Datenschutz-Konzept

gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

Stand vom 12.03.2018
work in progress

Mag. Christopher Temt
Verantwortliche gemäß DSGVO
Mooslackengasse 17
1190-Wien
Email: datenschutz@temt.at
Tel.: 0664 / 12 53 53 1

DISCLAIMER

Sämtliche zur Verfügung gestellten Inhalte wurden mit der größtmöglichen Sorgfalt erstellt. Der Autor übernimmt jedoch keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der bereitgestellten Informationen (einschließlich des Verweises auf externe Quellen). Die korrekte Datenschutzdokumentation und die TOMs erfordert stets eine **konkrete Prüfung im Einzelfall**, weshalb die Beiziehung eines Datenschutzberaters (z.B. datenschutz@temt.at bzw http://www.dataprivacydoctors.at/) sowie eines Rechtsanwaltes, insbesondere bei der Erstellung oder Überprüfung von Verträgen, dringend empfohlen wird. Die zur Verfügung gestellten Inhalte stellen keine Beratungsleistung welcher Art auch immer dar und können eine Beratung auch nicht ersetzen.

Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden, beziehen, die durch die Nutzung oder Nichtnutzung der zur Verfügung gestellten Informationen verursacht wurden, sind ausgeschlossen. Der Autor behält es sich ausdrücklich vor, Teile der zur Verfügung gestellten Information oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

Inhaltsverzeichnis

Inhaltsverzeichnis 2

1 Allgemeine Angaben 4

1.1 Datenschutz-Konzept 4

1.2 Sachliche und räumliche Tätigkeit 4

1.3 Datenschutzbeauftragter (DSB) 4

1.4 Verantwortliche (Stammdaten) 4

1.5 Schulung im Bereich Datenschutz und Datensicherheit 5

1.6 Weiterbildung und Stand der Technik 5

2 Datenverarbeitungen/Datenverarbeitungszwecke 5

2.1 Zwecke und Beschreibung der Datenverarbeitung: 5

2.1.1 Rechnungswesen und Geschäftsabwicklung: 5

2.1.2 Kundenbetreuung und Marketing 5

2.1.3 (Personalverwaltung) 5

2.2 Wurde eine Datenschutz-Folgenabschätzung durchgeführt? 6

3 Verfahrensverzeichnis 6

3.1 Rechnungswesen und Geschäftsabwicklung 6

3.1.1 Verantwortliche 6

3.1.2 Zweck 6

3.1.3 Kategorien der betroffenen Personen 6

3.1.4 Rechtsgrundlagen 6

3.1.5 Verträge , Zustimmungserklärungen oder sonstige Unterlagen 7

3.1.6 Kategorien der verarbeiteten Daten 7

3.1.7 Löschungs- und Aufbewahrungsfristen 9

3.1.8 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation) 9

3.1.9 Dokumentation 9

3.2 Kundenbetreuung und Marketing 9

3.2.1 Verantwortliche 9

3.2.2 Zweck 9

3.2.3 Kategorien der betroffenen Personen 9

3.2.4 Rechtsgrundlagen 10

3.2.5 Verträge , Zustimmungserklärungen oder sonstige Unterlagen 10

3.2.6 Kategorien der verarbeiteten Daten 10

3.2.7 Löschungs- und Aufbewahrungsfristen 12

3.2.8 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation) 12

3.2.9 Dokumentation 12

3.2.10 Weitere Verarbeitungsverzeichnisse 12

4 Checkliste für EPUs - IT-Safe (WKO) 12

5 Impressum und Datenschutzerklärung (WKO) 12

6 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs) 12
6.1 Selbstsschutz 12
6.2 Handy 12
6.3 Vertraulichkeit 13
6.4 Integrität 13
6.5 Verfügbarkeit und Belastbarkeit 13
6.6 Pseudo-, Ano-nymisierung und Verschlüsselung: 13
6.7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung 13

7 Betroffenenrechte wahren 14
7.1 Prozesse betreffs Betroffenenrechte 14
7.1.1 Profiling light 15
7.1.2 E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO) 15
7.2 Meldung von Datenschutzverletzungen 16

8 Risikoanalyse 17
8.1 Schutzbedarfsanalyse 17
8.2 Risikoanalyse ohne Maßnahmen 17
8.2.1 Bewertungsmaßstäbe 18
8.3 Maßnahmen 18
8.3.1 Vertraulichkeit 19
8.3.2 Integrität 19
8.3.3 Verfügbarkeit 19
8.4 Risikoanalyse mit Maßnahmen 19
8.5 Folgen der Maßnahmen betreffs Risiko 19

9 Mein angemessenes Datenschutzniveau 19
9.1 Visitenkarten und die DSGVO 20
9.2 Zusammenfassung 20

10 Anhang 21
10.1 Muster Datenschutzverletzung (WKO) 21
10.2 Mustervertrag Auftragsverarbeitung (WKO) 24
10.3 Muster -Technische und organisatorische Maßnahmen TOMS 27
10.4 Muster: Verpflichtungserklärung zum Datengeheimnis (WKO) 30
10.5 (Verarbeitungsverzeichniss – Personalwesen) 32

11 Danksagung 39
12 DISCLAIMER ..... 1 + 39

1 Allgemeine Angaben

1.1 Datenschutz-Konzept

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSVGO geforderte Einhaltung der Verordnungskonfomität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte (Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1).

1.2 Sachliche und räumliche Tätigkeit

Ich verarbeite als Kleinstunternehmen (EPU)* personenbezogene Daten von natürlichen Personen ab dem 18 Lebensjahr (Art 8 DSGVO) ganz oder teilweise automatisiert und habe meine Niederlassung in der EU, in der Mooslackengasse 17, 1190-Wien, Österreich.

* *Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung der DSGVO die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs „Kleinstunternehmen sowie kleine und mittlere Unternehmen“ sollte Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission maßgebend sein.*

Referenzen: Art 2 + 3 + 4 DSGVO, EuGH Entscheidung Weltimmo v. NAIH (C-230/34)

1.3 Datenschutzbeauftragter (DSB)

Trifft einer der nachfolgenden Kriterien zu, ist ein externer oder interner DSB notwendig und zu bestellen:

Kriterium	Ja	Nein
Verarbeitung der Daten durch eine Behörde oder eine öffentliche Stelle, mit Ausnahme der Gerichte		X
Verarbeitung der personenbezogenen Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person		X
Verarbeitung besonders schutzwürdige Kategorien personenbezogenen Daten (Art 9 Z 1 DSGVO wie zB Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit der Organisation dar		X

Referenzen: Art 37 DSGVO, Erwägungsgründe 97

Da für mein Kleinstunternehmen keiner der obigen Kriterien zutrifft, wird kein DSB bestellt.

1.4 Verantwortliche (Stammdaten)

Der Verantwortliche und für den Datenschutz Zuständige ist:

Mag. Christopher Temt
Mooslackengasse 17
1190-Wien
Email: datenschutz@temt.at
Tel.: 0664 / 12 53 53 1

Referenzen: Art 4 Z 7 DSGVO

1.5 Schulung im Bereich Datenschutz und Datensicherheit

Ich habe an folgende Schulungen bzw. Seminaren betreffs der DSGVO teilgenommen:

Bezeichnung der Veranstaltung	Veranstalter	Datum	Nachweis/Zertifikat Anhang Nr.:
Geprüfter Datenschutzexperte	incite	März 2018	Bestätigung
Ausbildung zum zertifizierten Datenschutzbeauftragten – DATB	WIFI	Oktober 2017	Lizenz bis 2020 DATB17W0012
Die EU-Datenschutz-Grundverordnung	ARS	25. Sep. 2017	Teilnahmebestätigung

Referenzen: Art 4, 5-11 DSGVO

1.6 Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze ich folgende Aktivität:

Aktivitäten	Veranstalter	sonstiges
Info- u. Weiterbildungsveranstaltungen	WKO-Wien	regelmäßig
Homepages bzw. Newsletter	https://www.privacyofficers.at	regelmäßig
	https://www.datens chutz-guru.de	regelmäßig
	http://www.dataprivacydoctors.at/	regelmäßig
	!!! DSGVO-Page der WKO !!!	
DAKO – Datenschutz Konkret	MANZ	5x jährlich

Referenzen: Art 4, 5-11 DSGVO

2 Datenverarbeitungen/Datenverarbeitungszwecke

Siehe auch meine DVR-Nr. 4018943.

2.1 Zwecke und Beschreibung der Datenverarbeitung:

2.1.1 Rechnungswesen und Geschäftsabwicklung:

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, sowie an der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

2.1.2 Kundenbetreuung und Marketing

Serviceorientierte Information und Betreuung von kategorisierten Kunden, Lieferanten und an der Geschäftsabwicklung mitwirkende Dritte bzw. Geschäftspartner inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Werbematerial.

Verarbeitung und Übermittlung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot

2.1.3 (Personalverwaltung)

Ich habe zur Zeit der Erstellung dieses Datenschutz-Konzeptes keine Mitarbeiter, da ich aber dies nicht ausschließen kann und will, habe ich auch ein Verarbeitungsverzeichnis für die Personalverwaltung erstellt, aber ohne pb Daten einzutragen. Die Idee ist, im Falle eines Dienstverhältnisses die pb Daten der Mitarbeiter von Anfang an DSGVO-konform verarbeiten und übermitteln zu können. Die DSGVO spricht auch davon, dass die Verarbeitungsverzeichnisse VOR der konkreten Verwendung erstellt werden sollen! (siehe Anhang)

2.1.3.1 Zweck

Verarbeitung und Übermittlung von 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 z.B. Korrespondenz) in diesen Angelegenheiten

Verarbeitung und Übermittlung von personenbezogenen Daten von Bewerbern, soweit diese Daten vom Betroffenen angegeben wurden.

2.2 Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

Ja ☐ **Nein** X

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?

Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, da. sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht – siehe Risikobewertung und Maßnahmen - ,da keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da keine umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Es gibt auch keine Überwachung öffentlich zugänglicher Bereiche durch Video.

