

## EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO): MUSTER (Erweiterung der Wiener Fachgruppe der Buch- und Medienwirtschaft)

Die Experten der Wirtschaftskammern Österreichs haben für ihre Mitgliedsbetriebe nachstehendes Muster eines Datenverarbeitungsverzeichnisses nach Art 30 Abs. 1 EU-Datenschutz-Grundverordnung (DSGVO) für **Verantwortliche** erstellt.

Als Ausfüllhilfe ist ein bereits ausgefülltes fiktives Beispiel unter Anwendungsbeispiel für Verantwortliche

(PDF-Version) im Download-Bereich verfügbar.

Das hinterlegte Wasserzeichen „**Muster**“ kann einfach aus dem Word-Dokument entfernt werden.

Die im „Muster“ **gelb** markierten Textstellen müssen von Ihnen noch befüllt werden.

Wir empfehlen Ihnen den Ankauf der WKÖ Broschüre zum Datenschutz, sofern Sie diese noch nicht haben. LINK zum Webshop:

<https://webshop.wko.at/datenschutzanpassungsgesetz-2018.html>

Auf den Seiten 138 ff dieser WKÖ Broschüre finden Sie eine Auswahl der wichtigen bundesgesetzlichen (Aufbewahrungs-)Fristen im Zusammenhang mit der datenschutzrechtlichen Speicherbegrenzung.

\*\*\*

Stand: März 2018

Dieses Merkblatt ist ein Produkt der Zusammenarbeit aller Wirtschaftskammern.  
Achtung: Die gelben Textpassagen wurden von der Wiener Fachgruppe der Buch- und Medienwirtschaft ergänzt.

**Hinweis!** Diese Information finden Sie auch im Internet unter <http://wko.at/datenschutz>. Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammern Österreichs ist ausgeschlossen. Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für beide Geschlechter!

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

**Inhalt**

<b>EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO): MUSTER</b> .....	1
A. Stammdatenblatt.....	3
B. Datenverarbeitungen/Datenverarbeitungszwecke .....	4
C. Detailangaben zu den Datenverarbeitungen .....	6
D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen .....	32

## A. STAMMDATENBLATT

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

a. Name(n) und Anschrift(en):

[Name und Anschrift Mitgliedsunternehmen.]

b. E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):

[Kontaktdaten Mitgliedsunternehmen.]

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten<sup>1</sup>:

[Hier würden wir die Kontaktdaten des Datenschutzkoordinators angeben und anmerken, dass kein Datenschutzbeauftragter bestellt wurde.]

d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Vertreters des (der) Verantwortlichen:<sup>2</sup>

[zu löschen falls nicht anwendbar]

---

<sup>1</sup> 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 (zB „Datenschutzkoordinator“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „[Datenschutzbeauftragter](#)“.

<sup>2</sup> Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

## B. DATENVERARBEITUNGEN/DATENVERARBEITUNGSZWECKE

### I. Zwecke und Beschreibung der Datenverarbeitung<sup>3</sup>:

#### 1. Kundenverwaltung, Rechnungswesen, Logistik und Buchführung

Zweck ist die Verarbeitung von personenbezogenen Daten im Rahmen jeglicher Geschäftsbeziehungen mit Kunden und Lieferanten im Rahmen der Gewerbeausübung samt systematischer Aufzeichnung aller die Einnahmen und Ausgaben betreffenden Geschäftsvorgänge, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten.

#### 2. Personalverwaltung für privatrechtliche Dienstverhältnisse

Zweck ist die Verarbeitung und Evidenthaltung von personenbezogenen Daten für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von Aufzeichnungs-, Auskunfts- und Meldepflichten, soweit dies auf Grund von Gesetzen oder Normen kollektiver Rechtsgestaltung oder arbeitsvertraglicher Verpflichtungen jeweils erforderlich ist, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenz) in diesen Angelegenheiten; Verwendung und Evidenthaltung von personenbezogenen Daten von Bewerbern, wenn diese Daten vom Betroffenen angegeben wurden.

