WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

BEISPIEL

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

(HINWEIS: 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.)

Inhalt

A. Stammdatenblatt

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

a. Name(n) und Anschrift(en):
Max Mustermann GmbH
Neuer Weg 1
ZZZZ Musterdorf

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

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten[1]:
Franz Fachmann e.U.
Datenstraße 5
YYYY Datenstadt

d. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB 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 (zB „*Datenschutzkoordinator*“). Dieser kann, muss aber nicht ins Verarbeitungsverzeichnis aufgenommen werden. Siehe dazu das WKO-Merkblatt „Datenschutzbeauftragter“.
[2] Darunter sind Vertreter von nicht in der EU niedergelassenen Verantwortlichen zu verstehen.

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. **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 zB Korrespondenzen oder Verträge) in diesen Angelegenheiten
   2. **Personalverwaltung:** Verarbeitung und Übermittlung von Daten für die Personalplanung, Personalanstellung, Personalentlohnung sowie die Personalentwicklung und die damit verbundenen Verarbeitungen und Übermittlungen für Lohn-, Gehalts-, Entgeltsverrechnung und Einhaltung von arbeits- und sozialrechtlich vorgegebener Aufzeichnungs-, Auskunfts- und Meldepflichten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (zB Korrespondenzen, Bewerbungsschreiben, Dienstzeugnisse, Testergebnisse, Stellenbeschreibungen) in diesen Angelegenheiten
   3. **Marketing: ……**
   4. **Geschäftspartnerdatenbank: …….**
   5. **usw.**

2. **Wurde eine Datenschutz-Folgenabschätzung durchgeführt?[4]**

   Ja ☐ X **Nein ☐**

   Wenn Ja, wann?
   zuletzt vor 6 Monaten

   Wenn Nein, aus welchem Grund nicht?[5]

[3] 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.
[4] 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.
[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 das Merkblatt „Datenschutz-Folgenabschätzung“.

C. Detailangaben zu (1) Rechnungswesen und Geschäftsabwicklung

1. Kategorien der betroffenen Personen

Lfd.Nr.	*Beschreibung der Kategorien betroffener Personen (zB 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

2. Rechtsgrundlagen[6]

Art 6 Abs 1 lit a (*Einwilligung der Betroffenen*), lit b (*zur Vertragserfüllung erforderlich*), lit c (*gesetzliche Verpflichtungen nach der BAO und dem UGB*), lit f (*berechtigte Interessen des Verantwortlichen*) DSGVO
§ 132 BAO
§§ 190, 212 UGB

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten[7]) sind abgelegt:[8] (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.

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[9]

a. Kategorien der verarbeiteten Daten und ankreuzen bzw. anführen, ob sie an Empfänger[10] übermittelt werden

---

[6] 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“.

[7] Siehe zu den Informationspflichten das Merkblatt „Informationspflichten“.

[8] 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).

[9] Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verarbeitungsverzeichnis 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 (zB „nach Ablauf des Vertrages“).

[10] In 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).

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO[11], strafrechtlich relevant iSd Art 10 DSGVO[12]	Muttergesellschaft Fa. YYY	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder	Gerichte im Anlassfall	Verwaltungsbehörden Im Anlassfall	Inkassounternehmen Im Anlassfall	Fremdfinanzierer (zB Leasing)	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
1	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-Nummer	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 odgl.)	Nein		X	X	X	X	X	X	X	X	X	X
	11	Vertragstexte und Geschäftskorrespondenzen			X	X	X	X	X	X	X		X	
2	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
3	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
	18	Kontaktdaten (Tel., Mail, Fax odgl.)	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 odgl.)	Nein		X	X	X	X	X	X	X	X	X	X
	22	UID-Nummer	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						

[11] 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.

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

Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-4; 6-25;	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
5; 25;	Bis zur Beendigung der Geschäftsbeziehungen

5. Kategorien von Empfängern[13], 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 bzw. Empfänger in Drittstaaten oder Internationalen Organisationen (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Banken		
Rechtsvertreter im Geschäftsfall		
Wirtschaftstreuhänder		
Gerichte		
Verwaltungsbehörden		
Inkassounternehmen		
Fremdfinanzierer (zB Leasing)		
mitwirkende Vertrags- und Geschäftspartner: Firma N.N.	Kanada	
Versicherungen um Anlassfall		
Provider (IT-Dienstleister)		

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):[14]

Für Kanada gibt es einen Angemessenheitsbeschluss der Europäischen Kommission.