Ob für meine Anwendungen eine Datenschutz-Folgenabschätzung gesetzlich vorgeschrieben bzw. nicht vorgeschrieben ist, kann nicht gesagt werden, da diese Listens seitens der Datenschutzbehörde noch nicht vorliegen (Art 35 Z4 + Z5)

Referenzen: Art 35 Z1-3 DSGVO

3 Verfahrensverzeichnis

Referenzen: Art 30, Art 31 DSGVO, Erwägungsgründe 13, 75, 76, 82, 89

3.1 Rechnungswesen und Geschäftsabwicklung

3.1.1 Verantwortliche

Mag. Christopher Temt
Mooslackeng. 17, 1190-Wien
Email: datenschutz@temt.at
Tel.: 0664 / 12 53 53 1

3.1.2 Zweck

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Kunden und Lieferanten, sowie an der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

3.1.3 Kategorien der betroffenen Personen

Lfd.Nr.	Beschreibung der Kategorien betroffener Personen
1	Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten
2	An der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen

3.1.4 Rechtsgrundlagen

- Art 6 Z 1 lit a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen) DSGVO
- § 132 BAO
- §§ 190, 212 UGB
- EStG, UStG
- Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004
- (Beraternorm EN16114)

3.1.5 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu aufrechten Geschäftsabwicklungen, Rechnungen, erledigte Geschäftsfälle, Unterlagen gemäß Beraternorm EN16114 und Zustimmungserklärungen sowie Verträge mit Auftragsverarbeitern * sind im Archiv abgelegt.

** Auskunft meiner Bank: Sie verarbeitet die Daten ihrer Kunden als Verantwortlicher im Sinne der Datenschutzgrundverordnung (DSGVO) und nicht als Auftragsverarbeiter. Es muss daher mit in Kraft treten der DSGVO (25.5.2018) keine gesonderten Auftragsverarbeitung nach Art 28 DSGVO mit mir abgeschlossen werden. Bei Überweisungsaufträgen wird lediglich der IBAN des Empfängers auf Kohärenz geprüft und der Überweisungsauftrag ausgeführt. Die Empfängernamen, die in einen Überweisungsauftrag eingegeben werden, werden nicht im Sinne des Art 4 DSGVO verarbeitet und dienen dem Kunden lediglich zu Dokumentationszwecken, damit dieser seine Zahlungen zuordnen kann.*

3.1.6 Kategorien der verarbeiteten Daten

- Vorlage ist die Muster-Anwendung der WKO (siehe https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-DSGVO-BEISPIEL-Verarbeitungsverzeichnis-Verantwortlicher.pdf , siehe Disclaimer).

- Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden sind auf Grund der konkreten Prüfung gemäß Datenminimierung nach Art 5 Z 1 DSGVO für mein Kleinstunternehmen mit **(X)** angekreuzt.

Kategorien der betroffenen Personengruppe	Lfd. Nr.	Datenkategorien	Besondere Datenkategorien iSd Art 9 und Art 10 DSGVO[1]	Banken	Geschäftsfall Rechtsvertreter	Steuerberater	Gerichte im Anlassfall (i.A.)	Verwaltungsbehörden i.A.	Inkassounternehmen i.A.	Mitwirkende Vertragspartner	Versicherungen i.A.	Provider (IT-Dienstleister)	Externer Datenschutzbeauftragter
1. Kunden und Lieferanten inkl. Kontaktpersonen beim Kunden und Lieferanten	1	Ordnungsnummer	*Nein*		X	X	X	X	X	X	X	X	
	2	Name, Firma oder sonstige Geschäftsbezeichnung	*Nein*	X	X	X	X	X	X	X	X	X	
	3	Anzahl Mitarbeiter	*Nein*		X		X						
	4	Anschrift bzw Lieferadresse	*Nein*	X	X	X	X	X	X	X	X	X	
	5	Homepage, Xing	*Nein*		X		X	X					
	6	Kontaktdaten (Tel., Handy, Skyp, signal.org, email, Fax)	*Nein*	X	X	X	X	X	X	X	X	X	
	7	Firmenbuchdaten	*Nein*	X	X	X	X	X	X	X	X	X	
	8	Daten zur Bonität inkl. Mahn -und Klagsdaten	*Nein*		X		X						
	9	Bankverbindungen	*Nein*	X	X	X	X	X	X	X	X		
	10	Kreditkartennummern und unternehmen	*Nein*	X	X	X	X						
	11	Kenn-Nummern für Zwecke amtlicher Statistik wie UID-, Intrastat-Kenn-, Steuer-Nummer	*Nein*	X	X	X	X	X	X	X	X		
	12	Namen Kontaktpersonen	*Nein*	X	X	X	X	X	X	X	X	X	
	13	Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.)	*Nein*	X	X	X	X	X	X	X	X	X	
	14	Funktion/Rolle der Kontaktperson	*Nein*		X	X	X	X	X	X	X		

1

	15	Zuordnung zu einer bestimmten Kunden- und Lieferanten, Interessentenkategorie (einschließlich regionale Zuordnung, usw.)	*Nein*		X		X	X			X		
	16	Bonus-, Provisionsdaten und dgl.	*Nein*		X	X	X						
	17	Auftragserfassung gem. Beraternorm EN16114	*Nein*		X		X						
	18	Art der Beratung	*Nein*		X		X						
	19	Vertragstext und Geschäftskorrespondenzen	*Nein*	X	X	X	X	X	X		X		
	20	Mahnsperre	*Nein*		X		X						
	21	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*		X		X						
	22	Serienbrief-Sperre	*Nein*		X		X						
	23	Newsletter-Sperre	*Nein*		X		X						
	24	Telefon-Aquise-Sperre	*Nein*		X		X						
2. An der Geschäftsabwicklung mitwirkende Dritte inkl. Kontaktpersonen bei den Dritten	25	Name, Firma oder sonstige Geschäftsbezeichnung	*Nein*	X	X	X	X	X	X	X	X	X	
	26	Anschrift, Lieferadresse	*Nein*	X	X	X	X	X	X	X	X	X	
	27	Homepage, Xing	*Nein*		X		X	X		X			
	28	Kontaktdaten (Tel., Skyp, signal.org, Mail, Fax,)	*Nein*	X	X	X	X	X	X	X	X	X	
	29	Firmenbuchdaten	*Nein*	X	X	X	X	X	X	X	X	X	
	30	Daten zur Bonität inkl. Mahn -und Klagsdaten	*Nein*		X		X						
	31	Bankverbindungen	*Nein*	X	X	X	X	X	X	X	X		
	32	Kreditkartennummern und unternehmen	*Nein*	X	X	X	X						
	33	Kenn-Nummern für Zwecke amtlicher Statistik wie UID-, Intrastat-Kenn-, Steuer-Nummer	*Nein*	X	X	X	X	X	X	X	X		
	34	Namen Kontaktpersonen	*Nein*	X	X	X	X	X	X	X	X	X	
	35	Zuordnung zu einer bestimmten Kategorie (einschließlich regionale Zuordnung, usw.)	*Nein*		X		X	X	X		X		
	36	Art der Kooperation	*Nein*		X		X						
	37	Vertragstext und Geschäftskorrespondenzen	*Nein*	X	X	X	X	X	X		X		
	38	Mahnsperre	*Nein*		X		X						
	39	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*		X		X						
	40	Serienbrief-Sperre	*Nein*		X		X						
	41	Newsletter-Sperre	*Nein*		X		X						
	42	Telefon-Aquise-Sperre	*Nein*		X		X						

3.1.7 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1 – 22; 24-40; 42	Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
23 + 41	Recht auf Widerspruch (Art 21 DSGVO)

3.1.8 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

Empfängerkategorien (aus 4.a.)	Drittstaat (Angabe des Drittstaats, d.h. Staaten außerhalb der EU)	Internationale Organisation
Banken	Nein	Nein
Rechtsvertreter im Anlassfall	Nein	Nein
Steuerberater, Bilanzbuchhalter	Nein	Nein
Gerichte im Anlassfall	Nein	Nein
Verwaltungsbehörden im Anlassfall	Nein	Nein
Inkassounternehmen im Anlassfall	Nein	Nein
Vertrags- und Geschäftspartner	Nein	Nein
Versicherung im Anlassfall	Nein	Nein
Provider (IT-Dienstleister)	Nein	Nein
Externer Datenschutzbeauftragter	Nein	Nein

3.1.9 Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten

3.2 Kundenbetreuung und Marketing

3.2.1 Verantwortliche

Mag. Christopher Temt
Mooslackeng. 17, 1190-Wien
Email: datenschutz@temt.at
Tel.: 0664 / 12 53 53 1

3.2.2 Zweck

Serviceorientierte Information und Betreuung von kategorisierten Kunden, Lieferanten und an der Geschäftsabwicklung mitwirkende Dritte bzw. Geschäftspartner inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie teil-automatisierte Übermittlung von Newsletter und Werbematerial.

Verarbeitung und Übermittlung von eigenen oder zugekauften Kunden- und Interessentendaten für die Geschäftsanbahnung betreffend das eigene Lieferungs- oder Leistungsangebot.

3.2.3 Kategorien der betroffenen Personen

Lfd.Nr.	Beschreibung der Kategorien betroffener Personen
1	Kunden; Lieferanten, an der Geschäftsabwicklung mitwirkende Dritte und Interessenten
2	Kontaktpersonen beim Kunden; beim Lieferanten, beim an der Geschäftsabwicklung mitwirkende Dritt, beim Interessenten
3	potenzielle Interessenten, deren Adressen von Adressverlagen zugekauft oder selbst ermittelt wurden:

3.2.4 Rechtsgrundlagen

- Newsletter: Art 6 Z 1 lit a (Einwilligung der Betroffenen)
- Ansonsten: Art: 6 Z 1 lit a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen)
- § 151 GewO 1994
- „SA022 Kundenbetreuung und Marketing für eigene Zwecke“ siehe Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004

3.2.5 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Zustimmungserklärungen bzw Verträge sowie Verträge mit Auftragsverarbeitern usw. sind im Archiv abgelegt.

3.2.6 Kategorien der verarbeiteten Daten

- Vorlage ist die Standardanwendung „SA022 Kundenbetreuung und Marketing für eigene Zwecke“

- Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden sind auf Grund **der konkreten Prüfung gemäß Datenminimierung nach Art 5 Z 1 DSGVO für mein Kleinstunternehmen mit (X)** angekreuzt.

