WIRTSCHAFTSRECHT

WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO):

REINHARD LIEDL

PRAXIS DER LEBENSKRÄFTE

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

Inhalt

A. Stammdatenblatt

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

a. Name(n) und Anschrift(en):
Reinhard Liedl, Starhembergstrasse 9;A-4211 Alberndorf i.d.Riedmark

b. E-Mail-Adresse(n) (und allenfalls weitere Kontaktdaten wie zB Tel.Nr.):
office@liedl.cc, 0676 / 44 60 410

c. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des Datenschutzkoordinator[1]:
Reinhard Liedl, Starhembergstrasse 9;A-4211 Alberndorf i.d.Riedmark
office@liedl.cc, 0676 / 44 60 410

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

[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 Verfahrensverzeichnis 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. **Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden/Klienten, einschließlich automationsunterstützt erstellter und archivierter Dokumente (z.B. Korrespondenz, Behandlungen) in dieser Angelegenheit**
   2. **Newsletterversand an Kunden zum Zweck der Information und Bewerbung**
   3. **Kundenschreiben zum Zweck der Information und Bewerbung**
   4.
   5.
   6.
   7.
   8.
   9.

   usw.

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

   Ja ☐ Nein ☒

   Wenn Ja, wann?

   Wenn Nein, aus welchem Grund nicht?[5]

   Eine Datenschutz-Folgenabschätzung wurde nicht durchzuführen, weil durch die Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte der Betroffenen besteht.

---

[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 ….. *(Einfügung der konkreten Datenverarbeitung aus dem B-Blatt, zB des Datenverarbeitungszweckes „Rechnungswesen"; das C-Blatt kann dann für jede der im B-Blatt angegebenen Datenverarbeitungszwecke verwendet werden, ohne dass die allgemeinen Angaben aus dem A- und B-Blatt wiederholt werden müssen)*

1. Kategorien der betroffenen Personen

Lfd.Nr.	*Beschreibung der Kategorien betroffener Personen (zB Kunden, Mitarbeiter, Lieferanten usw.)*
1	Kunde / Klient
2	Interessenten
3	Auftragsverarbeiter (IT-Unternehmen)
4	Ärzte und Krankenhäuser
5	Gerichte und Verwaltungsbehörden
6	Rechtsanwälte, Notare
7	Sachverständige, Schadensregulierungsbüros
8	Sozialversicherungsträger
9	Zeugen
10	IT-Dienstleister
11	Exekutive

2. Rechtsgrundlagen[6]

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

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

Kundenverträge in 4210 Gallneukirchen,Lederergasse 31/2C20
elektronische Scans in der Kundendatenbank (auch 4211 Alberndorf, Starhembergstrasse 9)
Verträge mit Auftragsverarbeitern in der 4210 Gallneukirchen,Lederergasse 31/2C20
Geschäftsunterlagen in 4210 Gallneukirchen,Lederergasse 31/2C20 sowie 4211 Alberndorf, Starhembergstrasse 9

---

[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 Verfahrensverzeichnis aufzunehmen. Allerdings unterliegt der verantwortliche Verarbeiter einer sogenannten Rechenschaftspflicht. Diese besagt eine Nachweispflicht bzgl. der Einhaltung der Pflichten nach der DSGVO. Dazu gehört unter anderem auch der Nachweis, dass die Datenverarbeitung nach den in der DSGVO normierten Rechtmäßigkeitsgrundlagen erfolgt. Siehe das Merkblatt „Grundsätze und Rechtmäßigkeit der Verarbeitung".

[7] 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).

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

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]	Empfängerkreise
1. Klient	1	Name	Nein	
	2	Titel	Nein	
	3	Geburtsdatum	Nein	
	4	Geburtsort	Nein	
	5	Geschlecht	Nein	
	6	Familienstand	Nein	
	7	Sozialversicherung, Sozialversicherungsnummer	Nein	
	8	Beruf	Nein	
	9	Staatsbürgerschaft	Nein	
	10	Anschrift	Nein	
	11	Kontaktdaten (Tel, Mail, Fax,.)	Nein	
	12	Beziehungsverhältnis	Nein	
	13	Bankverbindung	Nein	
	14	Risikoobjekte	Nein	
	15	Firmendaten (Frmenbuchnr., UID)	Nein	
	16	Kontaktpersonen bei Firmen	Nein	
	17	Kontaktdaten Kontaktpersonen (Tel, Mail, Fax)	Nein	
	18	Funktion der Kontaktperson	Nein	
	19	Korrespondenz	Nein	
	38	Biometrische Daten	Ja	
	39	Legitimationsdaten (RP, FS)	Nein	
	40	Hobbies, gefährliche Sportarten	Nein	
	41	Beschäftigungsverhältnis	Nein	
	42	Arbeitgeber	Nein	
	43	Ausbildung	Nein	
	44	Kundenklassifizierung	Nein	