[13] Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren. 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).

[14] Siehe dazu das Merkblatt „Internationaler Datenverkehr“. Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers.

C. Detailangaben zu (2) Personalverwaltung
(Beispiel einer anderen Gestaltungsmöglichkeit)

1. Kategorien der betroffenen Personen

Lfd.Nr.	*Beschreibung der Kategorien betroffener Personen (zB Mitarbeiter, Leiharbeitnehmer, freie Dienstnehmer, Lehrlinge, Ferialpraktikanten, Volontäre usw.)*
1	Arbeitnehmer, freie Dienstnehmer, Lehrlinge, Ferialpraktikanten, ehemalige Beschäftigte
2	Bewerber

2. Rechtsgrundlagen[15]

Art 6 Abs 1 lit b (*zur Vertragserfüllung inkl. Betriebsvereinbarungen erforderlich*), lit c (*gesetzliche Verpflichtungen*) DSGVO: ABGB, AMSG, AngG, ArbIG, ArbVG, ARG, ASchG, ASVG, AuslBG, BAG, BEinstG, BMVSG, BundesarbeiterkammerG, EFZG, EStG, FLAF, FLAG, GlBG, MSchG, PKG, UrlG, VersVG, VKG

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten[16]) sind abgelegt:[17] (freiwillig)

Unterlagen zu aufrechten Arbeits-, Dienst- und Ausbildungsverhältnissen sind in der Personalabteilung abgelegt.

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[18]

a) Kategorien der verarbeiteten Daten und ankreuzen bzw. anführen, ob sie an Empfänger[19] übermittelt werden

---

[15] 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“.

[16] Siehe zu den Informationspflichten das Merkblatt „Informationspflichten“.

[17] 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).

[18] Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verarbeitungsverzeichnis 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 (zB „nach Ablauf des Vertrages“).

[19] In 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).

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO[20], strafrechtlich relevant iSd Art 10 DSGVO[21]	Aufbewahrungsdauer (Jahre)	Empfänger
1(Arbeitnehmer)	Personalnummer		7	1-23, 25
	Name		30	1-25
	Frühere Namen (Namensteile)		7	1-23, 25
	Geburtsdatum		30	1-12, 14-22, 25
	Geburtsort		7	1-12, 14-21, 25
	Geschlecht		30	1-22, 25
	Personenstand		7	1-2, 4-5, 9-12, 16-18, 20-21, 25
	Kinder und sonstige Familienangehörige, im Zusammenhang mit Leistungen, die in Verbindung mit dem Arbeitsverhältnis des Betroffenen erbracht werden (insbesondere Name, Geburtsdatum, Sozialversicherungsnummer)		7	2, 4-5, 9-12, 16-18, 20-21, 25
	Gesetzlicher Vertreter		7	1-2, 4-5, 8-18, 20-21, 25
	Staatsbürgerschaft		7	2-11, 15, 20-21, 25
	Bankverbindung		7	1-2, 4-5, 9-10, 13, 19, 21-22, 25
	Organisatorische Zuordnung im Betrieb einschließlich Beginn und Ende		30	2-7, 9-10, 14-15, 20-21, 24, 25
	Elektronische Kontaktdaten, dienstlich (E-Mail-Adresse, Telefon-, Faxnummer..)		7	1-22, 24, 25
	Wohnadresse		30	1-16, 20-22, 25
	Elektronische Kontaktdaten, privat (E-Mail-Adresse, Telefon-, Faxnummer..)		7	1-16, 20-22, 25
	Sozialversicherungsnummer	ja	7	2, 4-5, 9-11, 17-23, 25
	Sozialversicherungsträger		7	2, 4-5, 9-11, 18-22, 25
	Daten zur Krankenscheinverwaltung	ja	7	2, 17, 20-22, 25
	Dienstnehmer-Sozialversicherungsdaten		7	2, 4-5, 18-21, 25
	Daten der Versichertenmeldung		7	2, 4-5, 18-21, 25
	Daten der Beitragsgrundlagenmeldung		7	2,4-5, 18-21, 25
	Daten zu Erstattungsantrag Krankenentgelt gemäß § 8 EFZG	ja	7	2, 4-5, 18-21, 25
	Daten zu Arbeits- und Entgeltbestätigungen für Krankengeld	ja	7	2, 4-5, 18-21, 25

[20] 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.

