

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO):

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

Inhalt

- A. Stammdatenblatt: Allgemeine Angaben**
- B. Datenverarbeitungen/Datenverarbeitungszwecke**
- C. Detailangaben zu den einzelnen Datenverarbeitungszwecken**
- D. Allgemeine Beschreibung organisatorisch-technischer
Maßnahmen**

A. Stammdatenblatt

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

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

Elektro Sabo GmbH

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

Email:

Tel.:

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzbeauftragten¹:

Es besteht keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, da keine umfangreiche Verarbeitung sensibler Daten erfolgt.

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 Verzeichnisses 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 Datenverarbeitung³:

1. Bautätigkeit

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, einschließlich automationsunterstützt erstellte und archivierte Dokumente (wie zB.: Korrespondenz oder Verträge) in diesen Angelegenheiten.

2. Planung

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden, einschließlich automationsunterstützt erstellte und archivierte Dokumente (wie zB.: Korrespondenz, Verträge, Pläne) in diesen Angelegenheiten.

2. Wurde eine Datenschutz-Folgenabschätzung durchgeführt?⁴

Ja Nein

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?⁵

Eine Datenschutz – Folgenabschätzung ist nicht erforderlich, da keine sensiblen personenbezogenen Daten, welche nicht auch öffentlich zugänglich sind strukturiert verarbeitet werden.

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 [„Risiko-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 [„Risiko-Folgenabschätzung“](#).

C. Detailangaben zu (1) Bautätigkeit

1. Kategorien der betroffenen Personen

Lfd.Nr

- 1 Mitarbeiter
- 2 Kunden (natürlich / juristisch)
- 3 Lieferanten inkl. deren Mitarbeitern und Sachbearbeitern
- 4 An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten.
- 5 Investoren und Teilhaber

2. Rechtsgrundlagen⁶

Art 6 Abs 1 DSGVO:

lit a: Einwilligung der Betroffenen

lit b: zur Vertragserfüllung erforderlich

lit c: gesetzliche Verpflichtung nach der BAO und dem UGB (§ 132 BAO „Aufbewahrungspflicht von Büchern, Aufzeichnungen und Belegen“; §§190 212 UGB „Führung von Büchern“ und „Aufbewahrungspflicht, Aufbewahrungsfrist“)

lit f: berechtigtes Interesse des Verantwortlichen

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten⁷) sind abgelegt:⁸ (freiwillig)

Unterlagen zu aufrechten Geschäftsabwicklungen eines Verkaufes oder einer Vermietung, Rechnungen (auch) in der Finanzabteilung bzw. im ausgelagerten Rechnungswesen, erledigte Geschäftsfälle im Archiv.

4. Kategorien der verarbeiteten Daten und Lösungs- bzw. Aufbewahrungsfristen⁹

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 Verzeichnisse 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 Verzeichnisse 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 Löschrufen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verzeichnisse aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschrufen angegeben werden,

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

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO ¹⁰ , strafrechtlich relevant iSd Art 10 DSGVO ¹¹	Empfänger													
				Banken ¹²	Rechtsanwälte und Notare	SV - Träger und BUAK	Lohnverrechnung	Rechnungswesen ausgelagert	Steuerberatung und	Verwaltungsbehörden im Anlassfall	Gerichte im Anlassfall	Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	IT und Telekomprovider	Plattformen und Webseiten		
1	1	Name	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	2	Anschrift (privat)	Nein	x	X	x	x	x	x	x	x	x		x			
	3	Kontaktdaten privat (Tel. Mail)	Nein	x	X	x	x	x	x	x	x	x		x			
	4	Anschrift (Firma)	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	5	Kontaktdaten geschäftlich (Tel. Mail)	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	6	Sozialversicherungsnummer	Nein			x	x	x			x	x					
	7	Funktion	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	8	Bankverbindung	Nein	x	x	x	x	x	x	x	x	x	x	x	x		
	9	Bearbeitete Fälle	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	
	10	Vertretungsbefugnisse	Nein	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	11	Verträge und Vereinbarungen	Nein		x	x	x	x	x	x	x	x		x			
2	12	Firma (inkl. FB, UID), Name und Anschrift	Nein	x	x			x	x	x	x	x	x				
	13	Kontaktdaten (Tel. Mail)	Nein	x	x			x	x	x	x	x	x	x	x		
	14	Sozialversicherungsnummer	Nein		x			x	x	x	x			x			
	15	Projektbezeichnung	Nein	x	x			x	x	x	x	x	x	x	x	x	x
	16	Projektanschrift	Nein	x	x			x	x	x	x	x	x	x			
	17	Grundbuchsdaten	Nein	x	x			x	x	x	x	x	x	x			
	18	Funktion	Nein	x	x			x	x	x	x	x	x	x			
	19	Vertretungsbefugnisse	Nein	x	x			x	x	x	x	x	x	x			
	20	Bonität, Mahn- und Klagsdaten	Nein	x	x			x	x	x	x	x	x	x			
	21	Bankverbindung	Nein	x	x			x	x	x	x	x	x	x			
	22	Umfang des Auftragsverhältnisses	Nein	x	x			x	x	x	x	x	x	x			x
23	Verträge und Korrespondenz	Nein	x	x			x	x	x	x	x	x	x				
3	24	Firma und Anschrift	Nein	x	x	x		x	x	x	x	x	x			x	