[9] Nach der DSGVO sind die Löschfristen bzw. Aufbewahrungsfristen nach Möglichkeit ins Verfahrensverzeichnis aufzunehmen. Beispielsweise kann bei unbefristeten Verträgen keine konkrete Löschfrist angegeben werden, da der konkrete Vertragsablauf unbestimmt ist. Es empfiehlt sich hier allerdings eine abstrakte Frist anzugeben (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 Sicherungsmaßregeln unter behördlicher Aufsicht.

b. Löschungs- und Aufbewahrungsfristen (wenn möglich)

Daten aus 4.a. (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1-42; 50-99; 70-79; 80-86; 90-93; 100-105; 110-115; 120-127; 130-136; 140-146; 150-159; 160-165	Aufgrund der gesetzlichen Aufbewahrungsfristen auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
43	Bis zur Beendigung der Geschäftsbeziehungen

5. Kategorien von Empfängern[12], an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern[14]

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

Nr.	Empfängerkategorien (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	International e Organisation (Angabe der intern. Organisation)
1	Ärzte und Krankenhäuser		
2	Gerichte u. Verwaltungsbehörden		
3	Bezugsberechtigte/Begünstigte		
4	Geschädigte		
5	Rechtsanwälte, Notare		
6	Sachverständige, Schadensreg.büros		
7	Konzernunternehmen (Versicherg.,Banken)		
8	Sozialversicherungsträger		
9	Zeugen		
10	IT-Dienstleister		
11	Exekutive		

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)**:**[13]

-

[12] Es sind vor allem Übermittlungsempfänger („Dritte“) als auch Auftragsverarbeiter hier zu dokumentieren.
[13] Siehe dazu das Merkblatt „Internationaler Datenverkehr“.

D. Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

a. Vertraulichkeit:

Zutrittskontolle: (Def.: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, zB: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;) / Büro ist einem Mehrparteienhaus, wo die Eingangstüre (Wohnungstüre) versperrt wird.

Zugangskontrolle: (Def.: Schutz vor unbefugter Systembenutzung, zB: Kennwörter einschließlich entsprechender Policy, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern) / im Einsatz ist ein Passwortmanager Dashlane / Passwort-Policy: sichere Passwörter verwenden: 12 Zeichen, Groß-, Kleinbuchstaben, Zahlen, Sonderzeichen / verwendet wird ein Passwortgenerator / Zugang nur für Verantwortlichen.

Zugriffskontrolle: (Def.: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, zB: Protokollierung von Zugriffen) / es gibt keine Zugriffskontrollen aufgrund Einzelunternehmerstatus

b. Integrität:

Weitergabekontrolle: (Def.: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, zB: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;) / es erfolgt keine Eingabekontrolle aufgrund Einzelunternehmerstatus

#Eingabekontrolle: (Def.: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, zB: Protokollierung, Dokumentenmanagement;) / es erfolgt keine Eingabekontrolle aufgrund Einzelunternehmerstatus

c. Verfügbarkeit und Belastbarkeit:

(Def.: Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, zB: Backup-Strategie, Virenschutz, Firewall)
Virenschutzprogramm: Kaspersky Internet Security
Firewall: Router mit IP-Sec-Tunnel und ReadyNAS BOX sowie Kaspersky Internetsecurity
Backup-Strategie: Tägliche Sicherung zwischen PC Standort Gallneukrichen und Alberndorf in der Riedmark, ACER Extensa im Büro; Automatisierte Syncronsisation SmartSYNC PRO und RESILIO SYNC. Zwischen PC OPTIPLEX (DELL) Gallneukirchen-ReadyNAS BOX- (und über IP-SEC Tunnel)-PC HOME Alberndorf in der Riedmark.

d. Pseudonymisierung und Verschlüsselung:

(Def.: Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.) / es erfolgt keine Pseudonymisierung

(Def.: Verschlüsselung: sofern für die jeweilige Datenverarbeitung möglich, werden folgende Verschlüsselungstechnologien eingesetzt

e. Evaluierungsmaßnahmen:

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

Risikoanalysen werden in regelmäßigen Abständen (jährlich, anlassbezogen) durchgeführt.

Stand: 20.10.2017