwecke und Beschreibung der Datenverarbeitung[3]:

1. Rechnungswesen und Geschäftsabwicklung: Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenzen oder Verträge) in diesen Angelegenheiten
2. Personalverwaltung: …….
3. Marketing: ……
4. Geschäftspartnerdatenbank: …….
5. usw.

(b) Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[4]

Ja ☑ Nein ❑

Wenn Ja, wann?
zuletzt vor 6 Monaten

Wenn Nein, aus welchem Grund nicht?[5]

3 Zum Begriff „Verarbeitung“; sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.

4 Zur Datenschutz-Folgenabschätzung im Verarbeitungsverzeichnis sind zwar Angaben zur Datenschutz-Folgenabschätzung nicht zwingend vorgesehen. Aus Gründen der Rechenschaftspflicht empfehlen sich aber grundsätzliche Angaben darüber auch ins Verarbeitungsverzeichnis aufzunehmen.

5 Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, wenn durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht oder die Datenverarbeitungsart in der sogenannten „white list“ der Datenschutzbehörde gelistet ist (derzeit besteht noch keine „white list“); Näheres dazu siehe auch „Risiko-Folgenabschätzung“. Download PDF – Was muss getan werden? https://business-view.photo/?p=14293

C. Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung

(a) Kategorien der betroffenen Personen

Lfd.Nr. Beschreibung der Kategorien betroffener Personen (z.B. Kunden, Mitarbeiter, Lieferanten usw.)

1. Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten
2. Sachbearbeiter beim Verantwortlichen
3. An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten

(b) Rechtsgrundlagen[6]

1. Art 6 Abs 1 lit
   a Einwilligung der Betroffenen (Freiwillig, ohne Vorauswahl)
   b zur Vertragserfüllung erforderlich
   c gesetzliche Verpflichtungen nach Handels- und Steuerrecht
   f berechtigte Interessen des Verantwortlichen
   DSGVO
   - AT[7] → § 132 BAO, §§ 190, 212 UGB
   - DE[8] → § 147 Abs. 2 i. V. m. Abs. 1 Nr.1, 4 und 4a AO, § 14b Abs. 1 UStG

(c) Verträge , Zustimmungserklärungen oder sonstige Unterlagen (z.B. Erledigung der Informationspflichten[9]) sind abgelegt:[10] (freiwillig)

Unterlagen zu aufrechten Geschäftsabwicklungen in der Verkaufsabteilung, Rechnungen (auch) in der Finanzabteilung, erledigte Geschäftsfälle im Archiv. Verträge mit Auftragsverarbeitern sind, je nach Thematik, in der Rechtsabteilung, Finanzabteilung, Vertriebsabteilung oder IT-Abteilung abgelegt.

(d) Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[11]

---

6 Die Rechtsgrundlagen (z.B. rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verfahrensverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt „Grundsätze und Rechtmäßigkeit der Verarbeitung“.

7 Österreich → https://www.jusline.at/bundesgesetze

8 Deutschland → https://www.gesetze-im-internet.de/

9 Siehe zu den Informationspflichten das Merkblatt „Informationspflichten“.

10 Die Angabe, wo die Unterlagen innerhalb der Organisation abgelegt wurden, ist nicht verpflichtend im Verarbeitungsverzeichnis zu dokumentieren, erleichtert aber vor allem in größeren, arbeitsteilig organisierten Organisationen das Auffinden der entscheidenden Unterlagen (dient also lediglich der innerbetrieblichen Arbeitserleichterung).

11 Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verfahrensverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (z.B. „nach Ablauf des Vertrages“).

1. Kategorien der verarbeiteten Daten und Ankreuzen, ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personen-gruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Beson-dere Daten-kate-gorien iSd Art 9 DSGVO[12] straf-rechtlich relevant iSd Art 10 DSGVO[13]	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden Im Anlassfall	Inkassounternehmen Im Anlassfall	Fremdfinanzierer (z.B. Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
a	1	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	x	x	x	x	x	x	x	x	x	x
	2	Anschrift	Nein	x	x	x	x	x	x	x	x	x	x
	3	Kontaktdaten (Tel., Mail, Fax)	Nein	x	x	x	x	x	x	x	x	x	x
	4	Firmenbuchdaten	Nein	x	x	x	x	x	x	x	x	x	x
	5	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		x		x						
	6	Bankverbindungen	Nein	x	x	x	x	x	x	x	x	x	
	7	Kreditkartennummern und -unternehmen	Nein	x	x	x	x						
	8	UID/TAX/VAT Nr.	Nein	x	x	x	x	x	x	x	x	x	
	9	Namen der Kontaktpersonen	Nein	x	x	x	x	x	x	x	x	x	x
	10	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift oä.)	Nein	x	x	x	x	x	x	x	x	x	x
	11	Vertragstexte und Geschäfts-korrespondenzen	Nein	x	x	x	x	x	x	x		x	
b	12	Name	Nein	x	x	x	x	x	x	x	x	x	x
	13	Funktion des betroffenen Sachbearbeiters beim Verantwortlichen	Nein	x	x	x	x	x	x	x	x	x	x
	14	Vom betroffenen Sachbearbeiter bearbeitete Fälle	Nein	x	x	x	x	x	x	x	x	x	x
	15	Umfang der Vertretungsbefugnis	Nein	x	x	x	x	x	x	x	x	x	x
c	16	Name, Firma oder sonstige Geschäftsbezeichnung	Nein	x	x	x	x	x	x	x	x	x	x
	17	Anschrift	Nein	x	x	x	x	x	x	x	x	x	x