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne der Art. 9 und 10 DSGVO im Rahmen dieser Ausnahme erfolgt ausschließlich aufgrund einer gesetzlichen Ermächtigung oder aufgrund rechtlicher Verpflichtungen.

#### 3. Kundenbetreuung und Marketing für eigene Zwecke

Zweck ist die Verarbeitung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot sowie zur Durchführung von Werbemaßnahmen und Newsletter-Versand, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Korrespondenz) in dieser Angelegenheit.

#### 4. [Weitere Datenverarbeitungen in Ihrem Unternehmen?--> individuell zu ergänzen]

---

<sup>3</sup> Zum Begriff „Verarbeitung“ siehe das Merkblatt [„Wichtige Begriffsbestimmungen“](#); sollten Daten auch an „Dritte“ oder an Auftragsverarbeiter übermittelt werden, sind auch die Zwecke dieser Datenübermittlungen im Verarbeitungsverzeichnis zu dokumentieren.

**[Das vorliegende Muster wurde ausschließlich zu Ihrer Arbeitserleichterung bei der Verzeichniserstellung für Ihr Unternehmen vorbefüllt mit den drei bisher wesentlichsten vormaligen Standardanwendungen SA001, 002, 022, nunmehr gemäß Entwurf der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), so genannte "white list" bezeichnet als DSFA-A01, DSFA-A02 und DSFA-04. Eigene Datenverarbeitungen, die dadurch noch nicht abgedeckt sind, wären zu ergänzen oder der Musterinhalt abzuändern, wenn die eigene Datenverarbeitung im Unternehmen von den Standardanwendungen abweicht. Achtung: Enthält nicht sämtliche Datenarten/-kategorien der Standardanwendungen, sondern nur diejenigen, welche unserer Einschätzung nach für die Buch- und Medienwirtschaft relevant sind → gegebenenfalls weitere Datenkategorie zu ergänzen!]**

II. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?<sup>4</sup>

Ja       Nein

Wenn Ja, wann? n/a

Wenn Nein, aus welchem Grund nicht?<sup>5</sup>

Bei den genannten Datenverarbeitungen handelt es sich um bisherige Standardanwendungen, bei denen gemäß Entwurf der Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), so genannte "white list", keine Datenschutz-folgenabschätzung durchgeführt werden muss.

---

<sup>4</sup> Zur Datenschutz-Folgenabschätzung siehe das Merkblatt „[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.

<sup>5</sup> 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 das Merkblatt „[Datenschutz-Folgenabschätzung](#)“.

## C. DETAILANGABEN ZU DEN DATENVERARBEITUNGEN

### I. Kundenverwaltung, Rechnungswesen, Logistik und Buchführung

#### 1. Kategorien der betroffenen Personen

Lfd.Nr.

1	Kunden und Lieferanten
2	Sachbearbeiter oder Kontaktperson beim Verantwortlichen
3	an der Geschäftsabwicklung mitwirkende Dritte
4	Kontaktpersonen beim Kunden, Lieferanten oder an der Geschäftsabwicklung mitwirkenden Dritten
5	Bloße Zustell-, Lieferungs-, Rechnungsadressaten und dgl.
6	Fremdkapitalgeber
7	Gesellschafter

#### 2. Rechtsgrundlagen<sup>6</sup>

Zur Vertragserfüllung erforderlich, rechtliche Verpflichtungen (insbesondere nach BAO und UGB), berechtigte Interessen des Verantwortlichen.

#### 3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten<sup>7</sup>) sind abgelegt:<sup>8</sup> (freiwillig)

**[siehe Fußnote – freiwillig zu befüllen, wie und sich gemäß Ihren konkreten innerbetrieblichen Abläufe die Daten und Unterlagen befinden, z.B. im Haus, beim Lohnverrechner, externer Provider etc]**

<sup>6</sup> Die Rechtsgrundlagen (zB rechtliche Verpflichtung, Einwilligung, Vertragserfüllung, lebenswichtige Interessen des Betroffenen, kein überwiegendes berechtigtes Interesse des Betroffenen) sind nach der DSGVO zwar nicht verpflichtend ins Verarbeitungsverzeichnis 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“](#).