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

	Daten zu Arbeits- und Entgeltbestätigungen für Wochengeld		7	2, 4-5, 18-21, 25
	Daten zu Mitarbeitervorsorge gemäß BMVG		7	2, 11, 19, 23, 25
	Eintrittsdatum		30	2-8, 10, 12, 15, 18, 20-21, 25
	Vordienstzeiten		30	12, 18, 20-21, 25
	Austrittsdatum, Kündigungsfrist		30	2-8, 10, 12, 15, 18, 20-21, 25
	Art und Beendigung des Dienstverhältnisses		30	2-5, 9-10, 20-21, 25
	Gesetzliche Beschäftigungsvoraussetzungen		7	4-8, 10, 20-21, 25
	Daten der Beschäftigungsbewilligung		7	4-7, 9, 20-21, 25
	Bezeichnung der Tätigkeit		30	2, 4-7, 9, 17, 20-21, 25
	Gruppenzugehörigkeit (Arbeiter/Angestellte)		30	2-7, 9, 14-15, 19-21, 25
	Sicherheitsstufe/Zugangs- (Zugriffs-)rechte		7	4-5, 20-21, 25
	Lichtbild des Betroffenen (für Ausweiskarten)		7	4-5, 20-21, 25
	Gültigkeitsdauer der Ausweiskarte		7	4-5, 20-21, 25
	Arbeitszeiterfassung		7	4-5, 20-21, 25
	Sonstige Daten zur Arbeitszeit (insbesondere Geringfügigkeit, Arbeitsstunden, Überstunden, Gleitzeit, Nach- und Teilzeitarbeit)		7	2, 4-7, 9, 11, 20-21, 25
	Daten zur Urlaubsverwaltung		7	3-5, 9, 20-21, 25
	Religionsbekenntnis (zur Abwesenheitsverwaltung), nach Angabe des Betroffenen	ja	7	4-5, 20-21, 25
	Krankenstand, einschließlich Arbeitsunfall und Berufskrankheit (Beginn, Ende und Dauer)	ja	30	2-5, 17-18, 20-21, 25
	Zeitpunkt des Arbeitsunfalls	ja	30	2-5, 17-18, 20-21, 25
	Kuraufenthalte	ja	7	2-5, 17-18, 20-21, 25
	Mutterschutz (Beginn und Ende)	ja	7	2-5, 9, 17-18, 20-21, 25
	Karenzurlaub gemäß MSchG und EKUG (Beginn und Ende)	ja	7	2-5, 9, 14, 17-18, 20-21, 25
	Präsenzdienst, Ausbildungsdienst oder Zivildienst (Beginn und Ende)		7	2-5, 9, 14, 18, 20-21, 25
	Art und Dauer der sonstigen Abwesenheit wegen Dienstverhinderung oder Dienstfreistellung (einschließlich vereinbarte Karenzierung)		7	2-5, 9, 18, 20-21, 25
	Daten zur Entgeltfortzahlung		7	2-5, 19-21, 25
	Beschäftigungsrelevante Daten gemäß ArbeitnehmerInnenschutzgesetz, BGBl. Nr. 450/1994 idgF., Bazillenausscheidergesetz, BGBl.Nr. 153/1945 idgF., Tuberkulosegesetz, BGBl.Nr. 127/1968 idgF. und ähnlichen Rechtsvorschriften	ja	7	4-7, 17, 20-21, 25