Kategorien der betroffenen Personengruppe	Lf. Nr:	Datenkategorien	Art 9 und Art 10 DSGVO	rektwerbeunternehmen	nlassfallRechtsvertreter	im AnlassfallGericht	ragter DatenschutzExterner	Newsletter-TollExternes
1. eigene Kunden; Interessenten	01	Ordnungsnummer	*Nein*	X	X	X		
	02	Name bzw. Bezeichnung	*Nein*	X	X	X		X
	03	Anrede/Geschlecht	*Nein*	X	X	X		X
	04	Anschrift bzw. Lieferadresse	*Nein*	X	X	X		
	05	Telefon-, Handy-,Faxnummer, Emails, skyp, signal.org	*Nein*		X	X		Email
	06	Homepage, Xing	*Nein*		X	X		
	07	Einwilligung nach Art 4 abgelegt	*Nein*		X	X		
	08	Berufs-, Branchen- Geschäftsbezeichnung	*Nein*	X	X	X		
	09	Firmenbuchdaten	*Nein*		X	X		
	10	Korrespondenzsprache, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	*Nein*		X	X		
	11	Geburtsdatum	Gesonderte Einwilligung		X	X		
	12	Personenstand, nur Ehe und nicht Verpartnerung, da dies sexuelle Orientierung beinhaltet	Gesonderte Einwilligung		X	X		
	13	Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Kunden gegenüber dem Auftraggeber)	*Nein*		X	X		

	14	Kaufkraftklassifizierung	*Nein*		X	X		
	15	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrythmus etc.)	*Nein*		X	X		
	16	Kaufverhalten (Frequenz und Volumen)	*Nein*		X	X		
	17	Antwortverhalten zu Werbeaktivitäten	*Nein*		X	X		
	18	Bonus- und sonstige Vorteilsdaten	*Nein*		X	X		
	19	Newsletter-Sperre	*Nein*		X	X		
	20	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*		X	X		
	21	Serienbrief-Sperre	*Nein*		X	X		
Kontaktpersonen beim Kunden oder Interessenten:	22	Ordnungsnummer	*Nein*		X	X		
	23	Name bzw. Bezeichnung, Anrede/Geschlecht	*Nein*		X	X		
	24	Zugehöriger Kunde oder Interessent (Bezeichnung und Anschrift)	*Nein*		X	X		
	25	Telefon-, Handy-,Faxnummer, Emails, skyp, signal.org	*Nein*		X	X		
	26	Korrespondenzsprache	*Nein*		X	X		
	27	Funktion oder betreutes Aufgabengebiet beim Kunden oder Interessenten	*Nein*		X	X		
	28	Geburtstag, Personenstand und dgl.,	Gesonderte Einwilligung		X	X		
	29	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrythmus, etc.)	*Nein*		X	X		
	30	Einwilligung nach Art 4 abgelegt	*Nein*		X	X		
	31	Newsletter-Sperre	*Nein*		X	X		
	32	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*		X	X		
	33	Serienbrief-Sperre	*Nein*		X	X		
potenzielle Interessenten, deren Adressen von Adressverlagen zugekauft (gemietet) oder selbst ermittelt wurden:	34	Name bzw. Bezeichnung	*Nein*		X	X		
	35	Anschrift	*Nein*		X	X		
	36	Öffentlich zugängliche Daten, soweit diese für den Werbezweck relevant sind	*Nein*		X	X		
	37	Zugehörigkeit zu einer bestimmten Interessentenklasse	*Nein*		X	X		
	38	Antwortverhalten zu Werbeaktivitäten	*Nein*		X	X		
	39	Newsletter-Sperre	*Nein*		X	X		
	40	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*		X	X		

3.2.7 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1 – 33	Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen
34– 40	Die Daten werden nach Ablauf des dritten Jahres nach dem letzten Kontakt-(Versuch) gelöscht.
Newsletter	Recht auf Widerspruch (Art 21 DSGVO)

3.2.8 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

Empfängerkategorien	Drittstaat (d.h. Staaten außerhalb der EU)	Internationale Organisation
1.Adressverlage und Direktwerbeunternehmen gem. § 151 GewO 1994	Nein	Nein
2.Rechtsvertreter im Anlassfall	Nein	Nein
3.Gericht im Anlassfall	Nein	Nein
4.Externer Datenschutzbeauftragter	Nein	Nein
5. Externes Newsletter-Tool-Anbieter	Nein	Nein

3.2.9 Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten.

3.2.10 Weitere Verarbeitungsverzeichnisse

Weitere Muster bzw. Standard-Verzeichnisse für diverse Verarbeitungen/Anwendungen finden sich unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495&FassungVom=2018-05-24

4 Checkliste für EPUs - IT-Safe (WKO)

Ich bin die wirklich hilfreiche IT-Checkliste für EPUs unter https://itsafe.wkoratgeber.at/ durch gegangen und konnte feststellen, ob und wo es in meinem Kleinstunternehmen Probleme im IT-Bereich geben könnte. Die daraus folgenden Maßnahmen finden sich unter TOMs und werden bis zum 24. Mai 2018 umgesetzt sein.

5 Impressum und Datenschutzerklärung (WKO)

Wurden nach dem Muster der WKO erstellt:
https://www.temt.at/impressum/ https://www.temt.at/datenschutzerklaerung/ https://www.temt.at/agb/

6 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

6.1 Selbstsschutz

Ich versuche mein Such- und Surfverhalten soweit wie möglich „geheim“ zu halten und verwende daher den europäischen Open Source Browser https://cliqz.com/ inklusive Ghostery (verhindert und zeigt mir die Trackingversuche) und die europäische Suchmaschine: https://www.startpage.com /

6.2 Handy

Bei Apps ist es schwer festzustellen, worauf sie überall Zugriff nehmen, daher verwende ich, wenn überhaupt, nur Apps, die ich vorab kontrolliert habe (siehe http://app-ray.co/). WhatsApp zB habe ich aus gutem Grunde nie installiert. Ich verwende stattdessen das DSGVO-konforme https://www.signal.org/.

Mein Handy ist durch PIN geschützt. Es gibt die Möglichkeit die Daten „fern zu löschen" (Security App). Ich verwende „sichere Ordner" und lösche den SMS, WLAN- sowie Telefonverlauf, … mindestens 1x wöchentlich. Bluetooth-Funktion ist nur beim Autofahren eingeschaltet. In öffentliche WLAN-Netze wähle ich mich nicht ein und es gibt auch keine automatische Verbindung mit bekannten WLANs. Wenn ich ein neues Handy kaufe, so lass ich mein altes Handy von meinem IT-Fachmann immer vollständig löschen Falls ich USB-Sticks verwende, so sind die Daten darauf verschlüsselt und ein Passwort ist notwendig

6.3 Vertraulichkeit

Meine Unternehmensberatung befindet sich in einem besonderen Vertrauensverhältnis zu den Kunden und ich gehe daher mit allen erlangten Informationen verantwortungsbewusst um und wahre die Verschwiegenheit.

Eigenes Büro innerhalb von Nineteen:

i. **Zutrittskontrolle:** während Bürozeiten: Portier im EG, ansonsten nur zugang mit Chip; Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit Schlüssel.
ii. **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter (unterschiedlichen Zeichenzusammensetzung, Mindestlänge 8 Zeichen, Regelmäßiger Wechsel, Erstanmeldeprozedur) automatische Sperrmechanismen, Zwei Faktor - Authentifizierung, Verschlüsselung von Datenträgern;
iii. **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen, Protokollierung von Zugriffen
iv. **Klassifikationsschema** für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

6.4 Integrität

i. **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch Verschlüsselung, elektronische Signatur;
ii. **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement

6.5 Verfügbarkeit und Belastbarkeit

i. **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum
ii. Rasche **Wiederherstellbarkeit**; Backup-Strategie
iii. **Löschungsfristen** für pb Daten

6.6 Pseudo-, Ano-nymisierung 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. **Anonymisierung:** wo möglich und sinnvoll ist bzw. vor Löschung für interne Statistik
iii. **Verschlüsselung:**
- Verschlüsselung von Datenträgern/Geräten (**Data at Rest**)
  - Sicherheit der verwendeten Technologie (Wirksamkeit)
  - Durchgängige Umsetzung Laptop, Handy, …
- Verschlüsselung von Kommunikation (**Data in Motion**)
  - Datenaustausch mit Kunden/Lieferanten/Partnern
  - Zugriff auf Systeme
- Umgang mit Schlüsselmaterial
  - Verfügbarkeit -insbesondere bei Data at Rest

6.7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

i. Risikoanalyse
ii. Datenschutzfreundliche Voreinstellungen
iii. Ein Kontroll- und Verbesserungsprozess wir mindestens 1x jährlich durchgeführt

iv. Weiterbildung siehe Schulung

v. Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (zB. DATB, Vorabüberzeugungspflicht, Nachkontrollen)

Referenzen: Art 32 Z 1 DSVGO
Quelle 5.2 bis 5.6 : https://www.datenschutz-guru.de/files/**Ausfuellhilfe_TOM_9_BDSG_V2**.docx

7 Betroffenenrechte wahren

Grundsätzlich stelle ich jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version dieses Datenschutzkonzeptes auf meiner Homepage unter Datenschutz (siehe https://www.temt.at/datenschutzerklaerung/) zum Downloaden zur Verfügung.

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch (Art 21 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde

7.1 Prozesse betreffs Betroffenenrechte

i. Ich erhalte Kenntnis dass ein Betroffener seine Rechte geltend machen will, sei es zB mündlich, schriftlich. per Email (insbesondere datenschutz@temt.at), …

ii. Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:

„Sehr geehrte Frau/Herr …!
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie zB pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zu kommen zu lassen.
Ich danke Ihnen für Ihr Verständnis

P.S.: Mein aktuelles Datenschutzkonzept unter https://www.temt.at/datenschutzerklaerung/ .

iii. Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig..

iv. Identität zweifelsfrei festgestellt:
=> Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 14 Tagen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:

- Recht auf Auskunft (Art 15 DSGVO)
  Der Betroffene bekommt als Pdf
  - den Link: https://www.temt.at/datenschutzerklaerung/
    - sein Stammdatenblatt mit alle pb Daten
- Recht auf Berichtigung (Art 16 DSGVO)
  Der Betroffene bekommt als Pdf
  - den Link: https://www.temt.at/datenschutzerklaerung/
    - sein Stammdatenblatt mit den berichtigten pb Daten
- Recht auf Löschung (Art 17 DSGVO)
  Der Betroffene bekommt als Pdf

- den Link: https://www.temt.at/datenschutzerklaerung/
  - sein Stammdatenblatt ohne pb Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit den Hinweis, dass
- die Daten **anonymisiert** für die interne Statistik verwendet werden
- nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde

oder

  - Bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde ich alle Daten, bis auf jene, wo ich nach Art 6 Z 1 lit f ein berechtigte Interessen des Verantwortlichen DSGVO (vor allem Buchhaltungsunterlagen) geltend machen kann, löschen und daher aufgrund der gesetzlichen Aufbewahrungsfristen diese Daten auf jeden Fall erst nach 7 Jahre löschen; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die pb Daten löschen. In diesen Fällen tritt an Stelle einer Löschung der Daten eine Sperrung (Einschränkung).