<sup>7</sup> Siehe zu den Informationspflichten das Merkblatt [„Informationspflichten“](#).

<sup>8</sup> 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).

#### 4. Kategorien der verarbeiteten Daten und Ankreuzen, an welche Empfängerkategorien<sup>9</sup> sie übermittelt werden

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder . Buchhalter	Gerichte, Verwaltungsbehörden	Inkasounternehmen	Fremdfinanzierer	Beteiligte Vertrags-, Geschäftspartner	Versicherungen	Konzernleitung	Kunden
Kunden und Lieferanten	Name / Bezeichnung	Nein	X	X	X	X	X	X	X	X	X	
	Kontaktdaten (Anschrift, Telefonnummer, E-Mailadresse udgl) des Kunden, Lieferanten sowie der Kontaktperson beim Kunden, Lieferanten	Nein	X	X	X	X	X	X	X	X	X	
	Daten zur Bonität	Nein			X						X	
	Sperrkennzeichen (z. B. Kontaktsperre, Rechnungssperre, Liefersperre, Buchungssperre, Zahlungssperre)	Nein	X	X	X	X		X	X		X	
	Vertragsgegenstand (inkl. Vertragsbedingungen)	Nein	X	X	X	X	X	X	X	X	X	
	Bonus-, Provisionsdaten und dgl.	Nein	X	X	X	X		X			X	
	Daten zur Steuerpflicht und Steuerberechnung	Nein		X	X	X		X	X		X	
	Finanzierungs- und Zahlungsbedingungen	Nein	X	X	X	X	X	X	X	X	X	
	Bankverbindung	Nein	X	X	X	X	X	X	X	X	X	
	Kreditkartennummern und -unternehmen	Nein	X	X	X	X						
	Daten zum Kreditmanagement (z. B. Kreditlimit, Wechselimit)	Nein	X	X	X	X		X				
	Daten zum Zahlungs- oder Leistungsverhalten des Betroffenen	Nein	X	X	X	X	X	X	X	X		X
	Mahndaten/Klagsdaten	Nein	X	X	X	X	X	X	X			X

<sup>9</sup> n der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen. Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird zB die bloße Angabe von „Konzern“ als Empfänger nicht ausreichen, weil daraus nicht eruierbar sein wird, ob die Daten rechtmäßig an die Muttergesellschaft und/oder an Schwestergesellschaften übertragen werden).

	Konto- und Belegdaten	Nein	X	X	X	X	X	X	X	X	X	X	
Sachbearbeiter beim Verantwortlichen	Name, Anrede/Geschlecht	Nein	X	X	X	X	X	X	X	X	X	X	X
	Zusätzliche Daten zur Adressierung beim Verantwortlichen	Nein	X	X	X	X	X	X	X	X	X	X	X
	Korrespondenzsprachen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	Nein	X	X	X	X	X	X	X	X	X	X	X
	Funktion des Sachbearbeiters	Nein	X	X	X	X	X	X	X	X	X	X	
	Umfang der Vertretungsbefugnis	Nein	X	X	X	X	X	X	X	X	X	X	
	Bearbeitete Geschäftsfälle	Nein	X	X	X	X	X	X	X	X	X	X	
	Name bzw. Bezeichnung	Nein	X	X	X	X	X	X	X	X	X	X	X
An der Geschäftsabwicklung mitwirkende Dritte	Anrede/Geschlecht	Nein	X	X	X	X	X	X	X	X	X	X	X
	Anschrift	Nein	X	X	X	X	X	X	X	X	X	X	X
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	Nein	X	X	X	X	X	X	X	X	X	X	X
	Geburtsjahr (soweit zur Identifikation unbedingt notwendig)	Nein	X	X	X	X	X	X	X	X	X	X	X
	Geburtstag und -monat (soweit zur Identifikation unbedingt notwendig)	Nein	X	X	X	X	X	X	X	X	X	X	X
	Firmenbuchdaten	Nein	X	X	X	X	X	X	X	X	X	X	X
	Daten zur Bonität	Nein											
	Sperrkennzeichen (z. B. Kontaktsperre, Rechnungssperre, Liefersperre, Buchungssperre, Zahlungssperre)	Nein	X	X	X	X		X	X			X	
	Zuordnung zu einer bestimmten Kategorie der Leistungserbringer (einschließlich regionale Zuordnung, usw.)	Nein			X							X	X
	Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Nummer und Intrastat-Kenn-Nummer	Nein	X	X	X	X	X	X	X	X	X	X	X
	Zugehörigkeit zu einem bestimmten Einkaufsverband, Konzern	Nein	X	X	X	X	X	X	X	X	X	X	X
	Korrespondenzsprachen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	Nein	X	X	X	X	X	X	X	X	X	X	X
	Gegenstand der Lieferung oder Leistung	Nein	X	X	X	X	X	X	X	X	X	X	X
	Bonus-, Provisionsdaten und dgl.	Nein	X	X	X	X		X				X	





	Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben												
	Korrespondenzsprachen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	Nein	x	x	x	x	x	x	x	x			
	Angaben über besondere Bedingungen für die Annahme der Zustellung, Lieferung oder Leistung	Nein	x	x	x	x	x	x	x	x			
Fremdkapitalgeber	Name oder Bezeichnung, Anrede/Geschlecht	Nein	x	x	x	x						x	
	Anschrift	Nein	x	x	x	x						x	
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	Nein	x	x	x	x						x	
	Korrespondenzsprachen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	Nein	x	x	x	x						x	
	Bankverbindung	Nein	x	x	x	x						x	
	Forderungen an den Verantwortlichen	Nein	x	x	x	x						x	
	Gegenforderungen des Verantwortlichen	Nein	x	x	x	x						x	
Gesellschafter	Name oder Bezeichnung, Anrede/Geschlecht	Nein	x	x	x	x	x					x	
	Anschrift	Nein	x	x	x	x	x					x	
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	Nein	x	x	x	x	x					x	
	Korrespondenzsprachen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	Nein	x	x	x	x	x					x	
	Bankverbindung	Nein	x	x	x	x	x					x	
	Ausstehende Einlagen	Nein	x	x	x	x	x					x	
	Sonstige Forderungen des Verantwortlichen (z. B. Privatentnahmen)	Nein	x	x	x	x	x					x	
	Bezüge	Nein	x	x	x	x	x					x	
Gewinn- und Verlustanteile	Nein	x	x	x	x	x					x		

## 5. Lösungs- und Aufbewahrungsfristen<sup>10</sup> (wenn möglich)

Datenverarbeitung	Angabe bzw. Beschreibung der Lösungs- bzw. Aufbewahrungsfristen
Kundenverwaltung, Rechnungswesen und Logistik	Höchstdauer der zulässigen Datenaufbewahrung: Bis zur Beendigung der Geschäftsbeziehung oder bis zum Ablauf der für den Verantwortlichen geltenden Garantie-, Gewährleistungs-, Verjährungs- und gesetzlichen Aufbewahrungsfristen; darüberhinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden.
Buchführung	Gesetzliche Aufbewahrungsfristen ( 7 Jahre gemäß UGB / BAO)
Kunden- bzw. Lieferantenstammdaten	In der Regel mit Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Verantwortlichen.

## 6. Kategorien von Empfängern<sup>11</sup>, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

### a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien (aus 4.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Banken		
Rechtsvertreter		
Wirtschaftstreuhänder / Buchhalter		
Gerichte, Verwaltungsbehörden		
Inkassounternehmen		
Fremdfinanzierer		
Vertragspartner / Geschäftspartner		
Versicherungen		
Konzernleitung		
Kunden		
<b>[weitere Empfänger individuell ergänzen, z.B. von Ihnen eingesetzte</b>	<b>[z.B. USA]</b>	

<sup>10</sup> Nach der DSGVO sind die Lösfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Lösfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (zB „nach Ablauf des Vertrages“).

<sup>11</sup> Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.