	Grad der Behinderung gemäß Behinderten-einstellungsgesetz (nach Bekanntgabe des Betroffenen)	ja	7	2-5, 9, 10, 14, 20-21, 25
	Gesetzliche, kollektivvertragliche, betriebs-vereinbarungsmäßige und einzelvertragliche Grundlagen der Entgeltberechnung (Ein-stufung)		30	2, 4-5, 8-9, 19-21, 25
	Brutto- und Nettoentgelt (Daten des Gehalts-zettels)		30	1-2, 4-5, 9, 11, 13, 18-21, 25
	Daten der Entgeltfortzahlung		7	2-5, 18-21, 25
	Abzüge vom Nettoentgelt auf Grund Gesetzes oder betrieblicher Vereinbarungen		7	12-13, 16, 18-21, 25
	Sachbezüge		7	1-2, 4-5, 11, 13, 18-21, 25
	Aufwandsentschädigungen (wie Reisege-bühren)		7	1-2, 4-5, 11, 13, 18-21, 25
	Sozialleistungen im Zusammenhang mit dem Arbeitsverhältnis		7	2, 4-5, 11, 13, 19-21, 25
	Daten nach Bezügebegrenzungsgesetz, BGBl.Nr. 64/1997 idgF.		7	19-21, 25
	Höhe des Gewerkschaftsbeitrages und Bezeichnung und Adresse des Empfängers (nach Bekanntgabe des Betroffenen)	ja	7	13-14, 19-21, 25
	Versicherungsprämien als Leistung des Arbeitgebers		7	4-5, 12-13, 19-21, 25
	Verwaltung von Vorschüssen und Darlehen		7	1, 13, 19-21, 25
	Lohnpfändungsdaten		7	1, 4-5, 19-21, 25
	Daten des Lohnzettels (L-16 Formular)		7	11, 19-21, 25
	Alleinverdiener- oder Alleinerzieher-Absetz-betrag (ja/nein)		7	2, 11, 19-21, 25
	Wohnsitzfinanzamt		7	-
	Daten zur Pensionskasse (insbesondere Ein- und Austritt, Beitragsdaten und Versiche-rungszeiten in der gesetzlichen Sozialver-sicherung im Zeitraum der Beschäftigung)		7	5, 12 ,14, 19, 21-22
	Daten zur Verwendung von Dienstfahrzeugen (insbesondere Führerschein, Abrechnungen, Schadensfälle, Versicherungen)		7	4-5, 12, 20-21, 25
	Besondere Qualifikationen (z.B. Gewerbe-schein, besondere Ausbildung)		7	4-5, 7, 20-21, 25
	Nebenbeschäftigung		7	19-21, 25
	Daten nach dem Berufsausbildungsgesetz, BGBl.Nr. 142/1969 idgF., und einschlägigen kollektivvertraglichen Regelungen bei Lehrlingen, insbesondere Lehrvertragsdaten und sonstige Daten aus dem Ausbildungs-verhältnis und Berufsschulbesuch		7	4-5, 8-9, 15, 20-21, 25

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO22, strafrechtlich relevant iSd Art 10 DSGVO23	Aufbewahrungsdauer (Monate)	Empfänger
2(Bewerber)	Ordnungsnummer		6	25
	Name (wenn vom Betroffenen angegeben)		6	25
	Geburtsdatum (wenn vom Betroffenen angegeben)		6	25
	Staatsbürgerschaft (wenn vom Betroffenen angegeben)		6	25
	Geschlecht (wenn vom Betroffenen angegeben)		6	25
	Anschrift (wenn vom Betroffenen angegeben)		6	25
	Telefonnummer (wenn vom Betroffenen angegeben)		6	25
	E-Mail-Adresse (wenn vom Betroffenen angegeben)		6	25
	Lichtbild (wenn vom Betroffenen angegeben)		6	25
	Berufserfahrung und Lebenslauf (wenn vom Betroffenen angegeben)		6	25
	Angestrebte Beschäftigung (wenn vom Betroffenen angegeben)		6	25
	Beginn der angestrebten Beschäftigung (wenn vom Betroffenen angegeben)		6	25
	Sprachkenntnisse		6	25
	Testergebnisse, Bewertung		6	25
	Datum der Bewerbung		6	25
	Passwort (für Bewerber)		6	25
	Bewerberquelle (wie haben Sie von uns erfahren?)		6	25
	Art der Bewerbung (Kanal: online, Mail)		6	25
	Status der Bewerbung		6	25
	Bemerkungen		6	25
	Historie der Bewerbung (Datum, Uhrzeit, Bemerkungen)		6	25
	Korrespondenz mit dem Bewerber		6	25
	Status der Anmeldung zu Newsletter (angemeldet/nicht angemeldet)		6	25
	Einschätzung inwieweit der Bewerber die geforderten Anforderungen erfüllt		6	25

[22] 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.

