Datenschutz-Konzept-Vorlage
für
Katharina Münz

gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

Katharina Münz
Autorin

15.04.2018

Verantwortlich gemäß DSGVO

Katharina Münz
c/o Autorenservices
König-Konrad-Str. 22
36039 Fulda
Email katharina.munz@outlook.de

1 Inhalt

2 Allgemeine Angaben

2.1 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 DSGVO geforderte Einhaltung der Verordnungskonformität (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).

2.2 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.

* *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)

2.3 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 z. B. 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 (EPU)* keines der obigen Kriterien zutrifft, wird kein DSB bestellt.

2.4 Verantwortliche(r) (Stammdaten)

Der Verantwortliche und für den Datenschutz Zuständige ist:

Katharina Münz
c/o Autorenservices.de
König-Konrad-Str. 22
36039 Fulda
katharina.munz@outlook.de

Referenzen: Art 4 Z 7 DSGVO

2.5 Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze ich folgende Aktivität:

Aktivitäten	Veranstalter	sonstiges
Info- u. Weiterbildungsveranstaltungen	Internet-Recherche	regelmäßig
Homepages bzw. Newsletter	https://www.dataprivacydoctors.at	Newsletter
	https://www.datenschutz-guru.de	Newsletter
	https://www.dataprivacydoctors.at/	Newsletter
	DSGVO-Page der WKO	regelmäßig
	https://www.e-recht24.de/	Newsletter

Referenzen: Art 4, 5-11 DSGVO

3 Datenverarbeitungen/Datenverarbeitungszwecke

3.1 Zwecke und Beschreibung der Datenverarbeitung:

3.1.1 Rechnungswesen und Geschäftsabwicklung:

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

3.1.2 Lesern/Buchkäufern und Bloggern/Rezensenten betreuung und Marketing

Serviceorientierte Information und Betreuung von kategorisierten Lesern/Buchkäufern und Bloggern/Rezensenten, 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, Serienbriefe und Infomaterial.

3.2 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 Listen seitens der Datenschutzbehörde noch nicht vorliegen (Art 35 Z4 + Z5)

Referenzen: Art 35 Z1-3 DSGVO

4 Verfahrensverzeichnis

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

4.1 Rechnungswesen und Geschäftsabwicklung

4.1.1 Verantwortliche(r)

Katharina Münz
c/o Autorenservices.de
König-Konrad-Str. 22
36039 Fulda
katharina.munz@outlook.de

4.1.2 Zweck

Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Lesern/Buchkäufern und Bloggern/Rezensenten und Lieferanten, sowie von an der Geschäftsabwicklung mitwirkenden Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

4.1.3 Kategorien der betroffenen Personen

Lfd. Nr.	Beschreibung der Kategorien betroffener Personen
1	Leser/Buchkäufer sowie Blogger/Rezensente und Lieferanten inkl. Kontaktpersonen bei Lesern/Buchkäufern sowie Bloggern/Rezensenten und Lieferanten
2	An der Geschäftsabwicklung mitwirkende Dritte und Geschäftspartner inkl. deren jeweiligen Kontaktpersonen

4.1.4 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

4.1.5 Verträge, Zustimmungserklärungen oder sonstige Unterlagen

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

** 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 gesonderte Auftragsverarbeitung nach Art 28 DSGVO 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.*