Auftragsverarbeiter wie IT-Dienstleister (Provider) etc]		

- b. 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):<sup>12</sup>

[Betreffend alle unter a) angegebene Drittstaaten außerhalb der EU ohne angemessenes Datenschutzniveau, Angabe der Rechtsgrundlage zur Sicherstellung der Rechtmäßigkeit der Datenübermittlung]

<sup>12</sup> Siehe dazu das Merkblatt [„Internationaler Datenverkehr“](#).

## II. Detailangaben zu Personalverwaltung

### 1. Kategorien der betroffenen Personen

Lfd.Nr.

- 1 Arbeitnehmer, arbeitnehmerähnliche Personengruppen, Leiharbeitnehmer, freie Dienstnehmer, Lehrlinge, Volontäre und Ferialpraktikanten (auch ehemalige Beschäftigte)
- 2 Organe (und deren Mitglieder) und sonstige Funktionsträger von juristischen Personen und Personengemeinschaften, soweit sie nicht Beschäftigte gemäß Punkt 1 sind (umfasst auch ehemalige Organe und Funktionsträger)
- 3 Bewerber

### 2. Rechtsgrundlagen

Zur Vertragserfüllung erforderlich, rechtliche Verpflichtungen, Einwilligung, berechnigte Interessen des Verantwortlichen.

### 3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) sind abgelegt: (freiwillig)

[siehe Fußnote oben – freiwillig zu befüllen, wie und sich gemäß Ihren konkreten innerbetrieblichen Abläufe die Daten und Unterlagen befinden, z.B. im Haus, beim Lohnverrechner, externer Provider etc]

### 4. Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Gläubiger des Betroffenen	Sozialversicherungsträger	Wahlvorstand für Betriebsratswahl	Arbeitsinspektorat	Organe betrieb. Interessenvertretung	Gemeindebehörden in verwaltungspolizeilichen Agenden	Bezirksverwaltungsbehörde in verwaltungspolizeilichen Agenden	Lehrlinienstelle	Arbeitsmarktservice	Bundessozialamt	Finanzamt	Versicherungsanstalten	bei Auszahlung betroffene Banken	Gewerkschaft (mit Zustimmung Betroffener)	Gesetzliche Interessenvertretung	Betriebsratsfonds	Betriebsärzte	Pensionskassen	Rechtsvertreter	Gerichte	Mitversicherte	Mitarbeiterversorgungskassen	Kunden und Interessenten des Verantwortlichen		
Arbeitnehmer, arbeitnehmerähnliche Personengruppen, Leiharbeiter, freie Dienstnehmer, Lehrlinge, Volontäre und Feriapraktikanten (auch ehemalige Beschäftigte)	Personalnummer	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			
	Name	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
	Frühere Namen (Namensteile)	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
	Geburtsdatum	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
	Geburtsort	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
	Geschlecht	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
	Personenstand	Ja	x	x		x	x				x	x	x	x					x	x	x	x	x	x			
	Kinder und sonstige Familienangehörige, im Zusammenhang mit Leistungen, die iVm dem Arbeitsverhältnis des Betroffenen erbracht werden (insb. Name, Geburtsdatum, Sozialversicherungsnummer)	Nein		x		x	x				x	x	x	x					x	x	x	x	x				
	Gesetzlicher Vertreter	Nein		x		x	x				x	x	x	x	x	x	x	x	x	x	x	x	x	x			
	Staatsbürgerschaft	Nein		x		x	x	x	x	x	x	x						x				x	x				
	Bankverbindung	Nein		x		x	x					x	x									x	x				
	Organisatorische Zuordnung im Betrieb (inkl. Beginn und Ende)	Nein		x	x	x	x	x	x		x	x				x	x		x			x	x			x	
	Kontaktdaten	Nein		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Wohnadresse und private Kontaktdaten	Nein		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				x	x	x	x		
Sozialversicherungsnummer	Ja		x		x	x					x	x	x					x	x	x	x	x	x	x			



