- Recht auf Einschränkung (Art 18 DSGVO)

  Der Betroffene bekommt als Pdf
  - https://www.temt.at/datenschutzerklaerung/
    - sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Hackerl gesetzt ist und somit keine Verarbeitung seiner pb Daten erfolgt.
- Recht auf Übertragbarkeit (Art 20 DSGVO)

Der Betroffene bekommt als Pdf
  - https://www.temt.at/datenschutzerklaerung/
    - sein Stammdatenblatt mit alle pb Daten
    - gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit alle pb Daten als Cc.. an einen anderen Verantwortlichen, den der Betroffene mir genannt hat
- Recht auf Beschwerde bei der Datenschutzbehörde

7.1.1 Profiling light

Ich verarbeite (siehe Verfahrensverzeichnis Marketing) teil-automatisiert auch personenbezogener Daten von natürliche Personen, um Art und Form der jeweilig in Anspruch genommenen Dienstleistung/Produkt, Interessen, Ort, Branche, …, Verhalten dieser natürlichen Person, … zu kategorisieren und um im berechtigtes Interesse eine zielgerichtete Information und Betreuung (= simples Kundenprofil) sowie um eine personalisierte Direktwerbung (siehe E-Mail-Marketing) für meiner Kunde, Interessierten, Lieferanten, Projektpartner zu ermöglichen.

Da nur eine teil-automatisiert, keine umfassende Bewertung persönlicher Aspekte natürlicher Personen, keine Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt und auch ausdrücklich damit keinerlei automatische Generierung von Einzelentscheidungen verbunden ist und es gänzlich ohne rechtliche oder ähnliche Wirkung für den Betroffenen ist, ist dies Verarbeitung daher nicht als Profiling im Sinne des DSGVO (siehe unten Referenzen), sondern als **Profiling light**, als **kundenorientierte Service** zu sehen und es bedarf darüber hinaus auch keiner Datenschutz-Folgeabschätzung.

Referenzen: Art 4, Art 8, Art 9 DSGVO; Erwägungsgründe: 26ff, 51ff; § 4 Abs 4 DSG 2018

7.1.2 E-Mail-Marketing - Recht auf Widerspruch (Art 21 DSGVO)

Vorab beachte ich die sogenannte Robinson-Liste und setzte ein Hackerl bei „Keine Zusendungen von Werbematerial, Newsletter erwünscht“ für alle natürlichen und juristischen Personen, die in dieser Liste ausdrücklich auf die Zusendung von Werbematerial sowie Werbemails verzichten, siehe https://www.rtr.at/de/tk/TKKS_ECGListe
Referenz: § 7 E-Commerce-Gesetz (ECG)

Die Newsletter-Abonnenten, die ihre klare Einwilligung nach Art 4 DSGVO nachweislich abgegeben haben, werden hinreichend sowohl über Zweck, Art und Umfang der Datenverarbeitung als auch über ihre Rechte als Betroffene wie Recht auf Information, auf Auskunft und Richtigstellung, Widerspruchsrecht, auf Löschung und Einschränkung im E-Mail-Newsletter informiert

Darüber hinaus gibt es in jedem E-Mail-Newsletter die einfache und rasche Möglichkeit für den Betroffenen, sich vom E-Mail-Newsletter abzumelden (mit einem automatisierten Email, dass er von der Newsletterliste gelöscht wurde). Sollte dieses Mail-Newsletter-Tool von einem Dritten bereitgestellt sein, so gibt es dazu einen Vereinbarung mit diesem Auftragsverarbeiter nach Art 28 DSGVO (siehe Marketing-Verzeichnis). Individuelles Tracking, auch über eine Übermittlungs- bzw Lesebestätigung wird nicht gemacht, da dafür eine eigene Einwilligungserklärung notwendig ist.

Macht ein Betroffener seine Rechte auf Widerspruch nicht mit Hilfe des Links im Newsletter geltend, sondern in einer anderen Form, sei es zB mündlich, schriftlich. per Email (insbesondere datenschutz@temt.at), … so gilt folgendes:

i. Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:
„Sehr geehrte Frau/Herr …… !
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie zB pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zu kommen zu lassen.
Ich danke Ihnen für Ihr Verständnis

P.S.: Mein Datenschutzkonzept unter https://www.temt.at/datenschutzerklaerung/.

ii. Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig.

iii. Identität zweifelsfrei festgestellt:
=> Der Betroffene bekommt betreffs Recht auf Widerspruch (Art 15 DSGVO) innerhalb von maximal 14 Tagen folgende Antworten:

„Sehr geehrte Frau/Herr …… !
Gemäß Ihrem Wunsch habe ich Sie hiermit von der Newsletter-Verteiler-Liste gelöscht. Sie erhalten keinen Newsletter oder Werbezusendungen von mir mehr.“

7.2 Meldung von Datenschutzverletzungen

Die DSGVO definiert in Art 33 eine „Verletzung des Schutzes personenbezogener Daten“ (data breach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

i. Ich erlange Kenntnis von einer Datenschutzverletzung.

ii. **Innerhalb von 72 Stunden** mache ich eine Meldung mit Hilfe des „Muster Datenschutzverletzung“ (siehe Anhang) an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes pb Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

iii. Gemäß Art 34 Z3 DSGVO muss keine Benachrichtigung der Betroffenen erfolgt, da die Verletzung des Schutzes pb Daten aufgrund meiner TOMs (zB Verschlüsselung in Rest und Motion, BackUp, …) voraussichtlich kein **hohes Risiko** für deren persönlichen Rechte und Freiheiten zur Folge hat

iv. Die Datenschutzbehörde ist wohlbegründet gegenteiliger Meinung und fordert mich auf, alle/gewisse Betroffenen zu informieren, siehe Art 34 Z4 DSGVO.

i. Ich informiere Betroffenen umgehend mit einer entsprechenden Variation des „Muster Datenschutzverletzung“ (siehe Anhang)

v. Ich werde alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 Z5 DSGVO.

8 Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

8.1 Schutzbedarfsanalyse

Die Vorabanalyse ergab, dass es sich bei folgende pb Daten der Kunden, (potentiell) Interessenten, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit vernachlässigbaren bis geringem Schutzbedarf handelt, da. sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht und auch allgemeine TOMs gemäß DSGVO gesetzt wurden:

> *Öffentlich zugängliche Daten, Ordnungsnummer, Name, Firma oder sonstige Geschäftsbezeichnung, Anrede/Geschlecht, Anschrift, Homepage, Kontaktdaten (Tel., Skyp, Mail, Fax,), Berufs-, Branchen- und Geschäftsbezeichnung, Firmenbuchdaten, Keine Zusendungen von Werbematerial, Newsletter erwünscht, Untersagung der Übermittlung der Daten an Adressverlage, Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Nummer und Intrastat-Kenn-Nummer, Korrespondenzsprache, Namen der Kontaktpersonen, Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.), Funktion/Rolle der Kontaktperson, Zuordnung zu einer bestimmten Kunden- und Lieferanten, Interessentenkategorie (einschließlich regionale Zuordnung, usw.)*
>
> *Betreffs der Personalverwaltung wurden, da noch keine Mitarbeiter, keine pb Daten eingetragen!*

Eine Vorabanalyse ergibt, dass es sich bei folgende pb Daten der Kunden, (potentiell) Interessenten, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit einen **hohen** und **sehr hohen** Schutzbedarf handelt und daher eine erweiterte Risiko-Analyse durchgeführt werden muss.

> *Personenstand, Geburtsdatum, Daten zur Bonität inkl. Mahn -und Klagsdaten, Zahlungsverhalten, Kaufverhalten (Frequenz und Volumen), Bankverbindungen, Kreditkartennummern und -unternehmen, Bonus-, Provisionsdaten und dgl., Kaufkraftklassifizierung, Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Kunden gegenüber dem Auftraggeber), Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrythmus etc.), Sonstiges Antwortverhalten zu Werbeaktivitäten; Bonus- und sonstige Vorteilsdaten, Zugehörigkeit zu einer bestimmten Interessentenklasse, Vertragstext und Geschäftskorrespondenzen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch, Auftragserfassung gem. Beraternorm EN16114 und Mitschriften und Fotos*

8.2 Risikoanalyse ohne Maßnahmen

Schutzziele für meine Risikobewertung nach Art 4 Z 12 sind: Vertraulichkeit, Integrität und Verfügbarkeit. Die Risiko-Bewertung erfolgt nach „Schwere“ und „Eintrittswahrscheinlichkeit (EWK)“, siehe unten

Folgende Daten wurden analysiert und in die entsprechenden Kategorien eingetragen:

Kategorie	pb Daten
1	Vertragstext und Geschäftskorrespondenzen, Auftragserfassung gem. Beraternorm EN16114 inklusive Mitschriften u. Fotos, sonstige Vereinbarungen, Schlüssel zum Datenaustausch, Bonität => geheim/vertraulich
2	Bankverbindungen, Kreditkartennummern und unternehmen, Bonus-, Provisionsdaten und dgl., => geheim
3	Kaufkraftklassifizierung, Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Kunden), Kaufverhalten (Frequenz und Volumen), Bonus- und sonstige Vorteilsdaten, Personenstand, Geburtsdatum => intern/vertraulich
4	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrythmus etc.), Sonstiges Antwortverhalten zu Werbeaktivitäten; Zugehörigkeit zu einer bestimmten Kategorie, …) => intern
5	Pb Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe oben Vorabanalyse

Schwere					
Existenzgefährdend				1, 2	
Wesentlich				3, 4	
Begrenzt				5	
Vernachlässigbar					
	Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert	**EWK**

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Folgen ohne Maßnahmen:

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
		• Datenschutzbehörde **UND** Betroffene informieren • Folgeabschätzung notwendig

8.2.1 Bewertungsmaßstäbe

Schwere:

Schwere	Auswirkung auf Betroffene	Folgen überwinden	Beispiele
Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, …
Begrenzt	Wesentliche Unannehmlichkeiten	Unannehmlichkeiten sollten sich – trotz Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, …
Wesentlich	Wesentliche Folgen	Unannehmlichkeiten sollten sich – trotz großer Schwierigkeiten – überwinden lassen	Kategorien und Klassifizierungen werden bekannt, Missbrauch von Geldern, Vorladungen, Verschlechterung eines Verhältnisses, Weitergabe der Passwörter, Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte, …
existenz gefährdend	Irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	Bekanntwerden von Zahlungsverhalten und Bonität führen zu finanzielle Not; Betriebsgeheimniss und/oder vertrauliche Mitschriften werden Konkurrenz bzw. Öffentlichkeit bekannt und gefährden Betrieb; Identitätsdiebstahl; … langfristige Beschwerden, Tod, …

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Eintrittswahrscheinlichkeit:

EWK	Wahrscheinlichkeit	Beispiele
Vernachlässigbar	0-24% Wahrscheinlichkeit	zB Diebstahl von Unterlagen aus einem Safe
Möglich	25-69% Wahrscheinlichkeit	Zb gezielter und koordinierter Angriff durch einen Hacker, Verlust des Hardware bzw pb Daten durch Diebstahl oder durch fahrlässiges Handeln
Sehr wahrscheinlich	70-99% Wahrscheinlichkeit	zB Eindringung eines Schädigungs-Mails,
Garantiert	100% Wahrscheinlichkeit garantiert	zB Ausfall durch einen Festplattenausfall, Datenverluste durch technische Fehler

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

8.3 Maßnahmen

Siehe TOMs, insbesondere:

8.3.1 Vertraulichkeit

i. **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit Schlüssel
i. **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter, automatische Sperrmechanismen, Zwei Faktor – Authentifizierung; Verschlüsselung von Data in Rest und Motion
i. **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen, Protokollierung von Zugriffen

8.3.2 Integrität

i. **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement

8.3.3 Verfügbarkeit

i. **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum,
ii. Rasche **Wiederherstellbarkeit**: Backup

8.4 Risikoanalyse mit Maßnahmen

Schwere					
Existenzgefährdend					
Wesentlich					
Begrenzt		**1, 2**			
Vernachlässigbar	**5**	**3, 4,**			
	Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert	**EWK**

8.5 Folgen der Maßnahmen betreffs Risiko

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
	• Datenschutzbehörde informieren	
• Betroffene sind nicht zu informieren • Keine Folgenabschätzung notwendig		

Aufgrund der gesetzten TOMs muss bei einem DataBreach der betroffene Kunde nicht informiert werden, nichts destotrotz wird die Behörde bei DataBreach mit Risiko für pb Daten der Kategorie 1 + 2 informiert.

Referenzen: Art 22 + 35 DSGVO, Erwägungsgründe: 76, 84 und 89 – 93, Working Paper 240 der Art 29 Gruppe

9 Mein angemessenes Datenschutzniveau

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
	• Mit Datenschutzbehörde **kommunizieren**	
• Betroffene sind nicht zu informieren		

- Die pb Daten der Kategorie 1 + 2 habe ich „Risiko“ zugeordnet, da bei einer **möglichen** Datenschutzverletzung die Folgen **begrenzt** sind und so der betroffene Kunde nicht informiert werden muss, nichts des-

totrotz wird die Behörde über diesen Fällen informiert.

- Die Idee dahinter ist, dass die Datenschutzbehörde so von neuen Bedrohungsszenarien erfährt und ich mich mit ihr austauschen kann - und vielleicht Tipps bekomme.

- Meine Berufsvertretung, die WKO-Wien, sollte anonymisiert ebenso von solchen neuen Angriffen oder Datenschutzverletzungen erfahren, um mir geeignete Gegenmaßnahmen vorschlagen zu können!

- Als Verantwortlicher ist mir so auch bewusster, dass einmal gesetzte TOMS nicht für alle Zeiten alle möglichen und vor allem neuartige Datenschutzverletzungen auffangen können und ich bleibe so acht und wachsam.

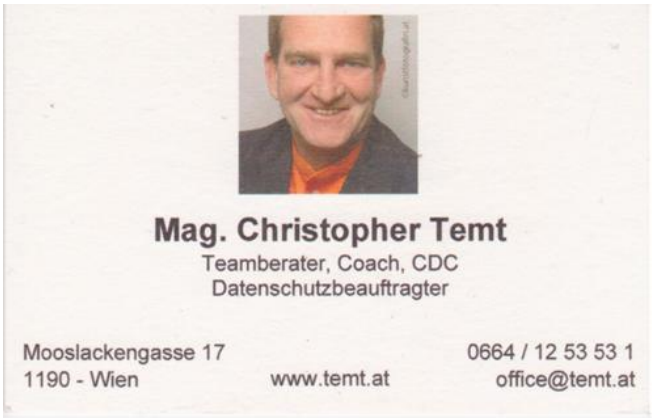
9.1 Visitenkarten und die DSGVO

9.1.1 Entgegennahme

Wenn mir Visitenkarten übergeben werden, so trage ich auf der Rückseite Datum und Ort ein und ob der Übergeber einen Newletter bzw Informationen zur Geschäftsanbahnung will. Noch besser wäre, wenn der Übergeber es selber auf die Rückseite schreibt und ich so zB bei Informationen auch ein berechtigtes Interesse geltend machen kann.

Die Daten/Visitenkarten werden nach Ablauf des dritten Jahres nach dem letzten Kontakt-(Versuch) gelöscht/vernichtet.

9.1.2 Übergabe



Vorderseite

Rückseite

So sind alle Interessierte gemäß DSGVO „auf der sicheren Seite“ und können entweder

- meine Kontaktdaten verarbeiten,

- bei **X** Newsletter - mir einen zusenden (jederzeitige Kündigung bleibt aufrecht) und/oder

- bei **X** Informationen - ihr berechtigtes Interesse zur Geschäftsanbahnung (Z1 lit f) geltend machen.

9.2 Zusammenfassung

Ich sehe das hier dokumentierte Datenschutzniveau mit den gesetzten TOMs für mich als Kleinstunternehmen (siehe Allgemeiner Teil) auch aufgrund meiner finanziellen, technischen und organisatorischen Beschränkungen als **angemessen und ausreichend** an.

Ich kann so gegenüber meinen Kunden mit gutem Gewissen sagen:

> *Liebe Kundin, lieber Kunden!*
>
> *Vertrauen zwischen mir und Ihnen ist die Grundlage und Voraussetzung für meine Beratung, daher sind auch alle Ihre persönlichen und beruflichen Daten bei mir in guten Händen.*
>
> *Ich sichern Ihnen zu, dass ich sorgsam und streng vertraulich damit umgehe und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen bin.*
>
> *Darauf können Sie vertrauen.*
>
> *Christopher Temt*

10 Anhang

10.1 Muster Datenschutzverletzung (WKO)

Datenschutzverletzung

Art 33 EU-Datenschutzgrund-Verordnung (DSGVO) -
Meldung an die Aufsichtsbehörde:
Österreichische Datenschutzbehörde,
Hohenstaufengasse 3, 1010 Wien
E-Mail: dsb@dsb.gv.at

1. Name und Kontaktdaten des **Verantwortlichen[2]:**

   a. Name und Anschrift:

   b. E-Mail-Adresse, Tel.Nr.:

2. Name und Kontaktdaten des **externen/internen Datenschutzmanagers/-beauftragten:**

   a. Name und Anschrift:

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

datenschutz@.....

2

3. Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

soweit möglich Kategorien und ungefähre Zahl der **betroffenen Personen**:

a. soweit möglich betroffene Kategorien und ungefähre Zahl der **personenbezogenen Datensätze**:

4. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

5. Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

a. ggf **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

6. **Datum und Uhrzeit** des Vorfalls:

☐ **Begründung**, falls die Meldung länger als 72h nach dem Vorfall erfolgte:

Wien, am …….

…….
Unterschrift

10.2 Mustervertrag Auftragsverarbeitung (WKO)

VEREINBARUNG

ÜBER EINE

AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

Der Verantwortliche:	Der Auftragsverarbeiter:
[*NN*]	**[*NN*]**
[*Anschrift*]	[*Anschrift*]
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

10.2.1 Gegenstand der Vereinbarung

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben: [*möglichst detaillierte Beschreibung der Aufgaben des Auftragnehmers, einschließlich Art und Zweck der vorgesehenen Verarbeitung].* {Falls es einen weitergehenden Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, udgl gibt} Diese Vereinbarung ist als Ergänzung zu [*Vertrag, etc samt Datum ergänzen*] zu verstehen.

(2) Folgende Datenkategorien werden verarbeitet: [*Datenkategorien aufzählen, zB Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, usw*].

(3) Folgende Kategorien betroffener Personen werden unterliegen der Verarbeitung: [*Betroffenenkategorien ergänzen, zB Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, usw.*]

10.2.2 Dauer der Vereinbarung

☐ {Einmalige Durchführung} Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.

☐ {Befristete Laufzeit} Die Vereinbarung ist befristet abgeschlossen und endet mit [*Fristende eintragen*]

☐ {Unbefristete Laufzeit} Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von [*Kündigungsfrist eintragen, zB ein Monat*] zum [*Kündigungstermin eintragen, zB Kalenderviertaljahr*] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

10.2.3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.
(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

10.2.4 Ort der Durchführung der Datenverarbeitung[3]

☐ {Ausschließliche Durchführung innerhalb der EU/des EWR} Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

☐ {Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR} Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar in [*Staaten aufzählen*]. Das angemessene Datenschutzniveau ergibt sich aus[4]

- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- einer Ausnahme für den bestimmten Fall nach Art 49 Z 1 DSGVO.
- verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Z 2 lit b DSGVO.
- Standarddatenschutzklauseln nach Art 46 Z 2 lit c und d DSGVO.
- genehmigten Verhaltensregeln nach Art 46 Z 2 lit e iVm Art 40 DSGVO.
- einen genehmigten Zertifizierungsmechanismus nach Art 46 Z 2 lit f iVm Art 42 DSGVO.
- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Z 3 lit a DSGVO.
- einer Ausnahme für den Einzelfall nach Art 49 Z 1 Unterabsatz 2 DSGVO.

10.2.5 Sub-Auftragsverarbeiter

☐ Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

☐ Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen: [*Firmenname und Sitz ergänzen, Art der Tätigkeiten]*.

3

4 siehe Merkblatt Internationaler Datenverkehr nach der EU-DSGVO.

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Z 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

☐ Der Auftragnehmer kann Sub-Auftragsverarbeiter [*Tätigkeiten*] hinzuziehen.

Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Z 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

[*Ort*], am [*Datum*]

Für den Auftraggeber:

.....

[*Name samt Funktion*]

[*Ort*], am [*Datum*]

Für den Auftragnehmer:

.....

[*Name samt Funktion*]

10.3 Muster -Technische und organisatorische Maßnahmen TOMS

10.3.1 Handy

Auf jeden Fall kein WhatsApp, sondern DGSVO-konform wie zB: https://www.signal.org/

Handy mit PIN, Passwort oder Biometrie geschützt

- Öffentliche WLAN werden nicht genutzt
- keine automatische Verbindung mit WLANs

alte Handys, USB-Sticks immer vollständig löschen

- Möglichkeit Daten „fern zu löschen“
- Security App

Bluetooth-Funktion nur beim Autofahren

USB-Stick:

- Daten verschlüsselt + Passwort

10.3.2 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Alarmanlage	Absicherung von Gebäudeschächten
Automatisches Zugangskontrollsystem	Chipkarten-/Transponder-Schließsystem
Schließsystem mit Codesperre	Manuelles Schließsystem
Biometrische Zugangssperren	Videoüberwachung der Zugänge
Lichtschranken / Bewegungsmelder	Sicherheitsschlösser
Schlüsselregelung (Schlüsselausgabe etc.)	Personenkontrolle beim Pförtner / Empfang
Protokollierung der Besucher	Sorgfältige Auswahl von Reinigungspersonal
Sorgfältige Auswahl von Wachpersonal	Tragepflicht von Berechtigungsausweisen
Verschlossene Türen bei Abwesenheit	Fenstersicherung (Erdgeschoss)

10.3.3 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Zuordnung von Benutzerrechten	Erstellen von Benutzerprofilen
Passwortvergabe	Authentifikation mit biometrischen Verfahren
Authentifikation mit Benutzername / Passwort	Zuordnung von Benutzerprofilen zu IT-Systemen
Gehäuseverriegelungen	Einsatz von VPN-Technologie
Sperren von externen Schnittstellen (USB etc.)	Sicherheitsschlösser
Schlüsselregelung (Schlüsselausgabe etc.)	Personenkontrolle beim Pförtner / Empfang
Protokollierung der Besucher	Sorgfältige Auswahl von Reinigungspersonal
Sorgfältige Auswahl von Wachpersonal	Tragepflicht von Berechtigungsausweisen
Einsatz von Intrustion-Detection-Systemen	Verschlüsselung von mobilen Datenträgern
Verschlüsselung von Smartphone-Inhalten	Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
Einsatz von Anti-Viren-Software	Verschlüsselung von Datenträgern in Laptops / Notebooks/USB
Einsatz einer Hardware-Firewall	Einsatz einer Software-Firewall

10.3.4 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern (Data-Safe)
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

10.3.5 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- E-Mail-Verschlüsselung
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen
- Verschlüsselung der übertragenen Daten

10.3.6 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

10.3.7 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) siehe Anhang

Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Auftragnehmer hat Datenschutzbeauftragten bestellt

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Vertragsstrafen bei Verstößen

10.3.8 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Unterbrechungsfreie Stromversorgung (USV)

Klimaanlage in Serverräumen

Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

Schutzsteckdosenleisten in Serverräumen

Feuer- und Rauchmeldeanlagen

Feuerlöschgeräte in Serverräumen

Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

Erstellen eines Backup- & Recoverykonzepts

Testen von Datenwiederherstellung

Erstellen eines Notfallplans

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Serverräume nicht unter sanitären Anlagen

In Hochwassergebieten: Serverräume über der Wassergrenze

10.3.9 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Logische Mandantentrennung (softwareseitig)

Erstellung eines Berechtigungskonzepts

Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

Versehen der Datensätze mit Zweckattributen/Datenfeldern

Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

Festlegung von Datenbankrechten

Trennung von Produktiv- und Testsystem

Datum

Verantwortlicher für die Erstellung (in Druckbuchstaben)

Unterschrift des Verantwortlichen

Quelle: https://www.datenschutz-guru.de/files/**Ausfuellhilfe_TOM_9_BDSG_V2**.docx

10.4 Muster: Verpflichtungserklärung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen (WKO)

Diese Verpflichtungserklärung betrifft:

Familienname:

_____

Vornamen:

_____

In Ausübung Ihrer beruflichen Tätigkeit erhalten Sie voraussichtlich Kenntnis über personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse. Alle diese Informationen sind absolut vertraulich zu behandeln und unterliegen den Bestimmungen des österreichischen und europäischen Datenschutzrechts sowie des Wettbewerbsrechts.

Mit Ihrer Unterschrift verpflichten Sie sich,

1. das Datenschutzrecht zu wahren, insbesondere § 6 DSG, einschließlich entsprechender betrieblicher Anordnungen;
2. Geschäfts- und Betriebsgeheimnisse zu wahren (§ 11 UWG);
3. bei einem Verstoß gegen das Datengeheimnis oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen, Schadenersatz zu leisten, und zwar ohne Rücksicht auf den tatsächlich eingetretenen Schaden durch Vereinbarung einer Konventionalstrafe pauschaliert, und zwar im Ausmaß von *[Anzahl eintragen]* Bruttomonatsentgelten.

Die zitierten Bestimmungen sind im Anhang zu dieser Erklärung abgedruckt.

Ihnen ist bekannt, dass

- die personenbezogenen Daten natürlicher wie juristischer Personen einem besonderen Schutz unterliegen und die Verwendung solcher Daten nur unter besonderen Voraussetzungen zulässig ist;
- personenbezogene Daten, die Ihnen auf Grund Ihrer beruflichen Beschäftigung anvertraut oder zugänglich gemacht wurden, nur auf Grund einer ausdrücklichen Anordnung des jeweiligen Vorgesetzten übermittelt werden dürfen;
- es untersagt ist, Daten an unbefugte Empfänger innerhalb und außerhalb des Unternehmens zu übermitteln oder sonst zugänglich zu machen;
- es untersagt ist, sich unbefugt Daten zu beschaffen oder zu verarbeiten;
- es untersagt ist, personenbezogene Daten zu einem anderen als dem zum rechtmäßigen Aufgabenvollzug gehörenden Zweck zu verwenden;
- anvertraute Benutzerkennwörter, Passwörter und sonstige Zugangsberechtigungen sorgfältig verwahrt und geheim zu halten sind;
- allfällige weiterreichende andere Bestimmungen über die Geheimhaltungspflichten ebenfalls zu beachten sind;
- diese Verpflichtung auch nach Beendigung Ihrer Tätigkeit fortbesteht;
- Verstöße gegen die hier genannten Verschwiegenheitsverpflichtungen nicht nur arbeitsrechtliche Folgen, sondern auch (verwaltungs-)strafrechtliche Folgen haben und schadenersatzpflichtig machen.

Hiermit erkläre ich, am [*Datum der Belehrung*] von meinem Arbeitgeber über das Datengeheimnis nach § 6 DSG und die Verschwiegenheitsverpflichtungen nach § 11 UWG belehrt worden zu sein.

Ort, Datum	Unterschrift des Verpflichteten

10.4.1 Anhang zum Datengeheimnis

Datengeheimnis nach § 6 DSG

(1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).
(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.
(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.
(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.
(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

Verletzung von Geschäfts- oder Betriebsgeheimnissen und Missbrauch anvertrauter Vorlagen nach § 11 UWG

(1) Wer als Bediensteter eines Unternehmens Geschäfts- oder Betriebsgeheimnisse, die ihm vermöge des Dienstverhältnisses anvertraut oder sonst zugänglich geworden sind, während der Geltungsdauer des Dienstverhältnisses unbefugt anderen zu Zwecken des Wettbewerbes mitteilt, ist vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen. (BGBl. Nr. 120/1980, Art. I Z 6)
(2) Die gleiche Strafe trifft den, der Geschäfts- oder Betriebsgeheimnisse, deren Kenntnis er durch eine der im Abs. 1 bezeichneten Mitteilungen oder durch eine gegen das Gesetz oder die guten Sitten verstoßende eigene Handlung erlangt hat, zu Zwecken des Wettbewerbes unbefugt verwertet oder an andere mitteilt.
(3) Die Verfolgung findet nur auf Verlangen des Verletzten statt.

10.5 (Verarbeitungsverzeichniss – Personalwesen)

10.5.1 Zuständigkeiten

Verantwortliche	Datenschutz Ansprechperson
Mag. Christopher Temt Mooslackengasse 17, 1190-Wien Email: office@temt.at Tel.: 0664 / 12 53 53 1	Mooslackengasse 17, 1190-Wien Email: datenschutz@temt.at Tel.:

10.5.2 Zweck

Verarbeitung und Übermittlung von 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 z. B. Korrespondenz) in diesen Angelegenheiten

Verwendung und Evidenthaltung von personenbezogenen Daten von Bewerbern, soweit diese Daten vom Betroffenen angegeben wurden.

10.5.3 Rechtsgrundlagen

- Art 6 Z 1 lit a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen), f (berechtigte Interessen des Verantwortlichen) DSGVO
- § 8 Arbeitsinspektionsgesetz
- Betriebsrat gemäß § 89 Z 4 ArbVG, Sicherheitsvertrauensperson nach § 10 ArbeitnehmerInnenschutzgesetz (ASchG), BGBl. Nr. 450/1994 idgF., Jugendvertrauensperson gemäß § 125ff ArbVG und Behinderten- vertrauensperson gemäß § 22a Behinderteneinstellungsgesetz
- Gewerbebehörde, Zuständigkeiten nach ASchG,
- § 16 Behinderteneinstellungsgesetz
- § 19 Berufsausbildungsgesetz
- § 73 Abs.3 ArbVG
- § 11 Abs.2 Z5 und § 13 BMVG
- BGBl. Nr. 142/1969 idgF
- „SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse“ (siehe http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495

10.5.4 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen und Verträge zum Personalwesen sowie Verträge mit Auftragsverarbeitern sind im Archiv abgelegt. Bewerbungsunterlagen werden nach Abschluss des Bewerbungsverfahren zurück gesendet

10.5.5 Kategorien der betroffenen Personen

Lfd.Nr.	Beschreibung der Kategorien betroffener Personen
1	Arbeitnehmer, arbeitnehmerähnliche Personengruppen, Leiharbeitnehmer, freie Dienstnehmer, Lehrlinge, Volontäre und Ferialpraktikanten (auch ehemalige Beschäftigte):
2	Bewerber

10.5.6 Kategorien der verarbeiteten Daten

- Vorlage ist dieStandardanwendung „SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse“

- Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden, müssen auf Grund **der konkreten Prüfung im Einzelfall gemäß Datenminimierung nach Art 5 Z 1 DSGVO mit der jeweiligen Nummer angegeben werden**.