4.1.6 Kategorien der verarbeiteten Daten

- Vorlage ist die Muster-Anwendung der WKO (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 Denkkategorien im Sinne der Art 9 und Art	Banken	Rechtsvertreterim Geschäftsfall	Steuerberater	Gerichte im Anlassfall (i.A.)	Verwaltungsbehörden i.A.	Vertrags-und Geschäftspartner	Versicherungen i.A.	Provider (IT-Dienstleister)	Externer Datenschutzbeauftragter
1. Lesern/Buchkäufern und Bloggern/Rezensenten und Lieferanten inkl. Kontaktpersonen beim Lesern/Buchkäufern und Bloggern/Rezensenten und Lieferanten	1	Kunden-/Lieferanten-Nr. Ordnungsnummer	*Nein*	***wird nicht verwendet/erhoben***								
	2	Name, Firma oder sonstige Geschäftsbezeichnung	*Nein*	X	X	X	X	X	X	X	X	
	3	Anzahl Mitarbeiter	*Nein*	***wird nicht verwendet/erhoben***								
	4	Anschrift bzw. Lieferadresse	*Nein*	X	X	X	X	X	X	X	X	
	5	Homepage	*Nein*		X		X	X				
	6	Kontaktdaten (E-Mail)	*Nein*	X	X	X	X	X	X	X	X	
	7	Firmenbuchdaten	*Nein*	***wird nicht verwendet/erhoben***								
	8	Daten zur Bonität inkl. Mahn- und Klagdaten	*Nein*	***wird nicht verwendet/erhoben***								
	9	Bankverbindungen	*Nein*	X	X	X	X	X	X	X		
	10	Kreditkartennummern und -unternehmen	*Nein*	***wird nicht verwendet/erhoben***								
	11	Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Intrastat-Kenn-, Steuer-Nummer	*Nein*	***wird nicht verwendet/erhoben***								
	12	Namen Kontaktpersonen	*Nein*	X	X	X	X	X	X	X	X	
	13	Kontaktdaten der Kontaktpersonen (E-Mail)	*Nein*	X	X	X	X	X	X	X	X	
	14	Funktion/Rolle der Kontaktperson	*Nein*		X	X	X	X	X	X		
	15	Zuordnung zu einem bestimmten Leser/Buchkäufer sowie Blogger/Rezensent und Lieferanten, Interessentenkategorie (einschließlich regionale Zuordnung, usw.)	*Nein*		X		X	X		X		
	16	Bonus-, Provisionsdaten und dgl.	*Nein*	***wird nicht verwendet/erhoben***								
	17	Auftragserfassung gem. Beraternorm EN16114	*Nein*	***wird nicht verwendet/erhoben***								
	18	Art der Beratung	*Nein*	***wird nicht verwendet/erhoben***								
	19	Vertragstext und Geschäftskorrespondenzen	*Nein*	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-Akquise-Sperre	*Nein*		X		X					

1

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	
	26	Anschrift, Lieferadresse	*Nein*	X	X	X	X	X	X	X	X	
	27	Homepage	*Nein*		X		X	X	X			
	28	Kontaktdaten (E-Mail)	*Nein*	X	X	X	X	X	X	X	X	
	29	Firmenbuchdaten	*Nein*	***wird nicht verwendet/erhoben***								
	30	Daten zur Bonität inkl. Mahn- und Klagdaten	*Nein*	***wird nicht verwendet/erhoben***								
	31	Bankverbindungen	*Nein*	X	X	X	X	X	X	X		
	32	Kreditkartennummern und -unternehmen	*Nein*	***wird nicht verwendet/erhoben***								
	33	Kenn-Nummern für Zwecke amtlicher Statistik wie UID-, Intrastat-Kenn-, Steuer-Nummer	*Nein*	X	X	X	X	X	X	X		
	34	Namen Kontaktpersonen	*Nein*	X	X	X	X	X	X	X	X	
	35	Zuordnung zu einer bestimmten Kategorie (einschließlich regionale Zuordnung, usw.)	*Nein*		X		X	X		X		
	36	Art der Kooperation	*Nein*		X		X					
	37	Vertragstext und Geschäftskorrespondenzen	*Nein*	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-Akquise-Sperre	*Nein*		X		X					

4.1.7 Löschungs- und Aufbewahrungsfristen

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

4.1.8 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
Vertrags- und Geschäftspartner	Nein	Nein
Versicherung im Anlassfall	Nein	Nein
Provider (IT-Dienstleister)	Nein	Nein
Externer Datenschutzbeauftragter	Nein	Nein

4.1.9 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

4.2 Betreuung von Lesern/Buchkäufern sowie Bloggern/Rezensenten und Marketing

4.2.1 Verantwortliche(r)

Katharina Münz
c/o Autorenservices.de
König-Konrad-Str. 22
36039 Fulda
katharina.munz@outlook.de

4.2.2 Zweck

Serviceorientierte Information und Betreuung von kategorisierten Lesern/Buchkäufern und Bloggern/Rezensenten, 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, Serienbriefe und Infomaterial.