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

5. Kategorien von Empfängern[24], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[25]

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

Lfd. Nr.	Empfängerkategorien bzw. Empfänger in Drittstaaten oder Internationalen Organisationen	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)	Rechtsgrundlage für Datenübermittlung
1	Gläubiger des Betroffenen sowie sonstige an der allen-falls damit verbundenen Rechts-verfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretungen für fällige Forderungen			Art. 6 Abs 1 lit a und DSGVO
2	Sozialversicherungsträger (einschließlich Betriebskranken-kassen)			Allgemeines Sozialversicherungs-gesetz (ASVG)
3	Wahlvorstand für Betriebs-ratswahlen			Arbeitsverfassungsgesetz (ArbVG)
4	Arbeitsinspektorat			§ 8 Arbeitsinspektoratsgesetz (ArbIG)
5	Organe der betrieblichen Interessenvertretung			Arbeitsverfassungsgesetz (ArbVG)
6	Gemeindebehörden in ver-waltungspolizeilichen Agenden (Gewerbebehörde, Zuständig-keiten nach ASchG, usw.)			Diverse BG, LG und VO
7	Bezirksverwaltungsbehörde in verwaltungspolizeilichen Agenden (Gewerbebehörde, Zuständigkeiten nach ASchG, usw.			Diverse BG, LG und VO
8	Lehrlingsstelle und Berufs-schule			§ 19 Berufsausbildungsgesetz
9	Arbeitsmarktservice			Arbeitsmarktservicegesetz (AMSG)
10	Bundesamt für Soziales und Behindertenwesen (Bundes-sozialamt) zB gemäß § 16 Behinderteneinstellungsgesetz			§ 16 Behinderteneinstellungs-gesetz (BEinstG)
11	Finanzamt			Einkommensteuergesetz (EStG 1988)
12	Versicherungsanstalten im Rahmen einer bestehenden Gruppen- oder Einzelver-sicherung			Versicherungsvertragsgesetz (VersVG)
13	Mit der Auszahlung an den Betroffenen oder an Dritte befassten Banken			Art. 6 Abs 1 lit b DSGVO

[24] Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren. 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).

[25] Siehe dazu das Merkblatt „Internationaler Datenverkehr“. Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers.

14	Vom Dienstnehmer angegebene Gewerkschaft, mit Zustimmung des Betroffenen			Art. 6 Abs 1 lit b DSGVO iVm Vereinsgesetz 2002
15	Gesetzliche Interessenvertretungen			Arbeiterkammergesetz 1992
16	Betriebsratsfonds			§ 73 Abs 3 Arbeitsverfassungsgesetz (ArbVG)
17	Betriebsärzte			§§ 79ff ArbeitnehmerInnenschutzgesetz (ASchG)
18	Pensionskassen			Pensionskassengesetz (PKG)
19	Externer Personalverrechner			Art. 6 Abs 1 lit b, Art 9 Abs 2 lit b DSGVO
20	Rechtsvertreter			Art. 6 Abs 1 lit f DSGVO
21	Gerichte			Art. 6 Abs 1 lit f DSGVO
22	Mitversicherte			Art. 6 Abs 1 lit f DSGVO
23	Mitarbeitervorsorgekassen			§ 11 Abs 2 Z 5 und § 13 Betriebliches Mitarbeitervorsorgegesetz (BMVG)
24	Kunden und Interessenten des Auftraggebers			Art. 6 Abs 1 lit f DSGVO
25	EDV Dienstleister			Art. 6 Abs 1 lit f DSGVO

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)**:**

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:

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:

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;

d. Pseudonymisierung und Verschlüsselung:

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

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;

Stand: April 2018

Dieses Merkblatt ist ein **Produkt der Zusammenarbeit aller Wirtschaftskammern**.
Bei Fragen wenden Sie sich bitte an die Wirtschaftskammer Ihres Bundeslandes:
Burgenland, Tel. Nr.: 05 90907, Kärnten, Tel. Nr.: 05 90904, Niederösterreich Tel. Nr.: (02742) 851-0,
Oberösterreich, Tel. Nr.: 05 90909, Salzburg, Tel. Nr.: (0662) 8888-0, Steiermark, Tel. Nr.: (0316) 601-0,
Tirol, Tel. Nr.: 05 90905-1111, Vorarlberg, Tel. Nr.: (05522) 305-0, Wien, Tel. Nr.: (01) 51450-1615,
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!