Kategorien der betroffenen Personengruppe	Lfd Nr	Datenkategorie	Empfängerkategorien	Datenkategorien iSd Art 9 und Art 10 DSGVO[5]
1. Arbeitnehmer, arbeitnehmerähnliche Personengruppen, Leiharbeitnehmer, freie Dienstnehmer, Lehrlinge, Volontäre und Ferialpraktikanten (auch ehemalige Beschäftigte):	01	Ordnungsnummer		Nein
	02	Name	1 – 25	Nein
	03	Frühere Namen (Namensteile)	1 – 24	Nein
	04	Geburtsdatum	1 – 13, 15 – 23	Nein
	05	Geburtsort	1 – 13, 15 – 22	Nein
	06	Geschlecht	1 – 23	Nein
	07	Personenstand	1, 2, 4, 5, 9 – 13, 17 – 19, 21, 22	Nein
	08	Kinder und sonstige Familienangehörige, im Zusammenhang mit Leistungen, die in Verbindung mit dem Arbeitsverhältnis des Betroffenen erbracht werden (insbesondere Name, Geburtsdatum, Sozialversicherungsnummer)	2, 4, 5, 9 – 13, 17 – 19, 21, 22	Nein
	09	Gesetzlicher Vertreter	1, 2, 4, 5, 8 – 19, 21, 22	Nein
	10	Staatsbürgerschaft	2 – 12, 16, 21, 22	Nein
	11	Bankverbindung	1, 2, 4, 5, 9 – 11, 14, 21, 22	Nein
	12	Organisatorische Zuordnung im Betrieb einschließlich Beginn und Ende	2 – 7, 9 – 11, 15, 16, 18, 21, 22, 25	Nein
	13	Betriebl. Telefon, Faxnummer Email und andere zur Adressierung im Betrieb erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	1 – 23, 25	Nein
	14	Wohnadresse	1 – 17, 21 – 23	Nein
	15	Private Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	1 – 17, 21 – 23	Nein
	16	Kostenstelle(n)	5, 19, 21, 22	Nein
	17	Sozialversicherungsnummer	2, 4, 5, 9 – 12, 18, 19, 21 – 24	Nein
	18	Sozialversicherungsträger	2, 4, 5, 9 – 12, 19, 21 – 23	Nein
	19	Daten zur Krankenscheinverwaltung	2, 18, 21 – 23	Nein
	20	• Dienstnehmer-Sozialversicherungsdaten Versichertenmeldung: • Beitragsgruppe • An-/Abmeldedatum und Änderungsdatum Zugehörigkeit (Arbeiter, Angestellter, ...) Geringfügigkeit • Verwandtschaftsverhältnis zum Dienstgeber Beteiligung am Unternehmen des Dienstgebers	2, 4, 5, 10, 19, 21, 22	Nein

5

		• Lehrzeit (1. Lehrjahr von – bis, Lehrzeitende) • Nacht- Schwerarbeit (Anfang, Ende • Art des Bezuges (Monatslohn, Zeitlohn) ● Beitragsgrundlagenmeldung: • Beitragszeitraum (von-bis-Monat, Jahr, Verrechnungsart) • Allgemeine Beitragsgrundlage Beitragsgrundlage Sonderzahlung • Anzahl der Tage mit Teilentgelt Beitragspflichtiges Teilentgelt • Zugehörigkeit (Arbeiter, Angestellter, ...) Anspruch auf Sonderzahlung (ja, nein) ● Erstattungsantrag Krankenentgelt gemäß § 8 EFZG • Anspruch auf Pauschalbetrag • Kennzeichen für Krankheit/Unglücksfall, Arbeitsunfall/Berufskrankheit • Anspruch in Wochen • Vorbezugstage (Summe, Angabe in Arbeitstagen oder Kalendertagen) Erstattungszeitraum (Beginn, Ende) Fortgezahltes Bruttoentgelt • Art der Beschäftigung (Arbeiter, Lehrling, Heimarbeiter, Sonstige) • Tagesturnus (Anzahl der Tage) • Berechnung der Ansprüche nach Kalenderjahr/Arbeitsjahr • Ende des Entgeltanspruches • Vordienstzeiten (von, bis) • Arbeitsfreie Tage ● Arbeits- und Entgeltsbestätigung für Krankengeld • Grund der Arbeitseinstellung • Beschäftigungsverhältnis (gelöst, nicht gelöst) • Bruttoentgelt im letzten Beitragszeitraum ohne Sonderzahlung • Bezug (von, bis, Betrag) • Betragssumme • Sonderzahlungsanspruch (ja, nein) • Sachbezug (Anzahl der Tage, Text) • Entgelt wird bezahlt bis • EFZ-Anspruch in Wochen • Berechnung der Ansprüche nach Arbeits-Kalenderjahr, Arbeits- Kalendertage • Teilentgelt – Prozentanteil des Gesamtentgeltes (Prozente, von, bis) • Provision während der Arbeitsunfähigkeit (ja,nein) • Anrechnung Vorerkrankungen (von, bis) ● Arbeits- und Entgeltsbestätigung für Wochengeld • Grund der Arbeitseinstellung Beschäftigungsverhältnis (gelöst, nicht gelöst) Urlaub vor Eintritt der Mutterschaft (von, bis) Arbeitsverdienst der letzten drei Kalendermonate (ohne SZ, minus gesetzliche Abzüge) Arbeitsverdienstzeitraum (von, bis) • Unterbrechung des Bezuges während der letzten drei Monate (von, bis) • Ausmaß der Sonderzahlung (Anzahl Monate, Anzahl Wochen) • Anspruch auf Fortbezug des Entgeltes (gesetzlich, vertrag-		

		lich, kein Anspruch) • Anspruch auf das halbe Entgelt (bis) • Anspruch auf mehr als das halbe Entgelt (bis ● Mitarbeitervorsorge gemäß BMVG • MVK-Leitzahl • MV-Beitragsgrundlage (inklusive Sonderzahlungen) • Beitragshöhe gemäß BMVG (Gruppensumme • Beginn und Ende der MV-Beitragszahlung (Stichtag) • Eingezahlter Betrag an MV • MV-Beitragszeiten (Beitragsmonat von – bis • Vordienstzeiten (bei Übertritt ins neue Abfertigungsmodell) • Übertragungsbetrag an die MVK und Zahlungsmodus • Zuordnung zu Dienstgeberkontonummer • Abmeldegründe (zB Unterbrechung der Beitragszahlung durch Karenzurlaub)		
	21	Eintrittsdatum	2 – 8, 10, 11, 13, 16, 19, 21, 22	Nein
	22	Vordienstzeiten	10, 13, 19, 21, 22	Nein
	23	Austrittsdatum, Kündigungsfrist	2 – 8, 10, 11, 13, 16, 19, 21, 22	Nein
	24	Art der Beendigung des Dienstverhältnisses	2, 4, 5, 9 – 11, 21, 22	Nein
	25	Gesetzliche Beschäftigungsvoraussetzungen	4 – 8, 11, 21, 22	Nein
	26	Daten der Beschäftigungsbewilligung	4 – 7, 9, 21, 22	Nein
	27	Bezeichnung der Tätigkeit	2, 4 – 7, 9, 18, 21, 22	Nein
	28	Gruppenzugehörigkeit (Arbeiter/Angestellte)	2 – 7, 9, 15, 16, 21, 22	Nein
	29	Kammerzugehörigkeit	2, 5, 16, 21, 22	Nein
	30	Sicherheitsstufe / Zugangs- (Zugriffs-)rechte	4, 5, 21, 22	Nein
	31	Lichtbild des Betroffenen (für Ausweiskarten)	4, 5, 21, 22	Nein
	32	Gültigkeitsdauer der Ausweiskarte	4, 5, 21, 22	Nein
	33	Arbeitszeiterfassung	4, 5, 21, 22	Nein
	34	Sonstige Daten zur Arbeitszeit (insbesondere Geringfügigkeit, Arbeitsstunden, Überstunden, Gleitzeit, Nacht- und Teilzeitarbeit)	2, 4 – 7, 9, 10, 12, 21, 22	Nein
	35	Daten zur Urlaubsverwaltung	3 – 5, 9, 10, 21, 22	Nein
	36	Religionsbekenntnis (zur Abwesenheitsverwaltung)	4, 5, 21, 22	nach Angabe des Betroffenen
	37	Krankenstand, einschließlich Arbeitsunfall und Berufskrankheit (Beginn, Ende und Dauer)	2 – 5, 10, 18, 19, 21, 22	Nein
	38	Zeitpunkt eines Arbeitsunfalls	2 – 5, 10, 18, 19, 21, 22	Nein
	39	Kuraufenthalte	2 – 5, 10, 18, 19, 21, 22	Nein
	40	Mutterschutz (Beginn und Ende)	2 – 5, 9, 10, 18, 19, 21, 22	Nein