6. Kategorien von Empfängern<sup>13</sup>, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern<sup>14</sup>

a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien (aus 4.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Gläubiger des Betroffenen sowie sonstige an der allenfalls damit verbundenen Rechtsverfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretungen für fällige Forderungen		
Sozialversicherungsträger (einschließlich Betriebskrankenkassen);		
Wahlvorstand für Betriebsratswahlen		
Arbeitsinspektorat, Verkehrs-Arbeitsinspektion und Land- und Forstwirtschaftsinspektion, insbesondere gemäß § 8 Arbeitsinspektionsgesetz;		
Organe der betrieblichen Interessensvertretung (insbesondere Betriebsrat gemäß § 89 Z 4 ArbVG, Sicherheitsvertrauensperson nach § 10 ArbeitnehmerInnenschutzgesetz (ASchG), BGBl. Nr. 450/1994 idgF., Jugendvertrauensperson gemäß § 125ff ArbVG und Behinderten-		

<sup>13</sup> Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.

vertrauensperson gemäß § 22a Behinderteneinstellungsgesetz);		
Gemeindebehörden in verwaltungspolizeilichen Agenden		
Bezirksverwaltungsbehörde in verwaltungspolizeilichen Agenden (Gewerbebehörde, Zuständigkeiten nach ASchG, usw.);		
Lehrlingsstelle gemäß § 19 Berufsausbildungsgesetz und Berufsschulen;		
Arbeitsmarktservice;		
Bundesamt für Soziales und Behindertenwesen (Bundessozialamt) z. B. gemäß § 16 Behinderteneinstellungsgesetz;		
Finanzamt		
Versicherungsanstalten im Rahmen einer bestehenden Gruppen- oder Einzelversicherung		
mit der Auszahlung an den Betroffenen oder an Dritte befasste Banken;		
vom Dienstnehmer angegebene Gewerkschaft, mit Zustimmung des Betroffenen;		
gesetzliche Interessensvertretungen		
Betriebsratsfonds gemäß § 73 Abs. 3 ArbVG		



Betriebsärzte		
Pensionskassen		
Rechtsvertreter		
Gerichte		
Mitversicherte		
Mitarbeitervorsorgekassen (MVK) gemäß § 11 Abs. 2 Z 5 und § 13 BMVG		
Kunden und Interessenten des Auftraggebers		
[weitere Empfänger individuell ergänzen, z.B. von Ihnen eingesetzte Auftragsverarbeiter wie IT- Dienstleister (Provider) etc]	[z.B. USA]	

- b. 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):<sup>14</sup>

[Betreffend alle unter a) angegebene Drittstaaten außerhalb der EU ohne angemessenes Datenschutzniveau, Angabe der Rechtsgrundlage zur Sicherstellung der Rechtmäßigkeit der Datenübermittlung]

<sup>14</sup> Siehe dazu das Merkblatt „[Internationaler Datenverkehr](#)“.

### III. Detailangaben zu Kundenbetreuung und Marketing für eigene Zwecke

#### 1. Kategorien der betroffenen Personen

Lfd.Nr.

- 1 eigene Kunden, Interessenten, die an den Verantwortlichen selbst herangetreten sind;
- 2 Kontaktperson beim Kunden oder Interessenten;
- 3 Potentielle Interessente, deren Adressen zugekauft oder selbst ermittelt wurden,

#### 2. Rechtsgrundlagen

Zur Vertragserfüllung erforderlich, Einwilligung, berechtigte Interessen des Verantwortlichen, bei bestehenden Kunden insbesondere § 107 TKG

#### 3. Verträge, Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten) sind abgelegt: (freiwillig)

[siehe Fußnote oben – freiwillig zu befüllen, wie und sich gemäß Ihren konkreten innerbetrieblichen Abläufe die Daten und Unterlagen befinden, z.B. im Haus, beim Lohnverrechner, externer Provider etc]

#### 4. Kategorien der verarbeiteten Daten

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO	Adressverlage und Direktwerbeunternehmen gem § 151 GewO 1994	Konzernleitung bei gewerblichen Kunden und Großkunden
eigene Kunden;	Name / Bezeichnung	Nein	x	x