da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (zB „nach Ablauf des Vertrages“).

¹⁰ 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.

¹¹ Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen unter behördlicher Aufsicht.

¹² In der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen.

	25	Kontaktdaten (Tel. Mail)	Nein	x	x	x		x	x	x	x	x	x		x
	26	Name Kontakt und Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		x
	27	Firmenbuchdaten	Nein	x	x	x		x	x	x	x	x	x		
	28	UID Nummer	Nein	x	x	x		x	x	x	x	x	x		
	29	Bonität, Mahn- und Klagsdaten	Nein	x	x	x		x	x	x	x	x	x		
	30	Bankverbindung	Nein	x	x	x		x	x	x	x	x	x		
	31	Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
	32	Vertretungsbefugnisse	Nein	x	x	x		x	x	x	x	x	x		
4	33	Firma und Anschrift	Nein	x	x	x		x	x	x	x	x	x		x
	34	Kontaktdaten (Tel. Mail)	Nein	x	x	x		x	x	x	x	x	x		x
	35	Name Kontakt und Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		x
	36	Firmenbuchdaten	Nein	x	x	x		x	x	x	x	x	x		
	37	UID Nummer	Nein	x	x	x		x	x	x	x	x	x		
	38	Bonität, Mahn- und Klagsdaten	Nein	x	x	x		x	x	x	x	x	x		
	39	Bankverbindung	Nein	x	x	x		x	x	x	x	x	x		
	40	Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
5	41	Vertretungsbefugnisse	Nein	x	x	x		x	x	x	x	x	x		
	42	Firma und Anschrift	Nein	x	x	x		x	x	x	x	x	x		
	43	Kontaktdaten (Tel. Mail)	Nein	x	x	x		x	x	x	x	x	x		
	44	Name Kontakt und Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
	45	Firmenbuchdaten	Nein	x	x	x		x	x	x	x	x	x		
	46	UID Nummer	Nein	x	x	x		x	x	x	x	x	x		
	47	Bonität, Mahn- und Klagsdaten	Nein	x	x	x		x	x	x	x	x	x		
	48	Bankverbindung	Nein	x	x	x		x	x	x	x	x	x		
49	Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x			
	50	Vertretungsbefugnisse	Nein	x	x	x		x	x	x	x	x	x		

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-19; 21-28; 30-37; 39-46; 48-50	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungen- oder Garantiefristen
20; 29; 38; 47	Bis zur Beendigung der Geschäftsbeziehungen

5. Kategorien von Empfängern¹³, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern¹⁴

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

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

Empfängerkategorien (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Banken		
Rechtsanwälte und Notare		
SV – Träger und BUAK		
Lohnverrechnung		
Rechnungswesen ausgelagert		
Steuerberatung und Wirtschaftsprüfung		
Verwaltungsbehörden im Anlassfall		
Gerichte im Anlassfall		
Vertrags- und Geschäftspartner		
Versicherungen im Anlassfall		
IT und Telekomprovider		
Plattformen und Webseiten		

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

¹⁴ Siehe dazu das Merkblatt „[Internationaler Datenverkehr](#)“.

C. Detailangaben zu (5) Planung

1. Kategorien der betroffenen Personen

Lfd.Nr

- 1 Mitarbeiter
- 2 Kunden (natürlich / juristisch)
- 3 Lieferanten inkl. deren Mitarbeitern und Sachbearbeitern
- 4 An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten.

2. Rechtsgrundlagen¹⁵

Art 6 Abs 1 DSGVO:

lit a: Einwilligung der Betroffenen

lit b: zur Vertragserfüllung erforderlich

lit c: gesetzliche Verpflichtung nach der BAO und dem UGB (§ 132 BAO „Aufbewahrungspflicht von Büchern, Aufzeichnungen und Belegen“; §§190 212 UGB „Führung von Büchern“ und „Aufbewahrungspflicht, Aufbewahrungsfrist“)

lit f: berechtigtes Interesse des Verantwortlichen

3. Verträge , Zustimmungserklärungen oder sonstige Unterlagen (zB Erledigung der Informationspflichten¹⁶) sind abgelegt:¹⁷ (freiwillig)

Unterlagen zu aufrechten Geschäftsabwicklungen eines Verkaufes oder einer Vermietung, Rechnungen (auch) in der Finanzabteilung bzw. im ausgelagerten Rechnungswesen, erledigte Geschäftsfälle im Archiv.

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen¹⁸

a. Kategorien der verarbeiteten Daten und Ankreuzen, ob sie an Empfänger 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 Verzeichnisse 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 Verzeichnisse aufzunehmen, 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 Verzeichnisse 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“).

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO ¹⁹ , strafrechtlich relevant iSd Art 10 DSGVO ²⁰	Banken ²¹	Rechtsanwälte und Notare	SV - Träger und BUAK	Lohnverrechnung	Rechnungswesen ausgelagert	Steuerberatung und	Verwaltungsbehörden im Anlassfall	Gerichte im Anlassfall	Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	IT und Telekommunikationsanbieter	Plattformen und Webseiten
1	1	Name	Nein	x	x	x	x	x	x	x	x	x	x	x	x
	2	Anschrift (privat)	Nein	x	X	x	x	x	x	x	x		x		
	3	Kontaktdaten privat (Tel. Mail)	Nein	x	X	x	x	x	x	x	x		x		
	4	Anschrift (Firma)	Nein	x	x	x	x	x	x	x	x	x	x	x	x
	5	Kontaktdaten geschäftlich (Tel. Mail)	Nein	x	x	x	x	x	x	x	x	x	x	x	x
	6	Sozialversicherungsnummer	Nein			x	x	x		x	x				
	7	Funktion	Nein	x	x	x	x	x	x	x	x	x	x	x	x
	8	Bankverbindung	Nein	x	x	x	x	x	x	x	x	x	x		
	9	Bearbeitete Fälle	Nein	x	x	x	x	x	x	x	x	x	x	x	
	10	Vertretungsbefugnisse	Nein	x	x	x	x	x	x	x	x	x	x	x	x
	11	Verträge und Vereinbarungen	Nein		x	x	x	x	x	x	x		x		
2	12	Firma (inkl. FB, UID), Name und Anschrift	Nein	x	x			x	x	x	x	x	x		
	13	Kontaktdaten (Tel. Mail)	Nein	x	x			x	x	x	x	x	x	x	
	14	Sozialversicherungsnummer	Nein		x			x	x	x	x		x		
	15	Projektbezeichnung	Nein	x	x			x	x	x	x	x	x	x	x
	16	Projektanschrift	Nein	x	x			x	x	x	x	x	x		
	17	Grundbuchdaten	Nein	x	x			x	x	x	x	x	x		
	18	Funktion	Nein	x	x			x	x	x	x	x	x		
	19	Vertretungsbefugnisse	Nein	x	x			x	x	x	x	x	x		
	20	Bonität, Mahn- und Klagsdaten	Nein	x	x			x	x	x	x	x	x		
	21	Bankverbindung	Nein	x	x			x	x	x	x	x	x		
	22	Umfang des Auftragsverhältnisses	Nein	x	x			x	x	x	x	x	x		x
23	Verträge und Korrespondenz	Nein	x	x			x	x	x	x	x	x			
3	24	Firma und Anschrift	Nein	x	x	x		x	x	x	x	x	x		x
	25	Kontaktdaten (Tel. Mail)	Nein	x	x	x		x	x	x	x	x	x		x
	26	Name Kontakt und Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		x
	27	Firmenbuchdaten	Nein	x	x	x		x	x	x	x	x	x		
	28	UID Nummer	Nein	x	x	x		x	x	x	x	x			

¹⁹ 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.

²⁰ Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen unter behördlicher Aufsicht.

²¹ In der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen.