4.2.3 Kategorien der betroffenen Personen

Lfd. Nr.	Beschreibung der Kategorien betroffener Personen
1	Leser/Buchkäufer und Blogger/Rezensenten; Lieferanten, an der Geschäftsabwicklung mitwirkende Dritte und Interessenten
2	Kontaktpersonen bei Lesern/Buchkäufern und Bloggern/Rezensenten; beim Lieferanten, beim an der Geschäftsabwicklung mitwirkende Dritt, beim Interessenten

4.2.4 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

4.2.5 Verträge, Zustimmungserklärungen oder sonstige Unterlagen

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

4.2.6 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.

Hier sind die üblichen Datenkategorien eingetragen, die von Euch entsprechend Eurer Software geändert oder ergänzt bzw. gelöscht gehören. Wenn mehrere Euer Felder mit einem Feld hier abgedeckt sind, so verwendet den allgemeineren Begriff hier.

Newsletter:
Bitte in der letzten Spalte schreibt entweder intern, wenn ihr Newsletter selber versendet oder extern, wenn ihr einen Anbieter aus der EU – eher nicht USA – verwendet

Bitte kontrollieren, ob die X auch für Euch so stimmen

Kategorien der betroffenen Personengruppe	Lfd. Nr.:	Datenkategorien	...r Art 9 und Art 10 DSGVO	...chtsvertreterim Anlassfall	Gerichtim Anlassfall	Externes Newsletter-Toll
1. eigene Leser/Buchkäufer sowie Blogger/Rezensente; Interessenten	01	Ordnungsnummer	*Nein*	*X*	*X*	*extern (EU)*
	02	Name bzw. Bezeichnung	*Nein*	*X*	*X*	*extern (EU)*
	03	Anrede/Geschlecht	***wird nicht verwendet/erhoben***			
	04	Anschrift bzw. Lieferadresse	*Nein*	*X*	*X*	
	05	E-Mails	*Nein*	*X*	*X*	*extern (EU)*
	06	Homepage	*Nein*	*X*	*X*	
	07	Einwilligung nach Art 4 abgelegt	*Nein*	*X*	*X*	*extern (EU)*
	08	Berufs-, Branchen- Geschäftsbezeichnung	***wird nicht verwendet/erhoben***			
	09	Firmenbuchdaten	***wird nicht verwendet/erhoben***			
	10	Korrespondenzsprache, sonstige Vereinbarungen und Schlüssel zum Datenaustausch	*Nein*	*X*	*X*	
	11	Geburtsdatum	***wird nicht verwendet/erhoben***			
	12	Personenstand, nur Ehe und nicht Verpartnerung, da dies sexuelle Orientierung beinhaltet	***wird nicht verwendet/erhoben***			
	13	Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Lesern/Buchkäufern und Bloggern/Rezensenten gegenüber dem Auftraggeber)	*Nein*	*X*	*X*	*extern (EU)*