12 Daten nach Art 9 DSGVO sind besondere Datenkategorien („sensible Daten): rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

13 Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln unter behördlicher Aufsicht.

	18	Kontaktdaten (Tel., Mail,Fax)	Nein	x	x	x	x	x	x	x	x	x	x
	19	Firmenbuchdaten	Nein	x	x	x	x	x	x	x	x	x	x
	20	Namen der Kontaktpersonen	Nein	x	x	x	x	x	x	x	x	x	x
	21	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift oä.)	Nein	x	x	x	x	x	x	x	x	x	x
	22	UID/TAX/VAT Nr.	Nein	x	x	x	x	x	x	x	x	x	x
	23	Bankverbindungen	Nein	x	x	x	x	x	x	x	x	x	
	24	Kreditkartennummern und -unternehmen	Nein	x	x	x	x						
	25	Daten zur Bonität inkl. Mahn- und Klagsdaten	Nein		x	x	x						
d Modell-vertrag	26	ethnischen Zugehörigkeit	Ja								x		
	27	Sprachen languages	Ja								x		
	28	Körperabmessungen	Ja								x		
	29	Geburtsdatum	Ja								x		

1. Löschungs- und Aufbewahrungsfristen (wenn möglich)
   Zu Beachten ist hier auch, das die Daten in einem evtl. IT-Backup unwiederbringlich gelöscht werden!

Daten aus (d)1 (Lfd. Nr.)	**Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen**
1-4; 6-24; 26;	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 10 Jahre[14]; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
5; 25;	Bis zur Beendigung der Geschäftsbeziehungen

(c) Kategorien von Empfängern[15], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern14

1. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie z.B. UNO, OSZE)

Empfängerkategorien aus (d)1	**Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)**	**Internationale Organisation (Angabe der intern. Organisation)**
Banken		
Rechtsvertreter im Geschäftsfall		
Wirtschaftstreuhänder		

14 Je EU-Land unterschiedlich, in „Verarbeitungstätigkeit“ ist ein Entsprechender Hinweis DE, AT... auswählbar
15 Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.

Gerichte		
Verwaltungsbehörden		
Inkassounternehmen		
Fremdfinanzierer (z.B. Leasing)		
mitwirkende Vertrags- und Geschäftspartner		
Versicherungen um Anlassfall		
Provider (IT-Dienstleister)		

2. Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Abs 1 Unterabsatz 1 DSGVO erfolgt (vor allem wenn kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, keine Standardvertragsklauseln der Europäischen Kommission oder der nationalen Datenschutzbehörde verwendet werden oder genehmigte Zertifizierungsmechanismen in Anspruch genommen werden, keine Corporate binding rules zur Anwendung kommen (genehmigte verbindliche konzerninterne Datenschutzvorschriften), die Übermittlung nicht für Vertragserfüllungszwecke erforderlich ist oder keine ausdrückliche Einwilligung vorliegt):[16]

(d) Angemessenheitsbeschluss der Europäischen Kommission[17], gibt es für folgende Länder:

Kanada

16 Download PDF – Was muss getan werden? https://business-view.photo/?p=14293

17 FAQ EU: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_de

C. Detailangaben zu (2) Personalverwaltung

…

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

HINWEIS: die hier angeführten Maßnahmen verstehen sich als beispielhafte Auflistung; es ist je nach Einzelfall und Risikobehaftung der Datenverarbeitung zu entscheiden, welche konkreten Maßnahmen zu treffen sind und welche im Einzelfall auch zumutbar sind!

(a) Vertraulichkeit:
   1. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
   2. Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
   3. iZugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Protokollierung von Zugriffen; oder: Zugriff nur für Unternehmensinhaber, Mitarbeiter der Abteilung Rechnungswesen und Mitarbeiter, die an der Geschäftsabwicklung beteiligt sind

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

(c) Verfügbarkeit und Belastbarkeit:
   1. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie, Virenschutz, Firewall;

(d) Pseudonymisierung und Verschlüsselung:
   1. Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
   2. Verschlüsselung: sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt: ….

(e) Evaluierungsmaßnahmen:
   1. Datenschutz-Management (z.B. Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen;