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

Inhalt:

A. Stammdatenblatt

Name und Kontaktdaten des für die Verarbeitung Verantwortlichen:

a. Name und Anschrift:
AZ Sonnenschutztechnik GmbH
GF Anton Zotter
Geschäftsführender Gesellschafter
Clementinengasse 10 / Ecke Turnergasse
1150 Wien
Österreich

b. Tel. Nr. und e-Mail-Adresse:
Telefon:**+43 (0) 1 / 892 04 11**
E-Mail: office@az-sonnenschutztechnik.at

c. Name und Kontaktdaten Anschrift, E-Mail und Tel.Nr. des Datenschutzkoordinators[1]:
DI(FH) Horst Hainzl
Schulweg 2
9081 Reifnitz
Hainzl@outlook.com
+43 664 73800907

[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“.

B. Datenverarbeitungen/Datenverarbeitungszwecke

1. Zwecke und Beschreibung der Datenverarbeitung:

1.1 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.

1.2 Personalverwaltung: Verarbeitung und Übermittlung von Daten für die Personalplanung, den Personaleinsatz, die Zeitaufzeichnungen, die Entlohnung sowie die Personalentwicklung und die damit verbundenen Verarbeitungen und Übermittlungen der Daten in diesen Angelegenheiten (z.B. Abrechnungsdaten, Korrespondenzen, Bewerbungsschreiben, Referenzen).

1.3 Marketing: Verwendung des Internetportales www.az-sonnenschutztechnik.at mit der Verbindung zu den sozialen Netzwerken facebook, instagram, youtube unter deren Datenrichtlinien z.B. www.facebook.com/privacy/explanation (siehe Datenschutzerklärung

1.4 Auftragsverarbeiter: Vereinbarungen nach Art.28 – EU-DSGVO

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

Ja ☐ Nein x

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?[3]

Keine Datenschutz-Folgenabschätzung (DSFA) ist für folgende Verarbeitungsvorgänge erforderlich: (Entwurf der DSB, Stand 2018/04/09)

Keine über die „White-List" hinausgehende Datenverarbeitung.

[2] 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.

[3] 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; Näheres dazu siehe auch das Merkblatt „Datenschutz-Folgenabschätzung" und „Prüfschema Internationaler Datenverkehr".

C. Detailangaben zu den einzelnen Datenverarbeitungszwecken

1. Kategorien der betroffenen Personen

1.1 Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten
1.2 Sachbearbeiter beim Verantwortlichen (Beschäftigte, freie Dienstnehmer)
1.3 An der Geschäftsabwicklung mitwirkende Dritte
inkl. Kontaktpersonen bei den Dritten

2. **Rechtsgrundlagen**[4]
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 sind abgelegt:[5]

Allgemeine Geschäftsbedingungen
www.az-sonnenschutztechnik.at/wp-content/uploads/2018/06/ABG.pdf
Geschäftsprozess, Anfrage, Angebot, Bestellung, Bestellbestätigung und allgemeinen Schriftverkehr
Lieferschein (Lieferung oder Abholung), Rechnung.
Verträge mit Lieferanten
Verträge mit Arbeitnehmern
Verträge mit Dienstleistern
Personenversicherung
Vereinbarung für Auftragsverarbeiter

4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen[6]

a. Kategorien der verarbeiteten Daten und ankreuzen, ob sie an Empfänger[7] übermittelt werden

[4] 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“.
[5] 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).
[6] 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“).
[7] In der Rubrik „Empfänger“ sind nur die „Empfängerkategorien“ (zB „Gerichte“, „Banken“ oder „Sozialversicherungsträger“) einzutragen. Dazu gehören auch Auftragsverarbeiter. Bei der Umschreibung der Empfängerkategorien ist darauf zu achten, dass eine Überprüfung der Rechtmäßigkeit ermöglicht wird (so wird

Kategorien der betroffenen Personengruppe aus Punkt 1 des C-Blattes (Lfd.Nr.)	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 DSGVO11 , strafrechtlich relevant iSd Art 10 DSGVO12	Banken	Rechtsvertreter im Geschäftsfall	Wirtschaftstreuhänder Steuerberater	Gerichte im Anlassfall	Verwaltungsbehörden im Anlassfall	Inkassounternehmen im Anlassfall	Fremdfinanzierer	Mitwirkende Vertrags- und Geschäftspartner	Versicherungen im Anlassfall	Provider (IT-Dienstleister)
1 Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten	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.,e Mail,Fax)	nein	X	X	X	X	X	X	X	X	X	X
	4	Handelsregister	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	UID Nummern	nein	X	X	X	X	X	X	X	X	X	
	8	Namen der Kontaktpersonen	nein	X	X	X	X	X	X	X	X	X	X
	9	Kontaktdaten der Kontakt-personen (Tel., Mail, Fax, Anschrift odgl.)	nein	X	X	X	X	X	X	X	X	X	X
	10	Vertragstexte und Geschäftskorrespondenzen	nein	X	X	X	X	X	X	X	X	X	
2 Sachbearbeiter beim Verantwortlichen	11	Name	nein	X	X	X	X	X	X	X	X	X	X
	12	Funktion des betroffenen Sachbearbeiters beim Verantwortlichen	nein	X	X	X	X	X	X	X	X	X	X
	13	Vom betroffenen Sachbe-arbeiter bearbeitete Fälle	nein	X	X	X	X	X	X	X	X	X	X
3 An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten	14	Name, Firma oder sonstige Geschäftsbezeichnung	nein	X	X	X	X	X	X	X	X	X	X
	15	Anschrift	nein	X	X	X	X	X	X	X	X	X	X
	16	Kontaktdaten (Tel., Mail, Fax odgl.)	nein	X	X	X	X	X	X	X	X	X	X
	17	Handelsregister	nein	X	X	X	X	X	X	X	X	X	X
	18	Namen der Kontaktpersonen	nein	X	X	X	X	X	X	X	X	X	X
	19	UID-Nummer	nein	X	X	X	X	X	X	X	X	X	X
	20	Bankverbindungen	nein	X	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 - 20	7 Jahre, unter Berücksichtigung der gesetzlichen Aufbewahrungspflicht
1 - 20	Darüber hinaus bis zur Beendigung eines allfälligen Rechtsstreits

5. Kategorien von Empfängern[8], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[9]

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)	Rechtsgrundlage für Datenübermittlung
Präventionsdienste			ASchG
Sozialversicherungsträger			Allgemeines Sozialversicherungs-gesetz (ASVG)
Gewerbebehörde			Diverse BG, LG und VO
Finanzamt			Einkommensteuergesetz
Versicherungsanstalten			Versicherungsvertrags-gesetz
Mit der Auszahlung an den Betroffenen oder an Dritte befassten Banken			Art. 6 Abs 1 lit b DSGVO
Rechtsvertreter			Art. 6 Abs 1 lit f DSGVO
Gerichte			Art. 6 Abs 1 lit f DSGVO
Kunden und Interessenten des Auftraggebers			Art. 6 Abs 1 lit f DSGVO
EDV Dienstleister			Art. 6 Abs 1 lit f DSGVO
Soziale Netzwerke		Facebook YouTube Instagram	Datenschutz in sozialen Netzwerken nach der Datenschutzgrund-verordnung

[8] 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). Bei Empfängern in Drittstaaten (speziell in den USA wegen dem „Privacy Shield“-System) empfiehlt sich eine namentliche Nennung des Empfängers.

[9] Siehe dazu das Merkblatt „Internationaler Datenverkehr“.

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit[10]:

1. Zutrittskontrolle: Schutz vor unbefugtem Zutritt zur Datenverarbeitungsanlage durch den separierten DV Raum, geschützt im Bürotrakt.
2. Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch sichere Kennwörter.
3. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Zugriff nur für Unternehmensinhaber und befugten Personen (z.B. Kundenlisten)
4. Personalunterlagen nur für Unternehmensinhaber und benannte Personen.

b. Integrität[11]:

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch die ausschließliche Bearbeitung der Unternehmensinhaber und Verträge zur Auftragsverarbeitung gemäß Art. 28 DS-GVO.

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch Backup Protokollierung, Dokumentenmanagement, örtlich getrennter Sicherungsserver, Sicherungskopie im 3 Monats Rhythmus.

c. Verfügbarkeit und Belastbarkeit:

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch die Backup-Strategie (Tresorsicherheit), Virenschutz, Firewall.

d. Evaluierungsmaßnahme:

Datenschutz Management durch die Fachkunde des Datenschutzkoordinators.

[10] Verhinderung von (unbeabsichtigter) Offenlegung oder unbefugten Zugang zu personenbezogenen Daten.
[11] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.