	14	Kaufkraftklassifizierung	***wird nicht verwendet/erhoben***			
	15	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrhythmus etc.)	*Nein*	***X***	***X***	***extern (EU)***
	16	Kaufverhalten (Frequenz und Volumen)	*Nein*	***X***	***X***	
	17	Antwortverhalten zu Werbeaktivitäten	*Nein*	***X***	***X***	***extern (EU)***
	18	Bonus- und sonstige Vorteilsdaten	*Nein*	***X***	***X***	
	19	Newsletter-Sperre	*Nein*	***X***	***X***	***extern (EU)***
	20	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*	***X***	***X***	
	21	Serienbrief-Sperre	*Nein*	***X***	***X***	
Kontaktpersonen bei Lesern/Buchkäufern und Bloggern/Rezensenten 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	E-Mails	*Nein*	***X***	***X***	
	26	Korrespondenzsprache	*Nein*	***X***	***X***	
	27	Funktion oder betreutes Aufgabengebiet beim Lesern/Buchkäufern und Bloggern/Rezensenten oder Interessenten	*Nein*	***X***	***X***	
	28	Geburtstag, Personenstand und dgl.,	***wird nicht verwendet/erhoben***			
	29	Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrhythmus, 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 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	

4.2.7 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1 – 33	Aufgrund der gesetzlichen Aufbewahrungsfristen wie z. B. § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüberhinausgehend 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)

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

Empfängerkategorien	Drittstaat (d.h. Staaten außerhalb der EU)	Internationale Organisation
1.Rechtsvertreter im Anlassfall	Nein	Nein
2.Gericht im Anlassfall	Nein	Nein
3. Externer Newsletter-Tool-Anbieter	*Nein*	*Nein*

4.2.9 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.

4.2.10 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

5 Checkliste für EPUs - IT-Safe (WKO)

Unbedingt: Ich bin die wirklich hilfreiche IT-Checkliste für EPUs unter https://itsafe.wkoratgeber.at/ durchgegangen 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.

6 Impressum und Datenschutzerklärung (WKO)

Wurden nach dem Muster der WKO erstellt

7 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

7.1 Selbstschutz

Ich versuche mein Such- und Surfverhalten soweit wie möglich sicher zu halten

7.2 Handy

7.2.1 Handy

- Kein Whatsapp für Geschäftliches
- Security App
- Handy mit PIN, Passwort oder Biometrie geschützt
- Bluetooth-Funktion immer ausgeschaltet ausgenommen beim Autofahren, ...

7.2.2 Zutrittskontrolle

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

- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Verschlossene Türen bei Abwesenheit

7.2.3 Zugangskontrolle

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

- Einsatz einer Hardware-Firewall Einsatz einer Hardware-Firewall
- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Verschlüsselung von mobilen Datenträgern
- Einsatz von Anti-Viren-Software
- Verschlüsselung von Datenträgern in Laptops / Notebooks/USB
- Einsatz von Anti-Viren-Software
- Einsatz einer Firewall

7.2.4 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 (EPU, nur der Verantwortliche ist berechtigt)
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert = 1
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- (EPU, nur der Verantwortliche ist berechtigt)
- Sichere Aufbewahrung von Datenträgern (Data-Safe)
- physische Löschung von Datenträgern vor Wiederverwendung
- ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

7.2.5 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.

- Keine Weitergabe von Daten

7.2.6 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 (EPU: Nur der Verantwortliche ändert, ...)
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) (EPU, nur der Verantwortliche ist berechtigt)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts (EPU, nur der Verantwortliche ist berechtigt)
- Klare Zuständigkeiten für Löschungen (EPU, nur der Verantwortliche ist berechtigt)

7.2.7 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
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) siehe Anhang
- Wenn Auftragnehmer hat Datenschutzbeauftragten bestellt hat
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Vertragsstrafen bei Verstößen
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7.2.8 Verfügbarkeitskontrolle

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

- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans

7.2.9 Trennungsgebot

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

- Erstellung eines Berechtigungskonzepts (EPU, nur der Verantwortliche ist berechtigt)
- Festlegung von Datenbankrechten (EPU, nur der Verantwortliche ist berechtigt)

7.2.10 Datenschutz-Management

Maßnahmen, die für ein Datenschutz-Konzept bzw. -System zumindest notwendig sind.

- Software-Lösungen für Datenschutz-Management im Einsatz
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz
- Regelmäßige Sensibilisierung (mindestens jährlich)
- Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / DatenPannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen (Newsletter/Blogabo)
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

30.04.2018
Datum

Katharina Münz
Verantwortlicher für die Erstellung (in Druckbuchstaben)

gez. Katharina Münz
Unterschrift des Verantwortlichen

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

7.3 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: Datenschutzkonzept verlangen, keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, sichere und verschlüsselte Speicherung und Übertragung, (z. B. DATB, Vorabüberzeugungspflicht, Nachkontrollen)

Jahr	Ergebnisse der Überprüfung, Bewertung und Evaluierung
2019	
2020	

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

8 Betroffenenrechte wahren

Grundsätzlich stelle ich jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version dieses Datenschutzkonzeptes auf meiner Homepage unter Datenschutz (siehe https://katharina-munz.com/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

8.1 Prozesse betreffs Betroffenenrechte

i. Ich erhalte Kenntnis, dass ein Betroffener seine Rechte geltend machen will, sei es z. B. mündlich, schriftlich. per Email
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 begehen wie z. B. personenbezogene Daten an eine falsche Person weiterzuleiten, mir eine Kopie/einen Scan Ihres Personalausweises/Reisepasses zukommen zu lassen.
Ich danke Ihnen für Ihr Verständnis

P.S.: Mein aktuelles Datenschutzkonzept https://katharina-munz.com/wp-content/uploads/2018/04/Datenschutz-Konzept.pdf

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 und Anfrage ist auch rechtens:
=> 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
  - https://katharina-munz.com/wp-content/uploads/2018/04/Datenschutz-Konzept.pdf
  - sein Stammdatenblatt mit allen personenbezogenen Daten (Screenshot)
- **Recht auf Berichtigung (Art 16 DSGVO)**
  Der Betroffene bekommt als PDF
  - https://katharina-munz.com/wp-content/uploads/2018/04/Datenschutz-Konzept.pdf
  - sein Stammdatenblatt mit den berichtigten personenbezogenen Daten (Screenshot)
- **Recht auf Löschung (Art 17 DSGVO)**
  Der Betroffene bekommt als PDF
  - https://katharina-munz.com/wp-content/uploads/2018/04/Datenschutz-Konzept.pdf
  - sein Stammdatenblatt ohne personenbezogene Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit dem Hinweis, dass
    - die Daten **anonymisiert** für die interne Statistik verwendet werden
    - nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde (Screenshot)

    oder
  - bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde ich alle Daten löschen (~ Marketingdaten) bis auf jene, wo ich nach Art 6 Z 1 lit f ein berechtigte Interessen des Verantwortlichen bzw. lit c (gesetzliche Verpflichtungen z. B. nach der BAO und dem UGB; vor allem Buchhaltungsunterlagen) DSGVO geltend machen kann und ich werde 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 personenbezogen Daten löschen.
    In diesen Fällen tritt an Stelle einer Löschung der Buchhaltungsdaten eine Sperrung (Einschränkung).
- **Recht auf Einschränkung (Art 18 DSGVO)**
  Der Betroffene bekommt als PDF
  - https://katharina-munz.com/wp-content/uploads/2018/04/Datenschutz-Konzept.pdf
  - sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Hackerl gesetzt ist und somit keine Verarbeitung seiner personenbezogenen Daten erfolgt. (Screenshot)
- **Recht auf Übertragbarkeit (Art 20 DSGVO)**
  Der Betroffene bekommt als PDF
  - https://katharina-munz.com/wp-content/uploads/2018/04/Datenschutz-Konzept.pdf
  - sein Stammdatenblatt mit allen personenbezogenen Daten (als PDF, da es maschinell lesbar sein sollte)
  - gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit allen personenbezogenen Daten als Cc. an einen anderen Verantwortlichen, den der Betroffene mir genannt hat per Email, wenn möglich über eine sichere und verschlüsselte Übertragung.
- **Recht auf Beschwerde bei der Datenschutzbehörde**

8.1.1 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 Leser-/Buchkäufer- und Blogger-/Rezensentenprofil) sowie um eine personalisierte Direktwerbung (siehe E-Mail-Marketing) für meine Leser/Buchkäufer und Blogger/Rezensenten, Interessierten, Lieferanten, Projektpartner zu ermöglichen.

Da nur eine teilautomatisierte und 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 diese Verarbeitung daher nicht als Profiling im Sinne des DSGVO (siehe unten Referenzen), sondern als **Profiling light**, als **kundenorientierter 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 DSGVO 2018

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

Vorab versende ich keine E-Mails ohne ausdrücklich Aufforderung des Adressaten (zum Beispiel, indem er mich selbst per E-Mail anschreibt oder sich per double opt in für meinen Newsletter bzw. das Blog-Abonnement eingetragen hat). Deshalb brauche ich die sogenannte Robinson-Liste für alle natürlichen und juristischen Personen, die in dieser Liste ausdrücklich auf die Zusendung von Werbematerial sowie Werbemails verzichten, nicht zu beachten.

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 Newsletter-Liste gelöscht wurde).

Mit meinem E-Mail-Newsletter-Dienstleister gibt es dazu eine Vereinbarung mit diesem Auftragsverarbeiter nach Art 28 DSGVO (siehe Marketing-Verzeichnis bzw. Anhang).

Macht ein Betroffener seine Rechte auf Widerspruch nicht mit Hilfe des Links im Newsletter geltend, sondern in einer anderen Form, sei es z. B. mündlich, schriftlich. per E-Mail, 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 z. B. personenbezogen Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zukommen zu lassen.
   Ich danke Ihnen für Ihr Verständnis

   P.S.: Mein Datenschutzkonzept unterhttps://katharina-munz.com/wp-content/uploads/2018/04/Daten-schutz-Konzept.pdf

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:
Idee
„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."

8.2 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 personenbezogen 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 personenbezogen Daten aufgrund meiner TOMs (z. B. 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 Betroffene umgehend mit einer entsprechenden Variation der „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.

9 Risikoanalyse

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

9.1 Schutzbedarfsanalyse

Meine Vorabanalyse ergab, dass es sich bei folgenden personenbezogenen Daten der Leser/Buchkäufer sowie Blogger/Rezensenten, von (potentiellen) Interessenten, Lieferanten, Geschäftspartnern und an der Geschäftsabwicklung mitwirkenden Dritten 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., Skype, 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 oder dgl.), Funktion/Rolle der Kontaktperson, Zuordnung zu einer bestimmten Lesern/Buchkäufern und Bloggern/Rezensenten - und Lieferanten, Interessentenkategorie (einschließlich regionale Zuordnung, usw.)*
>
> *Betreffs der Personalverwaltung wurden, da noch keine Mitarbeiter, keine personenbezogenen Daten eingetragen!*

Meine Vorabanalyse ergab, dass es sich bei folgenden personenbezogenen Daten der Leser/Buchkäufer sowie Blogger/Rezensenten, von (potentiellen) Interessenten, Lieferanten, Geschäftspartnern und an der Geschäftsabwicklung mitwirkenden Dritten inkl. der jeweiligen Kontaktpersonen um Daten mit einen **hohen und sehr hohen Schutzbedarf** handelt und daher eine erweiterte Risiko-Analyse durchgeführt werden muss:

> *Kaufverhalten (Frequenz und Volumen), Bankverbindungen, Bonus-, Provisionsdaten und dgl., Kaufkraftklassifizierung, Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Lesers/Buchkäufers sowie Bloggers/Rezensenten gegenüber dem Auftraggeber), Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrhythmus etc.), Sonstiges Antwortverhalten zu Werbeaktivitäten; Bonus- und sonstige Vorteilsdaten, Zugehörigkeit zu einer bestimmten Interessentenklasse, Vertragstext und Geschäftskorrespondenzen, sonstige Vereinbarungen und Schlüssel zum Datenaustausch, Mitschriften und Fotos.*
>
> *Personenstand, Geburtsdatum, Daten zur Bonität inkl. Mahn- und Klagdaten, Zahlungsverhalten, Kreditkartennummern und -unternehmen, und Auftragserfassung gem. Beraternorm EN16114 werden von mir weder erhoben noch verwendet.*

9.2 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	personenbezogene Daten
1	Vertragstext und Geschäftskorrespondenzen, Auftragserfassung g, Mitschriften u. Fotos, sonstige Vereinbarungen, Schlüssel zum Datenaustausch, Bonität => geheim/vertraulich
2	Kaufverhalten (Frequenz und Volumen), Bankverbindungen, Bonus-, Provisionsdaten und dgl., Kaufkraftklassifizierung, Bonus- und sonstige Vorteilsdaten
3	Nachfrageinteressen (auf Grund bisherigen Nachfrageverhaltens oder eigener Angaben des Lesers/Buchkäufers sowie Bloggers/Rezensenten gegenüber dem Auftraggeber), Betreuungsdaten (wie: zugesandtes Werbematerial, Besuchsrhythmus etc.), Sonstiges Antwortverhalten zu Werbeaktivitäten; Zugehörigkeit zu einer bestimmten Interessentenklasse
4	Personenstand, Geburtsdatum, Daten zur Bonität inkl. Mahn- und Klagdaten, Zahlungsverhalten, Kreditkartennummern und -unternehmen, und Auftragserfassung gem. Beraternorm EN16114 werden von mir weder erhoben noch verwendet
5	Personenbezogene Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe oben Vorabanalyse

Schwere					
Existenzgefährdend			**2**	**1**	
Wesentlich	**4**		**3**		
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

9.2.1 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; Betriebsgeheimnis 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	z. B. Diebstahl von Unterlagen aus einem Safe
Möglich	25-69% Wahrscheinlichkeit	Z. B. gezielter und koordinierter Angriff durch einen Hacker, Verlust der Hardware bzw. personenbezogenen Daten durch Diebstahl oder durch fahrlässiges Handeln
Sehr wahrscheinlich	70-99% Wahrscheinlichkeit	z. B. Eindringung eines Schädigungs-Mails,
Garantiert	100% Wahrscheinlichkeit garantiert	z. B. Ausfall durch einen Festplattenausfall, Datenverluste durch technische Fehler

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

9.3 Maßnahmen

Siehe TOMs

9.3.1 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
ii. **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen, Protokollierung von Zugriffen (EPU)

9.3.2 Integrität

i. **Eingabekontrolle**: Personenbezogene Daten in den Datenverarbeitungssystemen werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt (EPU), Dokumentenmanagement

9.3.3 Verfügbarkeit

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

9.4 Risikoanalyse mit Maßnahmen

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

9.5 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 Data-Breach der betroffene Kunde nicht informiert werden, nichtsdestotrotz wird die Behörde bei Data-Breach mit Risiko für personenbezogen Daten der Kategorie 1 + 2 informiert.

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

10 Mein angemessenes Datenschutzniveau

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

10.1 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 Lesern/Buchkäufern und Bloggern/Rezensenten mit gutem Gewissen sagen:

> *Liebe Leserin, lieber Leser, liebe Buchkäuferin, lieber Buchkäufer, liebe Bloggerin, lieber Blogger, liebe Rezensentin, lieber Rezensent,*
>
> *Vertrauen zwischen mir und dir ist die Grundlage und Voraussetzung für meinen persönlichen Umgang mit Lesern, Buchkäufern, Bloggern und Rezensenten, daher sind auch alle deine persönlichen Daten bei mir in guten Händen.*
>
> *Ich sichere dir zu, dass ich sorgsam und streng vertraulich damit umgehe und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen bin.*
>
> *Darauf kannst du vertrauen.*
>
> *15.04.2018*
>
> *Katharina Münz*
>
> *Hinweis: Original mit Unterschrift ist im Archiv abgelegt*