	41	Karenzurlaub gemäß MSchG und EKUG (Beginn und Ende)	2 – 5, 9, 10, 15, 18, 19, 21, 22	Nein
	42	Präsenzdienst, Ausbildungsdienst oder Zivildienst (Beginn und Ende)	2 – 5, 9, 10, 15, 19, 21, 22	Nein
	43	Art und Dauer der sonstigen Abwesenheit wegen Dienstverhinderung oder Dienstfreistellung (einschließlich vereinbarte Karenzierung)	2 – 5, 9, 10, 19, 21, 22	Nein
	44	Daten zur Entgeltfortzahlung	2 – 5, 10, 19, 21, 22	Nein
	45	Beschäftigungsrelevante Daten gemäß Arbeit- nehmerInnenschutzgesetz, BGBl. Nr. 450/1994 idgF., Bazillenausscheidergesetz, BGBl. Nr. 153/1945 idgF., Tuberkulosegesetz, BGBl. Nr. 127/1968 idgF. und ähnlichen Rechtsvorschriften	4 – 7, 18, 21, 22	Nein
	46	Grad der Behinderung gemäß Behinderteneinstellungsgesetz (nach Bekanntgabe des Betroffenen)	2 – 5, 9, 11, 15, 21, 22	Nein
				Nein
	47	Gesetzliche, kollektivvertragliche, betriebsvereinbarungsmäßige und einzelvertragliche Grundlagen der Entgeltberechnung (Einstufung)	2, 4 – 5, 8, 9, 10, 19, 21, 22	Nein
	48	Brutto- und Nettoentgelt (Daten des Gehaltszettels)	1, 2, 4, 5, 9, 10, 12, 14, 19, 21, 22	Nein
	49	Daten der Entgeltsfortzahlung	---	Nein
	50	Abzüge vom Nettoentgelt auf Grund Gesetzes oder betrieblicher Vereinbarungen	13 – 14, 17, 19, 21, 22	Nein
	51	Sachbezüge	1, 2, 4, 5, 10, 12, 21, 22	Nein
	52	Aufwandsentschädigungen (wie Reisegebühren)	1, 2, 4, 5, 10, 12, 14, 19, 21, 22	Nein
	53	Sozialleistungen im Zusammenhang mit dem Arbeitsverhältnis	2, 4, 5, 12, 14, 21, 22	Nein
	54	Daten nach Bezügebegrenzungsgesetz, BGBl. I Nr. 64/1997 idgF.	20, 21, 22	Nein
	55	Höhe des Gewerkschaftsbeitrages und Bezeichnung und Adresse des Empfängers	14, 15, 21, 22	nach Bekanntgabe des Betroffenen
	56	Versicherungsprämien als Leistung des Arbeitgebers	4, 5, 13, 14, 21, 22	Nein
	57	Verwaltung von Vorschüssen und Darlehen	1, 14, 21, 22	Nein
	58	Lohnpfändungsdaten	1, 4, 5, 21, 22	Nein
	59	Daten des Lohnzettels (L – 16 Formular)	10, 12, 21, 22	Nein
	60	Alleinverdiener- oder Alleinerzieher-Absetzbetrag (ja/nein)	2, 12, 21, 22	Nein
	61	Wohnsitzfinanzamt	21, 22	Nein
	62	Daten zur Pensionskasse (insbesondere Ein- und Austritt, Beitragsdaten und Versicherungszeiten in der gesetzlichen Sozialversicherung im Zeitraum der Beschäftigung)	5, 12, 14, 19, 21, 22	Nein
	63	Daten zur Verwendung von Dienstfahrzeugen (insbesondere Führerschein, Abrechnungen, Schadensfälle, Versicherungen)	4, 5, 13, 21, 22	Nein
	64	Besondere Qualifikationen (z. B. Gewerbeschein, besondere Ausbildung)	4, 5, 7, 21, 22	Nein
	65	Nebenbeschäftigungen	20, 21, 22	Nein

	66	Daten nach dem Berufsausbildungsgesetz, BGBl. Nr. 142/1969 idgF., und einschlägigen kollektivvertraglichen Regelungen bei Lehrlingen, insbesondere Lehrvertragsdaten und sonstige Daten aus dem Ausbildungsverhältnis und Berufsschulbesuch	4, 5, 8, 9, 16, 21, 22	Nein
	66 a	Schwerarbeitszeiten	2	Nein
2. Bewerber	67	Ordnungszahl(en)	21, 22	
	68	Name	21, 22	
	69	Geburtsdatum	21, 22	wenn vom Betroffenen angegeben
	70	Staatsbürgerschaft	21, 22	wenn vom Betroffenen angegeben
	71	Geschlecht	21, 22	wenn vom Betroffenen angegeben
	72	Anschrift	21, 22	wenn vom Betroffenen angegeben
	73	Telefonnummer	21, 22	wenn vom Betroffenen angegeben
	74	E-Mail-Adresse	21, 22	wenn vom Betroffenen angegeben
	75	Lichtbild)	21, 22	wenn vom Betroffenen angegeben
	76	Ausbildungsdaten	21, 22	wenn vom Betroffenen angegeben
	77	Berufserfahrung und Lebenslauf	21, 22	wenn vom Betroffenen angegeben
	78	Angestrebte Beschäftigung	21, 22	wenn vom Betroffenen angegeben
	79	Beginn der angestrebten Beschäftigung	21, 22	wenn vom Betroffenen angegeben
	80	Sprachkenntnisse	21, 22	wenn vom Betroffenen angegeben
	81	Spezielle Berufserfordernisse	21, 22	
	82	div. Testergebnisse	21, 22	

10.5.7 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungs-fristen
? - ?	Fristen mit **weniger als 7** Jahren für Personalwesen, siehe https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-speicher-und-aufbewahrungsfristen.html
? - ?	Bis zur Beendigung der Beziehung mit dem Betroffenen und darüber hinaus solange als gesetzliche Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 bestehen somit auf jeden Fall **7 Jahre** oder solange Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können
67-82	Bewerbungen werden nur auf dem Postweg akzeptiert und bei nicht Anstellung an den Bewerber vollständig wieder zurück gesendet. Für alle anderen Bewerber-Daten gilt eine **6-Monatsfrist** gemäß Gleichbehand-lungsgesetz …..
Dienstzeugnisses	Anspruch auf Ausstellung eines Dienstzeugnisses nach § 1163 iVm § 1478 ABGB: **30 Jahre**

10.5.8 Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern

10.5.8.1 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

Lf. Nr	Empfängerkategorien	Drittstaat (Angabe des Drittstaats, d.h. außerhalb der EU)	Internationale Organisation
1	Gläubiger des Betroffenen sowie sonstige an der allenfalls damit verbun-denen Rechtsverfolgung Beteiligte, auch bei freiwilligen Gehaltsabtretun-gen für fällige Forderungen;	Nein	Nein
2	Sozialversicherungsträger (einschließlich Betriebskrankenkassen);	Nein	Nein
3	Wahlvorstand für Betriebsratswahlen;	Nein	Nein
4	Arbeitsinspektorat, Verkehrs-Arbeitsinspektion und Land- und Forstwirt-schaftsinspektion, insbesondere gemäß § 8 Arbeitsinspektionsgesetz;	Nein	Nein
5	Organe der betrieblichen Interessensvertretung (insbesondere Betriebsrat gemäß § 89 Z 4 ArbVG, Sicherheitsvertrauensperson nach § 10 Arbeit-nehmerInnenschutzgesetz (ASchG), BGBl. Nr. 450/1994 idgF., Jugendver-trauensperson gemäß § 125ff ArbVG und Behindertenvertrauensperson gemäß § 22a Behinderteneinstellungsgesetz);	Nein	Nein
6	Gemeindebehörden in verwaltungspolizeilichen Agenden;	Nein	Nein
7	Bezirksverwaltungsbehörde in verwaltungspolizeilichen Agenden (Gewer-bebehörde, Zuständigkeiten nach ASchG, usw.);	Nein	Nein
8	Lehrlingsstelle gemäß § 19 Berufsausbildungsgesetz und Berufsschulen;	Nein	Nein
9	Arbeitsmarktservice;	Nein	Nein
10	Bauarbeiter- Urlaubs- und -Abfertigungskasse;	Nein	Nein
11	Bundesamt für Soziales und Behindertenwesen (Bundessozialamt) z. B. gemäß § 16 Behinderteneinstellungsgesetz;	Nein	Nein
12	Finanzamt;	Nein	Nein
13	Versicherungsanstalten im Rahmen einer bestehenden Gruppen- oder Einzelversicherung;	Nein	Nein

14	mit der Auszahlung an den Betroffenen oder an Dritte befasste Banken;	Nein	Nein
15	vom Dienstnehmer angegebene Gewerkschaft, mit Zustimmung des Betroffenen;	Nein	Nein
16	gesetzliche Interessensvertretungen;	Nein	Nein
17	Betriebsratsfonds gemäß § 73 Abs. 3 ArbVG;	Nein	Nein
18	Betriebsärzte;	Nein	Nein
19	Pensionskassen;	Nein	Nein
20	Rechnungshof;	Nein	Nein
21	Rechtsvertreter; Wirtschaftstreuhand, externe Buchhalter	Nein	Nein
22	Gerichte;	Nein	Nein
23	Mitversicherte;	Nein	Nein
24	Mitarbeitervorsorgekassen (MVK) gemäß § 11 Abs. 2 Z 5 und § 13 BMVG;	Nein	Nein
25	Kunden und Interessenten des Auftraggebers.	Nein	Nein
26	Externer Datenschutzbeauftragter	Nein	Nein

10.5.8.2 Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten

10.5.8.3 Risiko-Analyse fehlt!

Da ich noch keine Mitarbeiter habe, habe ich auch noch keine Risiko-Analyse für das Personalwesen durchgeführt.

Um das Risiko für die Mitarbeiter und die Betroffenen gering zu halten, sollen die Verträge DSGVO-konform sein, von einem Rechtsanwalt erstellt/gegengelesen werden und die TOMs (siehe hier im Anhang) soweit als möglich und vertretbar durchgeführt worden sein.

11 Danksagung

Ausdrücklich möchte ich mich bei der Wirtschaftskammer
für all die professionelle Arbeit betreffs der DSGVO bedanken!

Für alle Unterlagen, Muster, Links und Tipps der WKO und anderer Quellen gilt auch der Disclaimer (keine Haftung, keine Gewähr, ..)

12 DISCLAIMER

Sämtliche zur Verfügung gestellten Inhalte wurden mit der größtmöglichen Sorgfalt erstellt. Der Autor übernimmt jedoch keine Gewähr für die Aktualität, Richtigkeit oder Vollständigkeit der bereitgestellten Informationen (einschließlich des Verweises auf externe Quellen). Die korrekte Datenschutzdokumentation und die TOMs erfordert stets eine **konkrete Prüfung im Einzelfall**, weshalb die Beiziehung eines Datenschutzberaters (z.B. datenschutz@temt.at bzw http://www.dataprivacydoctors.at/) sowie eines Rechtsanwaltes, insbesondere bei der Erstellung oder Überprüfung von Verträgen, dringend empfohlen wird. Die zur Verfügung gestellten Inhalte stellen keine Beratungsleistung welcher Art auch immer dar und können eine Beratung auch nicht ersetzen.

Haftungsansprüche gegen den Autor, welche sich auf Schäden materieller oder ideeller Art, einschließlich entgangenen Gewinn oder sonstige direkte oder indirekte Folgeschäden, beziehen, die durch die Nutzung oder Nichtnutzung der zur Verfügung gestellten Informationen verursacht wurden, sind ausgeschlossen. Der Autor behält es sich ausdrücklich vor, Teile der zur Verfügung gestellten Information oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.