	29	Bonität, Mahn- und Klagsdaten	Nein	x	x	x		x	x	x	x	x	x		
	30	Bankverbindung	Nein	x	x	x		x	x	x	x	x	x		
	31	Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
	32	Vertretungsbefugnisse	Nein	x	x	x		x	x	x	x	x	x		
4	33	Firma und Anschrift	Nein	x	x	x		x	x	x	x	x	x		x
	34	Kontaktdaten (Tel. Mail)	Nein	x	x	x		x	x	x	x	x	x		x
	35	Name Kontakt und Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		x
	36	Firmenbuchdaten	Nein	x	x	x		x	x	x	x	x	x		
	37	UID Nummer	Nein	x	x	x		x	x	x	x	x	x		
	38	Bonität, Mahn- und Klagsdaten	Nein	x	x	x		x	x	x	x	x	x		
	39	Bankverbindung	Nein	x	x	x		x	x	x	x	x	x		
	40	Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
	41	Vertretungsbefugnisse	Nein	x	x	x		x	x	x	x	x	x		
5	42	Firma und Anschrift	Nein	x	x	x		x	x	x	x	x	x		
	43	Kontaktdaten (Tel. Mail)	Nein	x	x	x		x	x	x	x	x	x		
	44	Name Kontakt und Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
	45	Firmenbuchdaten	Nein	x	x	x		x	x	x	x	x	x		
	46	UID Nummer	Nein	x	x	x		x	x	x	x	x	x		
	47	Bonität, Mahn- und Klagsdaten	Nein	x	x	x		x	x	x	x	x	x		
	48	Bankverbindung	Nein	x	x	x		x	x	x	x	x	x		
	49	Funktion der Kontaktperson	Nein	x	x	x		x	x	x	x	x	x		
	50	Vertretungsbefugnisse	Nein	x	x	x		x	x	x	x	x	x		

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-19; 21-28; 30-37; 39-46; 48-50	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungen- oder Garantiefristen
20; 29; 38; 47	Bis zur Beendigung der Geschäftsbeziehungen

5. Kategorien von Empfängern²², an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern¹⁴

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

Empfängerkategorien (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation (Angabe der intern. Organisation)
Banken		
Rechtsanwälte und Notare		
SV – Träger und BUAK		
Lohnverrechnung		
Rechnungswesen ausgelagert		
Steuerberatung und Wirtschaftsprüfung		
Verwaltungsbehörden im Anlassfall		
Gerichte im Anlassfall		
Vertrags- und Geschäftspartner		
Versicherungen im Anlassfall		
IT und Telekomprovider		
Plattformen und Webseiten		

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):²³

²² Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.

²³ Siehe dazu das Merkblatt „[Internationaler Datenverkehr](#)“.

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit²⁴:

- i. Es bestehen per 01/2018 keine zentralen Datenverarbeitungsanlagen (Datenbanken) mit sensiblen personenbezogenen Daten
- ii. Stationäre (Desktop PC) sowie mobile Geräte (Laptop, Mobiltelefone) sind passwortgeschützt.
- iii. Mobile Zugriffe auf das Netzwerk sind über ein passwortgeschütztes VPN Netzwerk erreichbar.

b. Integrität²⁵:

- i. Zugriffsberechtigungen auf die Netzwerkordner sind entsprechend den Betätigungsprofilen erstellt.
- ii. Mitarbeiter haben eine Vertraulichkeitserklärung unterschrieben
- iii. Das Vervielfältigen von Firmendaten aller Art zu privaten Zwecken ist den Mitarbeitern untersagt.
- iv. Dritte natürliche oder juristische Personen, bei denen nach angemessener Sorgfaltspflicht angenommen wird, dass sie über keine ausreichende Dokumentation (AGB's, Datenverarbeitungsverzeichnis) verfügen, haben eine Vereinbarung über eine *Auftragsverarbeitung nach Art. 28 DSGVO* (siehe Anlage) zu unterfertigen

c. Verfügbarkeit und Belastbarkeit:

- i. Datenbackups werden in regelmäßigen Abständen auf dem Server angelegt.
- ii. Serverdatenbackups werden in regelmäßigen Abständen auf den Arbeitsstationen bzw. externen Festplatten der Geschäftsführung abgelegt.
- iii. Mobilfunkgeräte (Kontaktdaten, Kalender) werden zumindest wöchentlich mit dem Netzwerk synchronisiert
- iv. Serverbackups werden zumindest wöchentlich erstellt
- v. Backups auf externen Geräten bzw. Festplatten der Geschäftsführung werden zumindest monatlich erstellt.
- vi. Eine Backup – Überprüfung der gesicherten Daten wird zumindest halbjährlich durchgeführt.

d. Pseudonymisierung und Verschlüsselung:

²⁴ Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten.

²⁵ Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

- i. Es bestehen per 01/2018 keine zentralen Datenverarbeitungsanlagen (Datenbanken) mit sensiblen personenbezogenen Daten welche pseudonymisiert bzw. verschlüsselt werden müssen.

e. Evaluierungsmaßnahmen:

- i. Sämtliche Mitarbeiter werden hinsichtlich der Auflagen der DSGVO zumindest jährlich geschult.

Stand: Jänner 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!