Interessenten, die an den Verantwortlichen selbst herangetreten sind	Anschrift	Nein	x	x
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	Nein		
	Sperrenzeichen für Werbeaktionen	Nein		
	Untersagung der Übermittlung an Adressverlage	Nein		
	Berufs-, Branchen- und Geschäftsbezeichnung	Nein	x	x
	Geburtsdatum, wenn angegeben	Nein	x	
	Personenstand, wenn angegeben	Nein		
	Nachfrageinteressen	Nein		
	Kaufkraftklassifizierung	Nein		
	Betreuungsdaten	Nein		
	Kaufverhalten	Nein		x
	Sonstiges Antwortverhalten zu Werbeaktivitäten	Nein		
	Bonus- und sonstige Vorteilsdaten	Nein		
	Potentielle Interessenten, deren Adressen zugekauft oder selbst ermittelt wurden	Name /Bezeichnung	Nein	
Kontaktdaten (Anschrift, Telefonnummer, E-Mailadresse udgl)		Nein		
Öffentlich zugängliche Daten, soweit diese für Werbezwecke relevant		Nein		
Zugehörigkeit zu einer bestimmten Interessentenklasse		Nein		
Antwortverhalten zu Werbeaktivitäten		Nein		

Kontaktperson beim Kunden oder Interessenten	Ordnungsnummer	Nein		
	Name bzw Bezeichnung, Anrede/Geschlecht	Nein		
	Zugehöriger Kunde oder Interessent (Bezeichnung und Anschrift)	Nein		
	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	Nein		
	Korrespondenzsprache	Nein		
	Funktion oder betreutes Aufgabengebiet beim Kunden oder Interessenten	Nein		
	Geburtstag, Personenstand und dgl., soweit die Verwendung vom Betroffenen für Zwecke der Kontaktpflege gestattet wird	Nein		
	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrythmus, etc.)	Nein		

MUSTER

## 5. Lösungs- und Aufbewahrungsfristen (wenn möglich)

Datenverarbeitung	Angabe bzw. Beschreibung der Lösungs- bzw. Aufbewahrungsfristen
Kundenbetreuung und Marketing für eigene Zwecke	Die Daten dürfen bis zum Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Verantwortlichen aufbewahrt werden.

## 6. Kategorien von Empfängern<sup>15</sup>, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern<sup>14</sup>

### a. Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation wie zB UNO, OSZE)

Empfängerkategorien (aus 4.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Adressverlage gemäß § 151 GewO		
Konzernleitung bei gewerblichen Kunden und Großkunden		
[weitere Empfänger individuell ergänzen, z.B. von Ihnen eingesetzte Auftragsverarbeiter wie IT-Dienstleister (Provider) etc]	[z.B. USA]	

### b. 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):<sup>16</sup>

<sup>15</sup> Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.

<sup>16</sup> Siehe dazu das Merkblatt „[Internationaler Datenverkehr](#)“.

[Betreffend alle unter a) angegebene Drittstaaten außerhalb der EU ohne angemessenes Datenschutzniveau, Angabe der Rechtsgrundlage zur Sicherstellung der Rechtmäßigkeit der Datenübermittlung]

MUSTER

IV. Detailangaben zur [falls weitere Datenverarbeitungen im Unternehmen]

MUSTER

## 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 und tatsächlichen Gegebenheiten in Ihrem Unternehmen zu entscheiden, welche konkreten Maßnahmen von Ihnen zu treffen sind und welche im Einzelfall auch zumutbar sind)

### a. Vertraulichkeit<sup>17</sup>:

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

### b. Integrität<sup>18</sup>:

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

### c. Verfügbarkeit und Belastbarkeit:

- i. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, zB: Backup-Strategie, Virenschutz, Firewall;

---

<sup>17</sup> Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten.

<sup>18</sup> Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.



**d. Pseudonymisierung und Verschlüsselung:**

E. i. Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.

F. ii. Verschlüsselung: sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt: ....

**e. Evaluierungsmaßnahmen:**

i. Datenschutz-Management (zB Risikoanalyse, Datenschutz-Folgenabschätzung), einschließlich regelmäßiger Mitarbeiter-Schulungen;

MUSTER